Active Directory

Théorie : introduction à Active Directory

Objectifs ICT

☐	Connaitre le principe d'un domaine (forêt, arbre, domaine)
☐	Connaitre le principe de base d'Active Directory
☐	Etre capable de différencier un serveur autonome d'un serveur membre et d'un contrôleur de domaine
☐	Etre capable d'expliquer le principe de base de réplication d'un contrôleur de domaine

Au terme de ce chapitre, je suis capable de …

Thème 1	
☐oui ☐non	d'expliquer la différence entre un système poste à poste et centralisé.
☐oui ☐non	d'énumérer les avantages d'un domaine.
☐oui ☐non	d'expliquer la différence entre un serveur autonome, un serveur membre et un contrôleur de domaine.
☐oui ☐non	d'expliquer ce qu'est un domaine, un arbre, une forêt.
Thème 2	
☐oui ☐non	d'expliquer le principe de fonctionnement d'un domaine d'Active Directory.
☐oui ☐non	d'expliquer comment structurer Active Directory.
☐oui ☐non	d'expliquer le principe de fonctionnement de base de la réplication des contrôleurs de domaine.

Table des matières

Informations sur le chapitre

Durée

Durée prévue :
- *2 périodes, avec les exercices*

Références

- *Activer les services d'un Serveur, DRZ-DS-LE-TF, 16/05/2017*

- *https://fr.wikipedia.org/wiki/Active_Directory*

1. Notion de domaine

1.1 Avantages du domaine

- **Compte utilisateur et ouverture de session unique :** Les domaines offrent aux utilisateurs un processus d'ouverture de session unique pour accéder aux différentes ressources réseaux (imprimantes, fichiers, applications). Tous les comptes utilisateurs sont stockés dans un même emplacement central (La base de données Active Directory).
- **Gestion centralisée des services :** Les domaines offrent une administration centralisée des ressources (imprimantes, fichiers, applications). Toutes les informations relatives aux utilisateurs/groupes sont centralisées sur un serveur unique (le contrôleur de domaine) qui contient la base de données (Active Directory). Toutes les informations relatives aux services d'impressions sont centralisées sur le(s) serveur(s) d'impression. Toutes les ressources fichiers (répertoires personnels, répertoires commun, …) sont stockées sur le(s) serveur(s) de fichiers, etc.

1.2 Un peu de vocabulaire…

1.2.1 Serveur autonome :

C'est un serveur faisant parti d'un groupe de travail. Il n'appartient à aucun domaine.

1.2.2 Serveur membre :

C'est serveur intégré à un domaine au même titre qu'une station. Il ne possède pas de droits au niveau du domaine.

1.2.3 Contrôleur de domaine :

C'est serveur sur lequel Active Directory a été installée.

1.2.4 Domaine :

Dans l'environnement de réseau Microsoft, la notion de domaine définit un ensemble d'ordinateurs organisés en mode client/serveur. Les ordinateurs d'un domaine partagent deux choses :

- Un nom (de domaine) commun : Par exemple, tous les ordinateurs du CPLN font partie du domaine s2.rpn.ch et chaque ordinateur possède un nom de type NomMarchine.s2.rpn.ch

(Par exemple : LMB-113a-00.s2.rpn.ch).

- Des données d'annuaire communes : Comprenez par-là, une base de données unique (appelée Active Directory) contenant entre autres (en plus des imprimantes, des machines) tous les utilisateurs pouvant se connecter au domaine.

1.2.5 Arbre :

Un arbre est une hiérarchie de domaine et de sous-domaines. Le premier domaine créé dans un arbre s'appelle le domaine racine.

Par exemple, le domaine rpn.ch est le domaine racine, S2.rpn.ch (le domaine dont le CPLN fait partie) est un sous-domaine de rpn.ch, etc. Le domaine et ses sous-domaines forment une arborescence appelée : Arbre (Voir schéma page suivante). Un domaine seul (qui n'a pas de sous-domaine) forme tout de même un arbre.

