Windows 2000

Système d'exploitation qui gère :

- la mémoire
- les données
- le matériel
- les logiciels

Fonctionnalités

- Multitâche
- Prise en charge de la mémoire
- Evolutivité SMP
- Plug-and-play
- Mise en cluster (regrouper plusieurs ordinateurs pour exécuter une application commune)
- Système de fichiers
- Récupération de fichiers
- Taille de partition important
- Sécurité
- Quotas de disque
- Compression
- Cryptage
- Qualité de service (transmission, rapidité, fiabilité de transmissions des données)
- Services d'installation à distance

Edition de Windows 2000

EDITION	Pro.	Mémoire	Obs.
W2K Professionnel	**2**	Min **64** Mo (128 Mo) Max. **4 Go**	2Go disque dont 650 Mo disponible
W2K serveur	**4**	Min **128** Mo (256Mo) Max. **4 Go**	
W2k Advencer server	**8**	Min.**128** Mo (256Mo) Max. **8 Go**	2Go disque dont 850 Mo disponible Clustering
W2K datacenter server	**32**	Min Max. **64 Go**	+ 1000 users

Identification du système de fichiers

W2K prend en charge NTFS , FAT 32 , FAT

Double annorçage W9x / W2K choisir FAT ou FAT 32

NTFS

- Sécurité au niveau des fichiers et des dossiers
- Compression de fichiers
- Quotas de disques
- Cryptage de fichiers

Fat / Fat 32

Pas de sécurité au niveau des fichiers

Licences

Par siège

Par serveur

Note pour une connexion sur IIS / Telnet ou FTP pas d'accès licences requis.

Assistant de configuration serveur

- Active directory
- Serveur de fichier
- Serveur d'impression
- Web/Multimédia
- Mise en réseau
- Applications
- Options avancées (outils support technique, file d'attente)

Mise à niveau

- W9x ou WinNT 3.51 (ou +)è W2k Pro F Winnt32.exe
- Win 3.1 Worksgroup èWin NT4 FWinnt32.exe
- Win NT 3.5 èWin NT4 FWinnt32.exe
- Winnt.exe F nouvelle installation
- Winnt32 / checkupgradeonly F génération de compatibilité.
- C:\Chkupgrd.exe F génération de compatibilité

Attention :
Pour installer un service d'annuaire sur un client W95 il faut I.E. 4.0.1 et Active Desktop (pour installer le client voir sur le Cdron W2K server \Clients\Win9x\DsClient.exe)

Protocoles supportés par W2K

- TIP/IP
- ATM
- NetBUI
- NWLink
- IrDA
- Apple Talk
- DLC

Présentation sur les réseaux

Le réseau permet

- Partage de l'information
- Partage du matériel et des logiciels
- Administration centralisée

Composante du réseau

- Client
- Serveur
- Serveur d'impression
- Serveur d'annuaire
- Serveur de télécopie
- Serveur de messagerie
- Serveur de données

Type de réseaux

- Réseau point à point (pear to pear)
  Appelés Worksgroup (chaque ordinateur est à la fois client et serveur
- Réseau client - serveur

Fonctionnalité d'un domaine

- Session unique
- Compte unique
- Gestion centralisée
- Evolutivitée

Avantage du domaine

- Organisation des données
- Localisation des données
- Accès aux ressources
- Délégation de l'autorité

Organisation du domaine

- Contrôleur du domaine : serveur gérant chaque domaine
- Arborescence : organisation de plusieurs domaines hiérarchiques
- Forêts : organisation de plusieurs domaines non communes

Le compte utilisateur

Compte utilisateur local

- Permet d'ouvrir une session locale (1 ordinateur particulier)
- Résidant dans le gestionnaire SAM

Compte utilisateur de domaine

- Permet d'ouvrir une session sur le domaine
- Résidant dans l'Active Directory

Compte utilisateur prédéfini

- Administrateur
- Invité

Ils résident dans la SAM (localement) et sur "Active Directory".

Ils sont impossible à supprimer

Compte utilisateur modèle

Il peut servir à créer rapidement des utilisateur ayant les mêmes besoins que le modèle . Par convention il commence par (_) ex : _ventes_Modèle . définissez tous les paramètres et activez la case "**Le compte est désactivé**"

Ensuite pour créer un user suivant le modèle il suffit de faire clic droit sur le modèle , sélectionner "Copier" , mettre à jour les paramètres et désactiver la case "le compte est désactive"

Type de profils

Les paramètres des profils sont stockés dans "C:\Documents and setting\%username%"

- Profil d'utilisateur par défaut
- Profil d'utilisateur local
- Profil d'utilisateur itinérant
- Profil d'utilisateur obligatoire (modifications des paramètres interdites)

Note

Le fichier NTUSER.DAT (fichier caché) stocke les données du profil pour la base de registre en le renommant "*.MAN" le profil devient un profil obligatoire

Les groupes

Les groupes peuvent contenir 5000 membres

Le mode natif

tous les contrôleurs de domaine exécutent W2K

Dans le mode natif il existe :

2 types de groupes

- Groupe de sécurité
- Groupe de diffusion

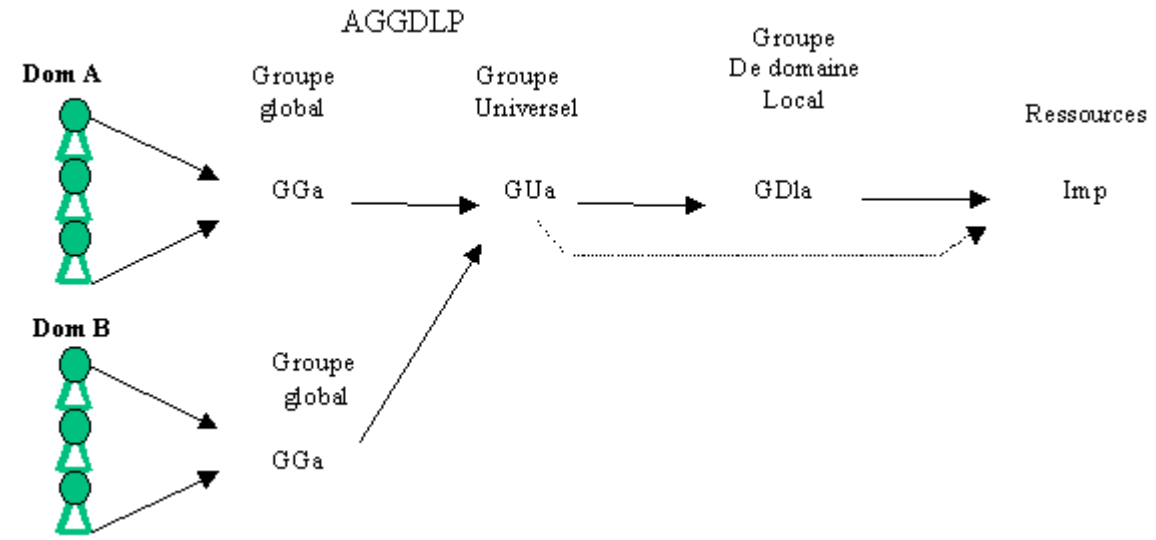
3 étendues de groupes

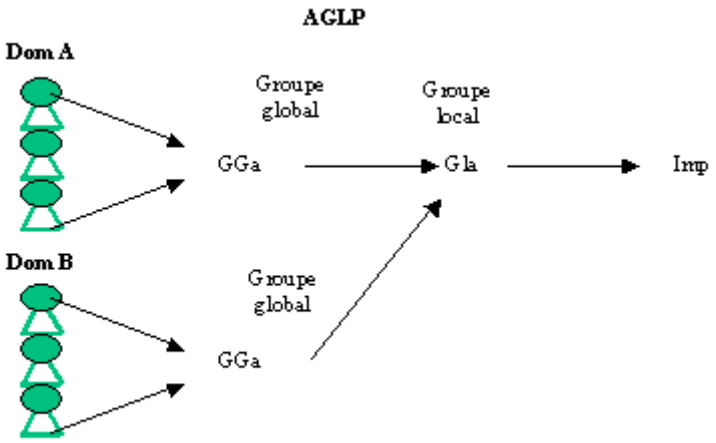
- Globale
- Local du domaine
- Universelle

Le mode mixte

les contrôleurs de domaine exécutent W2K et NT

Les groupes réagissent différemment selon le mode





Attention

Un utilisateur membre d'un groupe s'octroie les droits du groupe

Un utilisateur peut faire partie de plusieurs groupes

Un utilisateur en session se voit affecter la qualité d'un nouveau groupe lors de l'ouverture de sa prochaine session.

Le mot de passe

Attention : l'option "**L'utilisateur doit changer son mot de passe à la prochaine ouverture de session**" a priorité sur l'option "**Le mot de passe n'expire jamais**"

Option d'ouverture de sessions

Pour limiter le nombre d'ouverture simultanée d'un utilisateur de domaine sur la boite de dialogue "Propriété», "Compte" de l'utilisateur cliquez sur "Se connecter à" et ajouter tous les ordinateurs sur lesquels il pourra se loger

Attention : les connexions aux ressources du réseau ne sont pas interrompues à l'expiration des heures de sessions. Il n'est seulement plus possible de se connecter au réseau.

Création d'un dossier partagé sur le serveur

Créer un dossier sur le serveur, puis partagez-le

Accordez les droits appropriés sur ce dossier

Fournissez aux comptes utilisateurs le chemin d'accès valide

Le chemin par défaut sera

<\\non_de_la_machine>\<nom_du_partage>\%username%

ex :\\pentium\d\home\Patrick

Aide sur W2K

Dans **démarrer** puis **Aide**

Onglet *fonction*

Sommaire affiche la liste de toutes les rubriques

Index localise les informations à l'aide d'un mot clé

Rechercher localise sur un ou plusieurs mot clé

Sur W2K serveur des options disponibles pour optimiser la recherche par :

Résultats précédents

Mots similaires

Uniquement dans les titres

Favoris ajouter des rubriques souvent consultées

Taches administratives de routines

Utilisateurs et groupes (création, modification …)

Imprimantes (configuration, administration, files)

Sécurité (protection des accès aux ressources)

Evénements et ressources (surveillance et planification de job)

Intégrité du système (recherche de virus)

Sauvegarde et restauration

Application serveur (serveur de messagerie, de bd)

Disques (vérification de fiabilité et intégrité)

Planification des tâches

Menu **Démarrer** à **Programmes** à **Accessoires** à **Outils système** à **Tâches planifiées**

Permet d'effectuer des tâches répétitives automatiquement

Les types de démarrages

Touche **F8**

Mode sans échec

Utilise les fichiers et les drivers de base (souris écran clavier mémoire de masse services de base pas de réseau)

Mode sans échec avec réseau

Identique au mode sans échec avec prise en charge du réseau

Mode sans échec en mode console

Identique au mode sans échec en établissant une session invite de commande au lieu de l'interface graphique

Enregistrement du journal de démarrage

Création d'un fichier <ntbtlog.txt> dans le répertoire principal de Windows. Ne fonctionne qu'en complément des 3 modes précités.

Mode V.G.A.

Utilise le mode VGA de base. Accompagne les 3 modes sans échec.

Mode de restauration du service annuaire.

