

# Active Directory

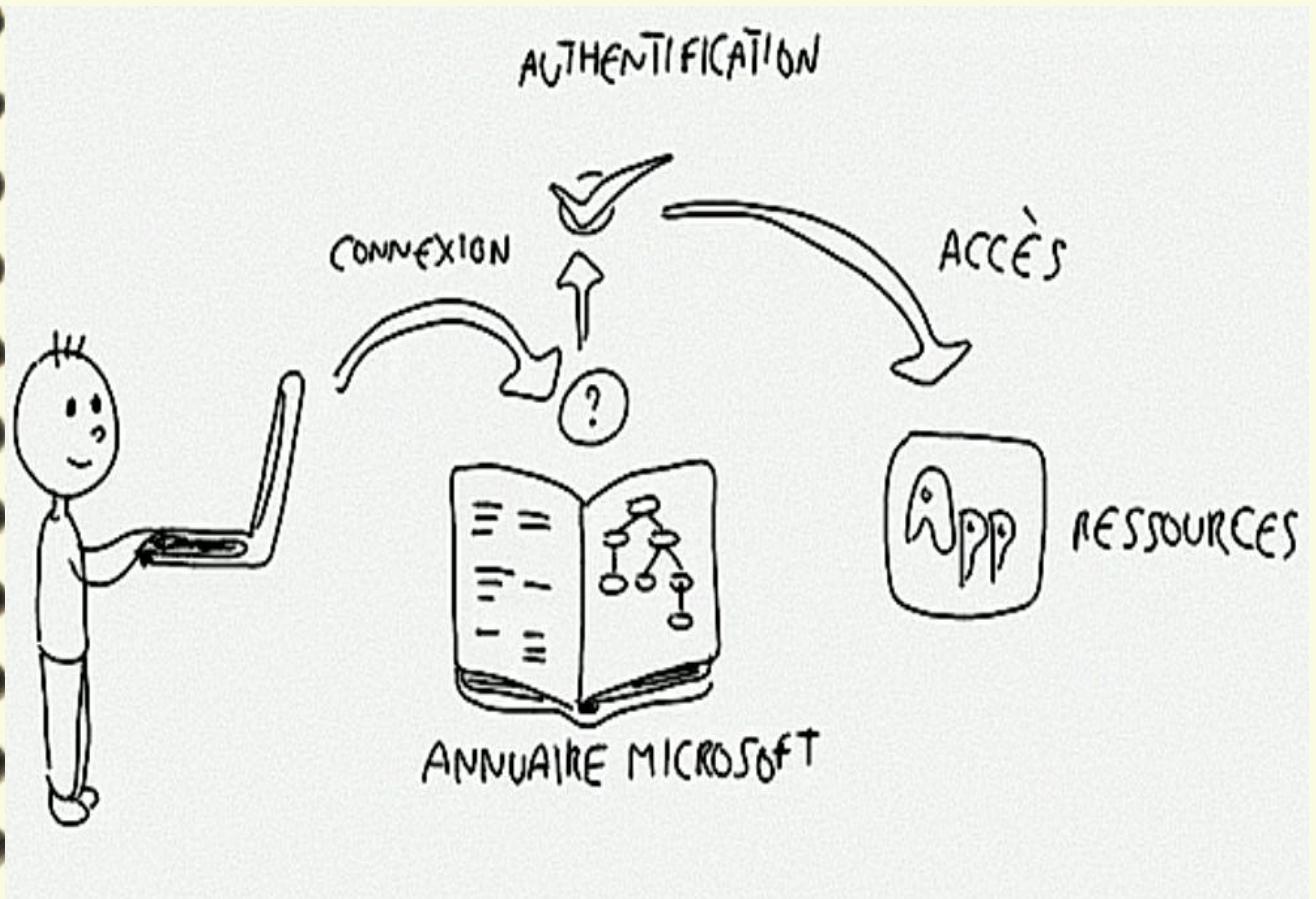
Comment assurer une administration centralisée ?

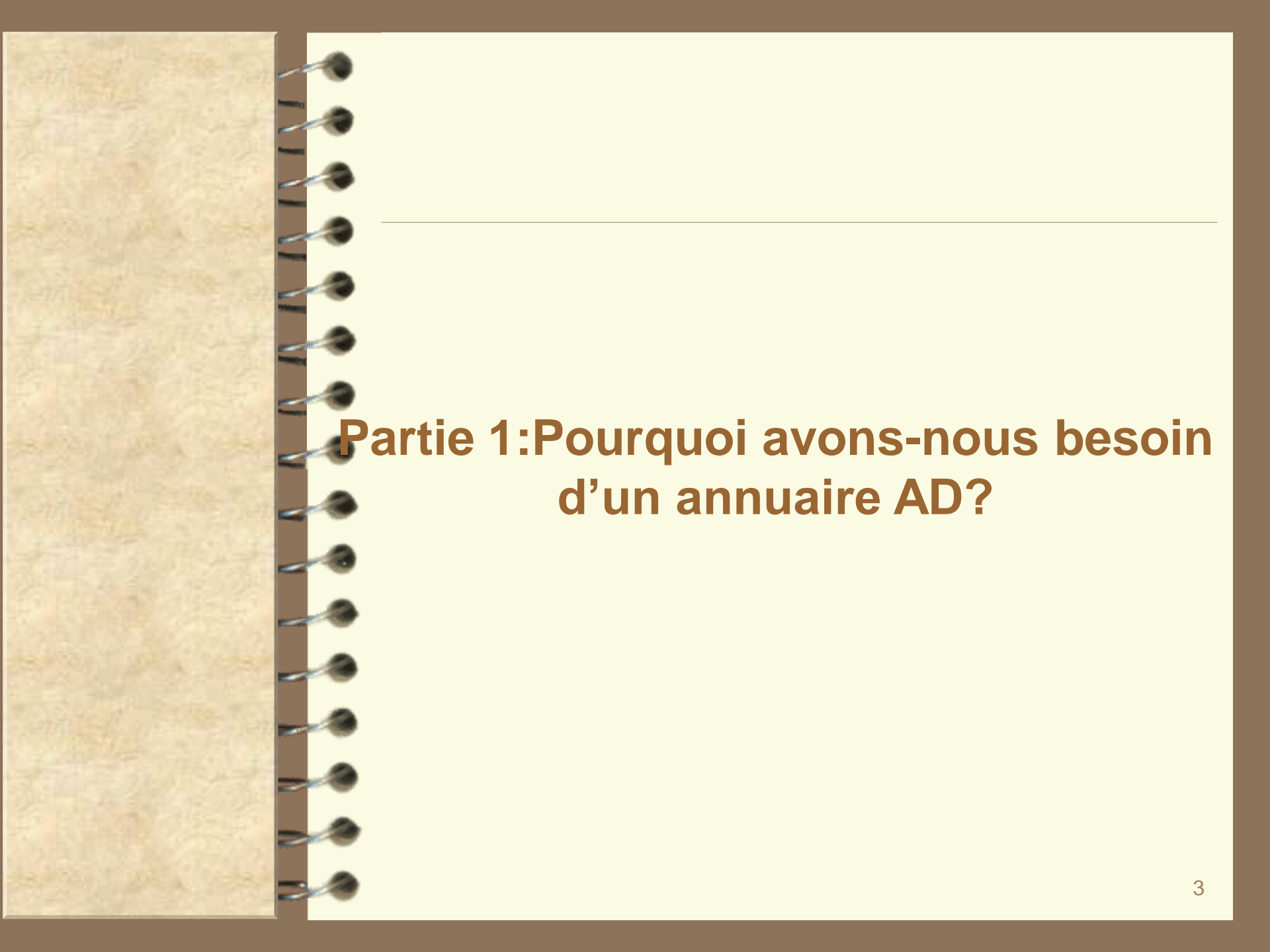
Intervenant : **ALI ABDALLAH**

Email: [alisillay2@gmail.com](mailto:alisillay2@gmail.com)

L3 Informatique

# Chapitre 4: Active Directory





## **Partie 1: Pourquoi avons-nous besoin d'un annuaire AD?**

# Plan du cours

---

- La nécessité d'avoir un annuaire AD
- Un peu d'histoire
- Présentation d'AD
  - Protocole LDAP
  - Protocole LDIF
- Objet d'un AD
- Les intérêts d'un annuaire
- La structure d'un AD
  - Les classes et les attributs
  - Le schéma
  - Les partitions d'annuaire

# L'utilité d'un annuaire AD

- L'Active Directory est un annuaire LDAP pour les systèmes d'exploitation Windows, le tout étant créé par Microsoft. Cet annuaire contient différents objets, de différents types (utilisateurs, ordinateurs, etc.), l'objectif étant de centraliser deux fonctionnalités essentielles : **l'identification** et **l'authentification** au sein d'un système d'information.
- Depuis Windows Server 2000, le service d'annuaire Active Directory ne cesse d'évoluer et de prendre de l'importance au sein des organisations dans lesquelles il est mis en place. De ce fait, il est notamment utilisé pour le déploiement de stratégie de groupe, la distribution des logiciels ou encore l'installation des mises à jour Windows.



# Un peu d'Histoire

---

- Avant l'apparition de l'AD, l'organisation d'un réseau s'articulait au tour de domaines non reliés entre eux ou lorsque cela était possible, la difficulté de la mise en relation était telle qu'elle en faisait râler plus d'un .
- De plus, la gestion du réseau était compliquée car chaque domaine nécessitait un administrateur et la modification des paramètres utilisateurs se faisait au cas par cas .
- l'Active Directory se nommait d'abord « **NTDS** » pour « NT Directory Services » que l'on peut traduire littéralement par « **Service d'annuaire de NT** », le tout à l'époque de Windows NT.

# Présentation

---

- **Active Directory** est un annuaire global permettant d'administrer à partir d'un point unique toutes les ressources (*applications, serveurs, imprimantes, groupes, ordinateurs* ) et les utilisateurs .
- Cet annuaire enregistre sous la forme hiérarchique les informations relatives aux objets du réseau et met ses informations à la disposition des administrateurs, des utilisateurs et des applications à l'aide de deux technologies:

**LDAP et LDIF**

# Présentation

## Protocole LDAP

---

- **LDAP** (*Lightweight Directory Access Protocol*) définit la méthode d'accès aux données sur le serveur au niveau du client et non la manière avec laquelle les informations sont stockées. Ce protocole repose sur TCP/IP.
- LDAP fournit à l'utilisateur des méthodes lui permettant de :
  - Se connecter, se déconnecter,
  - Rechercher des informations ,
  - Comparer des informations ,
  - Insérer des entêtes ,
  - Modifier des entrées ,
  - Supprimer des entrées ,
  - Etc. ...



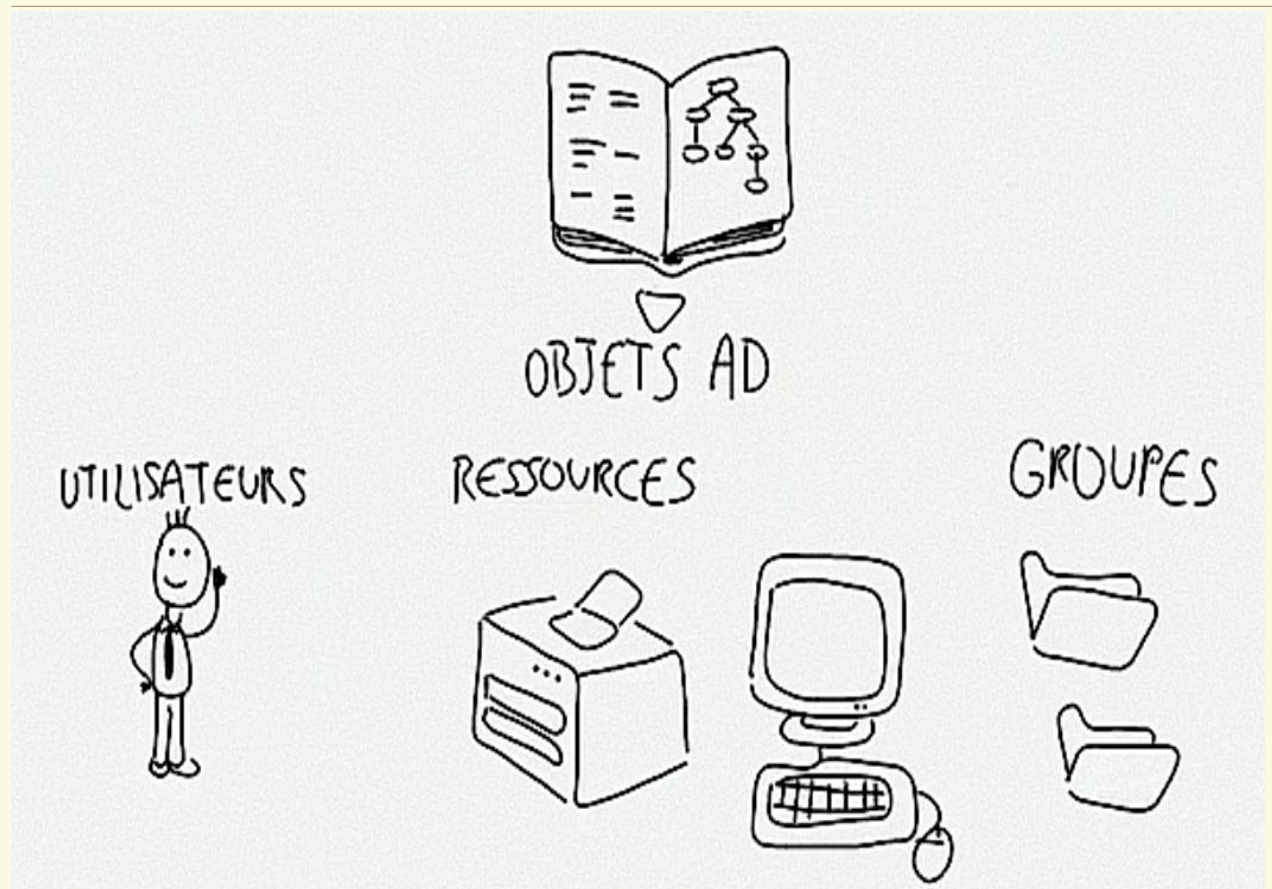
# Présentation

## Protocole LDIF

---

- **LDIF** (*LDAP Data Interchange Format*) est un format standardisé d'échange de données contenues dans un annuaire LDAP (AD).
- Il permet aussi la représentation d'opération sur les données de l'annuaire telle que l'ajout, la modification et la suppression .
- Cet annuaire permet d'organiser le réseau et ses objets à l'aide d'entités telles que les domaines , les arborescences, les forets, les relations d'approbation, les unités d'organisations et les sites .

# Objet d'un AD



# Les intérêts d'un Annuaire

---

L'importante présence de l'Active Directory dans les entreprises suffit pour se convaincre de ses intérêts, mais alors, quels sont ces derniers ?

Administration  
centralisée et  
simplifiée

Unifier  
l'authentification

Identifier les  
objets sur le  
réseau

Référencer les  
utilisateurs et  
ordinateurs

# Les intérêts d'un Annuaire

---

- **Administration centralisée et simplifiée** : la gestion des objets, notamment des comptes utilisateurs et ordinateurs est simplifiée, car tout est centralisé dans l'annuaire Active Directory. De plus, on peut s'appuyer sur cet annuaire pour de nombreuses tâches annexes comme le déploiement de stratégies de groupe sur ces objets .

# Les intérêts d'un Annuaire

- **Unifier l'authentification** : un utilisateur authentifié sur une machine, elle-même authentifiée, pourra accéder aux ressources stockées sur d'autres serveurs ou ordinateurs enregistrés dans l'annuaire (à condition d'avoir les autorisations nécessaires). Ainsi, une authentification permettra d'accéder à tout un système d'information par la suite, surtout que de nombreuses applications sont capables de s'appuyer sur l'Active Directory pour l'authentification. **Un seul compte peut permettre un accès à tout le système d'information**, ce qui est fortement intéressant pour les collaborateurs.



# Les intérêts d'un Annuaire

---

- Identifier les objets sur le réseau : chaque objet enregistré dans l'annuaire est unique, ce qui permet d'identifier facilement un objet sur le réseau et de le retrouver ensuite dans l'annuaire.

# Les intérêts d'un Annuaire

---

- **Référencer les utilisateurs et les ordinateurs** : l'annuaire s'apparente à une énorme base de données qui référence les utilisateurs, les groupes et les ordinateurs d'une entreprise. On s'appuie sur cette base de données pour réaliser de nombreuses opérations : authentification, identification, stratégie de groupe, déploiement de logiciels, etc.

# I. Structure de l'AD

## A. Les classes et les attributs

Au sein de l'annuaire Active Directory, il y a différents types d'objets, comme par exemple les utilisateurs, les ordinateurs, les serveurs, les unités d'organisation ou encore les groupes.