Le domaine racine et ses sous-domaines partagent une base de nom commune (Dans notre exemple: rpn.ch).

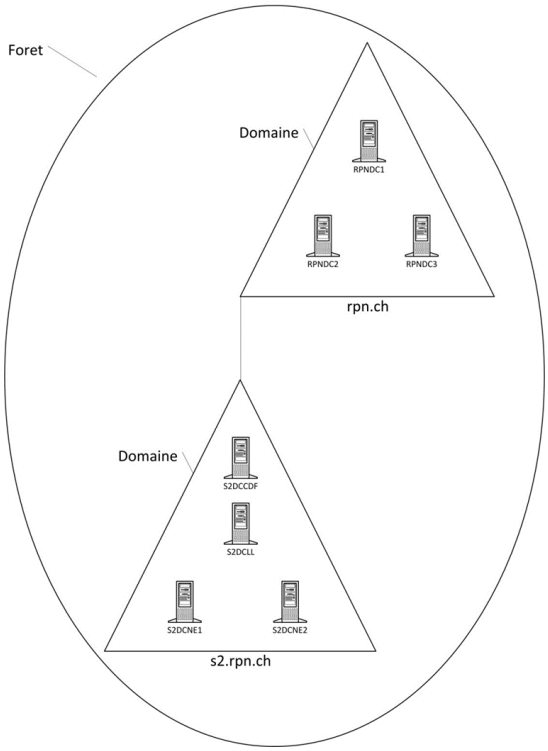
1.2.6 Forêt :

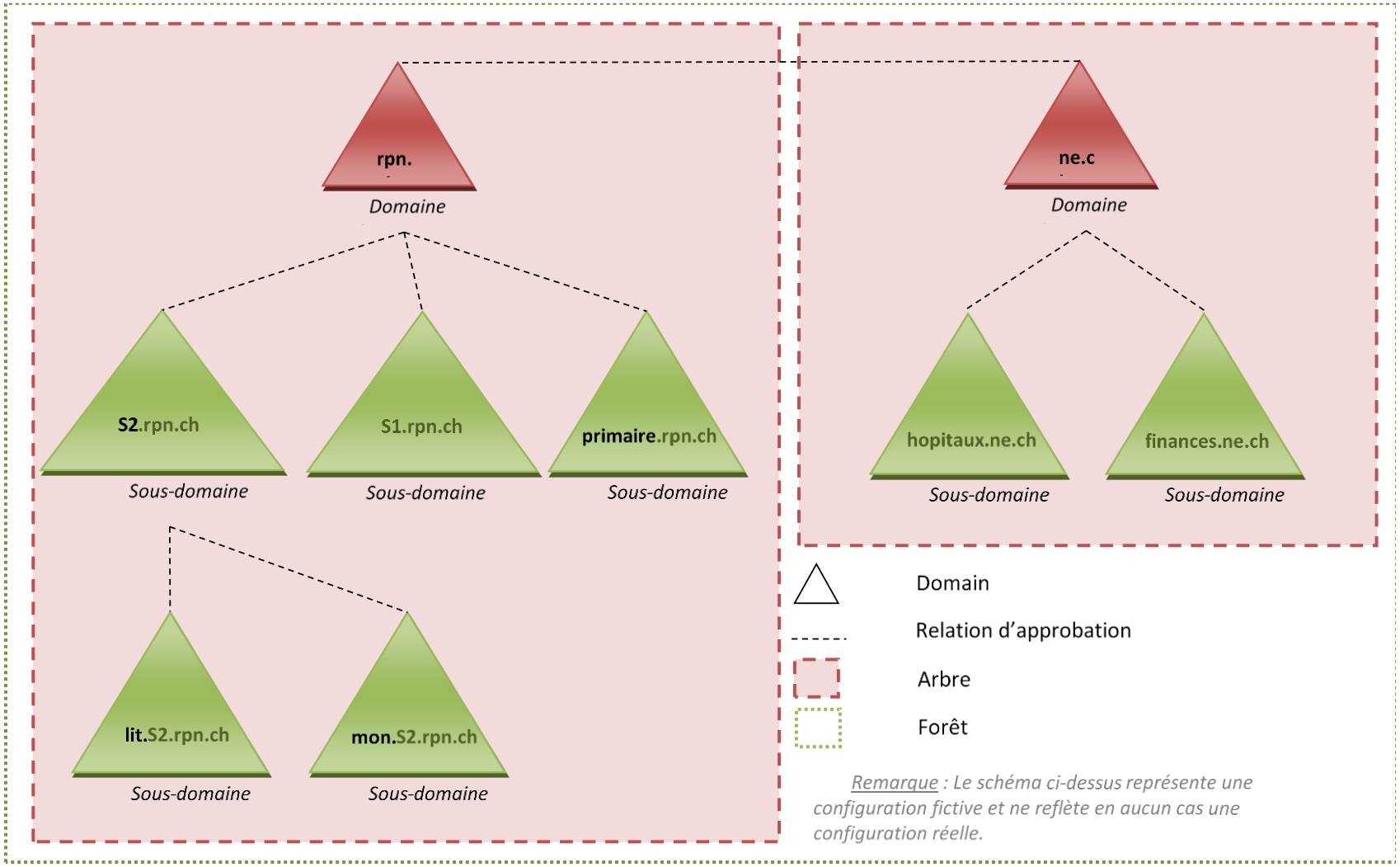
Une forêt est un groupe d'arbres (c'est sérieux!) qui ne forment pas un « espace de nom connexe ». C'est-à-dire que le nom commun qu'on retrouve dans tous les domaines d'un arbre ne se retrouve pas dans les autres arbres de la forêt (Voir schéma page suivante). Un arbre tout seul forme tout de même une forêt.