Mode restauration du service d'annuaire

Non disponible sur W2K Pro (uniquement sur les versions serveur) sert à restaurer le répertoire **SYSVOL** et l'**ADS.**

Mode debug

Réservé aux programmeurs. Les informations de mise au point sont envoyées sur le port série.

Topologie des réseaux

- Réseau LAN (Local Aéra Network)
- Réseau MAN (Métropolitan Aéra Network)
- Réseau WAN (Wide Aéra Network)

Type de câbles

	Type	**Long**	**Connexions Max**	**Type**	Carte	**connexion**
10 Base 5	coaxial épais	500M	100 boîtiers	Bus + bouchons	Coupleur Transceivers	Intruses ou vampires
10 Base 2	Coaxial fin	185M	30 stations	Bus + bouchons	Carte rso	BNC en T
10 Base T	Torsadé	100M	Limité par HUB	Etoile	Carte rso	RJ45
10 Base F	Fibre optique	1 Km		étoile		

Type de réseaux

- Le bus
- En étoile
- En anneau
- Maillé
- Hybride

Technologie réseaux

Ethernet: de 10Mb/s à 1Gb/s

- CSMA-CA (Carrier Sense Multiple Accès - Collision Avoidance)
- CSMA-CD (Carrier Sense Multiple Accès - Collision Détection)
- *Token -ring* : de 4Mb/s à 16 Mb/s
- passage de jeton

- *ATM* de 155Mb/s à 622Mb/s
- Point à point transfert de paquets fixe au moyen de commutateur ATM
- *Réseau FDDI* de 155Mb/s à 622Mb/s
- Passage de jeton sur deux fibres en boucle inversées
- *Relais de trame* : réseau point à point (Internet)

Extension de réseau

	Couche OSI
Répéteur concentrateur (HUB)	Physique
Pont	Liaison
Pont –routeur (Brouteur)	Réseau
Commutateur Switch	Liaison
Routeur	Réseau
Passerelle	Application

Type de connexion

- VPN (Virtual Private Network) protocole PPTP
- RTC (Réseau téléphonique Commuté) 9600 à 56Kb/s
- ADSL (A
- RNIS (Réseau Numérique à Intégration de Services) 64 ou 128Kb/s . 23 canaux à 64Kb + 1 canal à 64Kb de signalisation
- ATM (Asynchronous Transfert Mode) paquets de taille fixe
- X25 utilise un PAD

Les protocoles

Modèle OSI

Physique	1	Place les données sur le support
Liaison	2	Défini la méthode d'accès au support
Réseau	3	Accède aux message à la fois sur le réseau et aussi entre les réseaux
Transport	4	Garantit la livraison sans erreur des données
Session	5	Etabli et gère les canaux de communications
Présentation	6	Ajoute le formatage souvent utilisé pour la représentation des données
Application	7	Définit les interactions entre les applications

Les piles de protocoles

Réseau	1	ATM Ethernet
Internet	2	IP ICMP IGMP ARP
Transport	3	TCP UDP
Application	4	HTTP FTP

Identification des applications

SOCKET = @IP + type de service (UDP/TCP)+ N° Port

Résolution des noms

Type d'adressage	Netbios	Serveur de noms
Statique	Lmhosts	Hosts
Dynamique	Serveur Wins	Serveur DNS

Processus de résolution

Netbios

ŒCommande locale à Cache de nom Netbios à Žserveur Wins à Diffusion générale à Fichier Lmhots à ‘Fichier Hosts à ’Serveur DNS

Nom d'hôtes

ŒCommande locale à Nom d'hôte local à ŽFichier Hosts à Serveur DNS à cache de nom Netbios à ‘Serveur Wins à ’Diffusion générale à “Fichier Lmhosts

Terminologies des paquets

Segment :

Transmissions de protocoles TCP (Entête TCP + données application)

Message :

Unité de transmissions non fiable comme le protocole UDP ICMP IGMP ARP (Entête de protocole + données d'application ou de protocole)

Datagramme :

Unité du protocole non fiable IP (entête IP + données couche transport)

Trame :

Unité de transmission de la couche réseau (Entête ajouté au niveau de la couche réseau, ainsi que les données de la couche Internet)

Composants des trames

Signal d'alerte	@source	0,5Ko - 4Ko	CRC
	@dest.		

En-tête Données Délimiteur

Adressage IP

Classe des adresses IP

Classe	Masque	Plage d'adresses
A	w.0.0.0	1 – 126
B	w.x.0.0	128 – 191
C	w.x.y.0	192 – 223
D	Non disponible	225 – 239
E	Non disponible	240 – 255

Note

127 .0.0.1 = adresse de test réseau

224.0.0.0 = adresse de diffusion

L'*APIPA*

C'est une adresse automatique lors d'échec de connexion à un serveur DHCP.

Le routage CIDR

A pour but optimiser l'adressage IP.

Adresse IP	10 . 217 . 123 . 7
	00001010.11011001.01111011.00000111
Masque réseau	255 . 255 . 240 . 0
	11111111.11111111.11110000.00000000
NB bits poids forts	8 + 8 + 4 = 20
	10.217.123.7/20

InternetAdresse CIDR

@privées = @permanentes

@publique = @provisoires

Les protocoles d'Internet

- HTTP : Texte brut non-crypte
- HTTPS : connexion sécurisée par SSL
- FTP : Transfert de fichiers
- SMTP : Messagerie
- NNTP : Groupe de discussion
- HTML : Pages WEB
- DHTML Pages Web Animées interactives

Les connexions à Internet

Traducteur NAT :

Permet la translation d'adresse d'un réseau privé vers Internet

Serveur Proxy :

Permet la translation d'adresses IP locales sur une adresse IP Publique

Pare-feu :

Offre une barrière de sécurité entre intranet et Internet.

Microsoft Proxy Serveur :

Fait office de serveur Proxy et de pare-feu

Les outils d'administration

Installation

Pour installer les outils d'administration sur un poste W2K Pro. Ouvrez le dossier i\386 du CD-RON de la version W2K Server exécuter "**Adminpak.msi**"

Eventuellement utiliser la commande "Runas" pour disposer des droits Administrateur

Pour utiliser "Runas" Touche "Maj" enfoncée, clic droit sur "Utilisateurs et ordinateurs Active

Les droits NTFS

Les dossiers

l'onglet sécurité du dossier

LECTURE	**Afficher** les fichiers et les sous dossiers ainsi que les attributs, l'approbation et autorisation associés au dossier
ECRITURE	**Créer** des fichiers et des sous dossiers, **modifier** les attributs du dossier et afficher l'approbation et les autorisations associés au dossier
AFFICHER LE CONTENU DU DOSSIER	**Afficher** le mon des fichiers et sous dossiers contenus dans le dossier
LECTURE / EXECUTION	**Parcourir** les dossiers et effectuer les opérations permises par les autorisations Lecture et Afficher le contenu du dossier
MODIFIER	**Supprimer** le dossier et effectuer les opérations permises par les autorisation Ecriture et Lecture et Exécution
CONTROLE TOTAL	**Modifier** les autorisations, prendre possession d'un dossier, **supprimer** des sous-dossiers et des fichiers et effectuer les opérations permises par toutes les autre autorisations NTFS sur le dossier

Les fichiers

L'onglet sécurité du fichier

Les autorisations NTFS des fichiers sont prioritaire sur les autorisations NTFS des dossiers

LECTURE	**Lire** le fichier et afficher les attributs, l'appropriation et les autorisations associés au fichier
ECRITURE	**Remplacer** le fichier, **modifier** les attributs du fichier et afficher l'approbation et autorisations associés au fichier
LECTURE ET EXECUTION	**Exécuter** des applications et effectuer les opérations permises par les autorisations Lecture
MODIFIER	**Modifier** et supprimer le fichier, effectuer les opérations permises par les autorisations Ecriture et Lecture et Exécution
CONTROLE TOTAL	**Modifier** les autorisations, **prendre possession** du fichier et effectuer les autorisations permises par toutes les autres autorisations NTFS sur les fichiers

Attention :

Par défaut W2K accorde **Contrôle total pour Tout le monde** dans le dossier racine

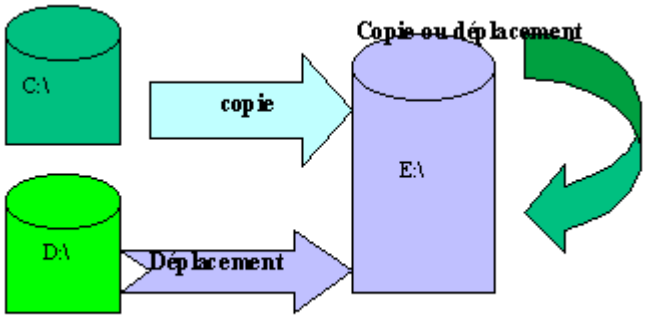
L'autorisation **Refuser** est prioritaire sur toutes les autres autorisations

L’héritage des autorisations

Les sous-dossiers héritent de toutes les autorisations des dossiers parents.

Le blocage d’héritage permet de ne pas hérité des autorisations des dossiers parents. Cette méthode n’est pas conseillée (Il n’existe pas d’outils pour voir les droits effectifs en cascade.)

Copies et déplacement de fichiers



Copies è Hérite des autorisations

Déplacement vers partition **==>** Hérite des autorisations

Déplacement vers même partition ==> Maintien des autorisations

Les autorisations spéciales NTFS

Permettent d’affiner les autorisations de bases.

Elles sont au nombre de 13.

Compression de fichiers

Un dossier compressé contient **uniquement** des fichiers compressés

Un dossier non compressé peut contenir des fichiers compressés ou non compressés

Copies ==> Héritage du dossier cible

Déplacement vers partition **==>** Héritage du dossier cible

Déplacement vers même partition ==> Maintien de la compression

Attention lors d’un déplacement d’un fichier compressé vers une autre partition le fichier est décompressé puis recompressé dans le répertoire de destination.