En fait, ces objets correspondent à des **classes**, **c'est-à-dire des objets disposant des mêmes attributs**.

De ce fait, un objet ordinateur sera une instance d'un objet de la classe « Ordinateur » avec des valeurs spécifiques à l'objet concerné.

Certains objets peuvent être des containers d'autres objets, ainsi, les groupes permettront de contenir plusieurs objets de types utilisateurs afin de les regrouper et de simplifier l'administration.

# I. Structure de l'AD

## A. Les classes et les attributs

Par ailleurs, les unités d'organisation sont des containers d'objets afin de faciliter l'organisation de l'annuaire et de permettre une organisation avec plusieurs niveaux.

Sans les unités d'organisations, l'annuaire ne pourrait pas être trié correctement et l'administration serait moins efficace.

Comparer les unités d'organisations à des dossiers qui permettent de ranger les objets à l'intérieur.

# I. Structure de l'AD

## B. Le schéma

Par défaut, tout annuaire Active Directory dispose de classes prédéfinies ayant chacune une liste d'attributs bien spécifique, et propre à tout annuaire, cela est défini grâce à **un schéma**.

Le schéma contient la définition de toutes les classes et de tous les attributs disponibles et autorisés au sein de l'annuaire. Il est à noter que le schéma est évolutif, le modèle de base n'est pas figé et peut évoluer selon les besoins.



# I. Structure de l'AD

## B. Le schéma

---

**Par exemple**, l'application de messagerie Microsoft Exchange effectue des modifications au schéma lors de son installation.

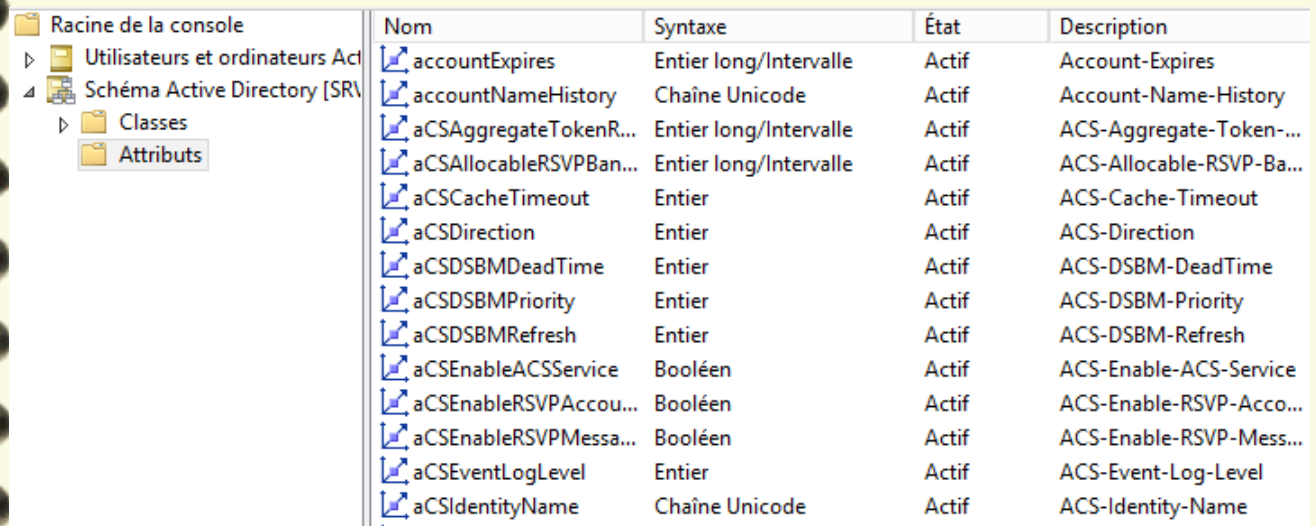
Les modifications du schéma doivent être réalisées avec précaution, car l'impact est important et se ressentira sur toute la classe d'objets concernée.

Pour preuve, le schéma est protégé et les modifications contrôlées, puisque seuls les membres du groupe « **Administrateurs du schéma** » peuvent, par défaut, effectuer des modifications.

# I. Structure de l'AD

## B. Le schéma

**Par exemple,** l'application de messagerie Microsoft Exchange effectue des modifications au schéma lors de son installation.



Nom	Syntaxe	État	Description
accountExpires	Entier long/Intervalle	Actif	Account-Expires
accountNameHistory	Chaîne Unicode	Actif	Account-Name-History
aCSAggregateTokenR...	Entier long/Intervalle	Actif	ACS-Aggregate-Token-...
aCSAllocableRSVPBan...	Entier long/Intervalle	Actif	ACS-Allocable-RSVP-Ba...
aCSCacheTimeout	Entier	Actif	ACS-Cache-Timeout
aCSDirection	Entier	Actif	ACS-Direction
aCSDSBMDeadTime	Entier	Actif	ACS-DSBM-DeadTime
aCSDSBMPriority	Entier	Actif	ACS-DSBM-Priority
aCSDSBMRefresh	Entier	Actif	ACS-DSBM-Refresh
aCSEnableACSService	Booléen	Actif	ACS-Enable-ACS-Service
aCSEnableRSVPAccou...	Booléen	Actif	ACS-Enable-RSVP-Acco...
aCSEnableRSVPMessa...	Booléen	Actif	ACS-Enable-RSVP-Mess...
aCSEventLogLevel	Entier	Actif	ACS-Event-Log-Level
aCSIdentityName	Chaîne Unicode	Actif	ACS-Identity-Name

# I. Structure de l'AD

## C. les partitions d'annuaire

La base de données Active Directory est divisée de **façon logique** en trois partitions de répertoire (appelé « **Naming Context** »). Ces trois partitions sont la partition de schéma, la partition de configuration, et la partition de domaine.

**La partition de schéma :** cette partition contient l'ensemble des définitions des classes et attributs d'objets, qu'il est possible de créer au sein de l'annuaire Active Directory. Cette partition est unique au sein d'une forêt.

# I. Structure de l'AD

## C. les partitions d'annuaire

---

**La partition de configuration** : cette partition contient la topologie de la forêt (informations sur les domaines, les liens entre les contrôleurs de domaines, les sites, etc.). Cette partition est unique au sein d'une forêt.

# I. Structure de l'AD

## C. les partitions d'annuaire

---

**La partition de domaine** : cette partition contient les informations de tous les objets d'un domaine (ordinateur, groupe, utilisateur, etc.). Cette partition est unique au sein d'un domaine, il y aura donc autant de partitions de domaine qu'il y a de domaines.



A spiral-bound notebook with a textured, light brown cover is shown on the left. The right page is a plain, off-white sheet of paper. A horizontal line is drawn across the upper portion of this page. The text 'Partie 2: Comment présenter un contrôleur de domaine et un domaine ?' is written in a bold, brown font, centered on the page below the line.

---

## **Partie 2: Comment présenter un contrôleur de domaine et un domaine ?**

# Plan du cours

---

- Du groupe de travail au domaine
  - Modèle « groupe de travail »
  - Modèle « Domaine »
- Les contrôleurs de domaine
  - Qu'est ce qu'un contrôleur de domaine ?
  - Le fichier de base de données NTDS.dit
  - La réplication des contrôleurs de domaine

# Du groupe de travail au domaine

## A. Modèle « Groupe de travail »

---

Pour continuer l'apprentissage de l'Active Directory, il est intéressant de voir ce que représente le passage du mode « Groupe de travail » au mode « Domaine ».

Pour rappel, toutes les machines sous Windows sont par défaut dans un groupe de travail nommé « WORKGROUP », et qui permet de mettre en relation des machines d'un même groupe de travail, notamment pour le partage de fichiers, mais il n'y a pas de notions d'annuaire, ni de centralisation avec ce mode de fonctionnement.

# Du groupe de travail au domaine

## A. Modèle « Groupe de travail »

---

- Une base d'utilisateurs par machine : appelée « base SAM », cette base est unique sur chaque machine et non partagée, ainsi, chaque machine contient sa propre base d'utilisateurs indépendante les unes des autres.
- Très vite inadapté dès que le nombre de postes et d'utilisateurs augmente, car cela devient lourd en administration et les besoins différents.

# Du groupe de travail au domaine

## A. Modèle « Groupe de travail »

---

- Création des comptes utilisateurs en nombre, car chaque utilisateur doit disposer d'un compte sur chaque machine, les comptes étant propres à chaque machine.
- Simplicité de mise en œuvre et ne nécessite pas de compétences particulières en comparaison à la gestion d'un annuaire Active Directory.

# Du groupe de travail au domaine

## B. Modèle « Domaine »

- Base d'utilisateurs, de groupes et d'ordinateurs centralisée. Un seul compte utilisateur est nécessaire pour accéder à l'ensemble des machines du domaine.
- L'annuaire contient toutes les informations relatives aux objets, tout est centralisé sur le contrôleur de domaine, il n'y a pas d'éparpillement sur les machines au niveau des comptes utilisateurs.
- Ouverture de session unique par utilisateur, notamment pour l'accès aux ressources situées sur un autre ordinateur ou serveur.



# Du groupe de travail au domaine

## B. Modèle « Domaine »

---

- Chaque contrôleur de domaine contient une copie de l'annuaire, qui est maintenue à jour et qui permet d'assurer la disponibilité du service et des données qu'il contient. Les contrôleurs de domaine se répliquent entre eux pour assurer cela.
- Administration et gestion de la sécurité centralisée.

# Contrôleur de domaine

## A. Qu'est ce qu'un CDD?

- Lorsque l'on crée un domaine, le serveur depuis lequel on effectue cette création est promu au rôle de « contrôleur de domaine » du domaine créé. Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine. De ce fait, il devra vérifier les identifications des objets, traiter les demandes d'authentification, veiller à l'application des stratégies de groupe ou encore stocker une copie de l'annuaire Active Directory.
- Un contrôleur de domaine est indispensable au bon fonctionnement du domaine, si l'on éteint le contrôleur de domaine ou qu'il est corrompu, **le domaine devient inutilisable.**

# Contrôleur de domaine

## A. Qu'est ce qu'un CDD?

- De plus, lorsque l'on crée le premier contrôleur de domaine dans une organisation, il en est également le premier domaine, la première forêt, ainsi que le premier site.
- Il est à souligner qu'un contrôleur de domaine est un serveur qui contient une copie de l'annuaire Active Directory.

# Contrôleur de domaine

## B. Fichier de base de données NTDS.dit?

- Sur chaque contrôleur de domaine, on trouve une copie de la base de données de l'annuaire Active Directory.
- Cette copie est symbolisée par un fichier « **NTDS.dit** » qui contient l'ensemble des données de l'annuaire.

À noter qu'il est possible de réaliser des captures instantanées de ce fichier afin de le consulter en mode « hors ligne » avec des outils spécifiques.

# Contrôleur de domaine

## C. La réplication des contrôleurs de domaine

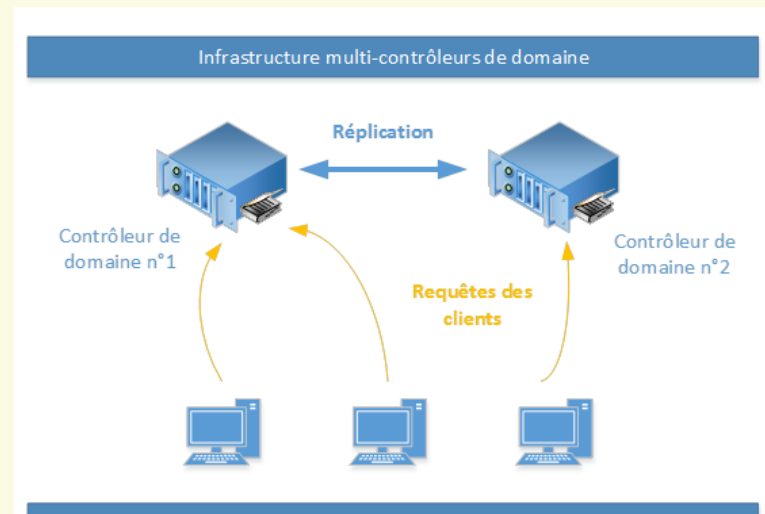
- De nos jours, il est inévitable d'avoir au minimum deux contrôleurs de domaine pour assurer la **disponibilité et la continuité de service des services d'annuaire**. De plus, cela permet d'assurer la pérennité de la base d'annuaire qui est très précieuse.
- À partir du moment où une entreprise crée un domaine, même si ce domaine est unique, il est important de mettre en place au minimum deux contrôleurs de domaine.



# Contrôleur de domaine

## C. La réplication des contrôleurs de domaine

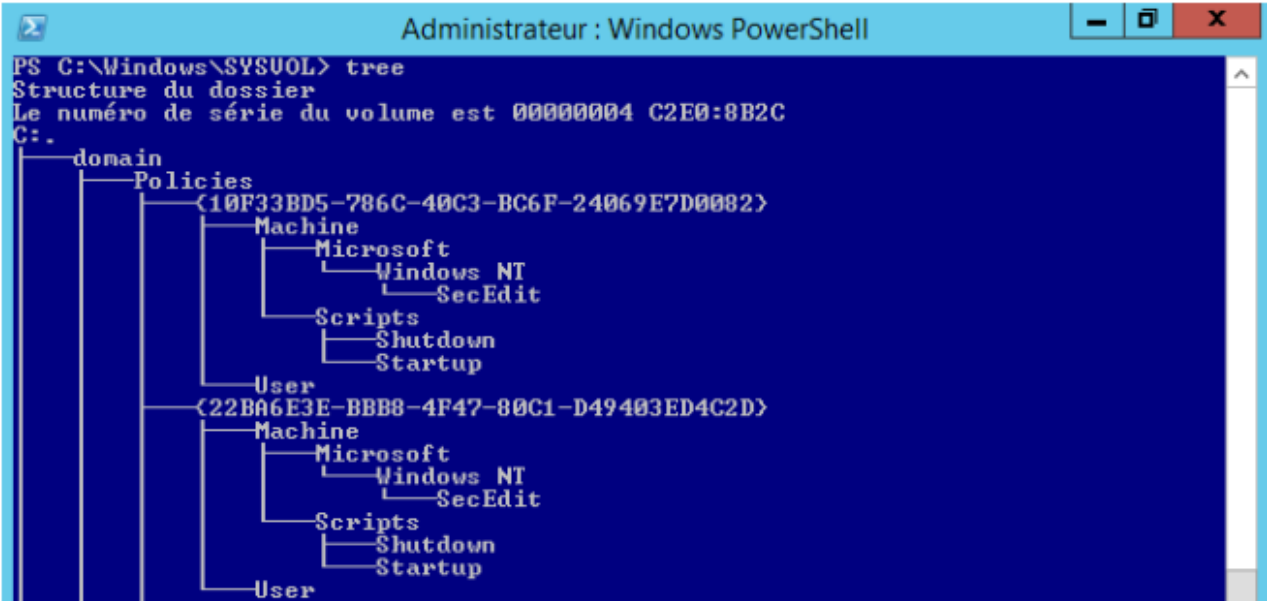
- Sur les anciennes versions de Windows Server, notamment Windows Server 2000 et Windows Server 2003, le mécanisme **FRS** (File Replication Service) était utilisé pour la réplication.
- Depuis Windows Server 2008, FRS est mis de côté pour laisser la place à **DFSР** (Distributed File System Replication), qui est plus fiable et plus performant.



# Contrôleur de domaine

## C. La réplication des contrôleurs de domaine

- Par ailleurs, les contrôleurs de domaine répliquent le dossier partagé « SYSVOL » qui est utilisé pour distribuer les stratégies de groupe et les scripts de connexion.



```
Administrateur : Windows PowerShell
PS C:\Windows\SYSVOL> tree
Structure du dossier
Le numéro de série du volume est 00000004 C2E0:8B2C
C:.\
├── domain
│   ├── Policies
│   │   ├── {10F33BD5-786C-40C3-BC6F-24069E7D0082}
│   │   │   ├── Machine
│   │   │   │   ├── Microsoft
│   │   │   │   │   ├── Windows NT
│   │   │   │   │   └── SecEdit
│   │   │   └── Scripts
│   │   │       ├── Shutdown
│   │   │       └── Startup
│   │   └── User
│   │       ├── {22BA6E3E-BBB8-4F47-80C1-D49403ED4C2D}
│   │       │   ├── Machine
│   │       │   │   ├── Microsoft
│   │       │   │   │   ├── Windows NT
│   │       │   │   │   └── SecEdit
│   │       │   └── Scripts
│   │       │       ├── Shutdown
│   │       │       └── Startup
│   │       └── User
```

Structure du dossier SYSVOL

A spiral-bound notebook is shown from a top-down perspective. The left side features a textured, brownish-gold cover. The right side is a cream-colored page with a horizontal line near the top. The spiral binding is visible in the center, with the wire looping through a series of holes. The text 'Partie 3: Notion de domaine, arbre et forêt' is printed in a bold, brown font on the cream page.