La nécessité de créer une forêt peut apparaître lors d'une fusion entre 2 entreprises, exemple : Swatch et Cartier qui possèdent tous deux leur arborescence respective.

1.2.7 Forêt particulière avec un seul arbre

Schéma de l'arborescence de domaine du RPN




rpn.
Domaine
ne.c
Domaine
S2.rpn.ch
Sous-domaine
S1.rpn.ch
Sous-domaine
primaire.rpn.ch
Sous-domaine
hopitaux.ne.ch
Sous-domaine
finances.ne.ch
Sous-domaine
lit.S2.rpn.ch
Sous-domaine
mon.S2.rpn.ch
Sous-domaine
Domain
Relation d'approbation
Arbre
Forêt
Remarque : Le schéma ci-dessus représente une configuration fictive et ne reflète en aucun cas une configuration réelle.

2 La notion de domaine : Active Directory

2.1 Définition d' « Active Directory »

Un des principaux avantages du réseau de type client-serveur, c'est la possibilité de centraliser la gestion des comptes-utilisateurs dans une base de données uniques : Active Directory (ou AD).

AD est une grande base de données dans laquelle seront répertoriés une grande partie des ressources informatiques du réseau. Ces ressources sont appelées Objets Active Directory :

- Les comptes utilisateurs
- Les groupes d'utilisateurs
- Les ordinateurs
- Les serveurs
- Les imprimantes

Le serveur sur lequel est installé l'AD se nomme « contrôleur de domaine ». On installe l'AD en ajoutant le rôle « Contrôleur de domaine » sur un serveur ou en « promouvant » votre serveur « contrôleur de domaine » (anciennement commande DCPROMO).

2.2 Avantages d'« Active Directory »

AD permet de simplifier la gestion du parc informatique : la gestion des ressources est centralisée à partir du contrôleur de domaine (et non sur chaque machine individuelle). Cela diminue considérablement le temps et les coûts de la maintenance.