Le quotas de disque

Il s 'applique sur les disque physiques

Un message de pré-alerte et d';alerte peuvent être envoyés

L'E.F.S ou cryptage

On ne peut crypter et compresser un fichier

On ne peut partager un fichier crypté avec d';autres utilisateurs

Il faut au moins un agent de récupération pour décrypter un fichier

Les dossiers partagés : DFS

Peuvent contenir des applications, des données et des fichiers

Facilite l'administration

On peut avoir jusqu';à 32 réplicats de DFS

Les clients W2K NT4.0 W98 comportent un client DFS pour W95 il faut l';installer

Pour partager un dossier	Vous devez être membre du groupe
Domaine W2K	Administrateur ou opérateur de sauvegarde
Worksgroup	Administrateur ou utilisateur avec pouvoir
Ordinateur client W2K Pro	Administrateur ou utilisateur avec pouvoir

Autorisations sur les DFS

Se situe dans l'onglet partage

Les droits ne sont applicables qu'à travers le réseau. Les droits DFS ne s'appliquent pas sur une connexion locale

Lecture

Modifier

Contrôle total

Attention :

Par défaut W2K accorde **Contrôle total pour Tout le monde** dans le dossier partagé

L'autorisation **Refuser** est prioritaire sur tout las autres autorisations

Les partages peuvent se faire sur des volume NTFS, FAT32 et FAT

Combinaison NTFS et DFS

L'autorisation la plus restrictive qui fixe les droits effectifs

Les partages administratifs

C$

D$

E$

Admin$ dossier C:\WINNT ou %SYSTEMROOT%

Print$ dossier contenant les pilotes d'imprimantes C:\WINNT\Système32\Spool\Drivers

Type de racines DFS

Racine DFS autonome	Racine DFS de domaine
Stockée sur un seul ordinateur	Hébergée sur des contrôleur de domaine ou des serveurs membres
N'utilise pas Active Directory	La topologie est directement stockée dans AD
Ne peut pas disposer des dossiers partagés au niveau des racines DFS	Peut disposer des dossiers partagés au niveau de la racine DFS
Ne peut prendre en charge qu'un seul niveau de liens DFS	Peut prendre en charge plusieurs niveaux de liens DFS

Création d'un racine DFS

Outils d'administration è Système de fichiers distribués è Action è Nouvelle racine DFS

Gestionnaire de tâches

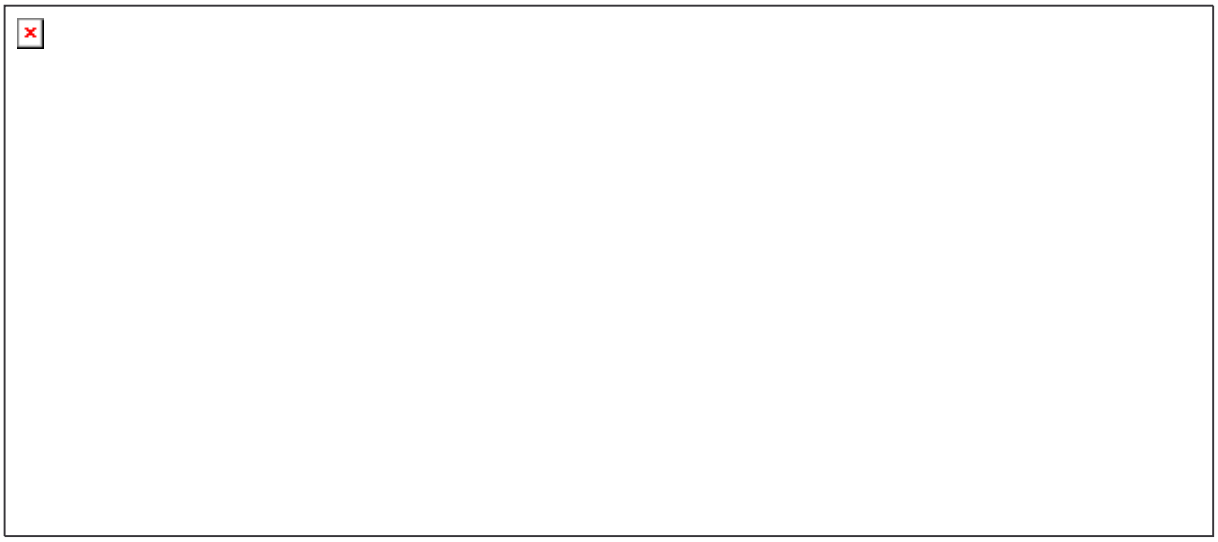
<Alt> +<Ctrl>+<Suppr>

Gestion de l’ordinateur

<Démarrer>+<Programmes>+<Outils d’administration>+<Gestion de l’ordinateur>

Analyseur de performances

<Démarrer>+<Programmes>+<Outils d’administration>+<Analyseur de performances>



Stratégie de sécurité locale

<Démarrer>+<Programmes>+<Outils d’administration>+<Stratégie de sécurité locale>

Observateur d’événements

<Démarrer>+<Programmes>+<Outils d’administration>+<observateur d’événements>

Service de composants

<Démarrer>+<Programmes>+<Outils d'administration>+<Services de composants>

utilisateur itinérant

W2K gère :

ACPI - APM

Configuration multiples (avec ou sans réseau par ex.)

Mise en veille prolongée

Hibernation (l'espace disque doit être minimum de la même capacité que celle de celle de la mémoire vive pour la conservation de l'environnement avant mise en hibernation.)

Fichiers hors connexion

L'utilisateur ferme sa session, les fichiers sont synchronisés avec les fichiers du serveur.

L'utilisateur travaille localement avec la copie du fichier

A l'ouverture de la session suivante les fichiers modifiés sont synchronisés à nouveaux

Pour cela 3 options

Mise en cache manuellement des documents

Mise en cache automatique de documents

Mise en cache automatique des programmes

Comment ?

Poste local : Dans l'explorateur de Windows <Outils> + **<Options des dossiers>** onglet **<Fichiers hors connexion>** case **<Autoriser l'utilisation des fichiers hors connexion>**

Serveur : dans le dossier partagé : cocher la case **<Rendre disponible hors connexion>**

Connexion à distance

C ‘est un connexion VPN avec les protocoles L2TP ou PPTP

Le serveur nécessite DEUX cartes réseaux

L’une sur le réseau local

L’autre sur Internet (Pour tunneling avec le client)

Gestion des disques

Disque de bases

Peuvent contenir jusqu’à 4 partitions principales ou

3 partitions principales et 1 étendues avec des lecteurs logiques.

On ne peut pas créer des volumes d’agrégat par bande (Miroir)

ou le Raid5 sur un disque de base

Il faut laisser 1Mo de disque non allouée pour pouvoir le transformer en disque dynamique

Attention pour les disques de base on parle de partition

Le disque dynamique

De 5 types

Volume simple :

Extension d’un volume simple : On doit être en NTFS, inclus un espace non alloué contigu ou non de n’importe quel disque Exception : volume système ou de démarrage ou d’échange actif

On ne peut étendre un volume qui à été crée sur un disque de base puis converti.

Volume agrégé par bande RAID 0

Volume fractionné

Volume en miroir RAID 1 (Miroir) (FTDISK.SYS)

Volume par RAID 5

On ne peut pas restaurer un disque de base qui à été transformé en disque dynamique. Il faut d'abord supprimer toutes les données et tous les volumes du disque dynamique.

Attention

Un volume simple peut être du format FAT, FAT32, NTFS Il ne peut être étendu. Donc un volume simple ne propose pas de tolérance de panne on peut faire du mirroring.

Le nombre de volume est illimité

A propos du RAID

Volumes en miroir	**Volumes RAID-5**
Prise en charge de la FAT et du NTFS	Prise en charge de la FAT et du NTFS
Possibilité de mise en miroir de volumes système ou d'amorçage	Pas de possibilité d'agrégat par bandes de volumes système ou d'amorçage
2 disques durs requis. Au minimum	3 disques durs requis.
Coût plus élevé par mégaoctet (50 pour cent d'utilisation).	Coût moins élevé par mégaoctet.
Bonnes performances de lecture et d'écriture.	Performances d'écriture moyennes et excellentes performances de lecture.
Moins de mémoire système utilisée.	Plus de mémoire système utilisée.
Prise en charge de 2 disques durs uniquement.	Prise en charge possible jusqu'à 32 disques durs.

Les sauvegardes

<Démarrer> + <Programmes> + <Accessoires> + <Outils système> + <Gestion des sauvegardes>

Type de sauvegardes

Sauvegarde normale/différentielle :

Les sauvegardes différentielles n'effacent pas les marques. Chaque sauvegarde inclut les modifications apportées depuis la dernière sauvegarde normale. Des données perdues le vendredi nécessite la restauration normale du lundi et la restauration différentielle du jeudi. Cette stratégie prend plus de temps pour la sauvegarde et moins de temps pou la restauration

Sauvegarde normale/incrémentielle :

Les sauvegardes incrémentielles effacent les marques de la veille. Les données perdues le vendredi nécessite un restauration du type normale du lundi puis une restauration incrémentielle du mardi au jeudi

Cette stratégie prend moins de temps pour la sauvegarde et plus de temps pour la restauration

Les sauvegarde normale/différentielle/copier

Elle est identique à l'exemple N°1 à ceci près que le mercredi on effectue une sauvegarde du type copier qui inclus tous les fichiers sélectionnés ; elle n'efface pas les marques et n'interrompe pas le calendrier normal de sauvegardes.

Terminal-server

Les services terminal-serveurs sont constitués de :

Serveur Terminal-serveur

Ordinateur client

Protocole RDP (Remote Desktop Protocol)

Personnalisation de l'installation

Avec WinNT.EXE

Commutateurs	Description
/a	Active les options d'accessibilité
/e[:commande]	Exécute une commande avant la phase finale du programme d'installation
/udf :id[,fichier_udf]	Modifie le fichier de réponses
/r [:dossier]	Spécifie un dossier facultatif à installer
/rx [:dossier]	Spécifie un dossier facultatif à copier
/s[:chemin_source]	Spécifie l'emplacement des fichiers d'installation de W2K
/t[:lecteur_temp]	Spécifie un lecteur pour l'installation
/u[:fichier_réponse]	Effectue une installation automatisée à l'aide d'un fichier de réponses

Exemple

C:\winnt.exe /u :fichier_réponses /s

Avec WinNT32.EXE

Commutateurs	Description
/copydir :dossier	Crée un dossier supplémentaire (utiliser aussi copysource)
/cmd :commande	Exécute une commande avant la phase finale du programme d'installation
/cmdcons	Installe des fichiers pour la console de réparation et de récupération
/debug[niveau] [:fichier]	Crée un journal de débogage au niveau spécifié
/s :chemin_source	Spécifie l'emplacement des fichiers d'installation de W2K

/syspart :lecteur	Copie les fichiers d'installation sur un lecteur que vous pourrez déplacer
/tempdrive :lecteur	Spécifié un lecteur pour l'installation
/unattend [nombre][fichier_réponse]	Réalise une installation automatisée avec un fichier de réponses facultatif
/udf :id[fichier_udf]	Procède à l'installation en utilisant un fichier udb

Les fichiers réponses

Fournissent automatiquement des réponses à certaines ou toutes les questions posées aux utilisateur durant l'installation. A utiliser pour spécifier les variante de configuration matérielle.

Les fichiers UDF

Permet d'automatiser l'installation à distance Le fichier UDF contient les information propre à l'ordinateur. notamment le nom réseau et les paramètres réseaux

L'association des deux fichiers permet une installation à distance automatisée réussie.

Assistant d'installation automatisé

Trouver <SETUPMGR.EXE> dans \Support\Tools\

Situé dans le dossier deploy.cab

Pour l'extraire faire clic droit sur le fichier et extraire

La duplication de disque

Permet de créer des image de W2K en vue de déploiement

L'outils **SYSPREP.EXE** permet cela.

Le fichier sysrep.inf permet de faire une installation avec un fichier de réponse automatique.

SYSPREP.EXE supprime les identificateurs SID et en génère d'autres

Commutateurs	**Description**
-quiet	Pas d'intervention de l'utilisateur
- pnp	Pas de détection plug and play
- reboot	Redémarre l'ordinateur au lieu de l'éteindre
-nosidgen	Ne génère pas de N° SID

Le RIS (Remote Installation Service)

Permet à une serveur RIS sous W2K server de déployer à distance des applications W2K Pro

Il faut

Pour le réseau

Serveur DNS (Prise en charge des enregistrements des ressources SRV (services).

