

Module 1 : intro à l'infrastructure d'AD

AD fournit les fonctions suivantes :

- centralisation du contrôle des ressources du réseau
- centralisation et décentralisation de la gestion des ressources : les admins font tout eux-mêmes partout ou délèguent des fonctions à d'autres admins à des autres endroits
- stockage des objets de manière sécurisée dans une structure logique.
- Optimisation du trafic réseau.

Structure logique d'AD inclut les composants suivants :

- les objets : regroupée dans une classe d'objets qui est définie par une liste d'attributs qui définissent les valeurs possibles pour un objet.
- Les OU : objets conteneurs qui permettent d'organiser d'autres objets.
- Les domaines : ensemble d'objets définis administrativement qui partagent une base de donnée d'annuaire commune.

Les domaines ont 3 fonctions :

- o limite d'administration pour les objets
- o méthode de gestion de la sécurité pour les ressources partagées
- o unité de réplication pour les objets
- les arborescences de domaines : domaines regroupés en structure hiérarchique
- les forêts : consistent en une ou plusieurs arborescences. Par défaut, les infos d'AD ne sont partagées que dans la forêt pour une question de sécurité

Structure physique d'AD comprend :

- les contrôleurs de domaines. Chaque contrôleur de domaine s'occupe du stockage et de la réplication
- les sites AD : groupes d'ordinateurs reliés par des connexions rapides. Créer des sites est utile pour optimiser la BP du réseau
- les partitions AD :
 - de domaines : contient les répliquas des objets du domaine
 - de configuration : contient la topologie de la forêt
 - de schéma : contient le schéma étendu au niveau de la forêt
 - d'applications facultatives

Définitions des maîtres d'opération

- réplication à maître unique : utilisée pour éviter les conflits de réplication. Elle désigne le seul contrôleur de domaine sur lequel on peut faire des modifications
- rôles de maître d'opération :
 - o rôles étendus au niveau d'un domaine : se comporte comme un PDC pour la prise en charge d'un contrôleur secondaire (BDC)
 - o le maître des identificateurs relatifs (maître RID) : il alloue des blocs d'identificateurs à chaque contrôleur de domaine.
 - o le maître d'infrastructure : met à jour les objets déplacés d'un domaine vers un autre

Schéma

Il contient une définition (description) de tous les objets d'une forêt. Il regroupe 2 types de définitions :

- les classes d'objets : décrivent les objets qu'ils est possible de créer

- les attributs : définis séparément des classes d'objets.

Le catalogue global contient :

- les attributs le plus souvent utilisés dans les requêtes
- les infos requises pour déterminer l'emplacement de tous les objets de l'annuaire
- un sous-ensemble d'attributs par défaut pour chaque type d'objet
- les autorisations d'accès pour chaque objet

Serveur de catalogue global

C'est un contrôleur de domaine qui traite les requêtes intra forêts dans le catalogue global. Le 1^{er} contrôleur de domaine créé dans AD est un serveur de catalogue global.

Le catalogue global permet de :

- trouver des infos AD dans une forêt
- utiliser des infos d'appartenance au groupe universel pour se connecter au réseau

Définition d'un nom unique et d'un nom unique relatif

Utilisation du protocole LDAP pour rechercher ou modifier des objets dans l'AD

- nom unique d'un objet : indique le domaine dans lequel se trouve l'objet et le chemin complet pour y accéder.
 - o Ex. CN=Laura Bertolli,OU=Sales,DC=contoso,DC=msft
 - CN : nom usuel de l'objet
 - OU : OU qui contient l'objet
 - DC (domain component) : composant de domaine (par ex. penchu.com)
- Nom unique relatif d'un objet : identifie l'objet de manière unique dans son conteneur
 - o Ex. OU = Sales, DC = contoso, DC = msft

Prise en charge de la gestion centralisée par AD : fonctionnalités

- info concernant tous les objets et les attributs.
- On peut interroger AD grâce au protocole LDAP
- On peut grouper des objets aux exigences similaires dans des OU
- On peut spécifier les stratégies de groupe pour un domaine, un site ou une OU.