## **Partie 3: Notion de domaine, arbre et forêt**

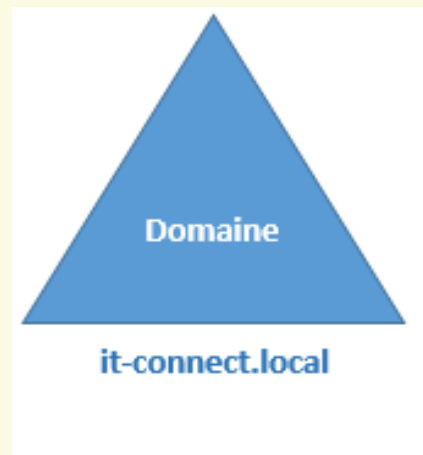
# Plan du cours

---

- Symbolisation d'un domaine
- Notion d'arbre
- Notion de foret
- Niveau fonctionnel
  - Définition d'un Niveau fonctionnel
  - Pourquoi augmenter le niveau fonctionnel ?
  - Quelle est la portée d'un niveau fonctionnel ?
- Ce qu'il faut retenir

# Symbolisation d'un domaine

Les schémas d'architecture Active Directory sont représentés par des triangles. Ainsi, le domaine « **it-connect.local** » pourrait être schématisé ainsi :

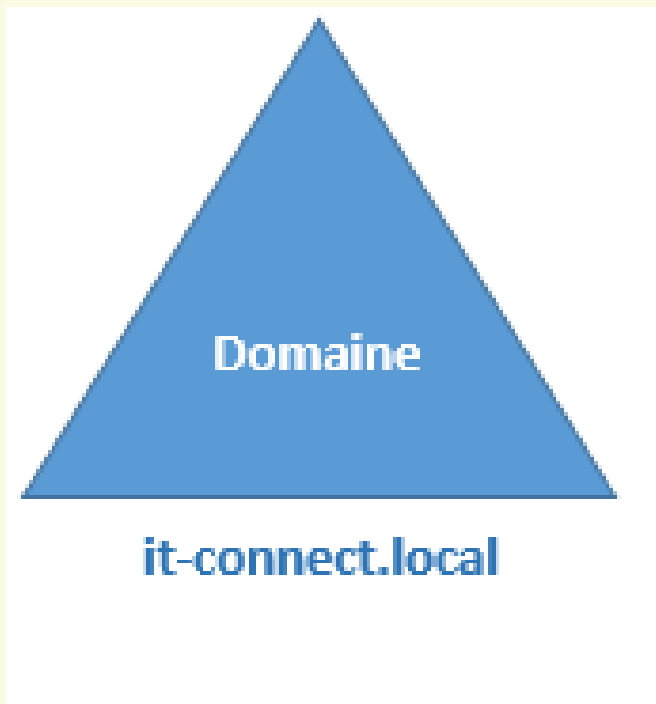


On retrouvera tout un ensemble d'Unités d'Organisation remplies d'objets de différentes classes : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, etc.



# Symbolisation d'un domaine

Au sein du domaine ci-dessous, on retrouvera tout un ensemble d'Unités d'Organisation remplies d'objets de différentes classes : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, etc.



# Symbolisation d'un domaine

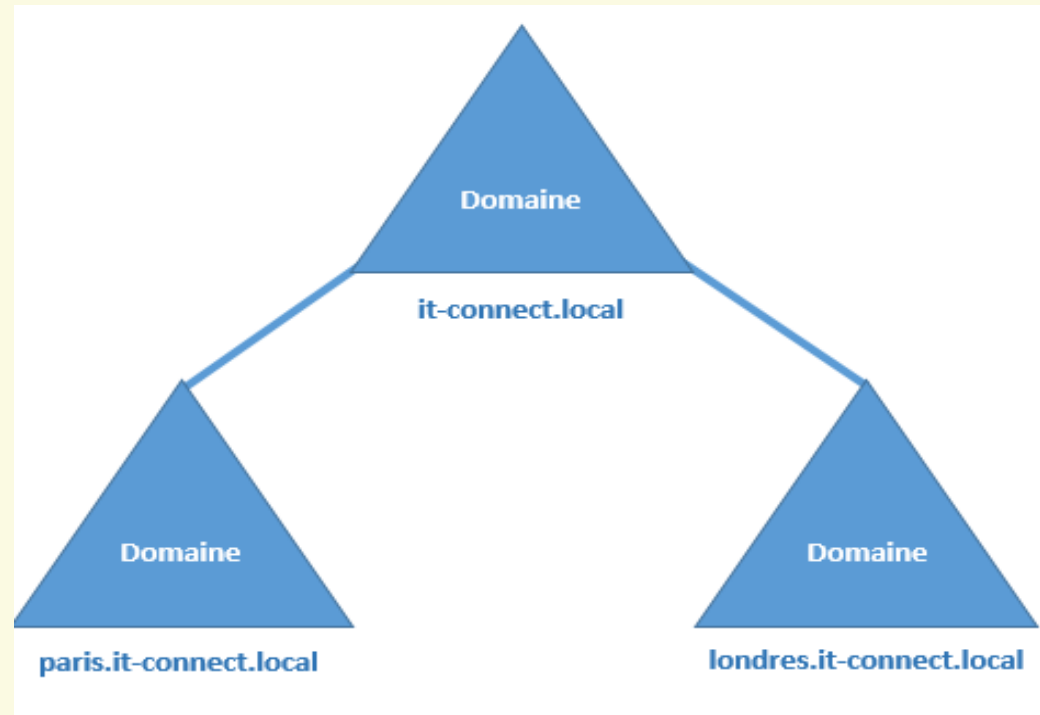
---

Des nombreuses entreprises ont plusieurs succursales, ce qui implique plusieurs sites sur différents emplacements géographiques. Selon l'importance de ces sites, on pourra envisager de créer un sous-domaine au domaine principal, voire même plusieurs sous-domaines selon le nombre de succursales. Prenons un exemple.

On part du domaine de base « **it-connect.local** », auquel on ajoute deux sous-domaines : « paris.it-connect.local » et « londres.it-connect.local » puisque nous avons deux succursales, une à Paris, l'autre à Londres.

# Symbolisation d'un domaine

Voici la représentation de cette arborescence :



Sur le cas ci-dessus, les domaines « **paris.it-connect.local** » et « **londres.it-connect.local** » sont des sous-domaines du domaine racine « **it-connect.local** ». On appelle généralement ces domaines, « **des domaines enfants** ».

# La Notion d'arbre

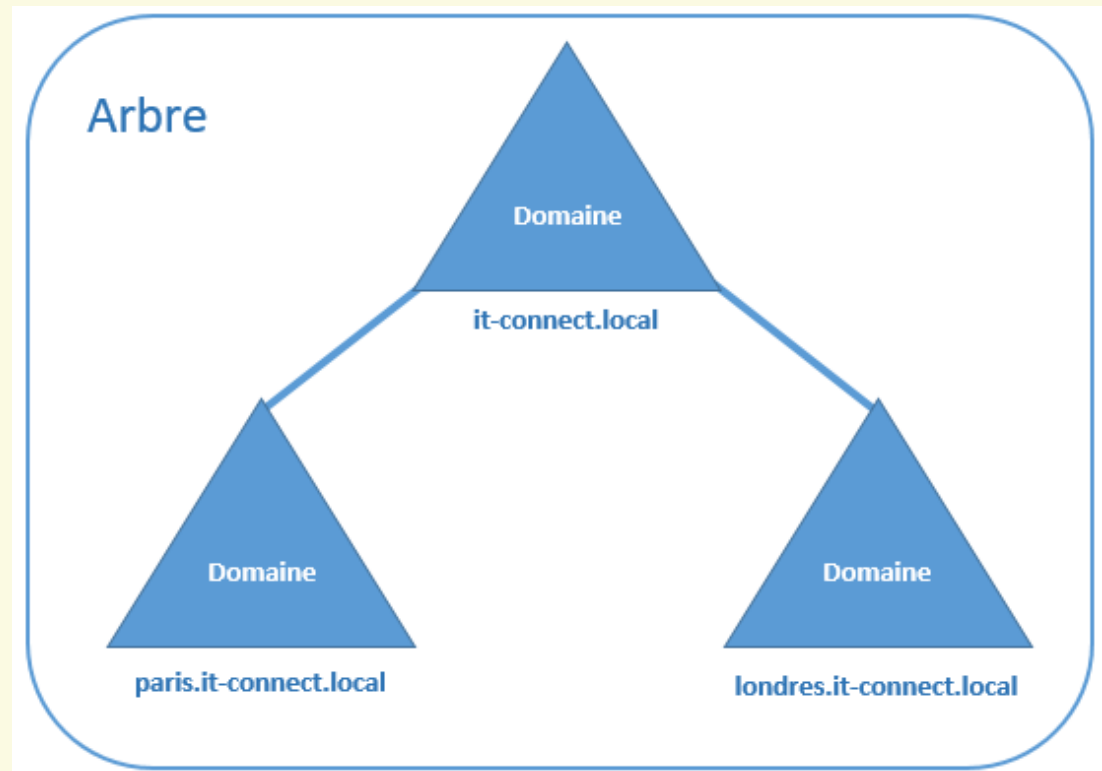
---

- La notion d'arbre nous fait penser à un ensemble avec différentes branches.
- En effet, lorsqu'un domaine principal contient plusieurs sous-domaines, on parle alors d'arbre, où chaque sous-domaine au domaine racine représente une branche de l'arbre.

**Un arbre est un regroupement hiérarchique de plusieurs domaines.**

# La Notion d'arbre

- Par exemple, la schématisation des domaines utilisés précédemment représente un arbre :





# La Notion d'arbre

---

Une forêt , c'est un ensemble d'arbres, alors vous avez déjà compris le principe de la notion de « forêt » dans un environnement Active Directory.

En effet, une forêt est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres. Ces arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt.

L'exemple que nous utilisons jusqu'à maintenant avec le domaine principal et les deux sous domaines représente une forêt. Seulement, cette forêt ne contient qu'un seul arbre.

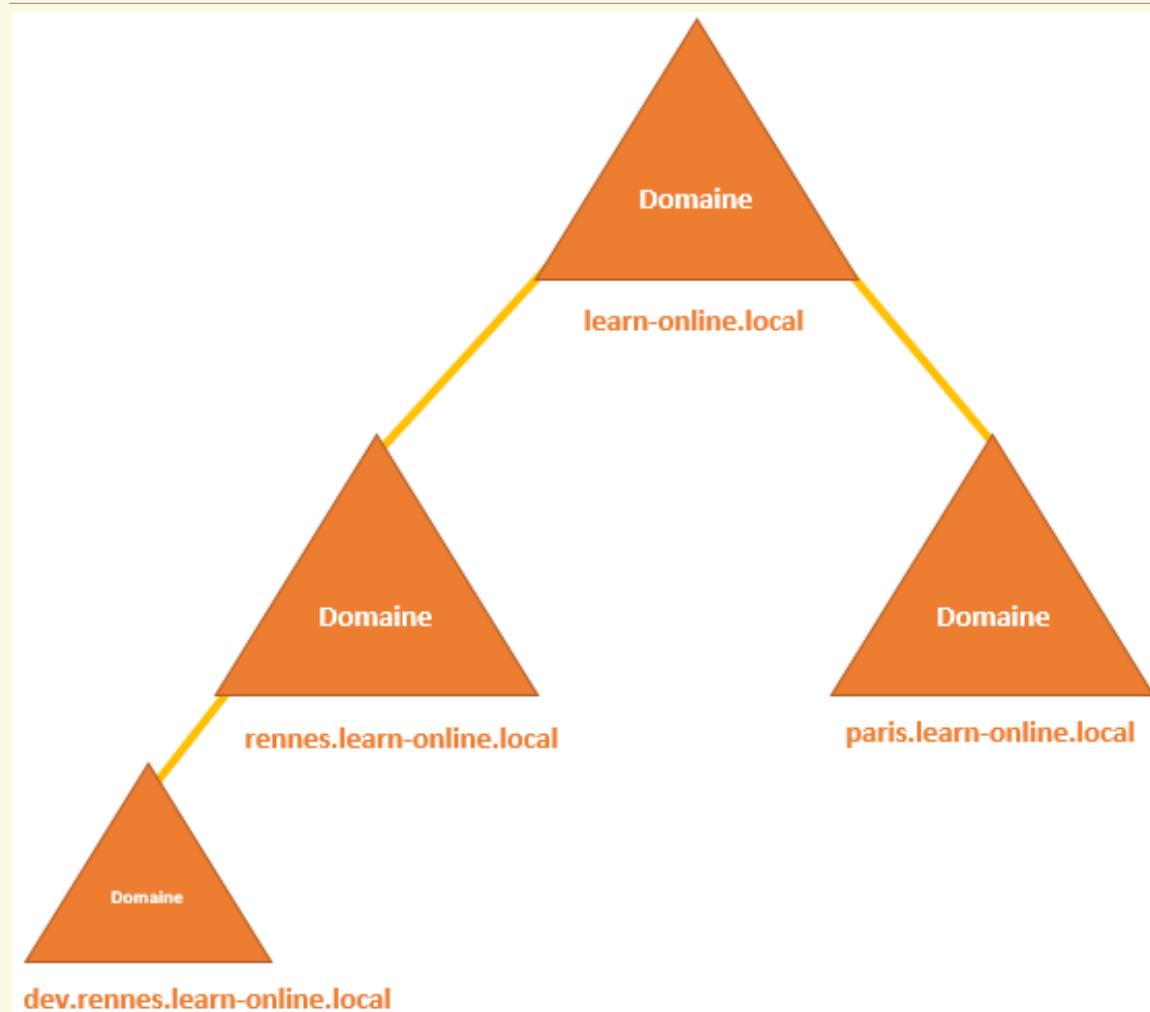
# La Notion d'arbre

---

Imaginons maintenant que nous rachetons la société « **Learn-Online** » et que nous décidons de créer un domaine racine « **learn-online.local** », ainsi que trois sous-domaines pour les deux succursales situées à Paris et Rennes, et un troisième sous-domaine pour un environnement de développement situé à Rennes.

On obtiendra : **paris.learn-online.local**, **rennes.learn-online.local** et **dev.rennes.learn-online.local**. On obtiendra un arbre avec la racine « **learn-online.local** ».

# La Notion d'arbre



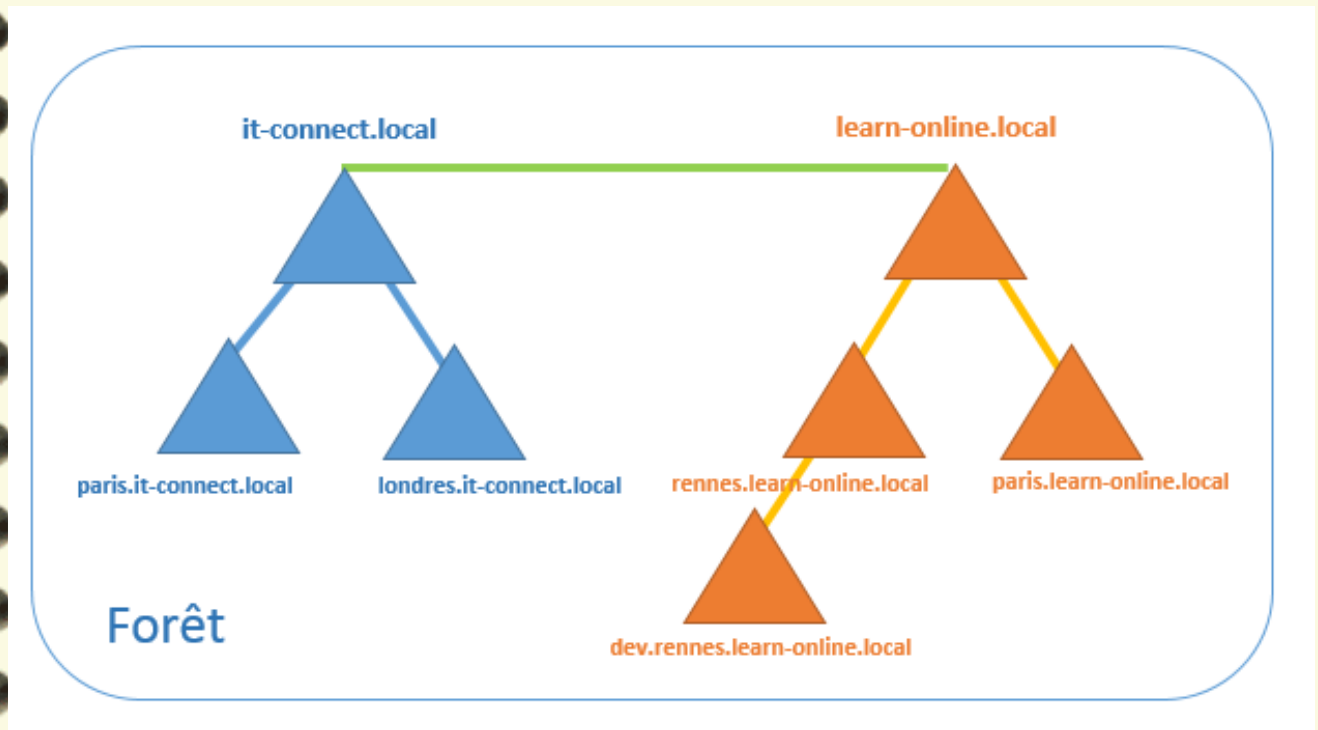
# La Notion d'arbre

---

- Pour simplifier l'administration, les accès et unifier le système d'information, on peut décider de créer cet arbre « Learn-Online » dans la même forêt que celle où se situe l'arbre « IT-Connect ».
- On peut alors affirmer que les différentes arborescences d'une forêt ne partagent pas le même espace de nom et la même structure

# La Notion d'arbre

- Ainsi, on obtiendra une jolie forêt :



# La Notion d'arbre

Mais alors, une forêt pour quoi faire ?