Serveur DCHP

Active Directory

Pour le serveur RIS

2 Go minimal d'espace disponible

Image stockées sur partition NTFS

≠ Partition système

≠ Partition d'amorçage

Pour le client

Configuration minimale requise pour W2Kpro

Capacité d'amorcage sur réseau (Disquette d'amorçage faite avec RBFG.EXE) ou carte réseau PXE

Un assistant d'installation

<Démarrer> <Exécuter> <risetup.exe> <OK>

Attention : n'activer la prise en charge des clients que lorsque vous avez terminé la configuration et l'installation des images et fichiers de réponses requis. Dans l'assistant désactiver cette option.

Autorisation au serveur RIS

Pour empêcher l'utilisation non autorisée.

L'autorisation RIS est identique à celle du serveur DHCP :

<Outils d'administration> <DCHP> Clic droit sur <DHCP>

choisir <Gérer les serveurs autorisés> <OK>

Windows installer

C’est un add-on pour créer des fichiers .MSI

Sur le CD-Rom W2K advencer

D:\VALUEADD\3RDPARTY\MGMT\WINTLE .EXE

Une fois installer aller dans

<Menu Démarrer> + <Programmes> + <Véritas software> + <Veritas Discover>

lancer un 1ere fois

Installer le logiciel dont on veux une image .MSI

Lancer une 2me fois Véritas

Un fichier .MSI est disponible pour une install rapide au travers du réseau

Présentation du déploiement

Créer un dossier partagé (En lecture seule)

Créer les dossiers approprié pour chaque application

Placer le package sur le point de distribution du logicel

Créer ou modifier un GPO

Configurer l’objet GPO

Duplication de disque

Méthode adaptée au déploiement d’un grand nombre d’ordinateurs identiques

Installer et configurer un W2K

Installer et configurer les applications

Executer **SYSPREP.EXE** Possibilité de faire un syprep.inf avec avec setupmrg.

SYSPREP crée un mini- programme d’installation

Le DHCP

Sert à gérer dynamiquement les adresses IP

Il envoie aux clients

Une adresse IP

Un masque de sous-réseau

En option :

Adresse de la passerelle par défaut

Adresse IP des serveur DNS et WINS

Nom de domaine

DHCP = Dynamic Host Configuration Protocol

Le serveur DHCP

Demande de bail = **DHCPDISCOVER** Le client recherche un serveur DHCP

Proposition de bail = **DHCPOFFERT** Le serveur propose un adresse

Choix du bail = **DHCPREQUEST** Le client accepte la proposition d'un serveur

Accusé de réception du bail = **DHCPPACK** Le serveur confirme la réservation d'adresse

Le client fait un **DHCPREQUEST** à 50% avant la fin du bail

Le client fait un **DCHPDISCOVERT** à 82,7% avant la fin du bail

Le port **UDP 67** et **68** sont utilisés pour la communication entre le client et le serveur

En cas d'échec de connexion au serveur DHCP le client s'attribue une adresse automatique :

APIPA de 169.254.0.1 à 169.255.255.254

Pour libérer une adresse

IPCONFIG /RELEASE

Pour *rechercher* une nouvelle adresse

IPCONFIG /RENEW

Pour connaître l'adresse DHCP

IPCONFIG –ALL

Installation du service

Dans **Ajout et suppression de programmes + Ajouter/supprimer des composant de Windows + Service et mise en réseau + Protocole DCHP**

Autorisation du service

Seul le serveur DHCP sous Windows 2000 Server vérifient l'autorisation auprès d'Active Directory (Contrôleur de Domaine) en envoyant un **DCHPINFORM** toutes les 5 mn. Les autres serveurs DHCP répondent par un DCHPACK , ainsi ils vérifient l'état de leur autorisations et se mettent à jour si nécessaire

Autoriser un serveur DCHP

Outils d'administration clic droit sur **DHCP** puis **Gérer les serveurs autorisés** puis **Autoriser**. Dans la zone **Nom ou adresse IP** de la boite de dialogue **Autoriser le serveur DHCP** , tapez le nom et l'adresse IP du serveur DHCP , puis cliquez sur **OK**. Dans le message **DHCP** cliquez **OUI** pour confirmer l'autorisation.

Création d'un configuration étendue

Permet de créer un pool d'adresse. La commande **netsh**

L'étendue peut être gérer au niveau du client, de la classe, de l'étendue, du serveur.

Attention on ne peut modifie un masque de sous réseau après l'avoir créer. Il faut supprimer l'étendue et la récréer avec le bon masque.

Réservation d'adresse

Permet de réserver une adresse IP à un ordinateur donné en fonction de l'adresse MAC cible.

Agent de relais DHCP

Dans un réseau routé on peut

Inclure au moins un serveur DHCP dans chaque sous-réseau

Configurer un routeur à la norme RFC 1542 pour l'envoi de messages DHCP entre les sous-réseaux

Configurer un agent de relais DHCP sur chaque sous-réseaux

Dans un sous-réseau local, un agent de relais DHCP intercepte les messages de diffusion contenant les demandes d'adresses DHCP client et les transmet à u serveur DHCP d'un autre sous réseau . Le serveur DHCP répond à l'agent de relais au moyen d'un paquet dirigé. L'agent de relais diffuse la réponse sur le sous-réseau pour le client demandeur

<Outils d'administration> <Service routage et accès distant> <Routage IP> clic droit sur <Général> puis <Nouveau protocole de routage> <Agent de relais DHCP> puis <OK> ouvrez

la boite de dialogue <Propriétés> dans la zone <Adresse du serveur> tapez l'adresse IP d'un serveur DHCP et <Ajouter>

Surveillance du service DHCP

Lors de l'activation de la journalisation , le serveur DHCP crée des fichiers journaux appelés DHCPSrvLogxxx dans le répertoire racine_système\système32\DHCP et une sauvegarde dans le repertoire backup\jet\new.

Un utilitaire de restauration de la base : jetpack DHCP .mdb *temp*

Désinstaller DHCP

<Démarrer> + <Paramètres> +<Panneau de configuration> + <Ajout/Suppression de programmes> + <Ajouter/supprimer des composants de Windows> + <Services de mises en réseau> + <Détails> + <Protocoles DHCP>

Active directory

Stocke des informations sur les ressources de tout le réseau et permet aux utilisateurs de localiser, gérer et utiliser ces ressources.

Utilise le protocole LDAP (Lightweight Directory Acces Protocole)

Fonctionnalités

Organise l'annuaire en section

Espace de stockage central

Sécurité intégrée

Avantages :

Réduction du T.C.O.

Administration souple

Évolutivité

Administration simplifiée

Le chemin LDAP comprend :

Les noms uniques

Identifie le domaine dans lequel est situé l'objet, ainsi que le chemin complet

CN=David Dubois,OU=Sales ,DC=Consoto,DC=msft

é

Les noms uniques relatifs

Est la parti du nom unique qui permet d'identifier l'objet dans le conteneur.

Accès au réseau

session sur le domaine

Le mon de l'utilisateur peut être écris : nom@domaine + password

Le compte utilisateur Є au domaine

(est stocké sur le serveur et sur le poste client)

session locale

Compte utilisateur = nom d'authentification + password

Le compte utilisateur Є a un groupe

Session locale uniquement

(est stocké sur le poste client sur la S.A.M.)

Création de compte utilisateur

Pour importer en bloc des comptes utilisateurs utiliser

Csvde crée plusieurs comptes utilisateurs . Commande **csvde –i –f <*fichier*>**

Ldifde crée, modifie et supprime plusieurs comptes utilisateurs

Attention ne pas mettre de mot de passe sur le fichier d'exportation : il sont en clair

Format du fichier

Cn=Suzan fine, ou=Human Ressources, dc=asia, dc=consoto, dc=msft, user=suzanf, suzanf@consoto.msft, Suzan fine, 512

Attribut	valeur
Dn(nom unique)	Cn=Suzan fine, ou=Human Ressources, dc=asia, dc=consoto, dc=msft,
ObjectClass	user

SAM AccountName suzanf

UserPrincipalName suzanf@consoto.msft

DisplayName Suzan Fine

UserAccountControl la valeur 512 active le compte la valeur 514 désactive le compte

Structure d'active direrctory

Domaine

Est une limite de sécurité : l'administrateur ne peut administrer que son domaine, à moins qu'il ne soit habilité à intervenir sur d'autres domaines.

Est un unité de duplication : les domaines constituent également des unité de duplication. Dans un domaine, les ordinateurs appelés contrôleurs de domaine contiennent un réplica de l'annuaire d'Active Directory. Chaque contrôleur d'un domaine donné est en mesure de recevoir des modifications et de les dupliques vers l'ensemble de ses homologue au sein du domaine.

Unité d'organisation

Est un objet conteneur utilisé pour organiser les objets d'un domaine. Une OU peut contenir des comptes d'utilisateur, des ordinateurs, des imprimantes, ainsi que d'autres OU.

Hiérarchisation des unités d'organisation

Par type d'objet

Par type organisationnelle

Arborescences

Est une organisation hiérarchique de domaines Windows 2000 partageant un espace de noms contigus.

Le nouveau domaine est le domaine est un domaine enfant d'un domaine parent. Chaque domaine enfant à une relation bidirectionnelle transitive avec son domaine parent

Forêts

Comprend une ou plusieurs arborescences. Les forêts ne forment pas un espace de nom contigu. En revanche les forêts partagent une schéma et un catalogue global commun

Catalogue global

Est un référentiel d'information qui contient un sous-ensemble d'attributs relatifs à tous les objets d'Active Directory

Le catalogue global permet

Trouver des informations Active Directory dans toute la forêt

Utiliser des informations d'appartenance à des groupes universels pour ouvrir des cessions sur le réseau.

Un serveur de catalogue global est un contrôleur de domaine qui conserve une copie du catalogue global et qui traite les requêtes qui lui sont destinées. Le premier contrôleur de domaine que vous créez dans Active Directory devient automatiquement le serveur de catalogue global, par la suite on peut rajouter d'autres contrôleurs de catalogue global

Activer / désactiver un catalogue global

Dans la console Site et service Active Directory , dans l'arborescence console , développer le contrôleur de domaine qui va héberger ou héberge le catalogue global

Clic droit sur **NTDS Settings** puis **Propriété**

Activer ou désactiver la case à cocher catalogue global

Structure physique d'Active Directory

Dans Active Directory la structure logique est séparée de la structure physique. La structure logique organise les ressources réseau, tandis que la structure physique sert à configurer et à gérer le trafic réseau. Ce sont les contrôleurs de domaine et de sites qui forment la structure physique d'Active Directory.

Contrôleur de domaine

Est un contrôleur du domaine exécutant Windows 2000 server qui stocke un réplica de l'annuaire, gère les modifications et les duplique vers les autres contrôleurs du même domaine. Ils gèrent les ouvertures de session, d'authentification, et de recherche dans l'annuaire.

Les domaines mappent la structure logique de l'organisation.

Sites

Est une combinaison d'un ou plusieurs sous-réseaux IP connecté par une liaison haut débit.

Les sites mappent la structure physique du réseau.