Prise en charge de la gestion décentralisée par AD : fonctionnalités

On peut déléguer l'affectation des autorisations pour :

- des OU spécifiques à différents groupes de domaine local (ex. contrôle total pour l'OU Sales)
- modifier des attributs spécifique d'un objet dans une ou plusieurs OU

Outils et composants logiciels enfichables d'administration d'AD

Composant logiciel	Description
Utilisateurs et ordinateurs AD	Gestion de stratégies de compte et droits d'utilisateurs
Domaines et approbations AD	Gestion des approbations des domaines et forêts, modifications des niveaux fonctionnels des domaines et forêts
Sites et services AD	Gestion de la réplication de données d'annuaire
Schéma AD	Gestion du schéma

Outils	description
dsadd	Ajouter des objets dans AD
Dsmmod	Modifier des objets dans AD
Dsquery	Exécuter des requêtes dans AD
Dsmove	Déplacer un objet unique à l'intérieur d'un domaine ou le renommer sans le déplacer
Dsrmdir	Supprimer un objet dans AD
Dsget	Affiche les attributs d'un objet
Csvde	Importer et exporter des données AD dans un format avec séparation par virgule
Ldifde	Ajouter, modifier, supprimer des objets AD, ajouter des objets dans AD provenant d'un autre service d'annuaire

Environnement d'exécution de scripts

On peut utiliser des scripts utilisant ADSI pour :

- extraire des informations d'un objet AD
- ajouter des objets dans AD
- modifier les attributs des objets
- supprimer des objets dans AD
- étendre le schéma AD

Implémentation d'AD

Pendant le processus d'implémentation d'AD, les admins

- créent la structure du domaine et de la forêt et déploient les serveurs
- créent la structure de l'OU
- créent les comptes utilisateurs et ordinateurs
- créent des groupes de sécurité et de distribution
- créent des objets de stratégie de groupe
- créent les stratégies de distribution de logiciels
- créent des sites

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

Conditions requises pour installer AD

- un ordinateur fonctionnant sous Win 2003
- 250Mo de libre en NTFS
 - o 200 Mo pour l'installation d'AD
 - o 50 Mo pour les fichiers journaux de transactions de la base de données AD
- un dossier SYSVOL dans la partition NTFS
- des privilèges administratifs pour la création d'un domaine
- TCP/IP installé
- un serveur DNS

Processus d'installation d'AD

- démarrage du protocole d'authentification Kerberos 5
- définition de la stratégie de sécurité locale (LSA)
- créations des partitions AD : 5 partitions sont créées sur le 1^{er} contrôleur de domaine :
 - o partition d'annuaire de schéma
 - o partition d'annuaire de configuration
 - o partition d'annuaire de domaine
 - o zone DNS de la forêt
 - o partition de la zone de domaine DNS
- réplication des partitions sur chaque contrôleur de domaine de la forêt
- création de la base de données AD et des fichiers journaux (systemroot\Ntds)
- création du domaine racine de la forêt
- attribution des rôles de maîtres d'opérations au contrôleur de domaine
- création du dossier volume système partagé
 - o dossier SYSVOL : contient les infos sur la stratégie de groupe
 - o dossier Net Logon : contient les scripts de connexion des ordinateurs qui ne sont pas sous Win2003
- configuration de l'appartenance du contrôleur de domaine sur un site
- activation de la sécurité sur les services d'annuaire et sur les dossiers de réplication de fichier
- application du mot de passe pour le compte administrateur

Vérifier l'installation d'AD

- vérification de la création de la structure de dossier SYSVOL et des dossiers partagés
Aller dans le dossier SYSVOL : il doit contenir les sous dossiers domain, staging, staging areas et sysvol.
- vérification de la création de la base de données et des fichiers journaux
Aller dans le dossier systemroot\Ntds : il doit contenir les fichiers Ntds.dit, Edb.* et Res*.log
- vérification de la création de la structure d'AD par défaut
Exécuter dsget pour voir les objets par défaut d'AD

Résoudre les problèmes liés à l'installation d'AD

Problème	Solution
Accès refusé lors de l'installation ou de l'ajout d'un contrôleur de domaine	Fermer la session et rouvrir en tant qu'admin
Les noms de domaines Netbios ou DNS ne sont pas uniques	Modifier le nom pour qu'il soit unique
Le domaine ne peut pas être contacté	Vérifier la connexion réseau, faire un ping vers le contrôleur de domaine. Vérifier que le système DNS attribue bien les noms (taper le nom pleinement qualifié FQDN du contrôleur de domaine dans dos)
Espace disque insuffisant	Augmenter la taille de la partition ou installer la base de données et les fichiers journaux sur des partitions distinctes.