- Tous les arbres d'une forêt partagent un schéma d'annuaire commun
- Tous les domaines d'une forêt partagent un « Catalogue Global » **commun (nous verrons plus tard ce qu'est un catalogue global)**
- Les domaines d'une forêt fonctionnent de façon indépendante, mais la forêt facilite les communications entre les domaines, c'est-à-dire dans toute l'architecture.
- Création de relations entre les différents domaines de la forêt.



# La Notion d'arbre

---

- Simplification de l'administration et flexibilité. Un utilisateur du domaine « **paris.it-connect.local** » pourra accéder à des ressources situées dans le domaine « **rennes.learn-online.local** » ou se connecter sur une machine du domaine « **paris.learn-online.local** », si les autorisations le permettent.

# Le niveau fonctionnel

## A. Comment définir un niveau fonctionnel ?

---

Un niveau fonctionnel détermine les fonctionnalités des services de domaine Active Directory qui sont disponibles dans un domaine ou une forêt.

Le niveau fonctionnel permet de limiter les fonctionnalités de l'annuaire au niveau actuel afin d'assurer la compatibilité avec les plus anciennes versions des contrôleurs de domaine.

# Le niveau fonctionnel

## B. Pourquoi augmenter le niveau fonctionnel ?

Plus le niveau fonctionnel est haut, plus on peut bénéficier des dernières nouveautés liées à l'Active Directory et à sa structure. Ce qui rejoint la réponse à la question précédente.

Par ailleurs, on est obligé d'augmenter le niveau fonctionnel pour ajouter la prise en charge des derniers systèmes d'exploitation Windows pour les contrôleurs de domaine.

Par exemple, si le niveau fonctionnel est

« **Windows Server 2003** », on ne pourrait pas ajouter un nouveau contrôleur de domaine sous Windows Server 2012 et les versions plus récentes.

# Le niveau fonctionnel

## B. Pourquoi augmenter le niveau fonctionnel ?

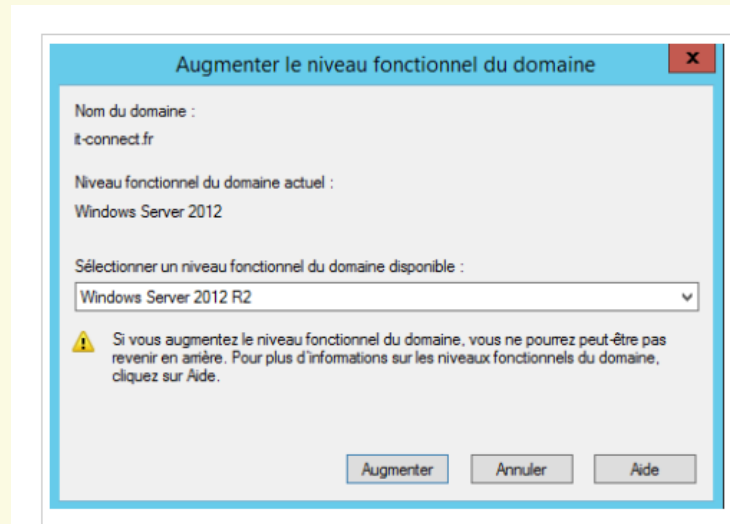
Ce phénomène implique qu'il est bien souvent inévitable d'augmenter le niveau fonctionnel lorsque l'on effectue une migration, afin de pouvoir supporter les nouveaux OS utilisés.

À l'inverse, si le niveau fonctionnel est « Windows Server 2012 », il sera impossible d'intégrer de nouveaux contrôleurs de domaine qui utilisent un système d'exploitation plus ancien que Windows Server 2012.

De plus, vous ne pouvez pas avoir un niveau fonctionnel plus haut que la version de votre contrôleur de domaine le plus récent.

# Le niveau fonctionnel

## B. Pourquoi augmenter le niveau fonctionnel ?



Une fois le niveau fonctionnel défini, il est impossible de passer à un niveau inférieur. Par exemple, on peut passer du niveau « Windows Server 2003 » à « Windows Server 2008 », mais pas l'inverse. Il existe toutefois une exception, il est possible rétrograder le niveau fonctionnel de Windows Server 2008 R2 à Windows Server 2008.

# Le niveau fonctionnel

## C. Quelle est la portée d'un niveau fonctionnel ?

---

Il y a deux niveaux fonctionnels différents, un qui s'applique au niveau du domaine et un autre qui s'applique au niveau de la forêt. Le plus critique étant le niveau fonctionnel de la forêt, car il doit correspondre au niveau minimum actuel sur l'ensemble des domaines de la forêt. De ce fait, il est obligatoire d'augmenter le niveau fonctionnel des domaines avant de pouvoir augmenter le niveau fonctionnel de la forêt.



## Ce qu'il faut retenir ...

---

Il faut garder à l'esprit qu'une forêt est un ensemble d'arbres, qu'un arbre est constitué d'une racine et potentiellement de branches qui sont représentées par des domaines et des sous-domaines.

Tous les domaines pourraient être créés indépendamment les uns des autres, mais cela compliquerait l'administration plutôt que de la rendre plus simple. En effet, le fait de créer cette arborescence et de regrouper les architectures (les arbres) au sein d'une même forêt facilite grandement la relation entre les différents acteurs.

les relations entre les différents éléments s'appellent des « **relations d'approbations** ».

The background of the slide is a spiral-bound notebook. The left side shows the brown, textured cover of the notebook. The right side is a cream-colored page with a silver metal spiral binding along the left edge. A thin horizontal line is drawn across the page, just above the main text.

## **Partie 4: Protocoles indispensables au fonctionnement de l'AD LDAP-DNS-Kerberos**

# Plan du cours

---

- Le protocole LDAP
  - Présentation
  - Que contient l'annuaire LDAP ?
  - Comment est structuré l'annuaire LDAP ?
- Le protocole DNS
- Le protocole kerberos
  - Fonctionnement
  - Composition d'un ticket Kerberos

Ce qu'il faut retenir ...

# Le protocole LDAP

## A. Présentation

- Le protocole LDAP (*Lightweight Directory Access Protocol*) est **un protocole qui permet de gérer des annuaires**, notamment grâce à des requêtes d'interrogations et de modification de la base d'informations. En fait, l'Active Directory est un annuaire LDAP.
- **Les communications LDAP s'effectuent sur le port 389**, en TCP, du contrôleur de domaine cible.
- Il existe une déclinaison du protocole LDAP appelée LDAPS (*LDAP over SSL*) et qui apporte une couche de sécurité supplémentaire avec du chiffrement.

# Le protocole LDAP

## B. Que contient l'annuaire LDAP ?

L'annuaire LDAP correspond directement à l'Active Directory, il contient donc un ensemble d'unités d'organisation qui forment l'arborescence générale.

Ensuite, on trouve tous les différents types d'objets classiques : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, voir même serveurs et imprimantes.

Pour chaque classe d'objets, il stocke les attributs correspondants et les différentes valeurs de ces attributs pour chaque instance d'un objet. Par exemple, il va stocker toutes les informations relatives à un utilisateur (nom, prénom, description, mot de passe, adresse e-mail, etc.).

# Le protocole LDAP

## C. Structure de l'annuaire LDAP

- **Un annuaire est un ensemble d'entrées**, ces entrées étant elles-mêmes constituées de plusieurs attributs. De son côté, **un attribut est bien spécifique et dispose d'un nom qui lui est propre, d'un type et d'une ou plusieurs valeurs.**
- Chaque entrée dispose d'un identifiant unique qui permet de l'identifier rapidement, de la même manière que l'on utilise les identifiants dans les bases de données pour identifier rapidement une ligne.



# Le protocole LDAP

## C. Structure de l'annuaire LDAP

- L'identifiant unique d'un objet est appelé GUID qui est « **l'identificateur unique global** ». Par ailleurs, un nom unique (**DN** – *Distinguished Name*) est attribué à chaque objet, **et il se compose du nom de domaine auquel appartient l'objet ainsi que du chemin complet pour accéder à cet objet dans l'annuaire** (le chemin à suivre dans l'arborescence d'unités d'organisation pour arriver jusqu'à cet objet).

# Le protocole LDAP

## C. Structure de l'annuaire LDAP

- Par exemple, le chemin d'accès suivant, correspondant à un objet « *utilisateur* » nommé « *Florian* », du domaine « *it-connect.local* » et étant stocké dans une unité d'organisation (OU) nommée « *informatique* » contenant elle-même une OU nommée « *system* » :

**it-connect.local, informatique, system, Florian**

# Le protocole LDAP

## C. Structure de l'annuaire LDAP

**it-connect.local, informatique, system, Florian**

Se traduira en chemin LDAP par :

**cn=Florian,ou=system,ou=informatique,dc=it-connect,dc=local**

Ainsi, la chaîne ci-dessus correspondra au *Distinguished Name* (unique) de l'objet.

- Dans un chemin LDAP vers un objet, on trouve toujours la présence du domaine sous la forme « *dc=it-connect,dc=local* », correspondant à « *it-connect.local* » dans cet exemple.

# Le protocole LDAP

## C. Structure de l'annuaire LDAP

- Dans un chemin LDAP vers un objet, on trouve toujours la présence du domaine sous la forme « *dc=it-connect,dc=local* », correspondant à « *it-connect.local* » dans cet exemple.

```
DistinguishedName : CN=Florian,OU=Informatique,DC=it-connect,DC=fr
Enabled            : True
GivenName          : Florian
Name               : Florian
ObjectClass        : user
ObjectGUID         : aad52b0f-f865-4426-b7c5-78124b535763
SamAccountName     : fburnel
SID                : S-1-5-21-594424403-2588294363-2768037708-1107
Surname            : BURNEL
UserPrincipalName  : fburnel@it-connect.fr
```

Exemple de DistinguishedName

# Le protocole DNS

- Active Directory s'appuie sur le DNS
- Le protocole DNS est utilisé pour la résolution des noms, ce qui permet aux postes clients de localiser les contrôleurs de domaine au sein du système d'information. De la même manière, lorsque l'on souhaite joindre un client au domaine, on utilise un nom comme « **it-connect.local** », ce qui implique une requête DNS pour savoir quelle est l'adresse IP correspondante à ce nom, on serait alors redirigé vers le contrôleur de domaine qui traitera la requête.

# Le protocole DNS

- Le serveur DNS crée une zone correspondante à au domaine et enregistre de nombreux enregistrements. Il y a bien sûr un enregistrement (de type A) pour chaque contrôleur de domaine, mais il existe une multitude d'enregistrements annexes, indispensable au bon fonctionnement de l'Active Directory :
- **Enregistrement pour localiser le « Primary Domain Controller »** : correspondant au contrôleur de domaine qui dispose du rôle FSMO « Émulateur PDC ».
- **Enregistrement pour localiser un contrôleur de domaine qui est catalogue global.**



# Le protocole DNS

- **Enregistrement pour localiser les KDC du domaine** (concept abordé au point suivant de ce cours).
- **Enregistrement pour localiser les contrôleurs de domaine du domaine cible.**
- **Enregistrer simplement la correspondance nom/adresse IP des différents contrôleurs de domaine.** Il est également possible de créer un second enregistrement avec les adresses IPv6.
- **Enregistrer les contrôleurs de domaine via le GUID pour assurer la localisation dans toute la forêt.**

# Le protocole DNS

---

- Il est même possible que l'ensemble des ordinateurs joint au domaine soit enregistré au sein du DNS, si vous le permettez. Ainsi, un ordinateur de l'entreprise pourra être joint via :

*pc-01.it-connect.local* s'il se nomme « *pc-01* ».

# Le protocole DNS

- Le serveur DNS peut être sur le contrôleur de domaine ou sur un autre serveur DNS du système d'information. Ce serveur DNS peut être sous Windows mais aussi sous Linux en utilisant le paquet « **Bind 9** » qui requiert alors une configuration particulière.
- Les contrôleurs de domaine doivent être capables d'écrire dans la zone DNS qui leur correspond, ceci dans le but de gérer les enregistrements dynamiquement. Lors de la création d'un domaine, tous les enregistrements nécessaires au bon fonctionnement du système seront créés automatiquement.

# Le protocole Kerberos

- Le protocole Kerberos est l'acteur principal de l'authentification au sein d'un domaine, il n'intervient ni dans l'annuaire ni dans la résolution de noms.
- Le protocole Kerberos est un protocole mature, qui est aujourd'hui en version 5. Il assure l'authentification de manière sécurisée avec un mécanisme de distribution de clés.

# Le protocole Kerberos

## A. Fonctionnement

---

Chaque contrôleur de domaine dispose d'un service de distribution de clés de sécurité, appelé « **Centre de distribution de clés (KDC)** » et qui réalise deux services :

- **Un service d'authentification (Authentication Service – AS)**
- **Un service d'émission de tickets (Ticket-Granting Service - TGS)**

# Le protocole Kerberos

## A. Fonctionnement

- **Un service d'authentification (Authentication Service – AS)**

Ce service distribue des tickets spéciaux appelés « *TGT* » (pour « ***Ticket-Granting Ticket*** ») qui permettent d'effectuer d'autres demandes d'accès auprès du service d'émission de tickets (TGS).

Avant qu'un client puisse obtenir un accès sur un ordinateur du domaine, il doit obtenir un TGT depuis le service d'authentification du domaine cible. Une fois que le service d'authentification retourne le TGT, le client dispose de l'autorisation pour effectuer sa demande auprès du TGS. Ce TGT obtenu pourra être réutilisé jusqu'à ce qu'il expire, mais la première demande qui déclenchera la création d'un nouveau TGT requiert toujours un passage par le service d'authentification.



# Le protocole Kerberos

## A. Fonctionnement

- **Un service d'émission de tickets (Ticket-Granting Service - TGS)** Ce service distribue des tickets aux clients pour la connexion de la machine du domaine. En fait, quand un client veut accéder à un ordinateur, il contacte le service d'émission de tickets correspondant au domaine auquel appartient l'ordinateur, il présente un TGT, et effectue sa demande pour obtenir un ticket d'accès sur cet ordinateur. On parlera alors de l'obtention d'un ticket TGS.

Les deux services décrits précédemment ont chacun des tâches et un processus précis. Ce mécanisme d'authentification est inévitable pour accéder aux ressources d'un domaine. Sans Kerberos, il n'y aura plus d'authentification, ce qui déclenchera des problèmes d'authentifications et d'accès.

# Le protocole Kerberos

## A. Fonctionnement

- Si le centre de distribution de clés (KDC) est indisponible depuis le réseau, l'Active Directory sera ensuite indisponible également, et le contrôleur de domaine ne contrôlera plus longtemps le domaine.

# Le protocole Kerberos

## B. Composition d'un ticket Kerberos

- Le ticket Kerberos distribué contient de nombreuses informations qui permettent d'identifier l'élément auquel est attribué ce ticket. Par exemple, pour un utilisateur, il sera possible de savoir son nom, son mot de passe, l'identité du poste initial ainsi que la durée de validité du ticket et sa date d'expiration.
- Par ailleurs, les tickets TGS et TGT contiennent une clé de session qui permet de chiffrer les communications suivantes afin de sécuriser les échanges.