Préparation de l'installation d'Active Directory

Configuration requise

Ordinateur exécutant Windows 2000 Server ou +

Espace disque de 200 Mo pour Active Directory et 50 Mo pour les fichiers journaux (création du dossier SYSVOL)

Partition NTFS

Protocole TCP/IP installé et configuré pour utiliser DNS

Privilèges administratif nécessaires

Création d'un premier domaine (Sous le nom de **Premier-Site-par-défaut**)

Lancer l'assistant d'installation

dcpromo.exe

Choisir le contrôleur de domaine et le type de domaine

Indiquer le nom de domaine, nom DNS , nom NetBIOS

L'emplacement du volume de base, du journal et du volume système partagé.

Autorisations

Mot de passe à utiliser en mode restauration des services d'annuaire

Ajout d'un contrôleur de domaine réplica

La tolérance de panne exige au moins deux contrôleurs de domaine par domaine.

Plusieurs contrôleurs de domaines permettent d'éviter de surcharger le contrôleur de domaine.

Lancer **dcpromo.exe** et suivre l'assistant

Utilisation d'un script d'installation sans assistance

Un fichier réponse contenant les paramètres requis pour une session d'installation sans assistance. Contient uniquement la section [DCInstall]

Ligne de commande **dcpromo /answer :<fichier_réponse>**

Voir Unattend.doc dans le cdrom \Support\Tolls\Deploy.cab

Configuration du service d'annuaire

Opération commune à toutes les installations

Création des entrées de Registre nécessaires

Paramétrage des compteurs de performances pour Active Directory

Configuration du serveur pour enrôler automatiquement un certificat de contrôleur de domaine X509.

Démarrage du protocole d'authentification Kerberos version 5

Paramétrage de la stratégie d'autorité de sécurité locale

Installation de raccourcis vers les outils d'administration dans Active Directory

Configuration des partition de l'annuaire

Création de la partition d'annuaire de schéma

Contient le conteneur Schéma, qui stocke les définitions de classe et d'attribut de tout les objets d'Active Directory .

Elle est dupliquée dans tous les contrôleurs de domaine de la forêt

Création de la partition de configuration d'annuaire.

Contient le conteneur configuration qui stocke les objets configuration de l'ensemble de la forêt. Les objets configuration stockent des informations sur les sites, les services, et les partitions d'annuaire.

Elle est dupliquée dans tous les contrôleurs de domaine la forêt.

Création de la partition d'annuaire de domaine

Contient un conteneur de domaine, tel que le conteneur consoto.msft, qui stocke les utilisateurs, les ordinateurs, les groupes et autres objets d'un domaine Windows 2000.

Elle est dupliquée dans tous les contrôleurs de domaine d'un même domaine.

Configuration des services et de la sécurité

Démarrage automatique des services

Localisateur RPC

Permet aux application distribuées d'utiliser le service de noms RPC (Remote Procédure Call)

Ouverture de session réseau

Exécute le service de localisateur de contrôleur de domaine. Crée un canal fiable pour l'enregistrement des ressources SRV dans DNS entre l'ordinateur client et le contrôleur de domaine.

Centre de distribution des clés

KDC (Key Distribution Center) : gère une base de données avec des information sur les comptes pour toutes les entités de sécurité dans son domaine

Messagerie intersite

ISM (interSite Messaging) utilisé pour la duplication du courrier intersite

Serveur Suivi de liaisons distribuées

Sert à résoudre les raccourcis et les liens OLE vers les fichiers résidents NTFS dont le nom et/ou le chemin ont changé.

Service de temps Windows

Synchronise les horloges des ordinateurs clients et des serveur exécutant W2K

Paramétrage de la sécurité

Active la sécurité sur le service d'annuaire et les dossiers de duplication des fichiers.

Configure des listes DACL sur les fichiers et les objets d'Active Directory

Autres opérations d'installation d'Active Directory

Règle le nom de domaine racine DNS de l'ordinateur

Détermine si le serveur est déjà membre du domaine

Crée un compte d'ordinateur dans l'unité d'organisation Domain Controllers

Applique le mot de passe fourni par l'utilisateur pour le compte administrateur

Crée un objet de référence croisé dans le conteneur Configuration

Ajoute des raccourcis

Crée le dossier partagé SYSVOL (qui contient les stratégie de groupe) et NETLOGON (qui contient les scripts d'ouverture de session des ordinateurs non Windows 2000)

Crée le conteneur Schéma et Configuration

Attribue des rôles spécifique au contrôleur de domaine

Vérification après installation

Vérification des enregistrements SRV

Utiliser la commande **nslookup** puis taper : **ls –t SRV** ***domaine***

Ou

Outils d'administration DNS double cliquer sur le serveur puis sur **Zone de recherche directe** : si les enregistrements SRV sont inscrit on trouve les dossiers

_msdcs

_sites

_tcp

_udp

Vérification du dossier SYSVOL et NETLOGON

Utiliser la commande **net share** , dans la liste des dossiers partagés on devrait voir

NETLOGON racine_système\SYSVOL\domaine\SCRIPTS

SYSVOL racine_système\SYSVOL

Ou

Menu **<Démarrer>** puis **<Exécuter>** taper **%systemroot%\sysvol**

L'explorateur de Windows s'ouvre et affiche le contenue du dossier SYSVOL qui doit comporter les sous dossiers suivants

Domain

Staging

Staging areas

Sysvol

Vérification de la base de données d'annuaire et des fichiers journaux

Menu **<Démarrer>** puis **<Exécuter>** taper **%systemroot%\ntds**

L'explorateur de Windows s'ouvre et affiche le contenue du dossier Ntds qui doit comporter les fichiers suivants

Ntds .dit : il s'agit du fichier de base de données d'annuaire

Edb.* : il s'agit des journaux de transaction et des fichiers de points de vérification

Res*.log : il s'agit des fichiers journaux réservé

Vérification des résultats de l'installation par le biais des journaux d'événements

Implémentation de zone de recherche intégrées dans Active Directory

Après l'installation d'Active Directory, intégrer une zone DNS à Active Directory afin que DNS puisse utiliser AD pour stocker et dupliquer les bases de données de zone DNS.

Utiliser DNS pour intégrer une zone DNS à Active Directory

Implémenter une zone de recherche directe

<outils d'administration> <DNS> <zone de recherche directe> puis clic droit sur **<Propriétés>**

Implémenter une zone de recherche inversée

Idem pour zone de recherche inversée

Plublication dans Active Directory

C'est l'action de créer ou rechercher des objets dans AD. Tout objet exécutant W2K est automatiquement publié dans AD. C'est le serveur d'impression qui publie les imprimantes sur AD.

Pour afficher les objets imprimante : Menu **Affichage** cliquer sur **Utilisateurs ,Groupes et Ordinateurs en tant que conteneurs.**

Pour mettre à jour des imprimantes orphelines utiliser le netttoyeur dedisque : **Démarrer Programmes Outils systèmes Nettoyeur de dique.**

Publication d'une imprimante n'exécutant pas W2K

Avec la console **Utilisateurs et ordinateurs Active Directory** en faisant : **Nouveau** puis cliquer sur **imprimante** taper le chemin UNC (\\serveur\partage\) de l'imprimante ou le script **Pubprn.vbs** . Taper **CSRIPT %systemroot%\system32\pubprn.vbs <*paramètre*s>**

Exemple : pour publier une imprimante sur un serveur dans l'OU Sales et le domaine consoto.msft : taper à l'invite

Pubprn.vbs *serveur* « **ldap://OU=Sales,DC=Consoto,DC=msft »**

Définition de l'emplacement des imprimantes

Active Directory repère les imprimantes du sous réseau. En conséquence il faut segmenter le réseau de façon logique pour pouvoir distribuer correctement les imprimantes dans un réseau.

Le nom de l'imprimante est limité à 32 caractères et le nom complet à 260 caractères.

Le nom détaillé peut aider les utilisateurs à repérer géographiquement les imprimantes. On peut ainsi donner dans ce champ des renseignements utiles

Configuration et administration d'un dossier partagé

Publication d'un dossier

Dans la console **utilisateurs et ordinateurs Active Directory** cliquer droit sur l'OU dans la laquelle vous souhaitez faire le partage , choisir **Nouveau** puis **dossier partagé** dans la zone nom taper le chemin UNC du dossier (\\serveur\partage)

Délégation du contrôle de l'administration

Dans la console **<Utilisateurs et ordinateurs Active Directory>** dans l'OU ou la délégation doit avoir lieu cliquer sur **<Action>** puis **<Déléguer le contrôle>** pour ouvrir l'assistant.

Suppression d'Active Directory

L'assistant d'installation permet de supprimer Active Directory.

Lancer dcpromo.exe

La console MMC

Mode auteur

Mode utilisateur

Accès total

Accès limité ; fenêtres multiples

Accès limité ,fenêtre simple

Note le mode auteur et le mode utilisateur peuvent modifier la MMC

Pour pouvoir modifier une MMC en mode utilisateur il est conseillé d'avoir une version en mode auteur

Pour empêcher les modification de la MMC il faut attribuer au fichier .MSC la permission lecture uniquement

Stratégie de groupe

Permet de contrôler l'administration des utilisateurs et des ordinateurs du réseau

Permet la décentralisation de l'administration

3 niveaux d'administrations 3 niveaux de stratégie de groupe

Admins de l'entreprise	Site
Admins du domaine	Domaine
Administrateurs	OU

La stratégie de groupe ne s'applique uniquement aux versions de Windows 2000 et non pas aux versions antérieures

Le GPO (Group Policy Object)

Permet de contrôler des configurations utilisateurs et ordinateurs spécifiques

Modèle d'administration : basée sur le registre

Sécurité : contrôle d'accès au réseau ,contrôle des comptes utilisateurs

Installation logicielle : ajout :suppression de logiciel automatiquement

Scripts : spécifie l'exécution des scripts au démarrage et à l'arrêt de l'ordinateur.

Service installation à distance : permet le contrôle via RIS aux clients

Maintenance Internet : personnalisation IE

Redirection de dossier : paramètrage du profil utilisateur et lien aux dossiers partagés.

Actualisation des stratégies

Par défaut 90 mn pour les ordinateurs W2K

5 mn pour les contrôleurs de domaine

ces valeurs peuvent être changée en modifiant le paramètre du modèle d'administration pour la configuration de l'utilisateur ou de l'ordinateur. L'actualisation ne peut être programmé à une heure donnée.

Conflit entre les stratégies de groupe

Entre le conteneur parent et le conteneur enfant c'est la stratégie du groupe du conteneur enfant qui sera appliquée

Entre deux stratégie de groupe dans le même conteneur c'est la stratégie la plus haute qui est appliquée.

