Infos comme ça

ENCODER = BASE 64

Chiffrement : BCRYPT

HASHER : SHA 512

**Active Directory**

Solution Microsoft

Présentée en 1996 et première utilisation en 1999 sur Windows 2000 Server Edition.

Annulaire LDAP(protocole) pour les systèmes d’exploitation Windows (mais aussi Linux) = SAMBA4 qui intègre le module AD.

Au tout début, il portait comme nom « NTDS » pour NT Directory Services / Service d’annuaire de NT

Il a comme rôle principal : l’identification et l’authentification

Présentation

L’AD est un rôle qui s’installe sur un serveur disposant d’un système d’exploitation Microsoft Windows Server.

Il existe 5 types d’Active Directory :

* AD DS : Directory Services
* AD LDS : Lightweight Directory Services
* AD RMS : Rights Management Services
* AD CS : Certificates Services
* AD FS : Federation Services (SSO en gros)

Le plus courant : AD DS – Directory Services

Le serveur qui détient ce rôle devient alors Contrôleur de Domaine (DC : Domain Controller)

ATOUTS DE L’AD DS

* Administration centralisée et simplifiée
* Unifier l’authentification
* Identifier les objets sur le réseau
* Référencer les ordinateurs et utilisateurs

Exemple d’ouverture de fichier avec des droits

* Envoi d’une requête à l’AD
* Identification validée
* Accès à une ressource protégée

**Classes d’objet Active Directory**

Active Directory est un annuaire qui répertorie et organise des informations qu’on appelle des objets Active Directory

* Ordinateur
* Contact
* Groupe
* Unité d’organisation
* Imprimante
* Utilisateur

**SCHEMA D’ARCHITECTURE ACTIVE DIRECTORY**

Au sein d’un domaine, on retrouvera tout un ensemble d’Unités d’Organisation remplies d’objets Active Directory.

Forêt : Quand on crée un domaine active directory, il se retrouve au sein d’une forêt. Plus haut point logique, hiérarchique dans un AD.

Domaine et sous domaine : Un Domaine peut avoir des sous domaines :

Domaine : Cybup.local (domaine racine)

Sous domaine :

* Saintetienne.cybup.local (domaines enfants)
* Paris.cybup.local (domaines enfants)

Arbre = domaine + sous domaine, l’arbre est intégré dans la forêt

Dans une forêt, il peut y avoir plusieurs arbres

**Le lien de confiance ou Trust Relationship peut être :**

* Unidirectionnel ou bidirectionnel
* Transitif
* Prédéfini
* Externe

Dans quel contexte arrive-t-on à une telle complexité de schéma ?

Exemple :

* Une multinationale qui scindera son SI en plusieurs domaines découpés par zones géographiques
* Fusion de 2 entreprises
* Une entreprise qui dispose de plusieurs filiales avec des domaines différents.

**Bonne pratique Microsoft :** Utiliser des TLD publics et créer des sous domaines pour un usage interne.

* Ex : Domaine : internal.cybup.fr

**CONTROLEUR DE DOMAINE**

* L’AD nécessite un ou plusieurs contrôleurs de domaine
* Les contrôleurs de domaine sont synchronisés et contiennent une copie de la base de données NTDS.DIT
* Lorsqu’un changement est effectué sur un objet dans l’AD, il est répliqué sur les autres contrôleurs de domaine.
* Chaque contrôleur de domaine peut authentifier un compte utilisateur ou ordinateur
* Les contrôleurs de domaine en lecture seule possèdent une partie de la base NTSDIT. Ils ne permettent pas de faire de modification dans l’AD. (RODC) Read Only Domain Controller)

**Niveau FONCTIONNEL**

Il existe 2 types :

* Niveau fonctionnel du domaine
* Niveau fonctionnel de la forêt

Pourquoi augmenter le niveau fonctionnel ?

* Bénéficier des dernières nouveautés liées à l’AD
* Obligation : Lors d’une migration vers un contrôleurs de domaine plus récent.

**Les versions diffèrent en fonction du système d’exploitation :**

Varie en fonction de la version du Win server installé