# Ce qu'il faut retenir ...

- Ces trois protocoles sont indispensables au bon fonctionnement de l'Active Directory. Ils assurent des fonctions critiques :

Gestion de  
l'annuaire

LDAP

Authentification et  
gestion des sessions

Kerberos

Communication et  
résolution des noms

DNS

A spiral-bound notebook is shown from a top-down perspective. The left side of the notebook has a brown, textured cover. The right side is a cream-colored page with a spiral binding on the left edge. A horizontal line is drawn across the page, just below the top edge. The text "Partie 5: les principaux attributs d'objets dans AD" is written in a bold, brown font, centered on the page.

## **Partie 5: les principaux attributs d'objets dans AD**

# Plan du cours

---

- Les principales classes
- Les identifiants uniques :
  - Le DistinguishedName
  - Le GUID
- Les attributs indispensables



# Les principaux attributs d'objets dans l'Active Directory

---

- Par défaut, tout annuaire Active Directory contient des instances d'objets de différentes classes, par exemple des comptes utilisateurs, des groupes, des unités d'organisation ou encore un ordinateur.
- Les classes d'objets disponibles sont définies directement dans le schéma Active Directory que l'on utilise .

# Les principales classes

Nom	Description
Ordinateur	Les ordinateurs clients intégrés au domaine, mais aussi les serveurs et les contrôleurs de domaine
Contact	Enregistrer des contacts, sans autorisation d'authentification
Groupe	Regrouper des objets au sein d'un groupe, notamment pour simplifier l'administration (attribution de droits à un service « informatique » qui correspond à un groupe nommé « informatique », par exemple)
Unité d'organisation	Dossier pour créer une arborescence et organiser les objets.
Imprimante	Ressource de type « imprimante »
Utilisateur	Comptes utilisateurs qui permettent de s'authentifier sur le domaine, et accéder aux ressources, aux ordinateurs

# Les identifiants uniques :

## **DistinguishedName et GUID**

---

- **DistinguishedName**, Cet identifiant unique également appelé « *DN* » représente le chemin LDAP qui permet de trouver l'objet dans l'annuaire Active Directory.

- Voici un exemple :

- **Domaine** : it-connect.local

- **Unité d'organisation où se trouve l'objet** :  
informatique

- **Nom de l'objet** : Florian

Le DN de cet objet utilisateur sera :

**cn=Florian,ou=informatique,dc=itconnect,dc=local**

# Les identifiants uniques :

## DistinguishedName et GUID

Dans ce DN, on trouve un chemin qui permet de retrouver l'objet, différents éléments sont utilisés :

Identification de l'élément	Description
cn	<i>CommonName</i> – Nom commun – Nom de l'objet final ciblé
ou	<i>OrganizationalUnit</i> – Unité d'organisation
dc	Composant de domaine – Utilisé pour indiquer le domaine cible, avec un élément « dc » par partie du domaine

# Les identifiants uniques :

## DistinguishedName et GUID

---

- Le **GUID** (*Globally Unique Identifier*) est un identificateur global unique qui permet d'identifier un objet d'un annuaire Active Directory. Il correspond à l'attribut « **ObjectGUID** » dans le schéma Active Directory.
- Il est attribué à l'objet dès sa création et ne change jamais, même si l'objet est déplacé ou modifié. Le GUID suit un objet de la création jusqu'à la suppression.
- **Codé sur 128 bits**, le GUID d'un objet est **unique au sein d'une forêt** et il est généré par un algorithme qui **garantit son unicité**. Des informations aléatoires, d'autres non, comme l'heure de création de l'objet .

# Les attributs indispensables

Nom de l'attribut dans le schéma	Nom de l'attribut dans la console Active Directory	Description
sAMAccountName	« Nom d'ouverture de session de l'utilisateur »	Valeur que devra utiliser l'objet pour s'authentifier sur le domaine
UserPrincipalName	« Nom d'ouverture de session de l'utilisateur » concaténé au nom du domaine sous la forme « @it-connect.local »	Nom complet de l'utilisateur avec le domaine inclus. Également appelé UPN
description	Description	Description de l'objet
mail	Adresse de messagerie	Adresse de messagerie attribuée à l'objet
adminCount	-	Égal à « 1 » s'il s'agit d'un compte de type « Administrateur », égal à « 0 » s'il ne l'est pas
DisplayName	Nom complet	Nom complet qui sera affiché pour cet utilisateur



# Les attributs indispensables

<b>givenName</b>	Prénom	Prénom de l'utilisateur
<b>logonCount</b>	-	Nombre d'ouverture de session réalisée par cet objet
<b>accountExpires</b>	Date d'expiration du compte	Date à laquelle le compte ne sera plus utilisable (peut être vide)
<b>ObjectSID</b>	-	Identifiant de sécurité unique qui permet d'identifier un objet
<b>pwdLastSet</b>	-	Dernière fois que le mot de passe fût modifié
<b>userAccountControl</b>	-	État du compte – Une dizaine de codes différents sont possibles



## **Partie 6:les différents types de groupes de l'AD**

# Plan du cours

---

- L'Etendue du groupe
  - Domaine local
  - Globale
  - Universelle
- Le type de groupe
  - Sécurité
  - Distribution
- Ce qu'il faut retenir ...

# Les différents types de groupe de l'Active Directory

---

- On dispose d'un dossier partagé, accessible via le réseau aux utilisateurs du domaine. Ce dossier se nomme « Comptabilité » et on souhaite que toutes les personnes du service comptabilité de l'entreprise accèdent à ce dossier.
- Plutôt que de donner les droits à chaque utilisateur du service comptabilité, tour à tour, on va créer un groupe. De ce fait, on va créer un groupe nommé « comptabilité » dont les membres sont l'ensemble des utilisateurs correspondant aux collaborateurs du service comptabilité.

# Les différents types de groupe de l'Active Directory

- Il existe différents types de groupe

Nouvel objet - Groupe

Créer dans : it-connect.fr/Informatique

Nom du groupe :

Nom de groupe (antérieur à Windows 2000) :

Étendue du groupe

☐ Domaine local

☒ Globale

☐ Universelle

Type de groupe

☒ Sécurité

☐ Distribution

< Précédent   Suivant >   Annuler

Assistant de création d'un groupe

# L'Étendue du groupe

---

- L'étendue d'un groupe correspond à sa portée au niveau de l'arborescence Active Directory, les étendues peuvent aller d'une portée uniquement sur le domaine local, mais aussi s'étendre sur la forêt entière.
- Il existe trois étendues différentes :
  - **Domaine local**
  - **Globale**
  - **Universel**



# L'Etendue du groupe

---

## Domaine local

- Un groupe qui dispose d'une étendue « **domaine local** » peut être utilisé uniquement dans le domaine dans lequel il est créé. Avec ce type d'étendue, le groupe reste local au domaine où il est créé.
- Cependant, les membres d'un groupe à étendue locale peuvent être bien sûr des utilisateurs, mais aussi d'autres groupes à étendues locales, globales ou universelles. Cette possibilité offre là encore une flexibilité dans l'administration.
- Il peut être défini pour contrôler l'accès aux ressources uniquement au niveau du domaine local.

# L'Etendue du groupe

---

## Globale

- Un groupe ayant une étendue « globale » pourra être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés par le domaine de base. Ainsi, si un « domaine A » approuve via une relation un « domaine B », alors un groupe global créé dans le « domaine A » pourra être utilisé dans le « domaine B ».
- Un groupe global pourra contenir d'autres objets du domaine, et être utilisé pour contrôler l'accès aux ressources sur le domaine local et tous les domaines approuvés.

# L'Etendue du groupe

## Universelle

- Un groupe disposant de l'étendue « universelle » à une portée maximale puisqu'il est accessible dans l'ensemble de la forêt, ce qui implique qu'il soit disponible sur tous les domaines de la forêt.
- Un groupe universel peut contenir des groupes et objets provenant de n'importe quel domaine de la forêt. De la même manière, il est possible de l'utiliser pour définir l'accès aux ressources sur tous les domaines de la forêt.

Ainsi, avec ce type d'étendue on pourra consolider plusieurs groupes qui doivent avoir une portée maximale sur l'ensemble du système.

- Une particularité de ce type de groupe, c'est qu'il est défini au sein d'un catalogue global.

# L'Etendue du groupe

## Précision sur les étendues

- Les étendues sont dépendantes du niveau fonctionnel de la forêt et du domaine, ainsi que de la complexité de l'architecture en place, notamment au niveau des relations d'approbations entre les différents domaines et arbres. Si l'on crée un groupe à étendue universelle, mais qu'il n'y a pas de relation avec un autre domaine ou une autre forêt, cela n'aura pas d'intérêt.

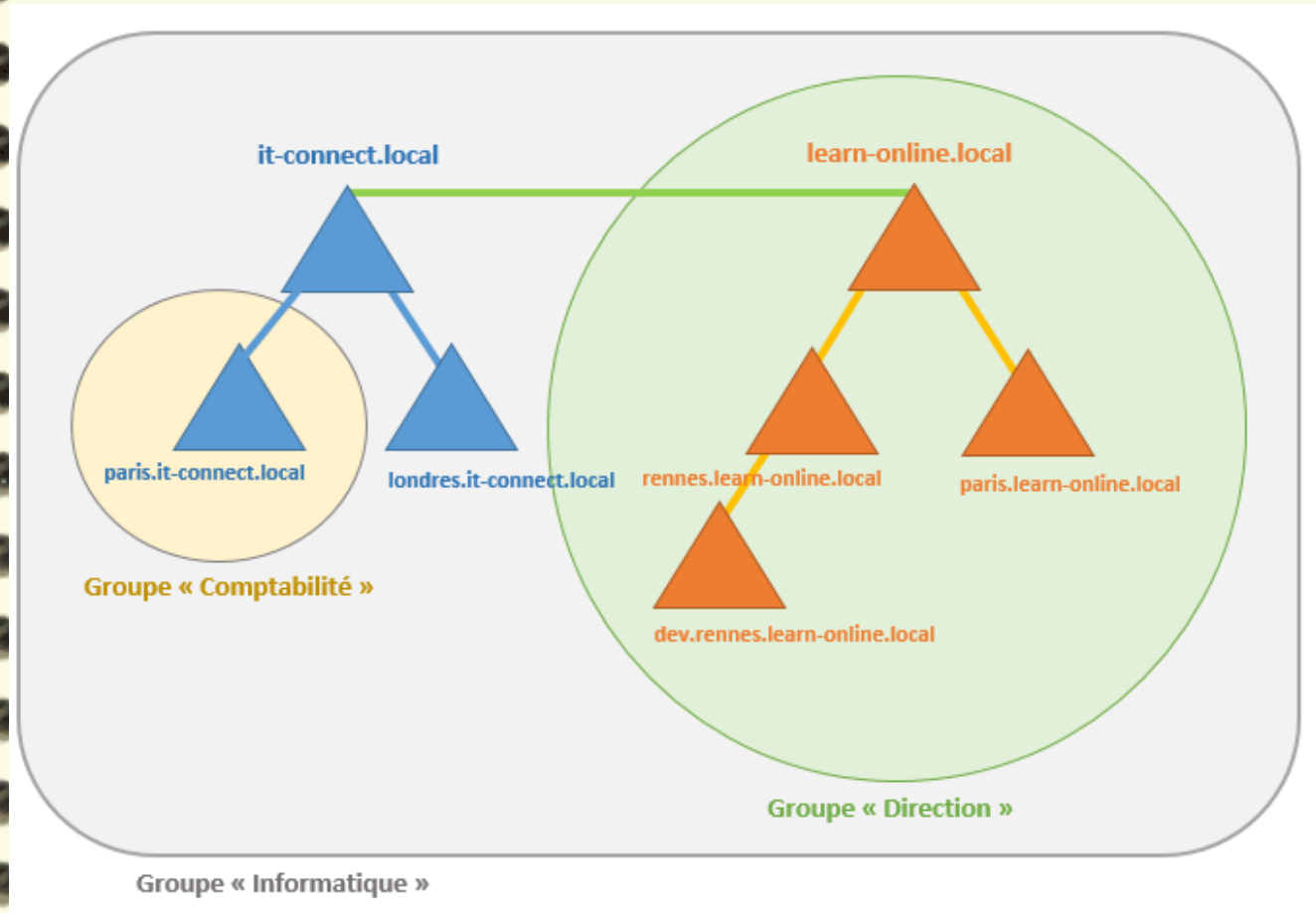
# L'Etendue du groupe

**Exemple** : Imaginons trois groupes et leurs étendues cohérentes :

- Comptabilité : étendue « domaine local » sur « **paris.it-connect.local** »
- Direction : étendue « globale » sur « learn-online.local » qui approuve tous les sous-domaines
- Informatique : étendue « universelle » sur la forêt

Ainsi, la portée de ces groupes pourra être schématisée comme ceci au sein de la forêt :

# L'Etendue du groupe





# Le type de groupe

---

- Il existe deux types de groupes

**Sécurité** : Les groupes de sécurité sont les plus utilisés et ceux que l'on manipule le plus souvent. Ils permettent d'utiliser les groupes pour gérer les **autorisations d'accès aux ressources**.

Par exemple, si vous avez un partage sur lequel vous souhaitez donner des autorisations d'accès, vous pourrez utiliser un « groupe de sécurité » pour donner des autorisations à tous les membres de ce groupe.

En résumé, ces groupes sont utilisés pour le contrôle d'accès, ce qui implique que chaque groupe de ce type dispose d'un **identifiant de sécurité** « **SID**

# Le type de groupe

---

- Il existe deux types de groupes

**Distribution** : L'objectif de ce type de groupe n'est pas de faire du contrôle d'accès, mais plutôt des listes de distribution. Par exemple, créer une liste de distribution d'adresses e-mail en ajoutant des contacts.

De ce fait, ces groupes sont utilisés principalement par des applications de messagerie, comme **Microsoft Exchange**.

Comme il n'y a pas de notion de sécurité, ce type de groupe ne dispose pas d'identifiant de sécurité « SID ».

# Les groupes par défaut

- **Les groupes intégrés (« Built-in »)** : Ce sont des groupes qui permettent d'assigner des autorisations d'administration, de façon générale ou sur des fonctionnalités précises afin de gérer la sécurité finement. Ces groupes sont directement intégrés et stockés dans l'annuaire Active Directory au sein du container « Builtin » accessible de la console « Utilisateurs et ordinateurs Active Directory ». Leur étendue est toujours de type local.

# Les groupes par défaut

---

- **Les groupes spéciaux** : Seul le système a la main sur ces groupes, qui sont pratique et qui permettent d'englober les utilisateurs à différentes échelles. On trouve par exemple les groupes « Tout le monde » et « Utilisateurs authentifiés ».
- Ces groupes peuvent être utilisés pour définir du contrôle d'accès (exemple : donner accès aux utilisateurs authentifiés l'accès à un partage).
- Par ailleurs, il n'est pas possible de gérer les membres de ces groupes, le système gère ces groupes en exclusivité.

# Les groupes par défaut

---

- **Les groupes prédéfinis** : On les trouve dans l'unité d'organisation « Users » au sein de la console « Utilisateurs et ordinateurs Active Directory ». Ces groupes prédéfinis sont là en complément des groupes intégrés, sauf que pour eux il y a différents niveaux d'étendues qui sont prédéfinies et qu'on ne peut pas modifier.

# Ce qu'il faut retenir ...

---

Groupe sécurité  
*Contrôle d'accès*

Groupe de  
distribution  
*Liste de diffusion*



The background of the slide is a spiral-bound notebook. The left side shows the brown, textured cover of the notebook, and the right side shows a cream-colored page with a silver spiral binding. A thin horizontal line is drawn across the page, just below the top edge.

## Partie 6:les différents rôles **ADDS,ADFS,ADCS**

The background of the slide is a spiral-bound notebook. The left side shows the brown, textured cover of the notebook, and the right side is a cream-colored page with a metal spiral binding visible along the left edge.

# Plan du cours

---

- Les différents rôles
- ADDS
- ADFS
- ADCS
- ADRMS
- ADLDS

# Les différents rôles

---

- Cinq rôles comprennent la mise en place d'un AD
- Ces cinq rôles permettent de répondre à des besoins différents, mais ils sont capables de fonctionner ensemble et de se « répartir les tâches », car ils sont conçus pour assumer un rôle bien spécifique.

# ADDS-Active Directory Domain Service

---

- ADDS permet la mise en place des services de domaine Active Directory, autrement dit la mise en œuvre d'un domaine et d'un annuaire Active Directory.
- Ce rôle permet de gérer au sein d'un annuaire les utilisateurs, les ordinateurs, les groupes, etc. afin de proposer l'ouverture de session via des mécanismes d'authentification et le contrôle d'accès aux ressources.

# ADCS-Active Directory Certificat Services

---

- Ce rôle apporte une couche sécurité supplémentaire au sein du système d'information puisqu'il permet de gérer et de créer des clés ainsi que des certificats. Ce rôle est compatible avec de nombreuses applications, ce qui offre un intérêt supplémentaire à l'utiliser pour augmenter la sécurité de manière générale.
- ADCS est composé de différents modules qui permettent d'effectuer des demandes de certificats de diverses façons : par le web, par le réseau, etc.

