# Cours 6

BTS SIO SR 1

# CAS PRATIQUE

**Le Système Informatique de la société :**

- 20 utilisateurs
- 20 postes clients
- Interconnectés en réseau par un switch
- Les échanges se font par email et par clé USB

**Les souhaits de la direction :**

- Restreindre les accès à certaines données
- Trouver plus facilement les données
- Avoir des mots de passe sur les postes clients

# Quelles solutions ?

- Comment répondre au besoin ?
- Un serveur qui hébergera les fichiers
- Mise en place d'une solution d'identification et de gestion des droits d'accès grâce à un annuaire LDAP
- Quels préconisations en tant que technicien informatique ?
- Mise en place d'une sauvegarde efficace possible puisque les données seront centralisées
- Etc.

# Sommaire – Cours 6 L'infrastructure Active Directory – DNS

- Pourquoi un annuaire ?
- Protocole LDAP
- Active Directory
- Best Practices et Sécurisations
- Travaux Pratiques

# Pourquoi un annuaire ?

- Un annuaire est une base de données regroupant l'ensemble des ressources du système d'informations
- Chacune de ces ressources sera composée de son nom mais aussi d'autres attributs selon le besoin
- Une ressource peut être un utilisateur, un ordinateur, une imprimante etc.
- L'annuaire permet de :
  - Référencer – Avoir la liste des ressources
  - Centraliser - Avoir la liste à un seul endroit
  - Identifier – Reconnaitre chacune des ressources
  - Authentifier – Vérifier quelle ressource à le droit d'interagir avec quelle autre ressource

  - Numéro unique – nom d'utilisateur – téléphone – adresse mail
  - <uid:125457> - kevin – 00000 – kevin.roth@test.fr

# Protocole LDAP – Mode de fonctionnement

Lightweight Directory Access Protocol

Base de donnée optimisée en lecture

Permet de centraliser et gérer des ressources : utilisateurs, ordinateurs, groupes, etc.

- Les ressources ont un identifiant unique (GUID)
- Un nom unique est également attribué (DinstinguishedName)
  - Exemple : cn=Kevin,ou=Profs,dc=sio,dc=local
    - Est le DN de l'utilisateur « Kevin », dans l'unité d'organisation « Profs » dans le domaine « sio.local »

# Active Directory - AD

- Active Directory est l'implémentation de LDAP par Microsoft
- Il repose sur un schéma et un catalogue global (GC) et s'installe en tant que rôle de Windows Server
- Le schéma gère la définition de chaque ressource de l'AD
- Le catalogue global contient l'ensemble des objets de l'annuaire
- Dans Active Directory, une ressource s'appelle un objet
- Une ressource peut être un serveur, un ordinateur, un utilisateur, une imprimante etc.

# Active Directory

- Active Directory regroupe le système d'information sous forme de forêt et de domaine
- Un domaine regroupe un ensemble de ressources qui utilise le même annuaire LDAP pour s'authentifier et a un nom de type :*nomsociété.local*
- Les forêts regroupent des domaines qui n'ont pas le même nom mais qui partage le même schéma et le même catalogue global
- Une ressource  peut être un sous domaine, un utilisateur, un ordinateur, une unité organisationnelle ou un groupe.
- C'est le serveur contrôleur de domaine (DC) qui gère les forêts et domaine

# Active Directory

- Un contrôleur de domaine recevra les requêtes de l'ensemble des ressources du domaine
- Ses rôles principaux seront l'identification et l'authentification
- Certains contrôleurs de domaines ont des rôles spécifiques qu'on appelle les maitres d'opérations

# Active Directory

- Les maitres d'opérations sont au nombre de 5 :
  - Unique au sein d'une forêt :
    - Le maître de schéma
    - Le maître d'attribution de noms de domaine
  - Unique au sein d'un domaine :
    - Le maître RID (Relative Identifier)
    - Le maître d'infrastructure qui gère les SID (Security Identifier)
    - L'émulateur primary domain controller (PDC)