L'héritage des stratégies

Bloquer l'héritage

Empêcher tout les GPO d'hériter des stratégies du conteneur parent

(S'applique au niveau du conteneur ou l'on souhaite bloquer la stratégie)

Aucun remplacement

Force toutes les stratégies du conteneur parents à être appliquées même si le conteur enfant fait un blocage de stratégie

Surveillance des stratégies

Activer l'option inscription dans le journal d'événement

<Démarrer> <Exécuter> taper **<regedit>** dans la clé**HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurentVersion** ajouter la valeur **dword <RunDiagnosticLoggingGlobal >** et entrer la valeur **<1>** (Augmenter la taille du journal d'événement)

Activation de l'option inscription commentée

<Démarrer> <Exécuter> taper **<regedit>** dans la clé**HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurentVersion\Winlogon** ajouter la valeur **dword <UserEnvDebudLevel >** et entrer la valeur

<30002> pour l'option inscription commentée

<30001> pour l'inscription des erreurs et des avertissements

<30001> pour ne rien inscrire

les outils dur le CD

répertoire Support tools

netdiag.exe outils de ligne de commande permet d'isoler les problèmes de connectivité et de gestion du réseau

replmon.exe outil graphique pour résoudre les problèmes de stratégie de groupe lié à une duplication incomplète du conteneur

le kit de ressource

gptools.exe utilitaire de ligne de commande pour vérifier la santé des GPO sur les contrôleur de domaine

gpresult.exe utilitaire en ligne de commande pour afficher l'impact d'un GPO sur un ordinateur local et l'utilisateur qui ouvre sa session

les modèles d'administration

Ils permettent de configurer, de vérifier et de d'implémenter des modèles de sécurité en vue de modéliser et simplifier l'implémentation d'un environnement utilisateur

Les paramètres ordinateurs

Dans la base de registre sous HKEY_LOCAL_MACHINE (HKLM)

Le GPO est dans la clé HKLM\Software\Microsoft\Windows\CurrentVersion\Policies

Les paramètres utilisateurs

Dans la base de registre sou HKEY_CURRENT_USER (HKCU)

Le GPO est dans la clé HKCU\Software\Microsoft\Windows\CurrentVersion\Policies

Application des paramètres de modèle d'administration sur les ordinateurs

l'ordinateur client démarre. Il récupère la liste des objets GPO approprié et l'utilisateur ouvre sa session

l'ordinateur client se connecte à SYSVOL et localise les fichiers Registry.pol

l'ordinateur client écrit dans les sous-aborescences du Registre HKCU HKLM

la boite de dialogue d'ouverture de session apparaît

Affectation de scripts à l'aide d'une stratégie de groupe

Pour automatiser l'exécution des scripts et appliquer les stratégies à un groupe ou un utilisateur lors du démarrage ou l'arrêt de l'ordinateur

La valeur du traitement d'un script est de 10mn si le script dure plus de 10mn il faut modifier ce temps d'attente sous Configuration ordinateur\Modèle d'administration\système\Ouverture de session

\delais d'attente maximal pour les scripts de stratégie de groupe

Affectation d'un script à un GPO

Localiser le modèle du script (.GPT) à l'aide de l'explorateur de Windows

Ouvrir le GPO

sous Configuration ordinateur pour les scripts de démarrage ou d'arrêt

sous Configuration utilisateur pour les scripts d'ouverture et fermeture de session

développer **Paramètres Windows** puis **Scripts** puis cliquer sur **Afficher les fichiers**puis **Ajouter** puis **Ouvrir** enfin <OK>

Utilisation d'une GPO pour rediriger des dossiers

Utiliser pour rediriger des dossier qui font partie du profil de l'utilisateur et les rediriger vers un répertoire partagé du serveur

Choix des dossiers à rediriger

Dossier	Contenu	Objectif de la redirection vers le serveur
Mes documents	Données personnelles	Accéder aux données personnelles à partir d'un ordinateur quelconque, ces données peuvent être sauvegardées et gérées de manière centralisée
Menu Démarrer	Dossiers et raccourcis du Menu Démarrer	Les menus Démarrer des utilisateur sont standardisés
Bureau	Tous fichiers que l'utilisateur place sur le bureau	Les utilisateurs ont le même bureau quelque soit l'ordinateur
Application DATA	Données spécifiques à un utilisateur stockées par application	Les applications utilisent les même données spécifique à l'utilisateur quelque soit l'ordinateur ou l'utilisateur ouvre sa session

Pour rediriger un dossier

Créer un GPO ou sélectionner un GPO existant ; cliquer sur **Modifier**

Développer **Configuration utilisateur, Paramètres Windows** puis **redirection de dossier**

Clic droit sur le dossier à rediriger puis **Propriété** puis indiquer l'emplacement cible et son chemin d'accès.

Utilisation d'une stratégie de groupe pour sécuriser un environnement utilisateur

indentifier ou créer un modèle de sécurité

Importer le modèle dans le GPO

Développer **Configuration ordinateur** , **Paramètres Windows** puis **Paramètres de sécurité** cliquer droit puis **Importer une stratégie** puis OK

Il est important de bien analyser les résultats de l'application avant le déploiement ; cela peut perturber gravement le réseau de plus le registre ne s'efface pas lors de la suppression de paramètre de sécurité

Gestion de la duplication Active Directory

Implique le transfert et le maintien des données Active Directory entre les contrôleur de domaine du réseau. AD utilise la duplication multi-maître

Fonctionnement de la duplication

La duplication intervient du fait des changement apportée à AD

nouveaux comptes utilisateurs

changement d'attributs d'objet

suppression d'objet

la latence de duplication

toute les 5 mn par défaut lors d'une modification

toute les heures en absence de modification

notification immédiate lors de duplication urgente (tout ce qui touche à la sécurité(ex verrouillage de comptes))

résolution des conflits

la duplication dans AD est conçue sur un modèle à plusieurs maîtres, ainsi tous les ordinateur proposant un mise à jour à plusieurs maîtres doivent gérer les conflits

Pour réduire les conflits, les contrôleur de domaine enregistre et dupliquent les changements apportés aux objets au niveau des attributs plutôt qu'au niveau des objets. Ainsi les modification portées à deux attributs différents d'un objet , tels que le mot de passe de l'utilisateur et le code postal, n'entraîneront pas de conflit même s'ils ont été modifié en même temps.

Cachet unique globaux

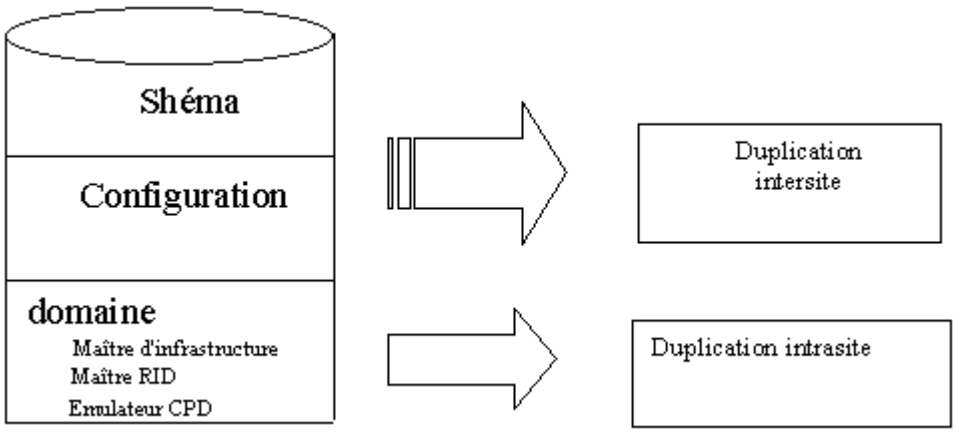
Il est défini par 3 composant

1 – numéro de version : augmente à chaque mise à jour ; le N° le plus petit est écrasé

2 – dateur : date heure système

3 – serveur GUID : il identifie le contrôleur du domaine à l'origine de la modification

partition de l'annuaire



Partition de schéma

Contient les définition de tous les objets et attributs qui peuvent être crées dans l'annuaire, ainsi que les règles de création et de gestion de ces objets et attributs

Est dupliquée sur tous les contrôleurs de domaine de la forêt

Il ne peut y avoir qu'un seul schéma dans la forêt

Partition de configuration

Contient les informations portant sur la structure d'AD , y compris quels domaines et quels sites existent, quel contrôleur de domaine existent dans chacun d'eux et quels services sont disponibles.

Est dupliquée sur tous les contrôleurs de domaine de la forêt

Il ne peut y avoir qu'une seule partition de configuration dans la forêt

Partition de domaine

Contient des informations concernant tous les objets spécifique au domaine crées dans AD, y compris les utilisateurs, les groupes , les ordinateurs, les OU ;

Est dupliquée au sein de son domaine

Il peut y avoir plusieurs partition de domaine par forêt

Le serveur de catalogue global

C'est un contrôleur de domaine qui stocke les partitions d'annuaire actualisables ainsi qu'un réplica partiel de partition d'annuaire qui contient un copie en lecture seule des parties d'informations stockées dans cette partition.

Le vérificateur de KCC

C'est un processus intégré sur chaque contrôleur de domaine qui génère automatiquement la topologie de duplication dans la forêt. Il calcule automatiquement la meilleure connexion possible entre chaque contrôleur de domaine et établi de nouveaux liens en cas de panne. Le KCC ne peut faire que 3 bonds donc il gènère une topologie de duplication automatique pour que le KCC n'ait pas plus de 3 sauts pour que tout les contrôleurs de domaine suivants soient à jour.

Réplication immédiate

Dans site et service Active Directory, développer **Sites**, **premier site par défaut** puis sur **serveurs** sélectionner le contrôleur de domaine sur lequel à mise à jour à été entreprise cliquer sur **NTDS Settings** cliquer droit sur l'objet de connexion du partenaire de réplication puis cliquer sur **répliquer maintenant** ensuite <OK>

Duplication intersite

On peut planifier manuellement la duplication intersite. Pour optimiser la bande passante on peut on peur compresser le trafic de duplication ce qui augmente le temps processeur du contrôleur de domaine.

Protocole de duplication

RPC

duplication intersites et intrasite

SMTP

duplication intersite (préferez RPC)

surveillance de duplication

réplication monitor

outils graphique ne peut être exécuté que sur tout controleur de domaine ,serveur membre ou tout ordinateur exécutant W2K advanced serveur

se trouve dans support tools

repadmin

outils en ligne de commande

le maître d'opération

est un contrôleur de domaine qui joue le rôle de contrôleur de modification

il à 5 rôles

contrôleur de schéma

contrôle toutes mise à jour apportées au schéma. Le schéma contien la liste des clases d'objets et d'attributs, liste qui sert à créer tout les objet d'Active Directory tels que les ordinateurs les utilisateurs les imprimantes

Rôle à l'échelle de la forêt

1 seul contrôleur de schéma par forêt

maître d'attribution de non de domaine

Contrôle l'ajout ou la suppression de domaine dans la forêt

le Contrôleur de domaine est aussi serveur de catalogue global

1 seul maître d'attribution de nom de domaine par forêt

émulateur CPD

Prend en charge les contrôleurs secondaires de domaines (CSD) exécutant Windows NT en mode mixte.

Il est le premier contrôleur de domaine crée dans un nouveau domaine.

Met à jour les modification des mots de passe pour les client antérieur à W2K.

Réduit le délais de duplication en cas de modification des mots de passe pour les ordinateurs client W2K

Gère la synchronisation horaire

Elimine les risque d'écrasement des objets GPO

maître d'identificateur relatif (RID)

Attribue des blocs d'identificateurs RID à chaque contrôleur de son domaine

Empêche la duplication d'objets s'ils se déplacent d'un contrôleur de domaine à un autre.

Pour afficher l'allocation du pool RID utiliser **dcdiag**

maître d'infrastrcuture

Mise à jour ,dans son domaine, des références à des objets situés dans un autre domaine. La référence à l'objet contient le GUID et éventuellement le SID

Le maître d'infrastructure ne doit pas être sur le même contrôleur de domaine que celui qui héberge le catalogue global

Dans une forêt à un seul domaine il n'y a pas de maître d'infrastructure

Le maître d'infrastructure d'un domaine étudie régulièrement le réplica des données de l'annuaire, les références aux objets qui ne se trouvent pas sur ce contrôleur de domaine. Il demande au serveur de catalogue global des informations courantes sur le nom unique et l'identificateur de sécurité de chaque objet référencés.