# ADFS-Active Directory Federation Services

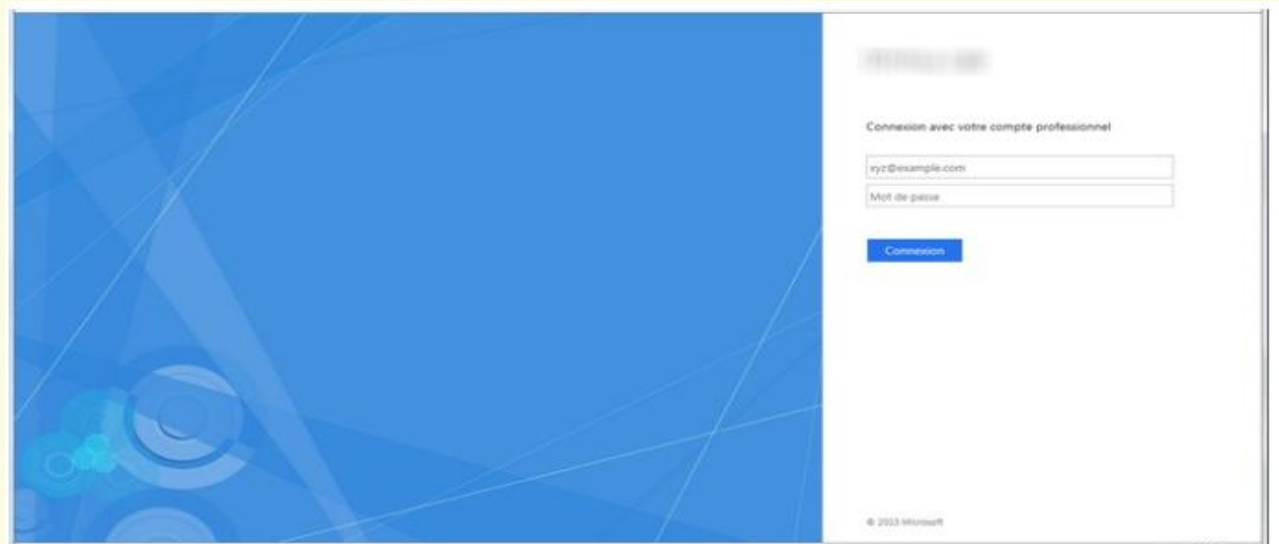
---

- Depuis Windows Server 2008, un rôle nommé « ADFS » est disponible. Il s'agit d'un service de fédération qui permet de simplifier l'accès à des applications, que l'on se trouve ou non sur le même réseau.
- Principalement, ADFS permet l'intégration d'un mécanisme SSO (Single Sign-On) c'est-à-dire l'authentification unique.
- On se connecte sur le portail ADFS avec ses identifiants, et si l'authentification réussit on obtient directement l'accès à l'application cible sans devoir se réauthentifier.
- Ainsi, les demandes d'authentification pour accéder aux applications sont centralisées et des jetons d'accès sont distribués aux clients, si l'accès est autorisé.



# ADFS-Active Directory Federation Services

- Ainsi, les demandes d'authentification pour accéder aux applications sont centralisées et des jetons d'accès sont distribués aux clients, si l'accès est autorisé.



Exemple de portail ADFS

# AD RMS-Active Directory Rights Management Services

---

- Depuis Windows Server 2008 R2, le rôle AD RMS est directement intégré au système d'exploitation. Il permet de gérer finement les autorisations sur les fichiers des utilisateurs.
- Il ne se limite pas aux simples autorisations comme « accès en lecture » ou « accès en lecture et écriture », ce sont plutôt des droits comme : « J'autorise les utilisateurs à sauvegarder le fichier, mais je n'autorise pas l'impression du fichier ».

# AD RMS-Active Directory Rights Management Services

---

- **AD RMS** est une application « **client – serveur** », cela implique qu'AD RMS s'intègre dans les applications pour créer de l'interaction. De ce fait, les applications doivent être compatibles, ce qui est le cas des versions de Microsoft Office Entreprise, Professional ,etc.
- Finalement, **AD RMS** augmente la sécurité de fichiers au **niveau des accès**, ce qui permet de mieux protéger l'information.

# AD LDS-Active Directory Lightweight Directory Services

- Historiquement appelé « ADAM » pour un Active Directory en mode application, le rôle **AD LDS** se rapproche du mode ADDS classique à la différence qu'il n'implique pas la création d'un domaine, mais fonctionne directement en mode instance, où plusieurs instances d'AD LDS peuvent être exécutées sur le serveur.
- L'intérêt est de pouvoir créer un annuaire autonome qui permettra de créer une base d'utilisateurs, pouvant être utilisé dans le cadre d'un processus d'authentification auprès de l'annuaire LDAP.

# AD LDS-Active Directory Lightweight Directory Services

---

- Par contre, ces utilisateurs ne peuvent pas être utilisés pour mettre en place du contrôle d'accès, car il n'y a pas cette notion de sécurité due à l'absence de contrôleur de domaine.
- AD LDS peut être utilisé pour créer un magasin d'authentification avec une base d'utilisateurs (comme des clients ou des prestataires externes) pour accéder à un portail web extranet, par exemple.



## **Partie 7:À la découverte du catalogue Global**



# Plan du cours

---

- Un catalogue global ,c'est quoi ?
- Est-il seul un Catalogue global?
  - Foret mono-domaine
  - Foret multi-domaines
- Les fonctions clé du CG

# Un catalogue Global ,

## Présentation

---

Le catalogue global est un contrôleur de domaine qui dispose d'une version étendue de l'annuaire Active Directory.

En fait, comme tout contrôleur de domaine, il dispose **d'une copie complète de l'annuaire Active Directory** de son domaine, mais en supplément il dispose de :

- Un répliqua partiel pour tous les attributs contenus dans tous les domaines de la forêt,
- Toutes les informations sur les objets de la forêt.

**Le catalogue global est un annuaire qui regroupe des éléments provenant de l'ensemble de la forêt, c'est en quelque sorte un annuaire central.**

# Un catalogue Global ,

## Présentation

---

On le différencie d'un contrôleur de domaine standard, car en temps normal, chaque contrôleur de domaine contient une copie de l'annuaire de son domaine. Quant au catalogue global, il contient une copie des attributs principaux de tous les domaines de la forêt.

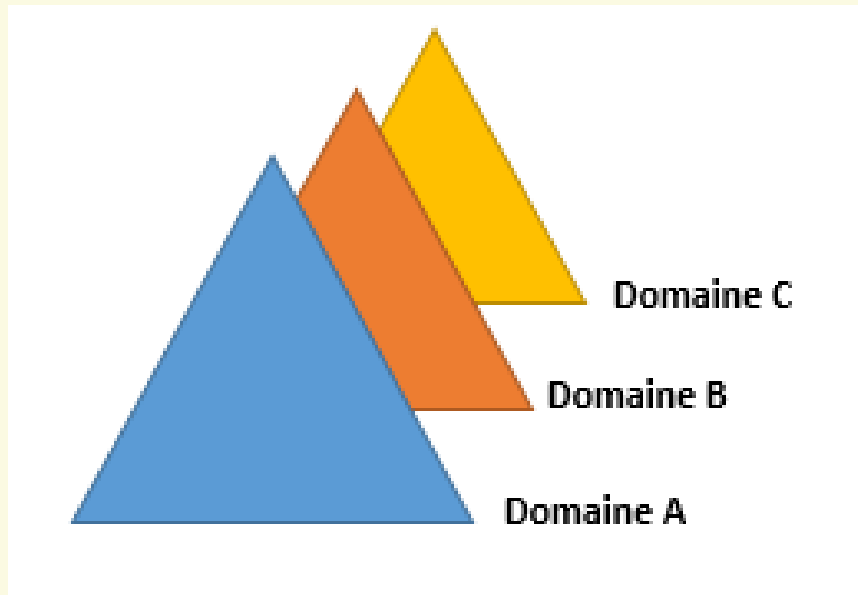
Ainsi, un contrôleur de domaine « catalogue global » sera capable de localiser des objets dans l'ensemble de la forêt, car il a une vue d'ensemble sur tous les objets. Les contrôleurs de domaine classique s'appuieront sur lui pour justement localiser des objets dans une forêt.

# Un catalogue Global , Présentation

## Exemple :

Il y a trois domaines : Domaine A, Domaine B, Domaine C.

Deux contrôleurs de domaine se trouvent au sein du domaine A, un contrôleur de domaine « standard » et un second qui dispose du rôle de « catalogue global ».



# Un catalogue Global ,

## Présentation

---

Le contrôleur de domaine standard disposera de la partition d'annuaire du domaine A

Le contrôleur de domaine catalogue global dispose des partitions d'annuaire du domaine A, mais aussi du domaine B et du domaine C

Les attributs du schéma qui doivent être répliqués sont identifiés par la valeur « Partial Attribute Set » définie dans l'Active Directory.

Microsoft définit par défaut cette politique de réplication de façon à prendre les attributs les plus utilisés dans une recherche, mais elle peut être personnalisée .

# Un catalogue Global ,

## Est-il tout seul ?

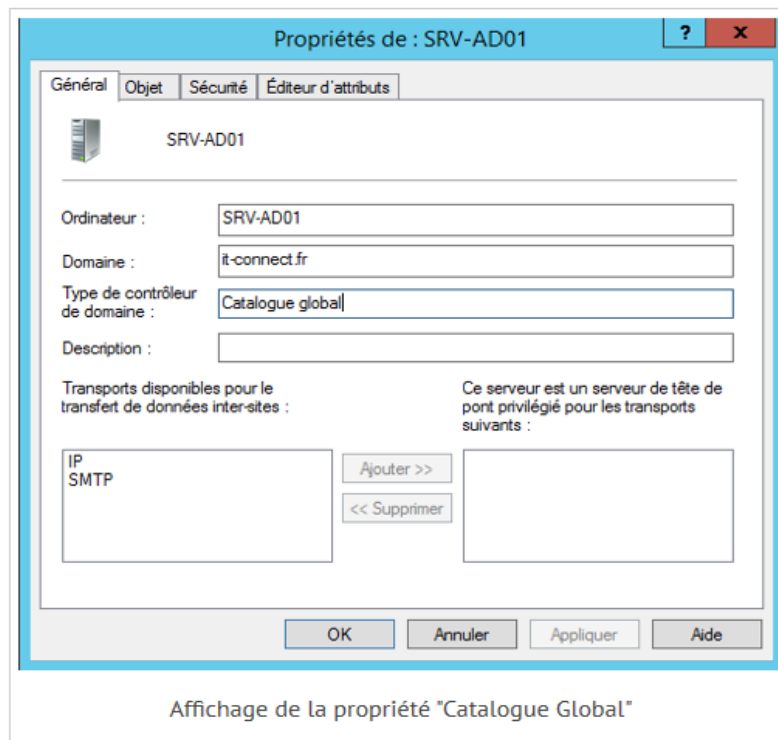
Le premier contrôleur de domaine créé au sein d'une forêt est automatiquement catalogue global. Autrement dit, lorsque l'on met en place un Active Directory, on crée automatiquement un nouveau domaine dans une nouvelle forêt, ce qui implique que le contrôleur de domaine soit le catalogue global.

Par ailleurs, il est fortement recommandé de définir au minimum **deux contrôleurs** en tant que catalogue global. Tout simplement pour assurer la disponibilité du rôle et répartir la charge au niveau des requêtes.



# Un catalogue Global , Est-il tout seul ?

Par ailleurs, il est fortement recommandé de définir au minimum **deux contrôleurs** en tant que catalogue global. Tout simplement pour assurer la disponibilité du rôle et répartir la charge au niveau des requêtes.



# Un catalogue Global ,

## Cas d'une Forêt Mono-domaine

- Il est recommandé d'activer le rôle de catalogue global sur l'ensemble des contrôleurs de domaine du domaine. En effet, l'impact sera faible sur les performances systèmes dans ce type de configuration, mais ça permettra d'assurer la redondance du service.
- Le catalogue global est essentiel à la localisation des objets, et c'est encore plus vrai lorsqu'il y a plusieurs domaines, mais aussi au bon fonctionnement de certaines applications.

# Un catalogue Global ,

## Cas d'une Forêt Multi-domaines

- Lorsqu'il y a plusieurs domaines au sein d'une forêt, il y aura surement des emplacements géographiques différents. Notamment si l'entreprise dispose de plusieurs sites, cela implique d'étendre le réseau à différents endroits.
- Ainsi, le réseau se doit d'être hautement disponible pour que le contrôleur de domaine d'un site A soit sûr de pouvoir contacter un catalogue global situé sur un site B. Par exemple, cela pourrait empêcher la connexion d'un utilisateur si la liaison est rompue, car le contrôleur de domaine ne pourra pas récupérer les informations auprès du catalogue global. Une alternative serait d'activer l'option de « mise en cache de l'appartenance aux groupes universels » sur un site distant, pour limiter le trafic réseau grâce à la mise en cache des informations.

# Un catalogue Global ,

## Cas d'une Forêt Multi-domaines

- La règle suivante est donnée par Microsoft : « **Définir un catalogue global (au minimum) sur un site lorsqu'il y a une centaine d'utilisateurs** ».
- C'est intéressant pour éviter d'être pénalisé par une liaison lente entre deux sites, puisque plus il y a d'utilisateurs, plus il y aura de demandes.
- Cas spécifique : certaines applications sont gourmandes et communiquent beaucoup avec le catalogue global, par exemple Microsoft Exchange. Dans ce cas-là, positionnez un catalogue global proche pour avoir de bonnes performances.
- En résumé, il faut positionner avec stratégie les contrôleurs de domaine « catalogue global » mais vous pouvez aussi opter pour une option simple : activer le rôle sur tous les contrôleurs de domaine de la forêt.

# Les fonctions clés du catalogue Global ,

- Le catalogue global assure quatre fonctions clés auprès du système Active Directory et pour « venir en aide » aux autres contrôleurs de domaine de la forêt, à savoir :

Rechercher des  
objets dans la forêt

Résolution des noms  
principaux  
d'utilisateur (UPN)

Informations sur les  
appartenances aux  
groupes universels

Vérification des  
références d'objets  
inter-domaines

Le catalogue global est un point central dans un environnement où il y a plusieurs domaines, puisqu'il doit faire le lien entre tous les objets de tous les domaines de la forêt. Lorsqu'il n'y a qu'un seul domaine dans la forêt, le catalogue global perd tout son intérêt, car les autres contrôleurs de domaine sauront « <sup>127</sup>se débrouiller seul ».

A spiral-bound notebook with a textured, light brown cover is shown on the left side of the image. The spiral binding is visible along the edge. The right side of the image shows a blank, cream-colored page. A horizontal line is drawn across the page, just below the top edge. The text "Partie 8:les cinq rôles FSMO" is centered on the page in a bold, brown font.

## **Partie 8:les cinq rôles FSMO**



# Plan du cours

---

- L'utilité du rôle FSMO
- Rôle « Maître d'attribution des noms de domaine »
- Rôle « contrôleur du schéma »
- Rôle « Maître Rid »
- Rôle « Maître d'infrastructure »
- Rôle « Emulateur PDC »
- Gestion des maîtres d'opération

# L'utilité du rôle FSMO

- Lorsque l'on met en place un environnement Active Directory, il y a de très fortes chances que l'on ait plusieurs contrôleurs de domaine. De ce fait, tous les contrôleurs de domaine « normaux » disposent d'un accès en écriture sur l'annuaire.
- Cependant, certaines tâches sont plus sensibles que d'autres, et il serait dangereux d'autoriser la modification de certaines données sur deux contrôleurs de domaine différents, en même temps. De ce fait et pour minimiser les risques de conflits, Microsoft a décidé d'implémenter les rôles FSMO qui permettent de limiter la modification de certaines données internes à l'annuaire Active Directory.

# L'utilité du rôle FSMO

- Au sein d'un environnement, on attribuera la notion de « rôle FSMO » à « maître d'opération ». En fait, le maître d'opération est le contrôleur de domaine qui détient un ou plusieurs rôles FSMO. Détenir un rôle signifie pour un contrôleur de domaine qu'il est capable de « réaliser une action particulière au sein de l'annuaire ».
- **Il est à noter qu'il ne peut pas y avoir plusieurs maîtres d'opérations pour le même rôle FSMO**, au sein d'un domaine ou d'une forêt (selon le rôle concerné).

