

## **Module 0**

Connaître config min requise : RELNOTES.HTML sur le cd

Config requise : P133, 128Mo RAM, 1Go

Installation :

- soit locale
- soit par réseau : copier i386 sur un serveur et le partager. Sur chaque pc, ya un mini os avec gestion réseau. Nécessite 120Mo pour fichiers temporaires. Exécuter winnt.exe (pour 95 ou moins), winnt32.exe pour les autres. Installation sans interaction de l'utilisateur : winnt32.exe/u

Mise à niveau :

- Win NT Server4.0 et SP5
- Win 2000 server et advanced server

Conformité matérielle :

- Sur le cd : Chek system compatibility
- Ligne de commande : winnt.exe/checkupgradeonly

Si ancien système contient domaines et forêts, il faut les préparer avant de mettre à jour :

- adprep/forestprep
- adprep/domainprep

IIS : sécurité est maximale par défaut

### **Stockage dynamique**

- Volume : portion de disque vue comme partie distincte
- Volume simple : créée à partir d'un espace non alloué sur HD
- Spanned volume : regroupement de différents espace non alloués en une seule partie.
- Striped volume : agrégat de bande : remplit les différents espace par blocs de 64Ko

Conversion en dynamique : gestion de disque, convertir en disque dynamique, rebooter 2x

Gestion de tolérance de panne : uniquement en dynamique, intégrée logiciellement

## **Module 1 : intro à AD**

### **Structure logique d'AD**

- Forêts : consistent en une ou plusieurs arborescences
- Arborescences de domaines : domaines regroupés en structure hiérarchique
- Domaines : ensemble d'objets qui partagent base de données d'annuaire commune
- OU : objets conteneurs qui permettent d'organiser d'autres objets
- Objets : pc, imprimantes, ... définis par des attributs

### **Structure physique d'AD**

- DC : s'occupent du stockage et de la réplication
- Sites AD : groupes d'ordinateurs reliés par connexions rapides.
- Partitions AD :
  - o de domaines : contient les répliquas des objets
  - o de config : contient la topologie de la forêt

- de schéma : contient le schéma étendu de la forêt
- d'applications facultatives

### Maîtres d'opération

- réplification à maître unique : pour éviter conflits de réplification
- rôles de maître d'opération :
  - rôle étendu sur un domaine : se comporte comme un PDC
  - maître d'identificateurs relatifs (RID) : alloue des identificateurs aux DC
  - maître d'infrastructure : met à jour les objets déplacés d'un domaine vers un autre

### Schéma

Contient une description de tous les objets d'une forêt (classes d'objets et attributs)

### Catalogue global

Contient les attributs le plus souvent utilisés dans les requêtes, les autorisations d'accès et les infos d'emplacement de chaque objet.

### Serveur de catalogue global

DC qui traite les requêtes intra forêts dans le catalogue global. Le 1<sup>er</sup> DC créé est un serveur de catalogue global.

Permet de trouver des infos AD dans une forêt.

### Définitions noms uniques et noms uniques relatifs

Utilisation du protocole LDAP pour rechercher et modifier des objets.

- nom unique : définit le nom et l'emplacement de l'objet
  - CN=Laura Bertolli, OU=Sales,DC=contoso,DC=msft
- nom unique relatif : définit seulement l'emplacement de l'objet
  - OU=Sales, DC=contoso,DC=msft

### Outils MMC et lignes de commandes pour gérer AD

- utilisateurs et ordinateurs : gestion de stratégie de comptes et droits utilisateurs
- domaines et approbations : gestion approbation des domaines et forêts, modification des niveaux fonctionnels
- sites et services : gestion de la réplification
- schéma : gestion du schéma
- dsadd, dsmod, dsquery, dsmove, dsrm, dsget : gestion objets AD
- csvde : importer et exporter données AD (format séparation par virgule)
- ldifde : gestion AD provenant d'un autre service d'annuaire.

