Active Directory: plan

- Présentation générale
- Gestion des utilisateurs dans un domaine
- Planification des groupes
- Délégation de tâches, console mmc

Active Directory

- Gère un domaine windows
- Service d'annuaire
- Base d'annuaire distribuée des ressources réseau : comptes utilisateurs, groupes, ordinateurs, imprimantes, dossiers partagés, ...
- Administration centralisée
- Tolérance de panne
- Protocoles standard => interopérabilité (clients)
- Produit propriétaire => pas de serveur AD non microsoft

Active Directory

- Gère un domaine windows
- Service d'annuaire
- Base d'annuaire distribuée des ressources réseau : comptes utilisateurs, groupes, ordinateurs, imprimantes, dossiers partagés, ...
- Administration centralisée
- Tolérance de panne
- Protocoles standard => interopérabilité (clients)
- Produit propriétaire => pas de serveur AD non microsoft

Structure logique

- Nom de domaine AD => nom de domaine DNS (mais ce sont deux notions distinctes !)
- Domaines
- Arborescences: domaines de noms hiérarchiquement liés
- Forêts: ensemble d'arborescences
- Unités d'organisation : organisation logique à l'intérieur d'un domaine

Domaine

- Limite de sécurité : stratégie de sécurité d'un domaine
- Unité d'administration
- Unité de réplication: réplication entre les CD du domaine
- Mode ou niveau fonctionnel d'un domaine: (dépend de l'OS des contrôleurs de domaine)
  - w2K: mixte ou natif
  - w2k3: w2k mixte, w2k natif, w2k3 version préliminaire (cas d'une màj depuis NT), w2k3

Niveau fonctionnel des domaines

Fonctionnalité	w2k mixte	w2k natif	w2k3
groupes universels	Non	Oui	Oui
groupes locaux de domaines	Non	Oui	Oui
contrôleur de domaine NT	Oui	Non	Non
contrôleur de domaine w2k	Oui	Oui	
renommage des contrôleurs de domaines	Non	Non	Oui
renommage des domaines	Non	Non	Oui

Unités d'organisations

- Organisation logique à l'intérieur d'un domaine
- Contient des objet active directory
- Permet
  - De déléguer des pouvoirs
  - De simplifier la sécurité
  - D'appliquer une stratégie à des ordinateurs ou utilisateurs
- Rend obsolète la construction usuelle domaine de compte/domaine de ressources NT4

Planification

- Pb: quelle structure logique adopter ?
  - Pb complexe, une grosse littérature
  - la politique de sécurité : au niveau d'un domaine
  - trafic de réplication non négligeable au sein d'un domaine
- typiquement:
  - utiliser la structure administrative ou géographique de l'entreprise
  - faire en sorte que les domaines et les UO de haut niveau ne changent pas
  - le plus simple (et le plus conseillé si c'est possible) : n'avoir qu'un seul domaine

Topologie Active Directory

- Site: regroupement de réseau reliés par des liaisons rapides
- entre Sites: liaisons de sites (supposées lentes ou coûteuses)
- but: minimiser et contrôler le trafic de réplication entre contrôleurs d'un même domaine appartenant à des sites différents
- ràf: à compléter

AD: dossiers et fichiers

- base de données, fichiers de journalisation:
  - sur une partition NTFS
  - par défaut dans %SystemRoot%\NTDS
    - NTDS.dit: magasin de données (base de données de l'annuaire)

AD: dossiers et fichiers

- SYSVOL:
  - AD crée le partage SYSVOL correspondant au dossier %SystemRoot\Sysvol\sysvol
  - contient
    - les pargages NETLOGON
    - les stratégies de groupes
    - les scripts d'ouverture/fermeture de session
    - ...