En résumé, AD offre :

- Une administration simplifiée : Administration de toutes les ressources du réseau d'un point unique. Un administrateur peut se connecter sur n'importe quel ordinateur pour gérer les ressources de tout ordinateur du réseau.
- Centralisation : Active Directory permet de gérer, à un seul endroit, des millions d'objets répartis sur plusieurs sites (géographiquement éloignés) si cela est nécessaire.

2.3 Structure d'« Active Directory »

Dans les versions NT (avant 2000 serveur), les informations concernant les clients étaient contenues dans une base SAM. Depuis Windows 2000 Serveur, tous les composants du réseau sont intégrés dans Active Directory.

Chaque composant (utilisateurs, groupes, ordinateurs, …) est enregistré sous la forme d'un objet active directory. Une base peut contenir plusieurs millions d'objet. Chaque objet est composé d'un ensemble d'attributs qui sont représentatifs de l'objet. Par exemple l'objet utilisateur aura comme attributs le nom, le prénom, etc…

Active Directory doit être imaginé comme une immense base de données. Sa structure (ses tables, les attributs de chacun de ses objets, …) est appelé schéma de l'Active Directory.

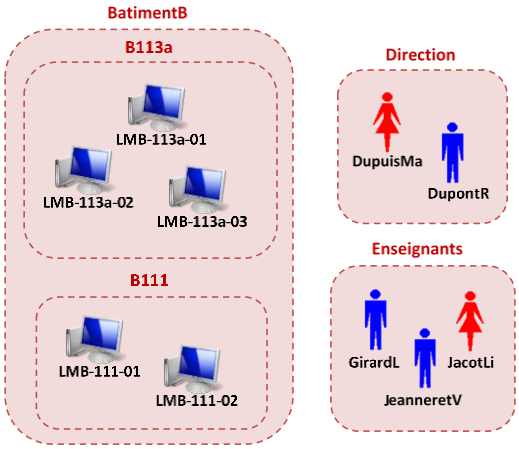
La structure d'Active Directory est hiérarchique, elle se décompose en :

- Objets
- Classe
- Unité organisationnelle (OU)
- Domaine
- Arbre
- Forêt

Les notions de domaine, arbre et forêt ont déjà été décrites dans le document "La notion de domaine – Partie 1". Décrivons maintenant ce qui se trouve à l'intérieur des domaines et des sous-domaines :

- **Objet :** Un Objet Active Directory est une ressource du réseau. Par exemple un ordinateur, un compte utilisateur, un groupe de sécurité, etc.
- **Classe :** Une classe est la description structurelle du type d'objet. Par exemple un utilisateur « DupontR » appartient à la classe « Utilisateurs » ou un ordinateur « LMB-113a-01 » appartient à la classe « Ordinateurs ».
- **Unité organisationnelle (OU) :** Une OU est un conteneur utilisé pour organiser les objets d'un domaine. Par exemple, tous les ordinateurs de la salle B113a seraient rassemblés dans l'OU « B113a ». Attention à ne pas confondre avec les groupes de sécurité! Les OU ne servent qu'à faire de l'ordre dans votre AD, aucun droit NTFS ne pourra être affecté à une OU. Elles servent aussi pour déployer des GPO ciblées (Group Policy Object, ou stratégie de groupe).

Dans la figure suivante, on voit apparaître des objets, des classes et des OU (unités organisationnelles) :



- ✓ **LMB-113a-01** est un objet de la classe « ordinateurs ».
- ✓ **DupontR** est un objet de la classe « utilisateurs ».
- ✓ **LMB-111-01 et LMB-111-02** sont regroupés dans l'OU **« B111 »**.
- ✓ Les OU **« B111 »** et **« B113a »** sont regroupés dans une OU parent nommée « **BatimentB** ».
- ✓ Le compte de **Mme Dupuis** (doyenne), ainsi que celui de **M. Dupont** (directeur) sont regroupés dans une OU **« Direction »**.
- ✓ Tous les comptes enseignants sont regroupés dans une OU **« Enseignants »**.