### Utilisation de scripts

Pour gérer les objets AD, étendre le schéma, modifier des attributs d'objets

### Processus d'implémentation

- création structure du domaine et forêt
- création OU
- création comptes utilisateurs et ordi
- création groupes
- création objets GPO
- création stratégie distribution logiciels

- création sites

## **Module 2 : implémentation d'une structure de forêt et de domaine AD**

### Conditions requises pour installer AD

- Win 2003
- 250 Mo en NTFS (200 pour AD et 50 pour les fichiers journaux)
- Un dossier SYSVOL
- Etre logué en admin
- Tcp/ip installé
- Un serveur DNS

### Vérifier l'installation d'AD

- dossier SYSVOL doit contenir les sous dossiers domain, staging, staging areas et sysvol
- dossier systemroot\Ntds doit contenir Ntds.dit, Edb.\* et Res\*.log
- exécuter dsget pour voir les objets par défaut d'AD

### Problèmes d'installation d'AD

- accès refusé pour créer ou ajouter un DC
  - o sol : se loguer en admin
- noms de domaines Netbios ou DNS pas uniques
  - o modifier le nom pour qu'il soit unique
- domaine ne peut pas être contacté :
  - o vérifier connexion réseau, pinger le DC, vérifier que DNS attribue les noms
- espace disque insuffisant :
  - o augmenter taille partition ou installer base de données et fichiers journaux sur partitions distinctes

### Enregistrement des ressources SRV

Enregistrements DNS dans lesquels ou sont stockés infos sur l'emplacements des ordi qui fournissent des services.

service, protocole, nomdomaine, ttl, classe, priorité, poids, port, nompcquifournitleservice  
ex. \_ldap.\_tcp.contoso.msft 600 IN SRV 0 100 389 london.contoso.msft

msdcs indique nom du sous domaine

dctype : spécifie le type de DC (DC ou serveur de catalogue global)

### Analyser les enregistrements SRV d'un DC

- console DNS : ouvrir les dossiers \_msdcs, \_sites, \_tcp et \_udp
- nslookup : dans Dos, tapez ls-t SRV (domaine)

### Augmentation des niveaux fonctionnels

- Win 2000 mixte => peut augmenter vers 2000 natif ou 2003
- Win 2000 natif => pour les domaines qui ont des 2000 et des 2003
- Win 2003 : le plus élevé
- Win 2003 préliminaire : pour les domaines qui ont des NT 4 et des 2003

### Conditions requises pour activer des nouvelles fonctionnalités

- être en 2003
- être admin
- niveau fonctionnel doit être augmenté vers 2003

Pour augmenter le niveau, Domaines et approbations

### Approbations

Elles permettent à un utilisateur d'accéder à tous les domaines approuvés.

Une relation d'approbation est représentée par un objet domaine approuvé (TDO). L'objet TDO contient les noms d'arborescences de domaines, les suffixes de nom principal, les espaces de noms de l'identificateur de sécurité (SID)

Pour créer des approbations, utilisez Domaines et approbations

Pour vérifier et révoquer un approbation :

- utiliser Domaines et approbations
- utiliser netdom :
  - o vérifier :
    - NETDOM TRUST nom\_domaine\_à\_approuver /domaine : nom\_domaine\_approuvé/verify
  - o révoquer
    - NETDOM TRUST nom\_domaine\_à\_approuver /domaine : nom\_domaine\_approuvé/remove

## **Module 3 : implémentation de la structure d'une OU**

### Création et gestion d'OU

- utilisateurs et ordinateurs
- dsadd, dsmov...
  - o dsadd ou nom\_unique\_de\_l'OU\_à\_ajouter-desc description -d Domaine -u nom\_utilisateur -p motdepasse
- ldifde (ligne de commande)
  - o dn :OU=Exemple,DC=nwtraders,DC=msft  
changetype :add  
objectclass :organizationalUnit
- scripts Windows
  - o Set objDom=GetObject(« LDAP://dc=nwtraders,dc=msft »)  
Set objOU=objDom.create(« OrganizationalUnit », « ou=NouvelleOU »)  
objOU.SetInfo

La 1<sup>ère</sup> ligne se connecte au domaine, la 2<sup>ème</sup> crée la nouvelle OU et la 3<sup>ème</sup> enregistre le script dans AD.