DNS et AD

- élément critique pour le bon fonctionnement d'active directory:
  - les noms de domaines sont des noms dns
  - les contrôleurs de domaines sont localisés via une requête DNS
- le serveur dns utilisé par les machines du domaine doit connaître le domaine et avoir les entrées SRV permettant la localisation des contrôleurs de domaines

DNS: mauvaise configuration

- symptomes d'une mauvaise configuration d'un poste client
  - l'intégration dans le domaine n'est pas possible en donnant le nom dns du domaine (ex.: test.shayol.org)
  - l'intégration dans le domaine reste possible en donnant le nom plat compatible Windows NT (ex.: TEST) mais c'est une mauvaise solution
- Solution: configurer le poste client (propriétés TCP/IP) pour utiliser un dns connaissant le domaine

DNS windows 2K+

- windows 2k ou 2k3 server peuvent être serveur dns
- les zones peuvent être stockées:
  - à l'ancienne sous forme de fichier séparés
  - sur un contrôleur de domaine, intégrée à Active Directory
    - sous W2K: les données du DNS sont répliquées et réparties sur tous les controleurs de domaines (même ceux qui ne sont pas serveur DNS)
    - sous W2K3: les données du DNS sont répliquées et réparties sur tous les controleurs de domaines qui sont aussi serveurs DNS

DNS : intégration des zones à AD

- intérêt:
  - tolérance de panne (répliqué avec les données AD, ...)
  - performances (bénéficie du moteur d'AD, de sa réplication, ...)
- défauts:
  - format non standard
- à noter: des dns avec des zones intégrés à AD continuent à respecter les RFC et peuvent interopérer avec des dns secondaire non AD ?

DNS et AD

- 3 solutions :
  - laisser w2k3 installer le dns lors de l'installation d'AD
  - avoir un dns supportant les mises à jour dynamiques
  - configurer le dns à la main à l'aide des fichiers %Systemroot\System32\config\netlogon.dns qui reprennent les lignes à copier dans le fichier de configuration de bind
- utiliser le dns microsoft est la solution la plus simple car AD saura configurer lui-même le dns.
- les mises à jour dynamiques sécurisées ne sont disponibles que si la zone est intégrée à AD

DNS

- zones créées par AD: voir demo installation AD

DNS: planification

- élément vital pour AD
- au moins un DNS par site
  - éviter de contacter un DNS distant pour localiser un CD local
  - survivre à une coupure du réseau distant
  - bonne pratique: un contrôleur de domaine du site doit être serveur DNS
- utiliser des zones intégrées à AD
- au moins 2 DNS configurés sur chaque machine membres du domaine

AD-DEMO: installation d'Active Directory

- Installation d'Active Directory sur une machine virtuelle windows 2003 server :
  - Domaine suzdal.shayol.org
  - Pas de dns présent => à installer
  - Premier domaine de l'entreprise (nouveau domaine dans une nouvelle arborescence dans une nouvelle forêt)
  - Pas de contrôleur NT => Mode natif
  - élever le niveau fonctionnel du domaine après le redémarrage

Les objets Active Directory

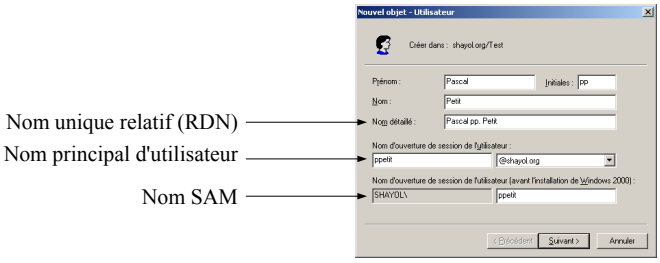
- Instances d'une classe définie dans le Schéma :
  - Comptes utilisateurs,
  - ordinateurs,
  - imprimantes,
  - groupes,
  - dossiers partagés publiés
- Objets conteneur, objet feuille

Nom des objets

CN= « Pascal PP Petit », OU=test, DC=shayol, DC=org

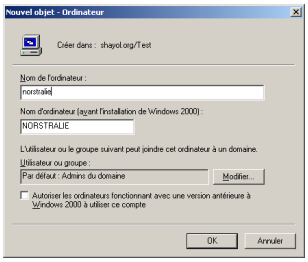
- Nom unique
- Nom unique relatif
- Identificateur global (GUID)
- Format des noms active directory
- Nom principal d'utilisateur
- Identifiant de sécurité :SID = RID + ID domaine