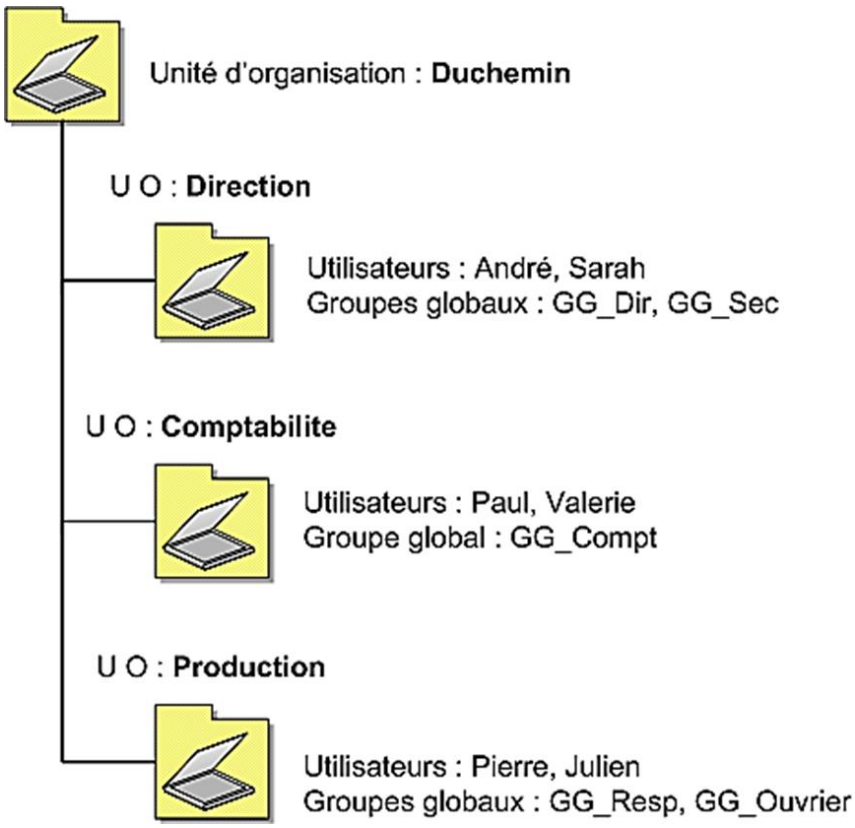
Les OU ne représentent pas nécessairement la structure physique des ressources du réseau (Mme Dupuis et M. Dupont ne se trouvent pas forcément dans le même bureau), mais la structure hiérarchique de l'établissement.

IMPORTANT : Les stratégies de groupe (GPO) sont appliquées sur les OU. Par exemple, on pourra définir une stratégie qui permet de forcer le changement du mot de passe tous les 3 mois et l'appliquer sur l'OU « Enseignants ». Ainsi, tous les comptes enseignants seront affectés par cette stratégie. Si on a besoin d'installer une mise-à-jour sur les postes de la salle B113a, on pourra créer une stratégie qui installe cette mise-à-jour et l'appliquer sur l'OU « B113a ». Ainsi, tous les ordinateurs de la salle B113a bénéficieront de cette mise-à-jour.

Information :
On constate alors qu'une bonne organisation de nos objets dans l'AD, via les OU, facilite la maintenance d'un grand parc informatique.

Il est fortement conseillé de bien réfléchir lors de la mise en place des OU et d'obtenir une décision commune (un consensus) ; toute l'équipe doit appliquer la même logique.

Représentation d'unités d'organisation dans Active Directory



2.4 Contrôleur(s) de domaine

Contrôleur(s) de domaine est le nom donné au(x) serveur(s) possédant la base de données AD.

Information :
C'est au moment où le premier contrôleur de domaine est installé que le domaine est créé.

