

Chapitre 3 : **Gestion des comptes d'utilisateur et de machine dans les Services de Domaine de l'Active Directory**

Sommaire du Chapitre

- Les comptes d'utilisateur
- Utilisation de requêtes LDAP pour localiser des objets dans Active Directory Domain Services
- Les comptes de machine

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Leçon 1: Les comptes d'utilisateur

- Notion de compte d'utilisateur
- Noms pour l'ouverture de session dans un domaine Active Directory
- Options de mot de passe des comptes d'utilisateur
- Outils pour gérer les comptes d'utilisateur
- Notion de modèle de compte

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Notion de compte d'utilisateur

Un compte d'utilisateur est un objet qui permet l'authentification d'un utilisateur

Les comptes d'utilisateur existent :

❖ Dans les domaines Active Directory (AD DS)

Les comptes de domaine permettent l'authentification au travers du réseau

❖ Dans la base locale d'un ordinateur

Les comptes locaux permettent l'authentification (locale) par rapport à une machine

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Noms pour l'ouverture de session dans un domaine Active Directory

Noms associés aux comptes de domaines :

Type de nom	Exemple	Contraintes d'unicité
Nom d'ouverture de session pré-Windows 2000	WoodgroveBank\Gregory	Doit être unique dans le domaine
Nom principal	Gregory@WoodgroveBank.com	Doit être unique dans la forêt

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Options de mot de passe des comptes d'utilisateur

Les mots de passe sont des composants essentiels de la sécurité; ils peuvent supporter les contraintes suivantes :

- ❖ Taille de l'historique (0 – 24)
- ❖ Longueur minimale (0 – 14)
- ❖ Complexité obligatoire

Dans une base de comptes de domaine Windows 2008, un mot de passe complexe doit comprendre au moins un caractère choisi dans 3 des 4 classes ci-dessous :

- ❖ Lettres majuscules
- ❖ Lettres minuscules
- ❖ Chiffres
- ❖ Caractères spéciaux



L'Active Directory peut enregistrer des mots de passe comportant au maximum 127 caractères (déconseillé)

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Outils pour gérer les comptes d'utilisateur

Les comptes locaux et les comptes de domaine utilisent des outils différents :

Type de compte	Outils
Comptes locaux	<ul style="list-style-type: none">• XP, Vista ou Seven : Panneau de Configuration / Comptes d'utilisateurs• Windows 2008 : Gestionnaire de serveur
Comptes de domaine	<ul style="list-style-type: none">• Utilisateurs et Ordinateurs Active Directory (outil graphique)• Utilitaires en ligne de commandes : dsadd, Powershell, CSVDE, LDIFDE

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

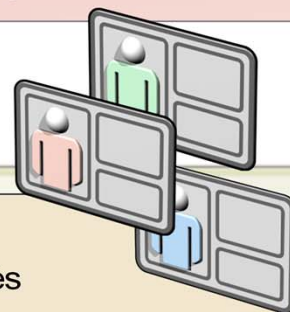
.....

Notion de modèle de compte

Un modèle de compte est un compte d'utilisateur, avec des propriétés configurées, utilisé pour créer des « copies » (comptes dérivés)

Lors d'une copie de compte d'utilisateur :

- ❖ Les groupes auxquels le compte source appartient sont copiés
- ❖ Les privilèges accordés au compte source ne sont pas copiés
- ❖ L'attribut activé / désactivé est copié
- ❖ L'adresse postale est partiellement copiée
- ❖ Les numéros de téléphone, adresse Email, ... ne sont pas copiés



Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Leçon 2 : Utilisation de requêtes LDAP pour localiser des objets dans un domaine Active Directory

- Comment effectuer des recherches dans Active Directory Domain Services
- Les types de requêtes LDAP
- Les requêtes sauvegardées

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Comment effectuer des recherches dans Active Directory Services de Domaines

❖ Tri des objets :
Dans la console "Utilisateurs et Ordinateurs Active Directory" chaque tête de colonne peut servir de critère de tri



❖ Recherches (LDAP) :
la liste des critères de recherche proposés varie automatiquement en fonction du contexte



Attention : par défaut la console "Utilisateurs et Ordinateurs Active Directory" n'affiche que les 2000 premiers objets

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Les types de requêtes LDAP

❖ Utilisateurs, Contacts et Groupes

❖ Ordinateurs

❖ Imprimantes

❖ Dossiers Partagés

❖ Unités d'organisation

❖ Requêtes communes

❖ Requêtes personnalisés

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

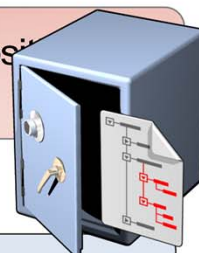
.....