### Déléguer le contrôle administratif

Utiliser utilisateurs et ordinateurs

## **Module 4 : implémentation de comptes utilisateurs, groupes et ordi**

### Types de groupes

- groupe de distribution : que pour les applications de messagerie (ex. Exchange)
- groupe de sécurité : donnent des droits aux utilisateurs et ordinateurs

### Appartenance au groupe local de domaine

- appartenance :
  - o en 2000 mixte : peuvent contenir comptes et groupes globaux de tous les domaines
  - o en 2000 natif : peuvent contenir comptes utilisateurs, groupes globaux et universels de tous les domaines
- peut être membre de :
  - o en 2000 mixte : ne peut pas être membre de n'importe quel groupe
  - o en 2000 natif : peut être membre de groupes locaux de domaines du même domaine
- étendue :
  - o visible uniquement dans son propre domaine
- autorisations :
  - o on peut donner des autorisations pour le domaine dans lequel il se trouve

### Appartenance au groupe global de domaine

- appartenance :
  - o en 2000 mixte : peut contenir des comptes utilisateurs du même domaine
  - o en 2000 natif et 2003 : peut contenir des utilisateurs et groupes globaux du même domaine
- peut être membre de :
  - o en 2000 mixte : peut être membre des groupes locaux de domaine dans tous les groupes
  - o en 2000 natif et 2003 : peut être membre de groupes universels et locaux de domaine dans tous les domaines
- étendue :
  - o visible dans tous les domaines
- autorisations :
  - o on peut donner des autorisations pour tous les domaines approuvés

### Appartenance au groupe universel

- appartenance :
  - o en 2000 mixte : on ne peut pas créer de groupes universels
  - o en 2000 natif et 2003 : peut contenir des comptes, groupes globaux et universels de tous les domaines
- peut être membre de :
  - o en 2000 mixte : ne s'applique pas
  - o en 2000 natif : peut être membre de groupes locaux de domaines et universels dans tous les domaines
- étendue :
  - o visible dans tous les domaines
- autorisations :
  - o on peut donner des autorisations pour tous les domaines

L'UPN est le nom d'ouverture de session, il doit être unique dans son conteneur et dans la forêt, mais le nom d'utilisateur doit seulement être unique dans la forêt.

### Stratégie de mot de passe

- historique avec min 24 mots de passe retenus
- durée de vie max du mot de passe de 42 jours
- durée de vie min du mot de passe de 2 jours
- longueur max du mot de passe de 8 caractères
- mot de passe doit respecter des exigences de sécurité

### **Module 5 : implémentation d'une stratégie de groupe**

Les données concernant les objets GPO se trouvent dans le dossier SYSVOL et dans AD. L'option appliquer (ne pas passer outre) force tous les conteneurs enfants à hériter de la stratégie du parent.

### Problèmes à l'implémentation de GPO

- vous ne pouvez pas ouvrir un GPO :
  - o obtenir les autorisations lire et écrire
- Impossible de modifier un GPO :
  - o S'assurer que le DNS fonctionne

### **Module 6 : déploiement et gestion des logiciels à l'aide d'une stratégie de groupe**

#### Déploiement de logiciels

- créer un point de distribution (dossier partagé sur le serveur)
- utiliser un GPO pour le déploiement
- modifier les propriétés de déploiement en fonction des besoins

Affecter un logiciel permet à l'utilisateur de disposer du logiciel en permanence.

Publier un logiciel permet rendre le logiciel disponible pour que l'utilisateur puisse l'installer.

#### Types de mise à niveau de logiciels

- mise à niveau obligatoire : l'utilisateur ne peut exploiter que la mise à niveau
- mise à niveau facultative : les utilisateurs ont le choix de l'installer ou pas
- mise à niveau sélective : on choisit les utilisateurs qui doivent se mettre à niveau

#### Suppression de logiciels

- suppression forcée : le logiciel est automatiquement supprimé d'un ordi
- suppression facultative : le logiciel n'est pas supprimé de l'ordi et on peut pas mettre à jour

#### Problèmes de déploiement de logiciels

- l'application a été publiée mais pas affectée (ou l'inverse), aucun GPO n'a été appliqué
  - o utiliser RSoP pour déterminer l'objet appliqué et modifier le GPO
- le point de distribution n'est pas accessible :
  - o installer Windows Installer manuellement et modifier les autorisations
- les applications précédemment installées empêchent toute nouvelle installation :
  - o créer le fichier journal Windows Installer et supprimer les composants de registre