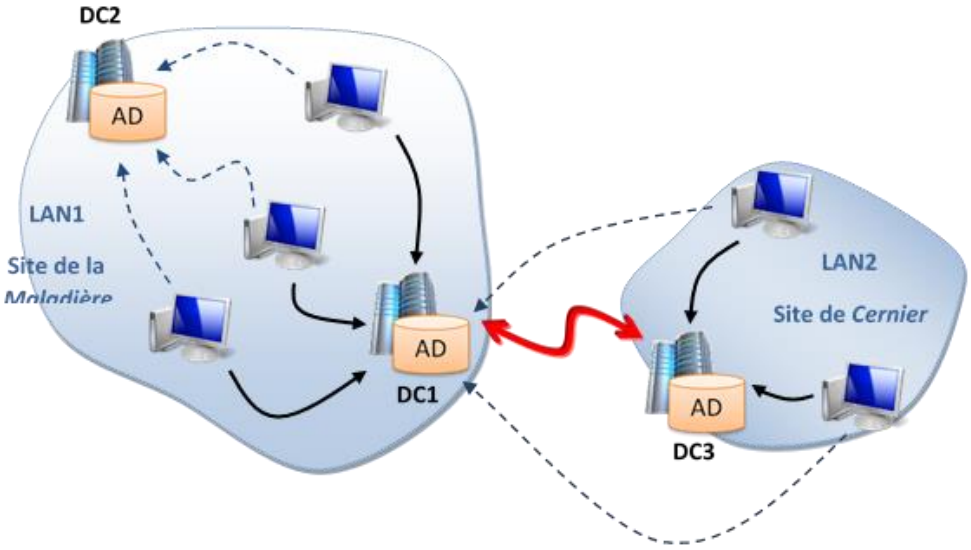
Un domaine ne peut exister sans contrôleur de domaine.

Un domaine peut posséder un ou plusieurs contrôleurs de domaine, ceci pour des questions de sécurité (redondance). Le nombre de contrôleur de domaine est défini selon la taille du parc informatique et la disposition géographique de celui-ci.

Information :
ATTENTION : Un contrôleur de domaine ne peut gérer qu'un seul domaine.

Une organisation de petite taille qui utilise un réseau local (LAN) unique peut se contenter d'un seul domaine avec deux contrôleurs de domaine. Si votre réseau est divisé en sites, il

est souvent conseillé de placer au moins un contrôleur de domaine dans chaque site pour améliorer les performances réseau. Lorsque les utilisateurs ouvrent une session sur le réseau, un contrôleur de domaine doit être contacté lors du processus d'ouverture de session. Si les clients doivent se connecter à un contrôleur de domaine situé dans un autre site, le processus d'ouverture de session peut être plus long. En cas de perte de la connexion, les utilisateurs pourront être authentifiés par le DC local.



2.5 Réplication de la base de données AD

Dans un environnement fonctionnant sous Windows Serveur, tous les contrôleurs de domaine stockent un répliqua (une copie) de la base d'annuaire Active Directory. Cela permet d'avoir une forte tolérance de pannes car tous les contrôleurs de domaine disposent de la même information.

Les objets du domaine (comptes utilisateurs, groupes, etc…) peuvent être modifiés depuis n'importe quel contrôleur de domaine. Pour maintenir l'intégrité et la cohérence des données stockées dans la base d'annuaire Active Directory, il est alors nécessaire d'avoir un processus qui s'occupe de mettre à jour les modifications sur l'ensemble des contrôleurs du domaine. Il s'agit de la réplication (ou duplication).

La réplication est donc un processus qui permet de synchroniser les données entre contrôleurs de domaine afin d'assurer le bon fonctionnement d'Active Directory.

On parlera plus précisément de réplication multi-maître car chaque contrôleur de domaine possède une copie de la base et peut répliquer les informations vers les autres contrôleurs. Ainsi, dans un domaine Windows 2000 - 2019 il n'y a plus de notions de serveurs primaires ou secondaires, tous les contrôleurs sont équivalents au niveau hiérarchique. Il subsiste un rôle de PDC pour le changement des mots de passe mais ce rôle peut être déplacé en cas de désastre.