Gestion des rôles de maître d'opérations

Lorsqu'on crée un domaine Windows 2000, le système d'exploitation configure automatiquement tous les rôles du maître d'opérations. Il peut être nécessaire de réattribuer un rôle de maître d'opérations un autre contrôleur de domaine dans la forêt ou dans le domaine. Il faut exécuter la procédure ci-desous

Identifier le conteneur du rôle de maître d'opération

Selon de maître d'opération à déterniner il faut utiliser l'une des console Active Directory

Utilisateur et ordinateur Active Directory

Domaine et approbation Active Directory

Schéma Active Directory

Identification du maître RID, de l'émulateur CPD et du maître d'infrastructure

- Ouvrir la console Utilisateur et ordinateur AD

Clic droit sur **Utilisateurs et ordinateurs AD** puis clic sur **Maître d'opérations**

Clic sur onglet **RID** , **PDC** ou **insfrastructure**

Le nom du maître d'opération actuel s'affiche dans la zone **Maître d'opération**

Identification du maître d'attribution de nom de domaine

Ouvrir la console Domaine et approbation AD

Clic droit sur **Domaine s et approbations AD** piuis clic sur **Maître d'opérations**

Le nom du maître d'attribution de nom de domaine actuel s 'affiche dans la boite de dialogue **Modifier le maître d'opérations**.

Identification du contrôleur de schéma

Enregistrer une MMC Schéma AD en exécutant la commande

Regsrv32.exe %systemroot%\system32\schmmgmt.dll

Cliquer **<OK>** pour fermer le message indiquant la réussite de l'enregistrament

Créer un MMC personnalisée

Ajouter le composant logiciel enfichable Schéma AD à cette console

Dans l'arborescence de la console, clic droit sur **Schéma AD** , puis sur **Maître d'opérations**

Le nom du contrôleur de schéma actuel s'affiche dans la boite de dialogue **Modifier le maître d'opérations**

Transfert de rôle de maître d'opérations

Matrître d'opération	Groupe autorisé
Contrôleur de schéma	Administrateurs du schéma
Maître d'attribution de nom de domaine	Administrateurs de l'entreprise
Emulateur CPD	Admins du domaine
Maître RID	Admins du domaine
Maître d'infrastructure	Admins du domaine

Transfert des rôle de maître RID, émulateur CPD et maître d'infrastructure

Ouvrir la console Utilisateur et Ordinateur AD

Dans l'arborescence de la console , clic droit sur **Utilisateur et ordinateurs AD** , puis clic sur **se connecter au domaine**

Dans la liste des contrôleurs de domaine disponibles, clic sur le contrôleur de domaine qui devient le nouveau maître d'opérations puis **<OK>**

Dans l'arborescence de la console, clic droit sur le contrôleur de domaine qui devient le nouveau maître d'opération, puis clic sur **Maître d'opérations**

Clic sur l'onglet correspondant au rôle de maître d'opération à transférer, par exemple CPD , puis clic sur **Modifier**

Attention : Vérifier que vous ne transférez pas le rôle de maître d'infrastructure dans un contrôleur de domaine qui héberge déjà un catalogue global

Transfert du rôle de maître d'attribution de nom de domaine

Ouvrir la console Domaine et approbation AD

Dans l'arborescence de la console , clic droit sur **Domaine et approbations AD** , puis clic sur **Se connecter au domaine**

Dans la liste des contrôleurs de domaine disponibles, clic sur le contrôleur de domaine qui devient le nouveau maître d'attribution de nom de domaine puis **<OK>**

Dans l'arborescence de la console , clic droit sur **Domaines et approbations AD** , puis clic sur **Maître d'opérations**

Le nom du contrôleur de domaine que vous avez spécifié s'affiche

Clic sur **Modifier**

Attention : Vérifier que le contrôleur de domaine qui contient le rôle de maître d'attribution de nom de domaine héberge également le catalogue global

Transfert du rôle de contrôleur de schéma

Ouvrir la console Schéma AD

Dans l'arborescence de la console, clic droit sur **Schéma AD**, puis clic sur **Modifier le contrôleur de domaine**

Clic sur **Spécifier un nom ,** taper le nom du contrôleur de domaine dans lequel transférer le rôle de contrôleur de schéma, puis <OK>

Dans l'arborescence de la console, clic droit sur **schéma AD**, puis sur **Maître d'opérations**

Le mon du contrôleur de domaine que vous avez spécifié s'affiche

Clic sur **Modifier**

Attention : Vous devez enregistrer la MMC d'administration de schéma , schmgmt.dll avant d'ouvrir AD

Prise du rôle de maître d'opérations

Le transfert d'un maître d'opération défaillant vers un nouveau contrôleur de domaine doit obligatoirement précédé de la déconnexion physique définitive du maître d'opération en panne

Utiliser la console AD ou la commande ntdsutil pour transférer le rôle.

Prise des rôle émunlateur CPD et maître d'infrastructure

Ouvrir la console Utilisateurs et ordinateurs AD

Dans l'arborescence de la console, clic droit sur **Utilisateurs et ordinateurs AD** , puis clic sur **Maître d'opérations**

Dans la boite de dialogue **Maître d'opérations,** clic sur onglet du rôle de maître d'opérations à prendre

Clic sur **Modifier**, puis lorsqu'un message indique qu'un transfert n'est pas envisageable, clic sur <OUI>

Clic sur <OK> dans la page d'avertissement, puis à nouveau <OK> pour effectuer un transfert forcé

Clic sur <OK> pour fermer la boite de dialogue **Maître d'opérations**

Vérifier que le rôle de maître d'opérations est bien réattribué

Prise des autres rôles de maître d'opérations

La perte temporaire du contrôleur de schéma, du maître de nom de domaine ou du maître RID n'est pas perceptible par l'utilisateur final et n'a généralement aucune incidence sur votre mission d'administrateur . En cas de panne définitive déconnecter physiquement l'ordinateur

Et utiliser la commande ntdsutil

Utilisation de la commande ntdsutil

A l'invite de commande taper **ntdsutil**

A l'invite de ntdsutil taper **roles**

A l'invite **fsmo maintenance**, taper **connections**

A l'invite **server connections** taper **quit**

A l'invite **fsmo maintenance** , taper l'une des commande suivantes approprié

Seize RID master

Seize PDC

Seize infrastructure master

Seize domain naminf master

Seize schéma master

A l'invite **fsmo maintenance** , taper **quit**

A l'invite **ntdsutil**, taper **quit**

Vérifier que le rôle de maître d'opérations a bien été réattribué

Défaillance de l'émulateur CPD

A de grave conséquence sur le fonctionnement du réseau

perte des modifications des mots de passe pour les ordinateurs antérieur à W2K

perte de la diminution de latence pour la mise à jour des mots de passe

perte de la synchronisation horaire entre contrôleurs

Défaillance du maître d'infrastructure

N'est pas grave tant qu'elle ne dure pas longtemps

Défaillance des autres maîtres d'opérations

ne doit être envisagée qu'en dernier recours

déconnecter l'ordinateur défaillant

utiliser **ntdssutil**

Défragmentation de la base de données

La défragmentation s'effectue automatiquement lors du processus de nettoyage de la mémoire. La défragmentation hors connexion doit être effectuée manuellement. Elle est nécessaire pour créer une version compressée du fichier de base de donnée d'origine (ntds.dit)

Procédure

sauvegarder AD par précaution

redémarrer le contrôleur en mode **menu d'option avancées de Windows 2000** touche **F8** au démarrage

sélectionner **Mode restauration des services d'annuaire** puis <Entrée>

ouvrir une session en Administrateur

à l'invite taper **ntdsutil** puis <Entrée>

taper **files** puis <Entrée> ; l'invite revoie **Files** pour gérer les fichiers de données

définir un emplacement ayant un espace disque suffisant pour stocker la base de données compressée : taper **compact to <lecteur>:\<répertoire>**

taper **quit** (2 fois pour sortir du processus)

copier le nouveau fichier ntds.dit sur l'ancien fichier ntds.dit dans le chemin actuel de la base de données d'AD que vous avez noté à l'étape 6

redémarer le contrôleur

Le DNS

DNS = Domain Name Service

Sert à résoudre les noms d'ordinateur en adresse IP.

Contention de dénomination pour les domaines Windows 2000 (nommage des domaines W2K)

Localisation des composants physique d'Active Directory.

Type de requêtes

Requête itérative

Le serveur DNS envoie la meilleure réponse qu'il peut fournir sans aucune aide d'un autre serveur.

Requête récursive

Le serveur DNS renvoie une réponse incomplète.

Type de recherche

Recherche directe

Nécessite une résolution Nom / Adresse

Recherche indirecte

Nécessite une résolution Adresse / Nom

Installation du service DNS

Programmes + Ajout/Suppression de programmes + Ajouter/Supprimer des composants de Windows + Services réseaux puis Détails activer **Systèmes des noms de domaines DNS** puis **OK**

Le client DNS

Dans Propriétés de protocole Internet (TCP/IP)

Obtenir une adresse des serveurs DNS automatiquement

Utiliser l'adresse du serveur de DNS préféré

Configuration d'un fichier HOST

Fichier texte contenant en « dur » l'adresse IP, le nom d'hôte, l'Alias

Situé dans : \racine_Système\Système32\Drivers\ETC

Configuration de zones

Une zone est définie par les informations stockées dans un fichier de zone sur le serveur DNS. Le serveur DNS de référence fournit la résolution des noms pour les clients DNS et d'autres serveurs DNS.

On doit promouvoir une zone principale avant de créer des zones secondaires.

Lorsque l'on ajoute un serveur de DNS secondaire il faut désigner un serveur de DNS maître.

On ne peut créer des zones intégrées Active Directory que sur les serveurs configurés en tant que contrôleur de domaines et sur lesquels le service DNS a été installé

Le serveur de cache DNS

Effectue la résolution des noms pour des clients éloignés du serveur DNS par une liaison à faible bande passante.

Différence entre un serveur secondaire et un serveur de cache DNS

Serveur secondaire mise à jour régulière et aux reboots

Serveur de cache utile sur les liaison à faible débit : pas de mise à jour sur le serveur siège

Surveillance DNS

Test du service DNS

Dans le système DNS ouvrez la boîte de dialogue **Propriétés** puis onglet **Analyse**.

Requête simple : test local utilisant le client DNS pour interroger le serveur

Requête récursive : Teste le serveur en transférant la requête à d'autres serveur DNS

Observateur d'événements

Pour visualiser le journal des événements du serveur DNS .Utile pour connaître les performances du serveur DNS

Activation des options de débogage

A des fins de dépannage avancé, enregistre un fichier dans \racine_système\Système32\Dns.log en activant dans l'onglet **Enregistrement** de la boîte de dialogue **Propriétés**

Attention peut nuire aux performances générale u serveur DNS et consomme de l'espace disque.