.....

.....

Les requêtes sauvegardées

L'enregistrement de requêtes LDAP permet de mettre celles-ci à disposition des utilisateurs ("Administrateurs" d'OU par exemple)



Avec les requêtes sauvegardées :

- ❖ Les gestionnaires de comptes possèdent un moyen simple pour sélectionner un ensemble d'utilisateurs afin d'effectuer des modifications "groupées" de propriétés (exemple : saisir l'adresse de messagerie pour tous les comptes qui en sont dépourvus)
- ❖ Les requêtes sauvegardées peuvent être exportées (et importées)

Les requêtes sauvegardées
sont stockées dans le profil de l'utilisateur

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Atelier : Création de comptes d'utilisateurs dans l'Active Directory



- ☐ Exercice 1 : Création et configuration de comptes d'utilisateurs
- ☐ Exercice 2 : Utilisation de modèles de compte
- ☐ Exercice 3 : Modification groupée de comptes
- ☐ Exercice 4 : Utilisation de requêtes sauvegardées

Ordinateurs virtuels

SC084-NYC-DC1
SC084-NYC-CL1

Durée approximative : 25 minutes

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Leçon 3: Les comptes de machine

- Présentation des comptes de machine
- Gestion des comptes de machine

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

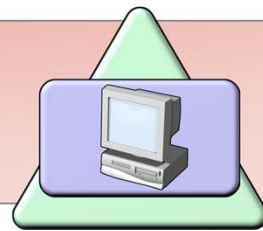
.....

.....

.....

Présentation des comptes de machine

Dans un domaine Active Directory (AD DS) un compte de machine est un objet qui permet l'authentification d'une machine



Les comptes de machine :

- ❖ Peuvent être créés automatiquement lorsqu'une machine rejoint un domaine
- ❖ Peuvent être créés manuellement (avant de rejoindre le domaine) par un administrateur pour définir des propriétés particulières
- ❖ Sont obligatoires pour les "clients" NT, 2000, XP, Vista, 7 si l'utilisateur veut ouvrir une session en domaine
- ❖ Sont aussi obligatoires pour les serveurs membre
- ❖ Permettent d'associer une Stratégie de Groupe (GPO) à des machines

Notes :

.....

.....

.....

.....

.....

.....

.....

.....






.....

.....

.....

Gestion des comptes de machine

Actions les plus courantes :

-  Ajout de comptes de machine : permet de configurer les propriétés des comptes de machine (droit de rejoindre le domaine, ...)
-  Suppression d'un compte de machine : l'ordinateur est supprimé du domaine
-  Désactivation de comptes de machine : aucun utilisateur pourra ouvrir une session en domaine à partir de cette machine
-  Réinitialiser un compte de machine : Le mot de passe du compte machine retrouve sa valeur initiale (mais pas la machine cliente !)
-  Affectation de stratégies de Groupe : modification du comportement de la machine (installation de logiciels, affichage lors de l'ouverture de session utilisateur, ...)

Par défaut les comptes de machine changent automatiquement de mot de passe tous les 30 jours (modifiable par stratégie de groupe)

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Atelier : Création de comptes d'ordinateurs dans l'Active Directory (services de domaine)



❏ Exercice 5 : Création et configuration de comptes d'ordinateurs

Ordinateurs virtuels

SC084-NYC-DC1
SC084-NYC-CL1

Durée approximative : 25 minutes

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Questions de révision

1. Peut-on ouvrir une session en saisissant DOM1\Karen comme nom d'utilisateur sachant que DOM1 est un nom de domaine NETBIOS valable et que le compte Karen existe bien dans ce domaine AD DS ?
2. Peut-on ouvrir une session en saisissant
cn=Karen, ou=itAdmins,DC=DOM1,DC=local
comme nom d'utilisateur sachant que le compte de Karen existe bien dans l'unité d'organisation itAdmins et que DOM1.local est le nom DNS du domaine où réside ce compte ?
3. En reprenant le contexte de la question précédente, que faut-il faire afin que Karen puisse ouvrir une session avec la saisie de :
Karen@simba.west
sans que son compte change de domaine ?
4. Si l'administrateur désactive le compte de la machine cliente utilisée par Karen, est-ce que celle-ci pourra ouvrir
 - une session en domaine à partir de sa machine ?
 - Une session locale à partir de sa machine ?
 - Une session en domaine à partir d'une autre machine ?

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Questions de révision (suite)

1. Est-ce que MzbKxZZyGg est un mot de passe complexe pour l'Active Directory Domain Services ?

Notes :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....