Analyse du système DNS intégré à AD

Espaces de noms DNS et AD

Un nom de domaine DNS (suffixe DNS) et le domaine AD auquel l'ordinateur appartient ont le même nom.

Les clients recherchent les contrôleurs de domaine et les services grâce aux enregistrements de ressources A et aux enregistrements SRV.

L'enregistrement de ressources A contient le nom FQDN et l'adresse IP du contrôleur de domaine.

L'enregistrement SRV contient le nom FQDN du contrôleur de domaine et le nom du service que fournit le contrôleur de domaine.

Définition des zones intégrées à Active Directory.

On peut intégrer des zones DNS dans une base de données AD. Une zone est une partie de l'espace de noms de domaine possédant un groupement logique d'enregistrements de ressources.

- Zones intégrées à AD :

Ce sont des zones DNS principales stockées en tant qu'objets dans la base de données AD.

- Avantages des zones intégrées à AD

- *réplication multi maître.* La zone peut être mise à jour par les serveurs DNS fonctionnant sur un contrôleur de domaine pour le domaine.
- *Mises à jour dynamiques sécurisées.* Les mises à jour qui utilisent le protocole de mise à jour dynamique ne peuvent provenir que des ordinateurs autorisés.
- *Transferts de zone standard vers d'autres serveurs DNS.* Méthode requise pour répliquer des zones vers des serveurs DNS dans d'autres domaines.

Définition des enregistrements de ressources SRV.

Ce sont des enregistrements DNS dans lesquels AD stocke les informations relatives à l'emplacement des ordinateurs qui fournissent ces services.

Ils établissent un lien entre un service et le nom d'ordinateur qui offre le service.

Ils peuvent contenir des informations permettant aux clients de localiser un contrôleur de domaine dans un domaine ou une forêt spécifique.

Format des enregistrements SRV

`_Service._Protocole.Nom Ttl Classe SRV Priorité Poids Port Cible`

Champ	Description
_Service	nom du service, (LDAP, Kerberos,...) fourni par le serveur qui enregistre cet enregistrement SRV.
_Protocole	Spécifie le type de protocole de transport (TCP, UDP,...)
Nom	Spécifie le nom du domaine auquel fait référence l'enregistrement de ressources.
Ttl	Spécifie la durée de vie (TTL, Time To Live). Durée pendant laquelle l'enregistrement est considéré valide.
Classe	Spécifie la valeur de la classe de l'enregistrement de ressources DNS
Priorité	priorité du serveur. Les clients tentent de contacter l'hôte dont la priorité est la plus faible.
Poids	mécanisme d'équilibre de charge que les clients utilisent lors de la sélection d'un hôte cible.
Port	port sur lequel le serveur écoute ce service.
Cible	nom FQDN (nom de domaine complet) de l'ordinateur qui fournit le service.

Exemple :

`_ldap._tcp.contoso.msft 600 IN SRV 0 100 389 London.contoso.msft`

=> il fournit le service LDAP grâce au protocole de transport TCP, enregistre l'enregistrement SRV dans le domaine DNS contoso.msft, a une durée de vie de 600 secondes et possède un nom FQDN de london.contoso.msft.

Enregistrements SRV enregistrés par les contrôleurs de domaine.

Pour permettre à un ordinateur de localiser un contrôleur de domaine, les contrôleurs de domaine enregistrent les enregistrements de ressource SRV en utilisant le format suivant :

`_Service._protocole.DcType._msdcs.Nom_domaine_Dns ou Nom_Forêt_Dns`

`_msdcs` indique un sous domaine dans l'espace de noms DNS, qui permet aux ordinateurs de localiser les contrôleurs de domaine ayant des fonctions dans le domaine ou la forêt.