Intégration DNS et DCHP

Par défaut les clients exécutant W2K peuvent mettre à jour le système DNS avec leur informations de mappage nom/adresse IP dès qu'un serveur DHCP leur affecte une adresse IP. Pour les version antérieure il faut configurer le serveur DHCP pour mettre cette mise à jour sur le serveur DNS. C'est le serveur DHCP qui se charge de cette opération

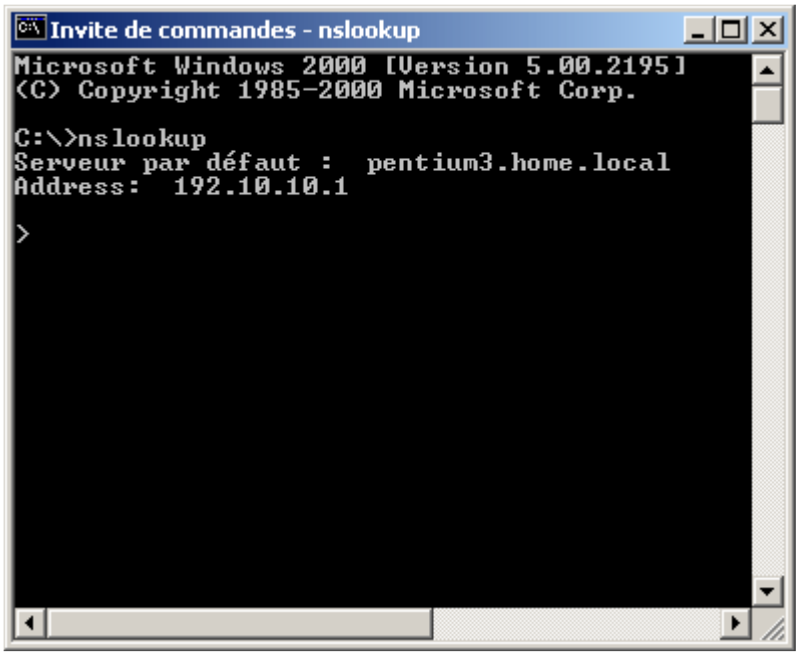
Mise a jour automatique

Le client W2K est capable de s'enregistrer dynamiquement au serveur DNS

Le client W98/NT4 est enregistré par le serveur DHCP

Pour un mise à jour automatique le serveur DNS doit être soit WINDOWS 2000 ou être serveur DNS BIND 8.2.1 minimum

Utilitaire Nslookup



Pour vérifier que les informations contenues dans les enregistrements de resources sont correctes

Désinstaller DNS

<Démarrer> + <Paramètres> +<Panneau de configuration> + <Ajout/Suppression de programmes> + <Ajouter/supprimer des composants de Windows> + <Services de mises en réseau> + <Détails> + <Systèmes de noms DNS>

IPSEC

Le protocole est utilisé pour sécuriser et fiabiliser les liaisons des entreprises utilisant des protocoles Internet.

On peut implémenter IPSec sur des liaisons VPN Internet ou Intranet.

L'objectif étant d'assurer la protection des paquets IP . Chaque ordinateur traite cette protection. Le protocole utilisé est L2TP

Mise en place de stratégie IPSec

A partir du composant logiciel enfichable Gestion de la stratégie de sécurité du protocole IP. A partir de ce composant on peut gérer

un ordinateur local

Gérer la stratégie de domaine de cet ordinateur

Gérer la stratégie de domaine pour un autre ordinateur

Gérer un ordinateur distant

Stratégie prédéfinie

Client (en réponse seule)

Serveur (demandez la stratégie)

Sécuriser le serveur (nécessite la stratégie)

Vérification de stratégie

IPSECMON. EXE à partir du menu exécuter

Attention : Lors d l'activation d'une stratégie un Ping peut échouer. Il faut du temps pour négocier la stratégie sur les deux ordinateurs

Désinstaller la stratégie IPSec

Console MMC « Gestion de la stratégie de sécurité du protocole IP », dans la fenêtre de droite passer à <non> l'état de stratégie attribuée.

Configuration de l'accès distant (RRAS)

Permet aux télétravailleurs ou aux utilisateurs mobiles d'accéder, via une liaison commuté au réseau de l'entreprise

Type de liaisons

Connexion d'accès distant è RTC ou RNIS

Connexion VPN è via Internet

Connexion directe avec un autre ordinateur via un câble

Protocole de transport

Protocoles d'accès distant	Protocoles LAN
PPP	TCP/IP
SLIP (Client uniquement)	NWLink
Microsoft RAS	NetBEUI
ARAP (Serveur uniquement)	Apple Talk

Protocole PPP (Point to Point Protocol)

Le plus employé. W2K serveur ne supporte que PPP

Protocole SLIP (Sérial Line Internet Protocol)

Employé avec Telnet; protocole utilisé par W2K Pro uniquement, un serveur n'utilise pas SLIP

Microsoft RAS

Employé par les clients Microsoft NT3.1, Windows pour Workgroups, MSDos et LAN Manager se connectant à un serveur W2K , Le client doit utiliser NETBEUI

Protocole ARAP

Les clients Apple Macintosh peuvent se connecter à un serveur exécutant W2K en utilisant ARAP

Protocole VPN

Le VPN ne requiert pas de connexion d'accès à distance. Il requiert un connectivité IP entre le client et le serveur. VPN est une connexion cryptée et sécurisée qui utilise PPTP et L2TP

PPTP	***L2TP***
L'interréseau doit utiliser IP	Interréseau utilise IP ou relais à trames X25 ou ATM
Sans compression d'en-tête	Compression d'entêté
Sans authentification en tunnel	Authentification en tunnel
Cryptage PPP intégré	Cryptage IPSec

Configuration de connexions entrantes

Sur un serveur contrôleur du domaine il faut configurer RRAS

Lors de sa mise en route RAS crée automatiquement 5 ports PPTP et 5 ports L2TP

Propriété de l'appel entrant

Autorisations

Permettre l'accès

Refuser l'accès

Contrôler l'accès via la stratégie d'accès distant (disponible qu'en mode natif)

Option de rappel

Si activé le serveur rappelle un N° de tel particulier

Attribution d'une adresse IP statique

Si activé W2K attribue une adresse particulière à l'utilisateur

Application des itinéraires statiques

Si activé l'administrateur définit une série d'itinéraires qui seront ajouté à la table de routage du RAS lors de l'établissement d'un connexion

Configuration de connexions sortantes

Ce sont les connexions depuis un client

Menu <Démarrer> + <Paramètres>+<Connexion réseau et accès à distance>

Les connexions multiples

Permet d'augmenter la bande passante en combinant plusieurs liaisons physiques.Le protocole PPP est utilisé conjointement avec plusieurs cartes modem RNIS ou X25

BAP (Bandwhicth Allocation Protocol)

Améliore les liaisons multiples en ajoutant ou supprimant dynamiquement des liaisons à la demande.

Configuration sur l'onglet PPP de la boite de dialogue Propriété de chaque serveur distant. Case à cocher « Connexion à liaisons multiples » et « Contrôle de largeur de bande dynamique en utilisant les protocoles BAT ou BACP »

Les protocoles d'authentification

PROTOCOLE	Sécurité	Circonstance d'utilisation
PAP (Password Authentification Protocol)	Faible	Le client et le serveur ne peuvent pas négocier en utilisant une validation plus sécurisée Utilise des mots de passe en clair ; si les mot de passe correspondent alors le serveur autorise l'accès au client distant
SPAP (Shiva Password Authentification Protocol)	Moyenne	Connexion à un Shiva LanRover, ou lorsqu'un client Shiva se connecte à un serveur d'accès distant W2K Données relative au mot de passe crypté
CHAP (Chalenge Handshake Authentification Protocol)	Haute	Vous disposez de clients n'exécutant pas un même système d'exploitation Connue sous le nom De MD5-CHAP le serveur distant envoie un challenge consistant à un identificateur de session et un chaîne de challenge arbitraire – Le client revoie le mon de l'utilisateur et un chaîne de challenge,

		l'identificateur de la session et le mot de passe – Le serveur distant vérifie la réponse et autorise la connexion.
MS-PAP (Microsoft Chalenge Handshake Authentification Protocol)	Haute	Vous disposez de clients exécutant Windows NT4.0 ou ultérieures ou Windows 95 et ultérieures Authentification par mot de passe crypté. Possibilité d'utiliser MPPE (Microsoft Point to Point Encryption) pour crypter les donner entre le serveur et le client
MS-CHAP version 2	Haute	Vous disposez de clients d'accès à distance exécutant Windows 2000 ou des clients VPN exécutant Windows NT 4.0 ou Win98

Prend en charge l'authentification

MD5-CHAP : crypte le mon d'utilisateur et le mot de passe

TLS :(Transport Layer Sécurity)est utilisé pour les périphériques intermédiaire comme les cartes à puces

Méthodes d'authentification supplémentaires : EAP autorise l'ajout de méthodes d'authentification propre aux fournisseurs

Configuration des protocoles de cryptage

Boîte de dialogue **Modifier un profil** onglet **Cryptage**

Il existe deux méthodes de cryptage par le biais d'une connexion d'accès distant W2K

MPPE : cryptage d'une connexion PPTP vers un serveur VPN (trois niveaux de cryptage)

IPSec : kerberos + certificats + clé partagée

Configuration du service d'accès distant

Adresse IP statique

Le client gère ses propres adresse IP

Plage d'adresse IP

Le serveur d'accès distant peut attribuer une adresse unique pour chaque client. Cette méthode nécessite autant d'adresse IP que de clients à connecter.

Ou adresse IP dynamique via un serveur DHCP

Un serveur DHCP gère le pool d'adressage dynamique. Cette méthode permet d' « économiser » les adresses pour les clients.

Configuration du service Routage d'accès distant

« Outils d'administration » + « Service de Routage et d'accès distant » sur le serveur approprié clic droit sur «Propriété » onglet « IP »

Activer « Pool d'adresses statiques » pour utiliser un plage d'adresse IP

Activer « Protocole DHCP » pour utiliser uns serveur DHCP

Sélectionner la carte réseau à activer

Dépannage réseau

net helpmsg ***numéro*** è information sur les messages d'erreurs

ipconfig –all è Pour vérifier les paramètres IP de la carte réseau

ipconfig /flushdns è vide le cache DNS

ipconfig /registerdns è oblige le client à renouveler son enregistrement

ping è Teste la connexion TCI/IP

<Impossible de joindre l'hôte destinataire> = Hôte n'est pas joignable

<délais d'attente dépassé> = hôte peut être contacté mais stratégie bloquante

<hôte inconnu> = pas de résolution de nom (voir serveur DNS)

pathping ***adresse IP*** è permet de détecter la perte de paquets acheminés en plusieurs bonds.

tracert è Permet de contrôler la route du paquet IP

arp –a è Affiche les entrées de cache ARP consignées sur l'ordinateur local

arp –d è Supprime les entrées de cache

arp – s è Enregistre les entrées de cache pour un prochain redémarrage de l'ordinateur

nslookup è permet de tester et dépanner un résolution DNS

nbtstast è Affiche les statistiques du protocole et les connexions TCP/IP en utilisant NetBIOS

netstat è Affiche les statistiques du protocole TCP/IP en cours

csvde è Crée plusieurs comptes utilisateurs

ldifde è Crée, modifie et supprime plusieurs comptes utilisateurs