PrÃ©sentation d'Active Directory

Soumis par MCP
28-07-2007
Dernière mise à jour : 23-12-2007

Active Directory est un annuaire sécurisé en réseau des ressources de l'entreprise qui permet de gérer les accès des utilisateurs, groupes et comptes d'ordinateurs aux objets d'un ou plusieurs domaines.

Services d'annuaire et contrôleurs de domaine

- 2 modèles de service d'annuaire MS Windows : Groupe de travail et Domaine

- Active Directory : annuaire unique des ressources d'un domaine (Who's who du domaine) installé sur un ou plusieurs contrôleurs de domaine

- contrôleur de domaine : serveur hébergeant une réplique d'Active Directory

- octroi du statut de domaine à un serveur

  - à l'installation via "Assistant Installation de Active Directory"

  - par promotion via DCPROMO ou "Gérer votre serveur"

- Réplication : tout changement apporté à Active Directory à partir d'un contrôleur de domaine est répliqué vers les autres contrôleurs du même domaine

- autres services d'Active Directory

  - fichiers de support (dont les journaux de transactions)

  - Sysvol (volume système contenant les scripts d'ouverture de session et les stratégies de groupe)

  - LDAP (Lightweight Directory Access Protocol), Kerberos (sécurité), FRS (File Replication Service).

Domaines, arbres et forêts

- Active Directory <=> au moins 1 domaine et vice-versa

- domaine : unité administrative fondamentale du service d'annuaire de Windows Serveur 2003

- arbre : modèle reposant sur plusieurs domaines Active Directory installés partageant des noms DNS contigus (ex. :

domaine.com, dom1.domaine.com, dom2.domaine.com sont regoupés dans un arbre commun)

- forêt : modèle reposant sur plusieurs domaines répartis sur un ou plusieurs arbres (DNS non contigus), ou un seul domaine

- "Catalogue Global" d'Active Directory : informations concernant les objets situés dans tous les domaines de la forêt.

Objets et Unités d'organisation (OU)

- objet Active Directory : ressource du domaine caractérisée par des propriétés (utilisateurs, groupes, ordinateurs, dossiers partagés, imprimantes, fichiers, bases de données, courriers électroniques, sites, liens, GPO, zones DNS, applications, ...)

- création d'un objet :

1. Ouvrez Outils d'administration / Utilisateurs et ordinateurs Active Directory
2. Développez le domaine
3. Cliquez droit sur un conteneur ou une OU, puis Nouveau type_objet

- Unités d'organisation (OU)

  - objet particulier d'Active Directory permettant de regrouper des objets (conteneur) pour partager leur administration

  - aptitudes administratives importantes où les fonctions d'administration peuvent être déléguées et les stratégies de groupe connectées.

Délégation

- Chaque objet Active Directory inclut une ACL (Access Control List) qui définit les permissions qui lui sont associées

- On regroupe dans une même OU les objets pour lesquels on souhaite assigner une délégation des permissions dont les objets contenus héritent alors (ex. : on regroupe dans une même OU tous les utilisateurs dont on souhaite qu'un administrateur secondaire puissent modifier les mots de passe).

Stratégie de groupe

-
- GP (Group Policy) : outil permettant d'implémenter des configurations centralisées (sécurité, déploiement, configuration des OS, accès applications, ...)

- GPO (Group Policy Organization) : ensemble de paramètres de configuration affectant tous les utilisateurs et ordinateurs situés dans un conteneur spécifié d'Active Directory (généralement une OU).