DcType spécifie les types de rôles du serveur suivants :

- dc pour le contrôleur de domaine
- gc pour le serveur de catalogue global

La présence du sous-domaine `_msdcs` signifie que les contrôleurs de domaine enregistrent également les enregistrements de ressources SRV suivants :

`_ldap._tcp.dc._msdcs.Nom_Domaine_DNS`
`_ldap._tcp.Nom_Site._sites.dc._msdcs.Nom_Domaine_Dns`
`_ldap._tcp.gc._msdcs.Nom_Forêt_DNS`
`_ldap._tcp.Nom_Site._sites.gc._msdcs.Nom_Forêt_Dns`
`_kerberos._tcp.dc._msdcs.Nom_Domaine_Dns`
`_kerberos._tcp.Nom_Site._site.dc._msdcs.Nom_Domaine_Dns`

Comment analyser les enregistrements enregistrés par un contrôleur de domaine.

En utilisant la console DNS :

- ouvrir les dossiers `_msdcs`, `_sites`, `_tcp` et `_udp`

En utilisant l'utilitaire Nslookup :

- dans Dos, tapez `ls-t SRV (domaine)` où *domaine* est le nom du domaine

Augmentation des niveaux fonctionnels des forêts et domaines

- définition de la fonctionnalité du domaine :
 - o Windows 2000 mixte : niveau par défaut. On peut augmenter le niveau vers Windows 2000 mode natif ou vers Win 2003
 - o Windows 2000 natif : niveau fonctionnel pour les domaines qui contiennent uniquement des contrôleurs de domaines 2000 ou 2003
 - o Windows 2003 : niveau fonctionnel le plus élevé.
 - o Windows 2003 préliminaire : niveau fonctionnel qui prend en charge les contrôleurs de domaines Win Nt 4.0 et Win 2003

Définition de la fonctionnalité de forêt.

Par défaut, les forêts opèrent au niveau fonctionnel Windows 2000 mais on peut élever le niveau fonctionnel vers Windows 2003 pour activer des nouvelles fonctionnalités

Conditions requises pour activer de nouvelles fonctionnalités étendues au domaine ou de la forêt

- Tous les contrôleurs de domaine du domaine doivent exécuter Windows Server 2003
- Le niveau fonctionnel du domaine doit être élevé au niveau Windows 2003
- Vous devez être administrateur de domaine.

Comment augmenter le niveau fonctionnel.

- Ouvrez Domaines et approbations AD.
- cliquez avec le bouton droit sur le noeud du domaine dont vous souhaitez augmenter le niveau fonctionnel puis cliquez sur Augmenter le niveau fonctionnel du domaine.

Rmq : Vous devez augmenter le niveau fonctionnel de tous les domaines d'une forêt vers Windows 2000 natif ou supérieur avant de pouvoir augmenter celui de la forêt.

Création de relations d'approbation

Les approbations permettent à un utilisateur authentifié dans son propre domaine d'accéder aux ressources de tous les domaines approuvés.

Dans Windows 2003, il existe deux types d'approbations :

- Approbations transitives/non transitives.

Dans une approbation transitive, la relation d'approbation étendue à un domaine est automatiquement étendue à tous les autres domaines qui approuvent ce domaine.

Direction de l'approbation.

- Unidirectionnel entrant
- Unidirectionnel sortant
- Bidirectionnelle.

Si, dans un domaine B, vous avez configuré une approbation unidirectionnelle entrante entre le domaine B et le domaine Q, les utilisateurs du domaine B peuvent être authentifiés dans le domaine Q.

Si vous avez configuré une approbation unidirectionnelle sortante entre le domaine B et le domaine Q, les utilisateurs du domaine Q peuvent être authentifiés dans le domaine B.

Dans une approbation bidirectionnelle, les deux domaines peuvent authentifier les utilisateurs de l'autre domaine.

Types d'approbations

Windows Server 2003 prend en charge les types d'approbations suivants, dans les catégories transitives et non transitives.

Les approbations de forêt peuvent uniquement être créées entre deux forêts et ne peuvent pas être étendues à une troisième forêt.

Définition des objets du domaine approuvé.

Chaque relation d'approbation d'un domaine est représentée par un objet connu sous le nom d'objet Domaine approuvé (TDO, Trusted Domain Object).

Le TDO stocke des informations sur l'approbation.