Nom des objets (2)



Compte d'ordinateur

- Nécessaire pour ordinateur WinNT ou W2K+
- Création depuis l'ordinateur lors de l'inclusion dans le domaine
- Création à l'avance
  - Création du compte dans AD à l'avance
  - Inclusion de l'ordinateur par un utilisateur déclaré à la création du compte



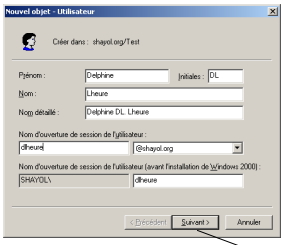
Compte utilisateur

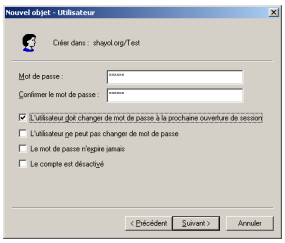
- Compte d'utilisateur local :
  - Stocké dans la base SAM de l'ordinateur
  - Donne accès aux ressources locales
  - Permet l'ouverture de session sur l'ordinateur
- Compte d'utilisateur du domaine :
  - Stocké au niveau du domaine dans Active Directory
  - Donne accès aux ressources réseau
  - Permet d'ouvrir des sessions sur les ordinateurs du domaine

Comptes prédéfinis dans un domaine

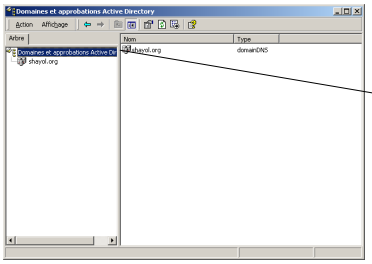
- Computers
- Users
- Comptes:
  - Administrateur
  - Invité
  - IUSR_NomOrdinateur et IWAM_NomOrdinateur

Création des comptes sur un domaine

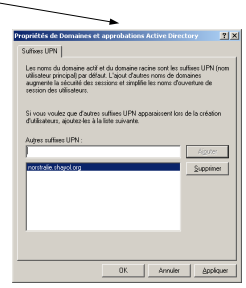




Création d'un suffixe UPN



Propriétés



Propriétés des comptes d'utilisateurs

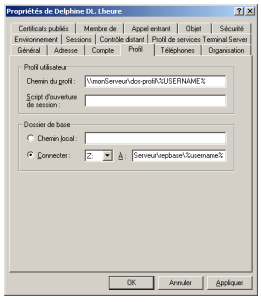
- Options de mot de passe
- Délégation: interdire la délégation, autoriser la délégation des tâches à d'autres utilisateurs
- Chiffrement de mot de passe: réversible, pas de pré authentification kherberos, chiffrement DES
- Expiration de compte
- Restrictions horaires
- Restriction d'accès (se connecter à)

AD-DEMO

- Intégration de deux stations de travail dans le domaine
- Création de compes utilisateur sur le domaine,L'utilisateur travaille sur sa station de travail (pas de répertoire de base réseau, pas de profil itinérant)
- Deux stations de travail : tout ce qui est fait sur l'une n'est pas automatiquement accessible depuis l'autre.
- Ouverture de session en utilisant le nom principal d'utilisateur

Profils utilisateurs, répertoire de base

- Profils locaux
- Profils itinérants
- Profils itinérant obligatoire
- Répertoire de base



AD-DEMO: profil itinérant

- Mettre le répertoire de base sur le serveur et constater qu'il est accessible depuis les deux stations mais que le profil reste propre à chaque station (fond d'écran par ex.)
- Définir un profil itinérant et constater que le profil est bien le même sur les deux stations et que les changements sont pris en compte sur les deux stations

Création de masse

- Par copie d'un compte désactivé
- Via addusers, csvde, ldifde
- Net account
- Net users
- Net group
- Net localgroup

Gestion des comptes

- Réinitialiation du mot de passe
- Désactivation
- Suppression
- déverrouillage
- déplacement