# L'utilité du rôle FSMO

- Voici les cinq rôles:

Maître  
d'attribution des  
noms de domaine

Contrôleur de  
schéma

Maître RID

Maître  
d'infrastructure

Emulateur PDC

# 1. Rôle « Maître d'attribution de noms de domaine »

- Le maître d'opération qui détient ce rôle est unique au sein de la forêt, et il est le seul autorisé à distribuer des noms de domaine aux contrôleurs de domaine, lors de la création d'un nouveau domaine.
- De ce fait, il est notamment utilisé lors de la création d'un nouveau domaine. Le contrôleur de domaine à l'initiative de la création doit impérativement être en mesure de contacter le contrôleur de domaine disposant du rôle FSMO « Maître d'attribution des noms de domaine » sinon la procédure échouera.
- Il a également pour mission de renommer les noms de domaine.
- En résumé, il **est unique au sein d'une forêt et attribue les noms de domaine.**

FSMO= Flexible  
Single Master  
Operation

## 2. Rôle « contrôleur de schéma »

- Pour rappel, le schéma désigne la structure de l'annuaire Active Directory, le schéma est donc un élément critique au sein de l'environnement Active Directory.
- Cela implique l'unicité au sein de la forêt de ce maître d'opération, qui sera le seul
- Contrôleur de domaine à pouvoir initier des changements au niveau de la structure de l'annuaire (schéma). En fait, **comme le schéma est unique, son gestionnaire est unique également.**
- En résumé, il est unique **au sein d'une forêt et gère la structure du schéma.**



FSMO= Flexible  
Single Master  
Operation

### 3.Rôle « Maître RID»

- Les objets créés au sein de l'annuaire Active Directory dispose de plusieurs identifiants uniques. Parmi eux, il y a notamment le **GUID** et le **DistinguishedName** mais aussi l'identifiant de sécurité « **SID** », c'est ce dernier qui nous intéresse dans le cadre du maître RID.

## 3.Rôle « Maître RID»

### Pourquoi le RID ?

- Le RID est un identifiant relatif qui est unique au sein de chaque SID, afin d'être sûr d'avoir un SID unique pour chaque objet de l'annuaire. Le SID étant constitué d'une partie commune qui correspond au domaine, le RID est essentiel pour rendre unique chaque SID. C'est là que le maître RID intervient.
- Unique au sein d'un domaine, ce maître d'opération devra allouer des blocs d'identificateurs relatifs à chaque contrôleur de domaine du domaine. Ainsi, chaque contrôleur de domaine aura un bloc (pool) de RID unique qu'il pourra attribuer aux futurs objets créés dans l'annuaire.

### 3. Rôle « Maître RID »

- Bien sûr, tous les contrôleurs de domaine ne vont pas épuiser le pool de RID au même rythme... Un contrôleur de domaine qui atteindra un certain niveau d'épuisement de son stock de RID disponible contactera le Maître RID pour en obtenir des nouveaux. Cela implique que la création d'un objet est impossible si le Maître RID du domaine n'est pas disponible.
- En résumé, il **est unique au sein d'un domaine et attribue des blocs de RID aux contrôleurs de domaine pour assurer que les SID des objets soient unique.**

FSMO= Flexible  
Single Master  
Operation

## 4. Rôle « Maître d'infrastructure »

- Unique au sein d'un domaine, le contrôleur de domaine qui dispose du rôle de Maître d'infrastructure a pour objectif de gérer les **références entre plusieurs objets**.
- Prenons un exemple pour mieux comprendre ce que cela signifie. Imaginons qu'un utilisateur d'un domaine A soit ajouté au sein d'un groupe du domaine B. Le contrôleur de domaine « Maître d'infrastructure » deviendra responsable de cette référence et devra s'assurer de la réplication de cette information sur tous les contrôleurs de domaine du domaine

FSMO= Flexible  
Single Master  
Operation

## 4. Rôle « Maître d'infrastructure »

- Ces références d'objets sont également appelées « **objets fantômes** » et permettent au contrôleur de domaine de faciliter les liens entre les différents objets. Un objet fantôme contiendra peu d'information au sujet de l'objet auquel il fait référence (DN, SID et GUID). Dans le cas de l'exemple, un objet fantôme sera créé sur le domaine B afin de faire référence à l'utilisateur du domaine A. De ce fait, si l'objet est modifié ou supprimé à l'avenir, le Maître d'infrastructure devra se charger de déclencher la mise à jour de l'objet fantôme auprès des autres contrôleurs de domaine. En quelque sorte, il accélère les processus de réplication et la communication entre les contrôleurs de domaine.

- **En résumé, il est unique au sein d'un domaine et doit gérer les références d'objets au sein du domaine.**



FSMO= Flexible  
Single Master  
Operation

## 5.Rôle « Emulateur PDC»

- L'émulateur PDC (Primary Domain Controller) est unique au sein d'un domaine et se doit d'assurer cinq missions principales :

- Modification des stratégies de groupe du domaine (éviter les conflits et les écrasements)
- Synchroniser les horloges sur tous les contrôleurs de domaine (heure et date)
- Gérer le verrouillage des comptes
- Changer les mots de passe
- Assurer la compatibilité avec les contrôleurs de domaine Windows NT

**En résumé, il est unique au sein d'un domaine et assure diverses missions liées à la sécurité et par défaut il joue le rôle de serveur de temps pour l'ensemble du domaine.**



# La gestion des maitres d'opération

FSMO= Flexible  
Single Master  
Operation

- Par défaut, le premier contrôleur de domaine du domaine détient les cinq rôles FSMO. Cependant, il est possible de transférer les rôles si vous souhaitez les répartir entre plusieurs contrôleurs de domaine, il y a une véritable flexibilité à ce niveau-là.
- Pour transférer un rôle d'un contrôleur de domaine vers un autre, on pourra utiliser l'interface graphique de Windows ou encore l'utilitaire « **ntdsutil** ».

A spiral-bound notebook is shown from a top-down perspective. The left side features a textured, brownish-gold cover. The right side is a cream-colored page with a horizontal line near the top. The metal spiral binding is visible along the left edge of the page.

## **Partie 9:les relations d'approbation**

# Plan du cours

---

- Présentation
- Cas d'utilisation des relations d'approbation
- Direction et transitivité
- Les approbations prédéfinies
- Les approbations externes
- Ce qu'il faut retenir ...

# Présentation

---

- Une **relation d'approbation** est un lien de confiance (*Trust Relationship*) établie entre deux domaines Active Directory, voir même entre deux forêts Active Directory. Ces relations permettront de faciliter l'accès aux ressources entre les domaines concernés, ce qui permet de mutualiser les accès bien que les domaines disposent d'une base de données Active Directory différente.
- On crée les relations d'approbations par l'intermédiaire de la console « *Domaines et approbations* » intégrée à Windows Server

# Cas d'utilisation d'une relation d'approbation

Les relations d'approbations peuvent s'avérer utiles et sont utilisées dans plusieurs cas de figure :

- Une entreprise dispose de plusieurs filiales avec des noms différents, donc des domaines différents, elle pourra créer des relations de confiance entre ses domaines
- La fusion de deux entreprises existantes, qui utilisent à la base chacune leur domaine. La relation d'approbation permettra de faciliter la fusion au niveau du système d'information (avant une éventuelle restructuration complète)

# Direction et transitivité

---

Lorsque l'on parle de relations d'approbations, on ne peut pas échapper à la notion de direction et de transitivité, il va falloir s'y faire. Définissons ces termes :

- Direction
- Transitivité



# Direction et transitivité

- Dans le cadre d'une relation d'approbation, la direction peut être **unidirectionnelle** c'est-à-dire uniquement dans un sens, ou **bidirectionnelle** c'est-à-dire dans les deux sens. Qu'est-ce que cela signifie ?
- Une relation d'approbation unidirectionnelle signifie qu'un domaine A approuve un domaine B, sans que l'inverse soit appliqué. De ce fait, un utilisateur du domaine B pourra accéder aux ressources du domaine A, alors que l'inverse ne sera pas possible !
- Pour que cela soit possible, il faut que la relation d'approbation soit bidirectionnelle pour que les deux domaines s'approuvent mutuellement. Un utilisateur du domaine A pourra alors accéder aux ressources du domaine B, et inversement.

# Direction et transitivité

- Une relation d'approbation, en plus d'être unidirectionnelle ou bidirectionnelle, peut être ou ne pas être transitive.
- La transitivité signifie que si un domaine A approuve un domaine B, et que ce domaine B approuve un domaine C, alors le domaine A approuvera implicitement le domaine C. Autrement dit, « comme A approuve B et que B approuve C, alors A approuve C ».
- Attention tout de même, cette transitivité se limite aux relations d'approbations entre les domaines, et non entre les forêts.

# Les approbations prédéfinies

- Les approbations prédéfinies sont des relations d'approbations créées automatiquement lorsque l'on étend une forêt ou un domaine. On entend par là , le fait d'ajouter un domaine enfant à un domaine existant, par exemple.
- Si l'on dispose d'un domaine « *it-connect.local* » et que l'on ajoute le domaine enfant « *paris.it-connect.local* », il y aura automatiquement une relation de confiance entre ces deux domaines. Une relation d'approbation transitive et bidirectionnelle sera créée entre ces deux domaines. On parlera d'approbation « parent/enfant ».

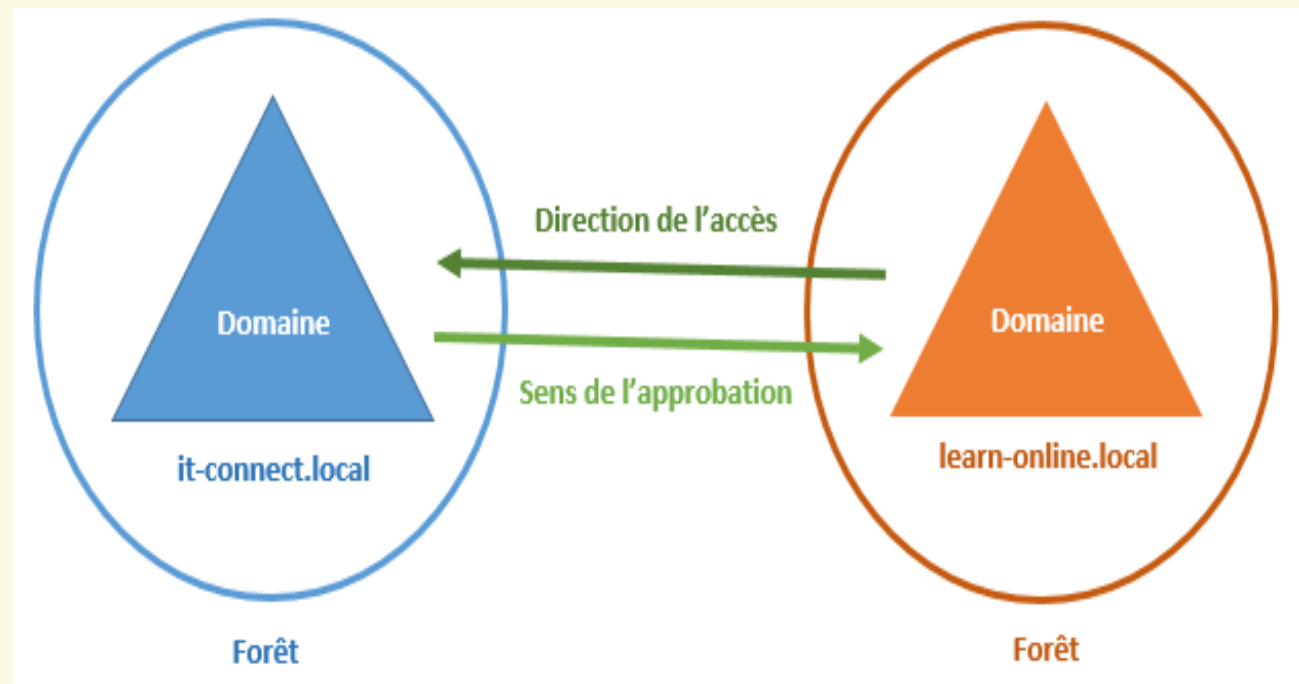
# Les approbations externes

---

- Il est possible de réaliser des relations d'approbations externes, c'est-à-dire entre des domaines situés dans des forêts différentes. Ces relations sont unidirectionnelles et non transitives.
- Pour que l'approbation soit réciproque, il faut que chaque domaine effectue une relation vers le domaine cible, ce qui permettra d'arriver indirectement à une relation bidirectionnelle.
- Avec une relation d'approbation externe, on donne l'accès uniquement au domaine depuis lequel la relation est établie. Voici un exemple :

# Les approbations externes

- Avec une relation d'approbation externe, on donne l'accès uniquement au domaine depuis lequel la relation est établie. Voici un exemple :



## Ce qu'il faut retenir ...

---

- Qu'il s'agisse des relations d'approbations créées automatiquement ou de celles que vous créerez manuellement, elles jouent un rôle important dans l'accès aux ressources.
- Une arborescence de domaine bien organisée facilitera la mise en place des relations d'approbations, ce qui simplifiera la vie aussi bien aux utilisateurs qu'aux administrateurs, puisque l'accès aux ressources sera plus « libre » et l'administration plus flexible.



## Ce qu'il faut retenir ...

---

- Il est important de noter qu'avec les relations d'approbations, l'étendue d'un compte utilisateur est agrandie, c'est-à-dire qu'il peut être utilisé au-delà du domaine auquel il appartient. De ce fait, la sécurité doit être pointilleuse sur l'ensemble des domaines et de l'infrastructure, pour ne pas laisser une porte ouverte sur un domaine et qui permettrait d'accéder à un autre domaine.
- Ces relations d'approbations évitent également la nécessité de créer des comptes en doublons sur plusieurs domaines, puisqu'un seul compte utilisateur pourra être utilisé pour accéder aux ressources de plusieurs domaines. Dans un environnement multi-domaine, la mutualisation devient encore plus forte grâce à ces liens de confiance inter-domaines.



## **Partie 10:Le partage SYSVOL et la réplication**

# Plan du cours

---

- Introduction
- Partage SYSVOL et réplication
  - Présentation SYSVOL
  - Réplication SYSVOL
  - Structure SYSVOL
- Réplication :Quoi ?Quand ?Comment ?

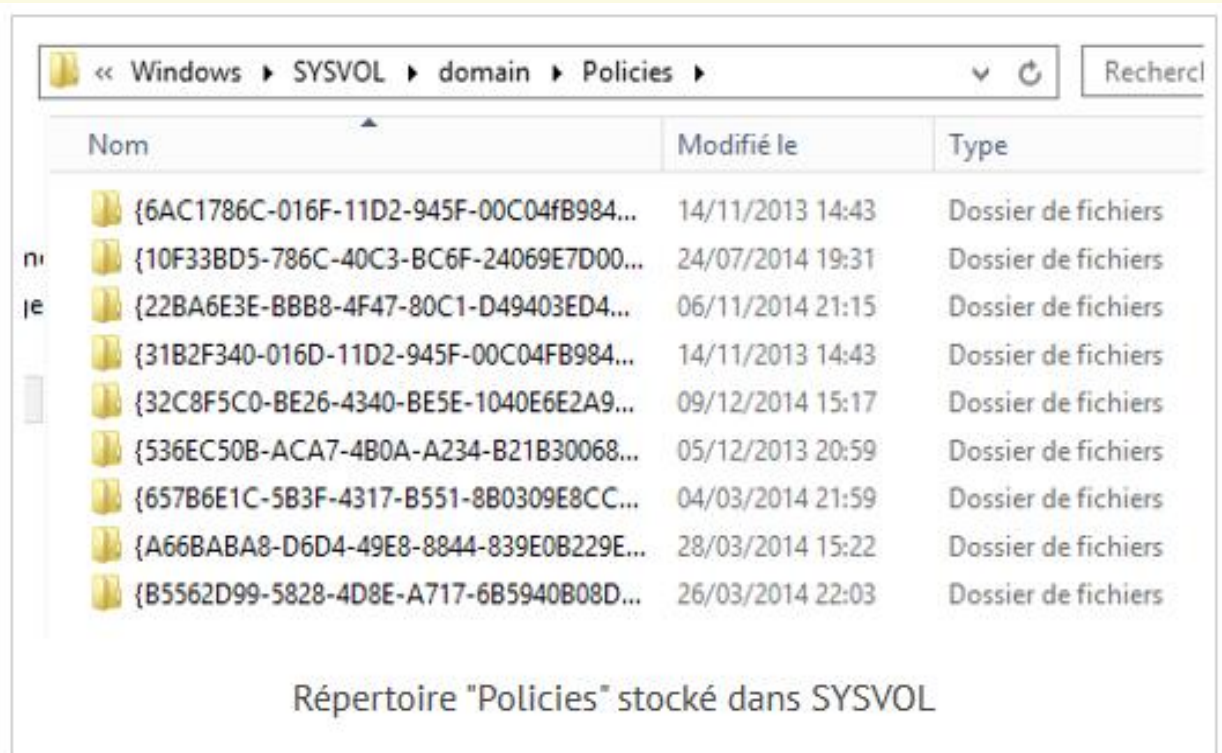
# Introduction

---

- Lorsqu'un contrôleur de domaine est installé, de nombreux éléments sont installés et créés sur le serveur, le partage SYSVOL en fait parti.
- Stocké à l'emplacement « C:\Windows\SYSVOL », « SYSVOL » signifie « System Volume », et il sert à stocker des données spécifiques qui doivent être répliquées entre les contrôleurs de domaine ou accessibles par les ordinateurs clients.