Ces informations contiennent :

- Les noms d'arborescence de domaine
- Les suffixes du nom principal du service (SPN, Service, Principal Name)
- Les espaces de noms de l'identificateur de sécurité (SID)

Lorsqu'un poste de travail demande un service qui est introuvable dans le domaine ou dans la forêt dont il est membre, les TDO recherchent le service dans toutes les forêts approuvées.

Comment fonctionnent les approbations dans une forêt.

Lorsqu'un utilisateur tente d'accéder à une ressource d'un autre domaine, le protocole d'authentification Kerberos 5 doit déterminer si le domaine à approuver possède une relation d'approbation avec le domaine approuvé.

Le protocole Kerberos 5 utilise le TDO pour obtenir une référence au contrôleur de domaine du domaine cible. Le contrôleur de domaine cible émet un ticket de service pour le service demandé.

Comment fonctionnent les approbations entre les forêts.

Lorsqu'un utilisateur tente d'accéder aux ressources d'une forêt approuvée, AD doit préalablement rechercher les ressources. Une fois que les ressources ont été localisées, l'utilisateur peut être authentifié et autorisé à accéder aux ressources.

Comment s'effectue l'accès à une ressource

- Un utilisateur qui a ouvert une session sur le domaine vancouver.nwtraders.msft tente d'accéder à un dossier partagé de la forêt contoso.msft.
- L'ordinateur de l'utilisateur contacte le KDC d'un contrôleur de domaine de vancouver.nwtraders.msft et demande un ticket de service
- Les ressources ne sont pas localisées dans vancouver.nwtraders.msft, le contrôleur de domaine de vancouver.nwtraders.msft demande donc au catalogue global de voir si elles se trouvent dans un autre domaine de la forêt.
- Il recherche alors dans sa base de données les informations sur des approbations de forêt qui ont été établies avec sa forêt.
- S'il en trouve une, il compare les suffixes de noms de répertoires dans le TDO de l'approbation de forêt par rapport au suffixe du SPN cible.
- S'il trouve une correspondance, le catalogue global fournit les informations de routage relatives à la manière de localiser les ressources au contrôleur de domaine de vancouver.nwtraders.msft.
- Le contrôleur de domaine de vancouver.nwtraders.msft envoie une référence à son domaine parent et à l'ordinateur de l'utilisateur.
- L'ordinateur de l'utilisateur contacte un contrôleur de domaine de mwtraders.msft pour obtenir une référence à un contrôleur de domaine du domaine racine de la forêt contoso.msft.
- L'ordinateur de l'utilisateur contacte un contrôleur de domaine de la forêt contoso.msft pour obtenir un ticket de service pour le service demandé.
- Le contrôleur de domaine contacte donc son catalogue global pour trouver le SPN. Le catalogue global trouve une correspondance pour le SPN et l'envoie au contrôleur de domaine.

- Le contrôleur de domaine envoie une référence à seattle.contoso.msft à l'ordinateur de l'utilisateur.
- L'ordinateur de l'utilisateur contacte le KDC sur le contrôleur de domaine de seattle.contoso.msft et négocie un ticket pour l'utilisateur afin de pouvoir accéder aux ressources du domaine seattle.contoso.msft.
- L'ordinateur de l'utilisateur envoie le ticket de service à l'ordinateur sur lequel se trouvent les ressources partagées, qui lit les informations d'identification de sécurité et crée un jeton d'accès permettant à l'utilisateur d'accéder aux ressources.

Comment créer des approbations.

- Utiliser Domaines et approbations AD.

Comment vérifier et révoquer une approbation.

- Utiliser Domaines et approbations Active Directory
- Utiliser la commande netdom
 - o Vérifier
 - NETDOM TRUST nom_du_domaine_à_approuver /Domaine : nom_domaine_approuvé/Verify
 - o révoquer
 - NETDOM TRUST nom_du_domaine_à_approuver /Domaine : nom_domaine_approuvé/Remove