Groupes: présentation

- Un groupe est un ensemble d'utilisateurs
- Les membres d'un groupe bénéficient des droits attribués au groupe
- Un utilisateur peut être dans plusieurs groupes
- Les groupes peuvent contenir d'autres groupes
- Les groupes simplifient l'administration
- Jusqu'à 5000 membres
- Groupes de distribution et groupes de sécurité

Groupes: étendue de groupes

- Groupes locaux sur un ordinateur autonome
- Groupes locaux de domaine
- Groupes globaux
- Groupes universels
- Restriction dans un domaine en mode mixte

Groupes locaux de domaine (LD)

- Peut contenir
  - des utilisateurs, des groupes globaux et des groupes universels de tous les domaines de la forêt;
  - des groupes de domaine locaux de son domaine
- Utilisable seulement dans son domaine;
- Peut être membre de DL de son domaine;
- On peut l'utiliser pour affecter droits et permissions
- Membres non copiés dans le catalogue global.

Groupes globaux

- Peut contenir des utilisateurs, des groupes globaux du **même** domaine;
- Peut être membre de groupes (DL, G, U) de tout domaine de la forêt
- On **ne** peut **pas** l'utiliser pour affecter droits et permissions
- Membres non copiés dans le catalogue global.

Groupes universels

- Peut contenir des utilisateurs, des groupes globaux et des groupes universels de **tous** les domaines de la forêt;
- Peut être membre de DL de tout domaine et de groupes universels
- On peut l'utiliser pour affecter droits et permissions
- Ses membres copiés dans le catalogue global.

Groupes prédéfinis: workgroup

Nom	Objet	appartenance initiale
administrateurs	réalisent les tâches d'administration	administrateur
Opérateur de sauvegarde	ouvrir une session, sauvegarder/restaurer des données	Vide
Invités	aucun droit sauf ajout explicite	invité
Utilisateurs avec pouvoir	installer des programmes, gérer les comptes locaux, les partages, créer des groupes, gérer les groupes utilisateur, utilisateurs avec pouvoir et invités. Ne peuvent pas visualiser les fichiers des autres utilisateurs.	
utilisateurs	ouvrir une session, accèder au réseau, enregistrer des documents, arrêter l'ordinateur mais pas installer des programme, ni modifier la configuration de la machine	
opérateur d'impression	existe sur un serveur. gére les imprimantes et les files d'attentes	Vide
Utilisateur du bureau à distance	autorisés à se connecter via bureau à distance	Vide

Groupes prédéfinis : domaines

- 4 types de groupes prédéfinis dans un domaine :
  - groupes locaux:
  - groupes locaux de domaine:
    - groupes locaux des contrôleurs de domaine
    - pour effectuer certaines tâches sur les contrôleurs de domaine ou sur Active Directory
    - on y ajoute des utilisateurs ou des groupes globaux qui héritent alors des permissions
  - groupes globaux prédéfinis:
    - obtiennent leurs privilèges en les ajoutant dans des groupes locaux
    - contiennent des utilisateurs par défaut
  - groupes système

groupes locaux prédéfinis

- sur des serveurs membres ou des stations du domaine
- identiques à ceux de l'environnement workgroup
- ajout à l'appartenance initiale:
  - administrateurs du domaine au groupe administrateurs
  - invités du domaine au groupe invités
  - utilisateurs du domaine au groupe utilisateurs

Gpes prédéfinis: locaux de domaine

Nom	Objet	appartenance initiale
administrateurs	réalisent les tâches d'administration sur les contrôleurs	administrateur
dnsAdmins	créé lors de l'installation du serveur dns. accès administratif au serveur dns.	Vide
duplicateurs	utiliser pour implanter la réplication de fichiers. ne pas y ajouter de membres manuellement	
Invités	aucun droit sauf ajout explicite	invité
opérateur d'impression	gère les imprimantes et les files d'attentes	Vide
Opérateur de comptes	création, suppression, modification des groupes et comptes utilisateurs sur un contrôleur (sauf groupes administrateurs & Co, opérateurs, ...). Ils peuvent ouvrir une session sur le contrôleur de domaine et l'arrêter.	