# Active Directory

- Le premier contrôleur installé est automatiquement le fondateur :
  - De la forêt
  - Du premier domaine
- Et détient l'ensemble des maîtres d'opérations

# Active Directory - Protocoles

- Active Directory utilise plusieurs protocoles pour fonctionner :
  - TCP/IP pour l'interconnexion réseau
  - LDAP pour la gestion de l'annuaire
  - DNS pour la gestion des noms
  - Kerberos pour la gestion de l'authentification
  - X.509 pour la gestion des certificats
  - SNTP pour la synchronisation de la date et l'heure

# Qu’est-ce que DNS ?

- DNS (Domain Name System) est service gérant la correspondance entre NOM et Adresse IP
- Il fonctionne via des enregistrement :
  - NS (Name Server): Qui est serveur DNS dans le domaine
  - SOA (Start of Authority) : Qui donne les informations générales de la zone
  - A (Address) : Correspondance NOM vers IP
  - PTR (Pointer): Correspondance IP vers NOM
  - CNAME (Canonical NAME): Un alias
  - MX (Mail eXchange) : Permet de spécifier qui est serveur de mail au sein du domaine
  - SRV : Permet de spécifier qui est le fournisseur d’un service précisé

# Qu’est-ce que DNS ?

- DNS (Domain Name System) est service gérant la correspondance entre NOM et Adresse IP
- Il fonctionne via des  zones qui regroupes ces enregistrements
- Elles peuvent être directe : Correspondance nom vers IP
- Elles peuvent être inversée : correspondance Ip vers NOM
- A chaque demande de service vers un nom, le client contactera le serveur DNS primaire indiqué pour obtenir l’IP correspondante et le stockera dans un cache local, Cela s’appelle faire une résolution DNS

# Qu’est-ce que DNS ?

- Un serveur DNS local connaitra les adresses IP interne de votre réseau
- S’il ne connait pas la correspondance nom-IP que le client demande, il contactera un autre serveur. Cela s’appelle un redirecteur DNS
- Un serveur DNS public (ex. : 9.9.9.9) connait les correspondances nom-IP d’Internet
- Commandes DOS utiles
  - Nslookup qui permet de vérifier que le serveur DNS répond
  - Ipconfig /flushdns qui permet de vider le cache
  - Ipconfig /registerdns qui permet de mettre à jour son propre enregistrement auprès du serveur DNS

# DNS et Active Directory

- Active Directory est lié à DNS pour bien fonctionner. Les ordinateurs et serveurs gérés par l'annuaire auront automatiquement un enregistrement dans le serveur DNS
- Pour son bon fonctionnement de votre DNS local :
  - Créer une zone de recherche inversée correspondant à votre réseau
  - Spécifier un redirecteur vers un serveur DNS publique pour pouvoir résoudre les noms d'hôte d'Internet
  - Spécifier l'IP du serveur DNS en serveur DNS primaire sur l'ensemble du réseau local
  - Spécifier la carte réseau d'écoute du serveur DNS pour qu'il ne réponde qu'en IPv4

# Best Practices et Sécurisations

Pour le bon fonctionnement d'Active Directory :

- Une adresse IP fixe est nécessaire sur le serveur
- Le serveur DNS principal doit être lui même
- Créer une zone de recherche inversée dans le serveur DNS correspondante à votre réseau IP
- Le nom de domaine doit se finir en *.local* et ne doit pas être trop long

# Best Practices et Sécurisations

Pour la sécurité :

- Un mot de passe fort pour l'administrateur général
- Des comptes administrateurs nominatifs avec mots de passe fort
- Aucun utilisateur avec des droits administrateurs
- Réaliser une sauvegarde périodique du système qui peut être complétée par les clichés instantanés pour faciliter la gestion
- Mettre le niveau fonctionnel au maximum
- Tenir le système à jour
- Ne pas attribuer d'autres rôle que Active Directory et DNS à ce serveur
- Recommandations ANNSI: (https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf)

# Travaux Pratiques

- Installation du rôle Active Directory et DNS sur votre serveur DNS
- Lié votre client Windows 10 au domaine crée