Module 3 : implémentation de la structure d'une OU

Méthodes de création et de gestion des OU

- utilisateurs et ordinateurs AD
- outils de service d'annuaire (dsadd, dsmov...)
 - o dsadd ou Nom_unique_de_l'OU_àajouter -desc description -d Domaine -u Nom_utilisateur -p Motdepasse
- ldifde (ligne de commande)
 - o dn :OU=ExempleOU,DC=nwtraders,DC=msft changetype :add objetClass :organizationalUnit
- environnement d'exécution de scripts Windows
 - o Set objDom=GetObject(« LDAP://dc=nwtraders,dc=msft »)
Set objOU=objDom.create(“OragnizationalUnit”,”ou=NouvelleOU”)
objOU.SetInfo

La 1^{ère} ligne se connecte au domaine

La 2^{ème} ligne crée la nouvelle OU

La 3^{ème} ligne enregistre le script dans la base de données AD

Pour exécuter le script, il faut le faire en ligne de commande

Tâches d'administration courantes pour des OU

- modification des propriétés sur un conteneur particulier
- création et suppression d'objets d'un type particulier
- mise à jour de propriétés spécifiques sur des objets d'un type donné.

Comment déléguer le contrôle administratif

- en utilisant la console Utilisateurs et ordinateurs AD et s'amuser avec l'option « Déléguer le contrôle ».

Comment vérifier la délégation

- en utilisant utilisateurs et ordinateurs AD et aller dans les fonctionnalités avancées.

Module 4 : implémentation de comptes utilisateurs, groupes et ordinateurs

Types de comptes

- Comptes d'utilisateurs
 - o compte d'utilisateur local : permet d'ouvrir une session sur 1 ordinateur
 - o compte d'utilisateur de domaine : permet de se connecter au domaine
 - o compte d'utilisateur intégré : permet de faire des tâches d'administration
- comptes d'ordinateurs
 - o chaque ordinateur qui rejoint un domaine possède un compte ordinateur
- comptes de groupes
 - o permet de gérer l'accès aux ressources du domaine

Types de groupes

- groupes de distribution
 - o utilisables uniquement avec des applications de messagerie (ex. Exchange)
- groupes de sécurité
 - o permettent de donner des droits et autorisations aux groupes d'utilisateurs et ordinateurs
 - droits : fonctions que les membres d'un groupe peuvent effectuer dans un domaine ou une forêt
 - autorisations : ressources accessibles à un membre d'un groupe

Appartenance au groupe local de domaine, étendues et autorisations

- appartenance
 - o En mode 2000 mixte : les groupes locaux de domaine peuvent contenir des comptes utilisateurs et des groupes globaux de n'importe quel domaine.
 - o En mode 2000 natif : les groupes locaux de domaines peuvent contenir des comptes utilisateurs, des groupes globaux, des groupes universels de n'importe quel domaine.
- Peut être membre de :
 - o En mode 2000 mixte : un groupe local de domaine ne peut pas être membre de n'importe quel groupe.
 - o En mode 2000 natif : un groupe local de domaine peut être membre de groupes locaux de domaine issus du même domaine
- étendue : un groupe local de domaine est visible uniquement dans son propre domaine
- autorisation : vous pouvez affecter une autorisation qui s'applique au domaine dans lequel le groupe local de domaine existe

Appartenance au groupe global de domaine, étendues et autorisations

- appartenance
 - o En mode 2000 mixte : un groupe global peut contenir des comptes utilisateurs du même domaine.
 - o En mode 2000 natif et 2003 : les groupes globaux peuvent contenir des comptes utilisateurs et des groupes globaux du même domaine.
- Peut être membre de :
 - o En mode 2000 mixte : un groupe global de domaine peut être membre des groupes locaux de domaine dans n'importe quel groupe.
 - o En mode 2000 natif et 2003 : un groupe global peut être membre de groupes universels et locaux de domaine dans n'importe quel domaine.
- étendue : un groupe global est visible dans tous les domaines.

- autorisation : vous pouvez affecter une autorisation à un groupe global qui s'applique à tous les domaines approuvés.

Appartenance au groupe universel, étendue et autorisations

- appartenance :
 - o En mode 2000 mixte : on ne peut pas créer de groupes universel.
 - o En mode 2000 natif et 2003 : des groupes universels peuvent contenir des comptes, des groupes globaux et des groupes universels de tous les domaines
- Peut être membre de :
 - o En mode 2000 mixte : le groupe universel ne s'applique pas
 - o En mode 2000 natif : un groupe universel peut être membre de groupes locaux de domaines et de groupes universels de n'importe quel domaine
- étendue : les groupes universels sont visibles dans tous les domaines
- autorisations : vous pouvez affecter une autorisation à un groupe universel qui s'applique à tous les domaines.