Quelques groupes locaux de domaine prédéfinis (contrôleur de domaine)

Gpes prédéfinis: locaux de domaine

Nom	Objet	appartenance initiale
Opérateur de sauvegarde	peuvent contourner les sécurités de fichiers pour effectuer des sauvegardes sur un contrôleur de domaine	Vide
Opérateur de serveur	partager des fichiers, sauvegarder le contrôleur de domaine, ... mais pas les options de sécurité.	
Utilisateur du bureau à distance	autorisés à se connecter via bureau à distance	Vide
utilisateurs	ouvrir une session, accéder au réseau, enregistrer des documents, arrêter l'ordinateur mais pas installer des programme, ni modifier la configuration de la machine	utilisateurs du domaine

Quelques groupes locaux de domaine prédéfinis (contrôleur de domaine)

Gpes prédéfinis: globaux

Nom	Objet	appartenance initiale
DnsUpdateProxy	créé lors de l'installation du dns: clients DNS qui peuvent mettre à jour le DNS dynamiquement au nom d'autres clients. (trad.: serveur DHCP)	Vide
administrateurs du domaine	automatiquement membre du groupe local de domaine administrateurs et des groupes Administrateurs des stations du domaine	Administrateur
Ordinateurs du domaine	tous les postes (CD inclus) en sont membres	
invités du domaine	membre du groupe local Invités.	Invité
utilisateurs du domaine	tous les utilisateurs du domaine en sont membres.	util. du domaine
administrateurs de l'entreprise	membre du groupe administrateurs de tous les contrôleurs du domaine	
propriétaires de la GPO du domaine	créer/modifier la stratégie de groupe du domaine	Administrateur
contrôleurs du domaine	tous les contrôleurs du domaine y sont	

Groupes système intégrés (identités spéciales)

- groupe dynamiques gérés par le système
- l'appartenance est décidée en fonction des actions des membres
- n'apparaissent pas dans les consoles de gestion des groupes

Groupes systèmes intégrés: exemples

- interactif: l'utilisateur est connecté localement en ayant utilisé le clavier de l'ordinateur
- propriétaire-créateur: ràf
- Réseau: tous les utilisateurs ayant ouvert une session sur des ordinateurs du réseau et accédant à une ressource de l'ordinateur local
- utilisateur authentifiés: tous les utilisateurs ayant des compte d'utilisateurs reconnus par l'ordinateur ou le domaine
- tout le monde: utilisateurs authentifiés + invité + utilisateurs anonymes (ràf)

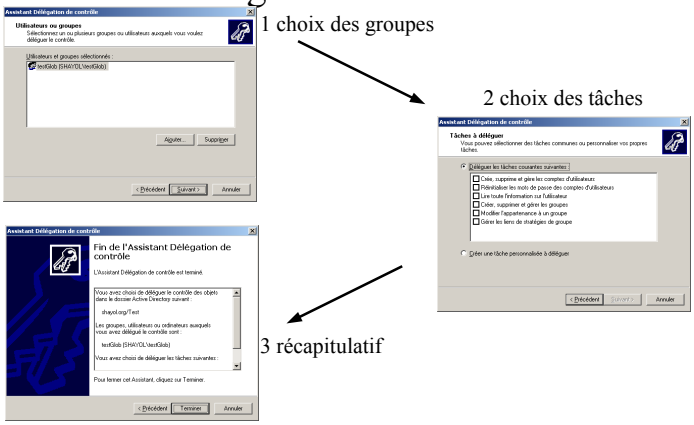
AD-DEMO: gestion des groupes dans un domaine

- Création d'un groupe Gtest sur le domaine (groupe local de domaine)
- Ajout de l'utilisateur test1 à Gtest
- Sur une station de travail, créer un dossier RepTest et donner le droit CT à Gtest et lecture au groupe « Tout le monde » sur RepTest
- Vérifier les accès
- Utiliser Gtest pour sélectionner les utilisateurs qui peuvent changer l'heure des stations de travail