# Introduction

- Plus précisément, voici les éléments principaux que l'on trouvera dans le partage SYSVOL :



« Windows » SYSVOL » domain » Politiques »			Recherch
Nom	Modifié le	Type	
{6AC1786C-016F-11D2-945F-00C04fB984...	14/11/2013 14:43	Dossier de fichiers	
{10F33BD5-786C-40C3-BC6F-24069E7D00...	24/07/2014 19:31	Dossier de fichiers	
{22BA6E3E-BBB8-4F47-80C1-D49403ED4...	06/11/2014 21:15	Dossier de fichiers	
{31B2F340-016D-11D2-945F-00C04FB984...	14/11/2013 14:43	Dossier de fichiers	
{32C8F5C0-BE26-4340-BE5E-1040E6E2A9...	09/12/2014 15:17	Dossier de fichiers	
{536EC50B-ACA7-4B0A-A234-B21B30068...	05/12/2013 20:59	Dossier de fichiers	
{657B6E1C-5B3F-4317-B551-8B0309E8CC...	04/03/2014 21:59	Dossier de fichiers	
{A66BABA8-D6D4-49E8-8844-839E0B229E...	28/03/2014 15:22	Dossier de fichiers	
{B5562D99-5828-4D8E-A717-6B5940B08D...	26/03/2014 22:03	Dossier de fichiers	

Répertoire "Politiques" stocké dans SYSVOL

# Introduction

---

- Pour rappel, les scripts de connexion s'exécutent à l'ouverture de session de l'utilisateur, ils sont généralement écrits en BATCH et comporte des commandes qui permettent de créer des lecteurs réseau sur les machines clientes (commande « net use »).
- Quant aux stratégies de groupe, elles sont récupérées par les clients puis appliquées, dans le but d'appliquer une stratégie de personnalisation de l'espace de travail de l'utilisateur



# Réplication de SYSVOL

---

- Le dossier SYSVOL est répliqué entre les différents contrôleurs de domaine, pour que le contenu soit identique, et que les clients bénéficient tous des mêmes données (à jour). Sur les anciennes versions de Windows Server, notamment Windows Server 2000 et Windows Server 2003, le mécanisme FRS (File Replication Service) était utilisé pour la réplication. Depuis Windows Server 2008, FRS est mis de côté pour laisser la place à DFSR (Distributed File System Replication), qui est plus fiable et plus performant.

# Réplication : Quoi ? Quand ? Comment ?

---

Qui dit redondance, dit nécessité de répliquer les données afin que les données soient identiques sur les différents membres. C'est le même principe pour les contrôleurs de domaine, puisqu'ils doivent se répliquer pour mettre à jour différentes choses :

# Réplication : Quoi ? Quand ? Comment ?

---

- **Base annuaire Active Directory**

Si un utilisateur est créé, modifié ou supprimé, il faut synchroniser les changements auprès des autres contrôleurs de domaine. De la même manière, si l'on intègre un nouvel ordinateur dans le domaine, cela créera un objet « ordinateur » dans l'annuaire, il est donc nécessaire de synchroniser ce changement.

Le protocole RPC over IP (Remote Procedures Call over Internet Protocol) est utilisé pour répliquer la base d'annuaire.

# Réplication : Quoi ? Quand ? Comment ?

---

- **Les stratégies de groupes et les scripts**

Une nouvelle stratégie de groupe créée, un paramètre modifié dans une GPO existante, ou encore la suppression d'une GPO, sont autant d'opérations qui impliquent un changement et donc la nécessité de répliquer des données.

# Réplication : Quoi ? Quand ? Comment ?

- le **DNS** joue un rôle important dans une architecture Active Directory. Pour assurer la continuité de service, on utilise au moins deux serveurs DNS. Ceci implique que les enregistrements des zones soient répliqués entre les serveurs DNS, pour que les informations retournées soient identiques.
- Imaginez si un serveur DNS n'est pas à jour et qu'il retourne une mauvaise adresse IP à une requête client, cela générera des problèmes de communication au sein de l'infrastructure.

Maintenant, vous savez ce qui doit être répliqué et pourquoi ça doit être répliqué, mais alors quand est-ce la réplication se déclenche ?

# Réplication : Quoi ? Quand ? Comment ?

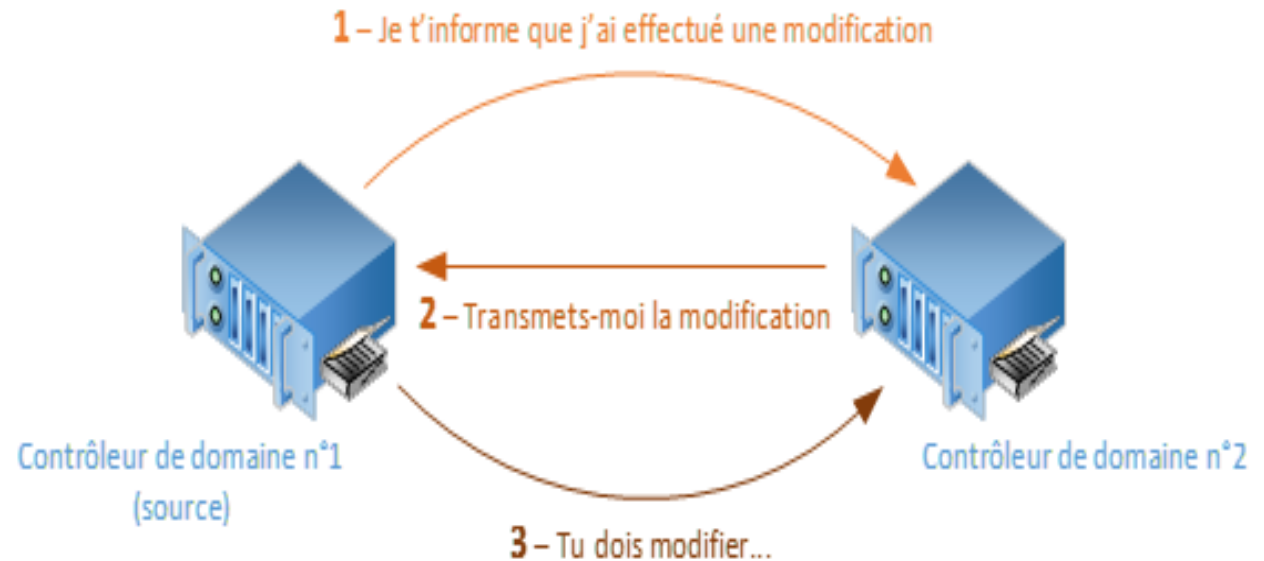
---

- **Délai de réplication**
- Il y a un temps de latence de 5 minutes (par défaut) entre le moment où vous effectuez la modification, et le moment où le contrôleur de domaine source va notifier un autre contrôleur de domaine qu'il a effectué une modification.
- Ensuite, s'il y a un second contrôleur de domaine à notifier, il y aura un intervalle de 30 secondes entre chaque réplication, pour éviter de surcharger le contrôleur de domaine source.



# Réplication : Quoi ? Quand ? Comment ?

- Délai de réplication



# Réplication : Quoi ? Quand ? Comment ?

---

- **Délai de réplication**
- Cependant, il existe des cas de « réplication urgente » où l'on n'observera aucune latence. C'est le cas par exemple lorsqu'on désactive un utilisateur, change un mot de passe ... Et de toute action liée à la sécurité.
- Imaginons maintenant qu'aucune modification ne soit effectuée pendant une heure, ce qui a des chances d'arriver, car on ne passe pas son temps à modifier les données de l'annuaire... Un processus de réplication est automatiquement déclenché pour contrôler que tout est bien à jour.

# Réplication : Quoi ? Quand ? Comment ?

## • **Méthode de réplication**

- La réplication avec le protocole RPC over IP est sûre, mais le contenu n'est pas compressé, ce qui répond plus à un fonctionnement de réplication intrasite. En fait le contenu est chiffré et les connexions authentifiées grâce au protocole Kerberos.
- Lorsque l'infrastructure est répartie sur plusieurs sites distants, le protocole utilisé pour la réplication dépendra de la vitesse de connexion, mais la plupart du temps il s'agira toujours du RPC. À la différence de la réplication intrasite, le trafic RPC généré lors d'une réplication intersites est compressé, ce qui permet d'économiser de la bande passante, mais nécessite des ressources CPU pour décompresser le contenu.

# Réplication : Quoi ? Quand ? Comment ?

- **Méthode de réplication**

- Dans certains cas, où la liaison intersites serait lente et avec un temps de latence fort, il est possible d'utiliser le protocole SMTP pour la réplication (Oui, oui, le SMTP, le protocole pour envoyer des mails). Cependant, il n'est pas en mesure de répliquer le répertoire « SYSVOL », il peut seulement répliquer des éléments précis : mises à jour du schéma, la configuration ou encore les données du catalogue global.

# Réplication : Quoi ? Quand ? Comment ?

- **Méthode de réplication**
- le protocole RPC over IP est au cœur de la réplication entre les contrôleurs de domaine, aussi bien en intrasites qu'en intersites. Le SMTP joue un rôle secondaire pour des répliques spécifiques sur des liaisons lentes, comme une liaison satellite, et il ne peut être utilisé que pour des contrôleurs se trouvant dans des domaines différents.

# Réplication : Quoi ? Quand ? Comment ?

- **Déclaration des sites**

- Les services Active Directory économisent la bande passante entre les sites, en réduisant au minimum la fréquence de réplication. De plus, on peut planifier la disponibilité des liens intersites pour la réplication.
- Par défaut, la réplication intersites a lieu toutes les 3 heures sur chaque lien intersites.
- Lorsque l'on dispose de nombreux sites, il y a des chances pour que les liaisons ne soient pas toutes de la même qualité. De ce fait, il pourra être nécessaire de répliquer moins souvent sur les liaisons lentes que sur les liaisons rapides.



# Réplication : Quoi ? Quand ? Comment ?

- **Déclaration des sites**

- Pour que l'Active Directory comprenne comment est organisée votre infrastructure de manière géographique. Il faut déclarer ses différents sites dans la console « Sites et services Active Directory », puis créer des liens entre les sites ainsi qu'indiquer les adresses réseau utilisées sur ces sites.
- Ainsi, on ajoutera nos différents sites, et dans ces sites on ajoutera des serveurs. Cela permettra de dire : « Sur le site Paris, j'ai le contrôleur de domaine nommé SRV-AD02 » et « Sur le site Rennes, j'ai le contrôleur de domaine nommé SRV-AD03 ».

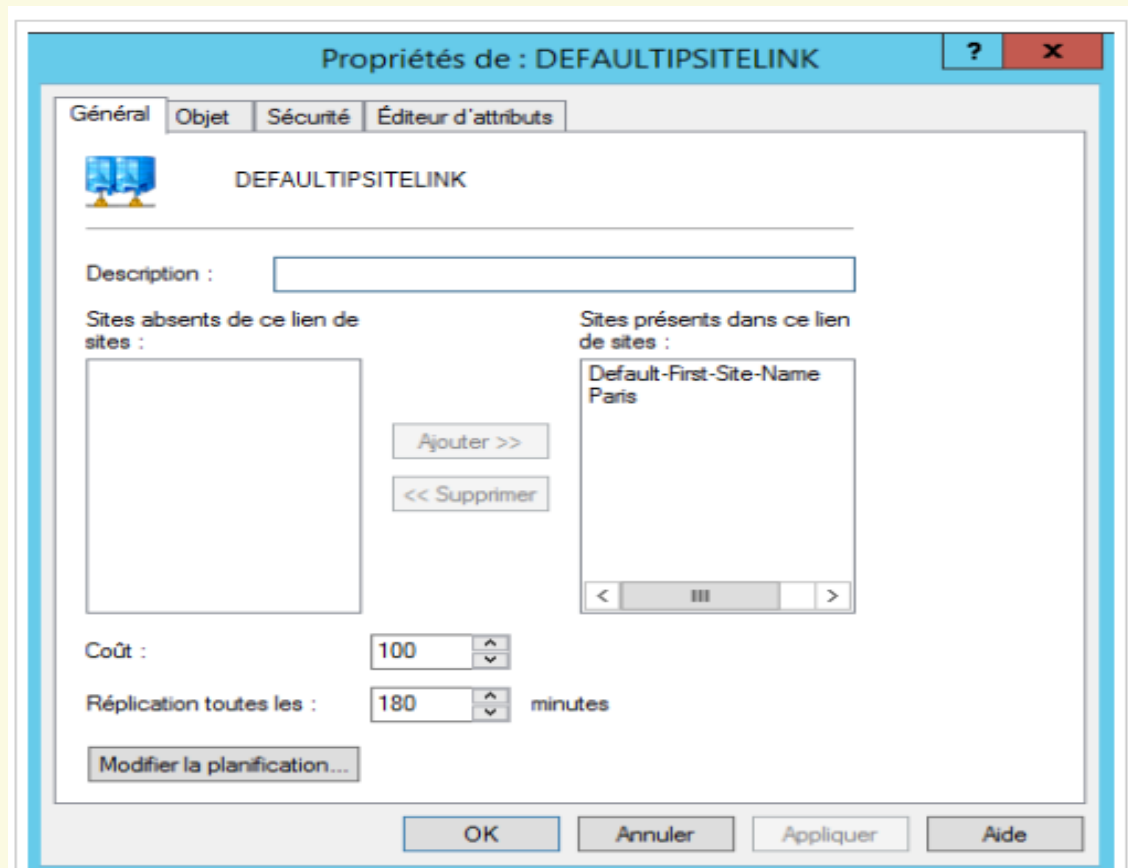
# Réplication : Quoi ? Quand ? Comment ?

- **Déclaration des sites**

- De plus, une notion de coût est intégrée pour chaque lien intersites. Ajustez sa valeur selon la vitesse, l'efficacité et la fiabilité de la liaison. Ainsi, si plusieurs liens connectent les mêmes sites, alors pour la réplication le lien ayant le coût le plus faible sera choisi. Le second lien faisant office de backup pour le mécanisme de réplication (cela n'empêche pas que ce lien soit utilisé pour autre chose).

# Réplication : Quoi ? Quand ? Comment ?

- **Déclaration des sites**



Propriétés du site par défaut

# Résumé

---

- AD DS fournit un service d'annuaire aux organisations qui leur permet d'offrir un accès sécurisé aux ressources réseau et une administration centralisée. ADDS permet l'authentification des utilisateurs, puis autorise ces derniers à accéder aux ressources réseau sur la base de cette authentification réseau. ADDS se compose de composants physiques et logiques. **Les composants logiques (domaines, forêts et unités d'organisation, par exemple)** permettent de regrouper des objets à des fins d'administration. **Les composants physiques (contrôleurs de domaine et sites, par exemple)** sont déployés pour offrir une expérience utilisateur cohérente au sein de l'environnement ADDS.

## Exercice scénarios pour l'implémentation de composants physiques et logiques AD DS

Déterminer les **composants physiques et logiques AD DS** à déployer dans les scénarios suivants :

- **Scenario 1** : La société **Zorro Bank** dispose d'un siège regroupant environ 100 salariés. Cette organisation possède également une petite succursale de 20 utilisateurs qui se connecte au siège par le biais d'une connexion réseau rapide et fiable. L'organisation comporte quatre services qui sont administrés par la même équipe.



Déterminer les **composants physiques et logiques** AD DS à déployer dans les scénarios suivants :

---

- **Scénario2:** La société **Océan indien** dispose de plusieurs sites situés dans deux pays. Dans chaque pays, la société possède 25 employés répartis dans deux services. Compte tenu des exigences de confidentialité des différents pays, les bureaux doivent être gérés dans chaque pays par un groupe différent d'administrateurs et ces derniers ne doivent pas pouvoir modifier les objets des autres pays.



A spiral-bound notebook is shown from a top-down perspective. The left side features a textured, light brown cover. The right side is a blank, cream-colored page with a thin horizontal line near the top. The metal spiral binding is visible along the left edge of the page.

Avez-vous des questions ?

A spiral-bound notebook is shown from a top-down perspective. The left side features a textured, light brown cover. The right side is a blank, cream-colored page with a thin horizontal line near the top. The metal spiral binding is visible along the left edge of the page.

Merci pour votre attention !