Implémentation des suffixes UPN (user principal name)

L'UPN est le nom d'ouverture de session.

- Règles :
- le nom complet doit être unique dans son conteneur et dans la forêt
 - le nom d'utilisateur doit être unique dans la forêt.

Détection et résolution des conflits de suffixe de noms

Un conflit se produit quand :

- un nom DNS est déjà utilisé
- un nom NetBios est déjà utilisé
- un SID de domaine est en conflit avec un autre SID.

Déplacement d'objets dans AD

- dans un domaine :
 - o pas de changements de SID ou GUID
- dans un forêt
 - o nouveau SID
 - o historique SID
- entre les forêts
 - o nouveau SID
 - o historique SID
 - o nouvel identificateur GUID
- implications sur la sécurité d'un historique SID
 - o un historique SID permet à des utilisateurs migrés d'accéder aux ressources situées dans leurs anciens domaines.
- autres applications de déplacements d'objets
 - o les comptes d'utilisateurs qui ont des privilèges administratifs pour l'OU vers laquelle le compte est déplacé
 - o les restrictions liées à la stratégie de groupe de l'OU du domaine ou du site depuis lequel le compte d'utilisateur a été déplacé ne s'appliquent plus au compte d'utilisateur
 - o les paramètres de stratégie de groupe du nouvel emplacement s'appliquent au compte d'utilisateur

Définitions d'une stratégie de mot de passe

- paramétrer l'option « conserver l'historique des mots de passe » sur un minimum de 24 mots de passe retenus.
- Définir la durée de vie maximale du mot de passe sur 42 jours
- Définir la durée de vie minimale du mot de passe sur 2 jours
- Définir la longueur du mot de passe sur 8 caractères maximum
- Activer l'option « le mot de passe doit respecter des exigences de sécurité

Instructions d'authentification, d'autorisation et d'administration des comptes

Aide à protéger le réseau.

On utilise les instructions suivantes :

- attribuer une valeur élevée au paramètre de stratégie seuil de verrouillage de compte.
- Eviter d'utiliser des comptes administrateurs pour répondre au besoin informatiques de routines
- Utiliser une authentification multifactorielle
- Utiliser des groupes de sécurité basée sur la stratégie C-G-U-LD-A
- Désactivez le compte admin et affecter aux utilisateurs et admins le moindre privilège nécessaire pour affecter leurs tâches professionnelles.

Instructions de planification d'une stratégie de groupe

- affecter les utilisateurs aux responsabilités professionnelles communes aux groupes globaux
- créer un groupe local de domaine pour partager les ressources
- ajouter des groupes globaux aux groupes locaux de domaine qui exigent l'accès aux ressources
- utiliser les groupes universels pour accorder l'accès aux ressources situées dans plusieurs domaines.
- Utiliser des groupes universels quand l'appartenance est statique.

Planification d'une stratégie d'audit AD

Ca sert à :

- enregistrer toutes les modifications réussies dans AD
- assurer un suivi de l'accès à une ressource ou par un compte spécifique
- détecter et enregistrer les tentatives d'accès infructueuses

Module 5 : implémentation d'une stratégie de groupe

Types de paramètres qu'on peut gérer avec une stratégie

- modèles d'administration
- scripts
- services d'installation à distance
- maintenance internet explorer
- redirection des dossiers
- sécurité
- installation des logiciels

Flux d'héritage

Un objet GPO associé à un domaine s'applique aussi aux OU et à tous les objets du domaine.

Fonctions avancées

- blocage de l'héritage
- option appliquer (ne pas passer outre) : force tous les conteneurs enfants d'hériter de la stratégie du parent

Filtrage des objets GPO

Permet de fixer une stratégie de groupe à un seul ordinateur par exemple.

Composant d'un objet GPO

- GPC (conteneur de stratégie de groupe) : contient l'état de la stratégie de groupe de chaque objet
- GPT (modèle de stratégie de groupe) : dans le dossier SYSVOL, il contient les paramètres de stratégie de groupe.