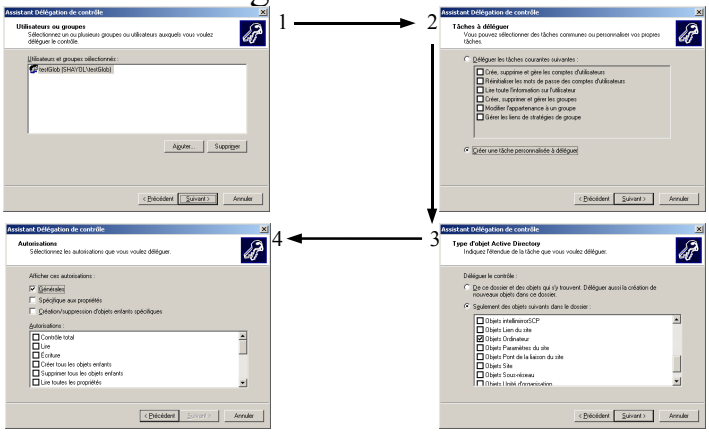
Délégation de tâche

- Délégation de contrôle sur le domaine ou sur une unité d'organisation : déléguer une partie des tâches d'administration sur certains objets à certaines personnes
- Création de console MMC personnalisées,
- Administration à distance

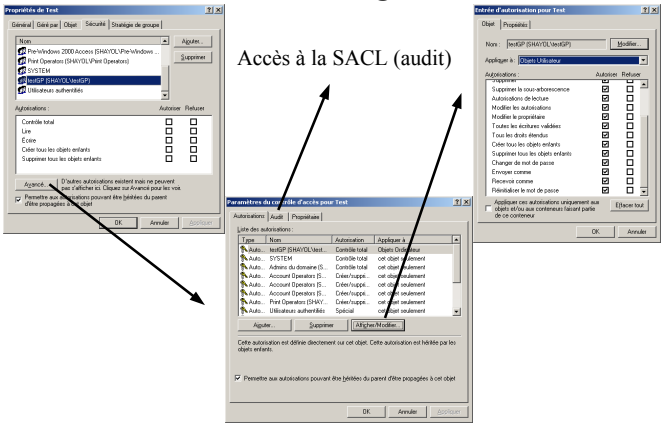
Délégation de contrôle



Délégation de contrôle



Modification de délégation, Audit



AD-DEMO: delegation de contrôle

- Création d'une unité d'organisation UOtest
- On y met les utilisateurs test2, test3
- On délègue la remise à zéro des mots de passe de l'UO à l'utilisateur test1
- Remarque: travailler avec un groupe plutôt qu'avec un utilisateur test1.

Outils d'administration

- utilisables à distance
- sur des ordinateur où elles ne sont pas par défaut : via l'installation de l'adminpak.msi (i386 du CD W2K3 server)
  - s'installe sur les postes w2k3server ou Wxp sp1+
  - les outils d'administration d'un domaine s'utilisent depuis un poste du domaine

Personnalisation des consoles MMC

- les consoles mmc sont personnalisables
  - ajout de composants enfichables à une console mmc existante ou vide
  - ouverture en un point précis de l'arborescence
  - ajout de bouton pour des tâches particulières
- mode opératoire: cf TD

Adminpak: 3 consoles d'accueil supplémentaires

- gestion active directory (ADMgmt.msc):
  - utilisateurs et ordinateurs AD, domaines et approbation AD, Sites et services AD, DNS
- gestion d'adresse IP:
  - dhcp, dns, wins
- gestion de clef publique:
  - autorité de certification, modèles de certificats, certificats pour l'utilisateur actuel, certificats pour l'ordinateur actuel

Outils d'administration : compatibilité w2k/w2k3

- problèmes de compatibilité:
  - les outils d'administration w2k3 sont prévus pour être utilisés depuis w2k3 ou WinXP (mais pas w2K) pour administratrer des serveurs w2k3 (et pas w2k pour certains outils)
  - les outils d'administration w2k sont prévus pour être utilisés depuis w2k pour administrer des serveurs w2k (mais pas w2k3 pour certains outils)