Gestion des objets GPO

Il est recommandé de spécifier un contrôleur de domaine pour la gestion des objets GPO pour éviter un conflit de réplication (par défaut, on utilise l'émulateur PDC pour ça).

Les données concernant les objets GPO se trouvent dans le dossier SYSVOL et dans AD.

Problèmes liés à l'implémentation de stratégie de groupe

problème	Solution
Vous ne pouvez pas ouvrir un objet GPO même en accès en lecture	Devenez membre d'un groupe de sécurité avec les autorisations lire et écrire
Un message dit qu'il est impossible d'ouvrir un objet GPO lors d'une modification	S'assurer que le DNS fonctionne correctement
La stratégie de groupe n'est pas appliquée aux utilisateurs d'un groupe de sécurité qui les contient alors qu'un objet GPO est lié à une unité d'organisation contenant le groupe de sécurité	Liez les objets GPO uniquement à des sites, domaines et OU
La stratégie de groupe n'affecte pas les utilisateurs et ordinateurs d'un conteneur AD	Liez les objets GPO à une unité d'organisation qui est parente du conteneur AD.
La stratégie de groupe n'est pas appliquée sur	Déterminez quels objets GPO sont appliqués

l'ordinateur client	via AD et si ces objets contiennent des paramètres en conflit avec les paramètres locaux
---------------------	--

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

Processus d'installation et de maintenance de logiciels

- Préparation
 - o Vérifier si on peut déployer le logiciel grâce à la structure des objets GPO courants
 - o Identifier les risques liés à l'utilisation de l'infrastructure courante qui empêcherait l'installation de logiciel
 - o Préparer les fichiers permettant le déploiement de logiciels.
- Déploiement
 - o Créer un objet GPO qui installe le logiciel sur l'ordinateur et relier l'objet GPO à un conteneur AD.
 - o L'installation commence dès que l'utilisateur se connecte à son pc
- Maintenance
 - o Les mises à jour se font automatiquement lorsque l'utilisateur se connecte
- Suppression
 - o Supprimer les paramètres du package logiciel dans l'objet GPO.
 - o Ce sera fait automatiquement dès que l'utilisateur se connecte

Déploiement de logiciels

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

Affectation et publication de logiciels

- affecter un logiciel : permet à l'utilisateur de disposer du logiciel en permanence.
- Publier un logiciel : s'assurer que le logiciel est disponible pour que l'utilisateur puisse l'installer.

Création d'un point de distribution de logiciels

- créer un dossier partagé en mode lecture
- créer les dossiers d'applications appropriées dans le dossier partagé.
- Copiez les package Windows Installer dans les dossiers appropriés.

Types de mises à niveau de logiciels

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

Méthodes de suppression de logiciels déployés

- suppression forcée : le logiciel est automatiquement supprimé d'un ordinateur
- suppression facultative : la logiciel n'est pas supprimé d'un ordinateur et aucune mise à niveau ne peut être installée.

Problèmes liés au déploiement de logiciels

Problème courant :

Symptôme	Cause possible
Les applications n'apparaissent pas dans Ajouter/supprimer des programmes ni dans le menu Démarrer	<ul style="list-style-type: none">- l'application a été affectée mais pas publiée- aucun objet GPO n'a été appliqué

Comment déterminer la cause du problème

Cause	Méthode de test
<ul style="list-style-type: none">- l'application a été publiée mais pas affectée- l'application a été affectée mais pas publiée- aucun objet GPO n'a été appliqué	Utiliser RSoP pour déterminer quel objet est appliqué
Le point de distribution logicielle n'est pas accessible	Installer manuellement Windows Installer
Les applications précédemment installées empêchent toute nouvelle installation	Créer le fichier journal Windows Installer

Comment résoudre les problèmes

Cause	Méthode de résolution
<ul style="list-style-type: none">- l'application a été publiée mais pas affectée- l'application a été affectée mais pas publiée- aucun objet GPO n'a été appliqué	Modifier l'objet GPO
Le point de distribution logicielle n'est pas accessible	Modifier les autorisations
Les applications précédemment installées empêchent toute nouvelle installation	Supprimer les composants de registre