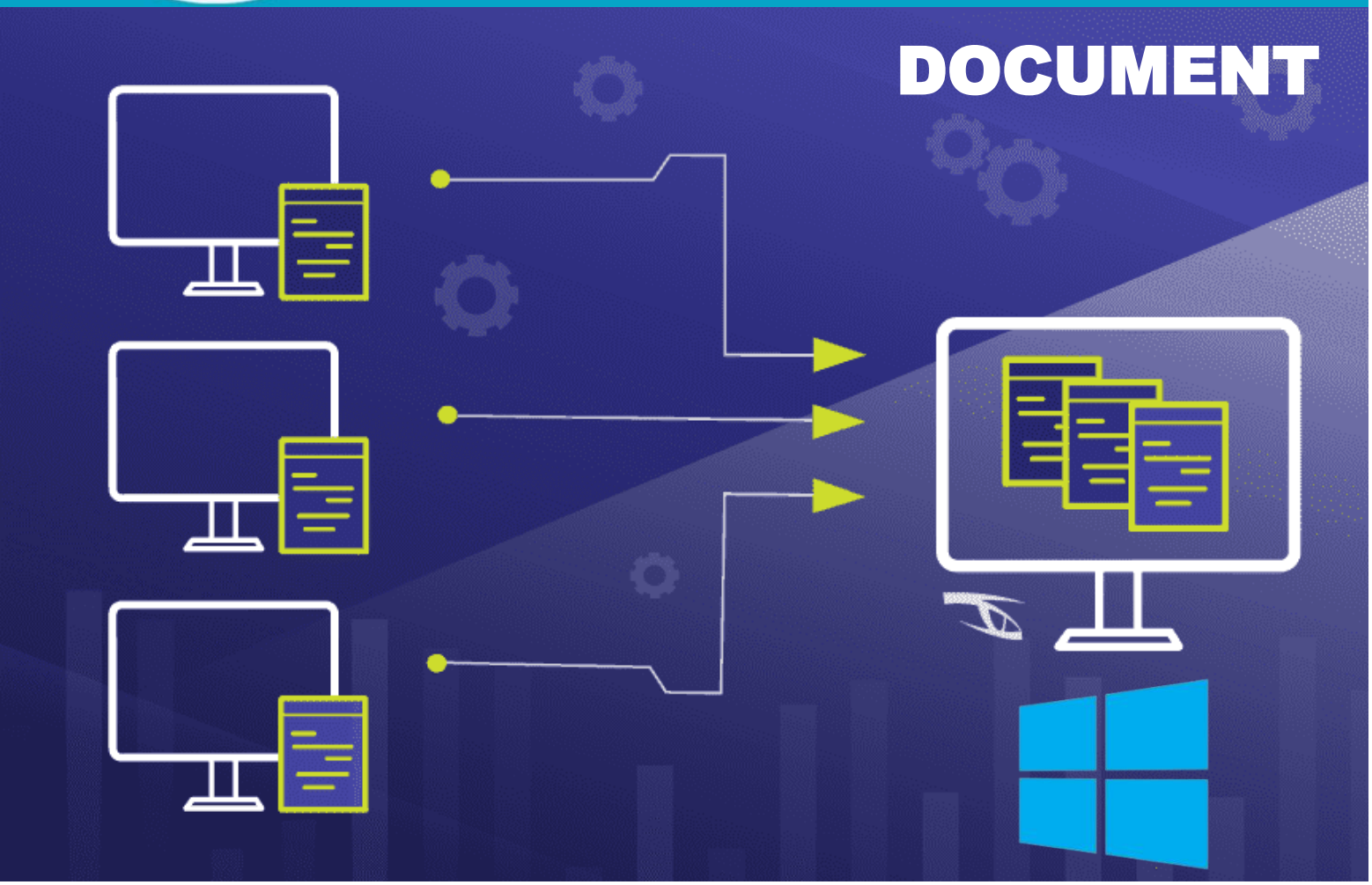
TUTOS-INFO

L'informatique par l'exemple

DOCUMENT



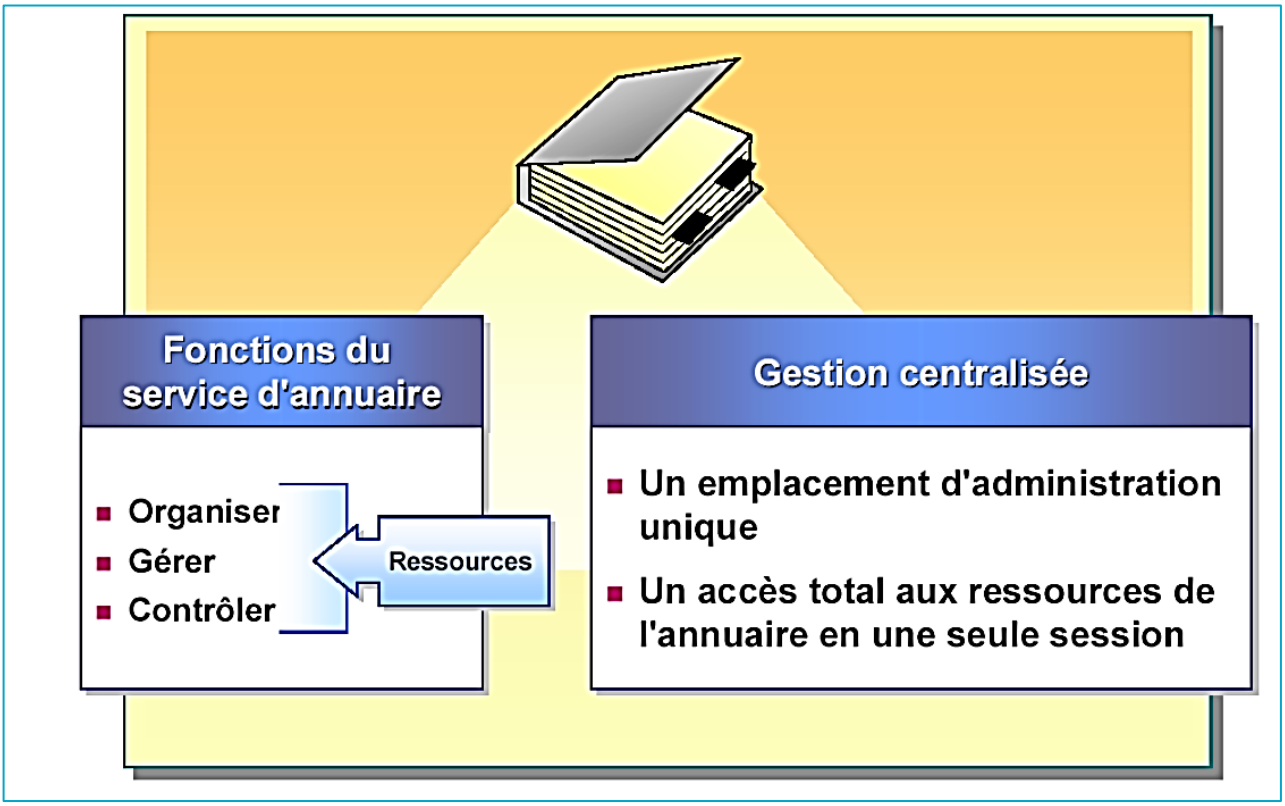
Active Directory

Comprendre Active Directory

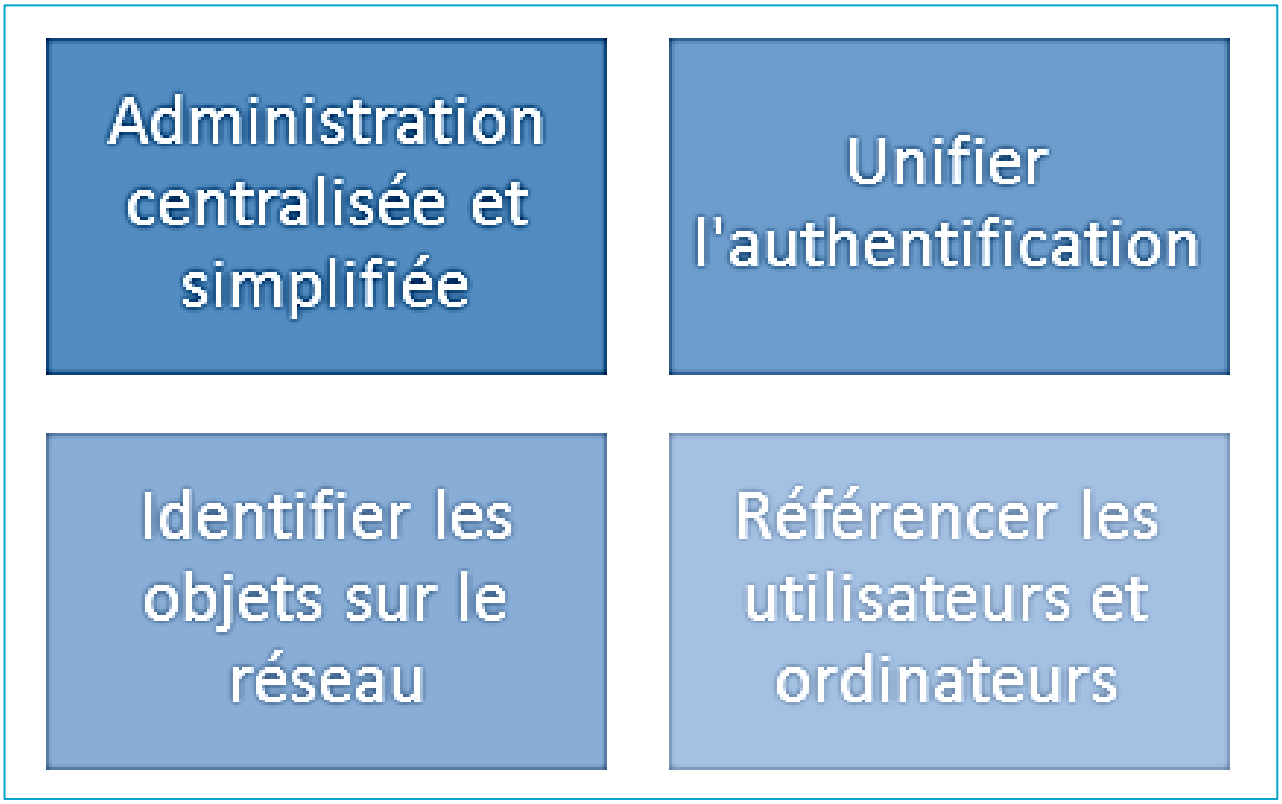
1. QU'EST-CE QUE L'ACTIVE DIRECTORY ?

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.



Comparé à un environnement « workgroup » (groupe de travail par défaut lorsque le serveur est dit « autonome », c'est-à-dire sans aucun rôle), un Active Directory apporte les avantages suivants :

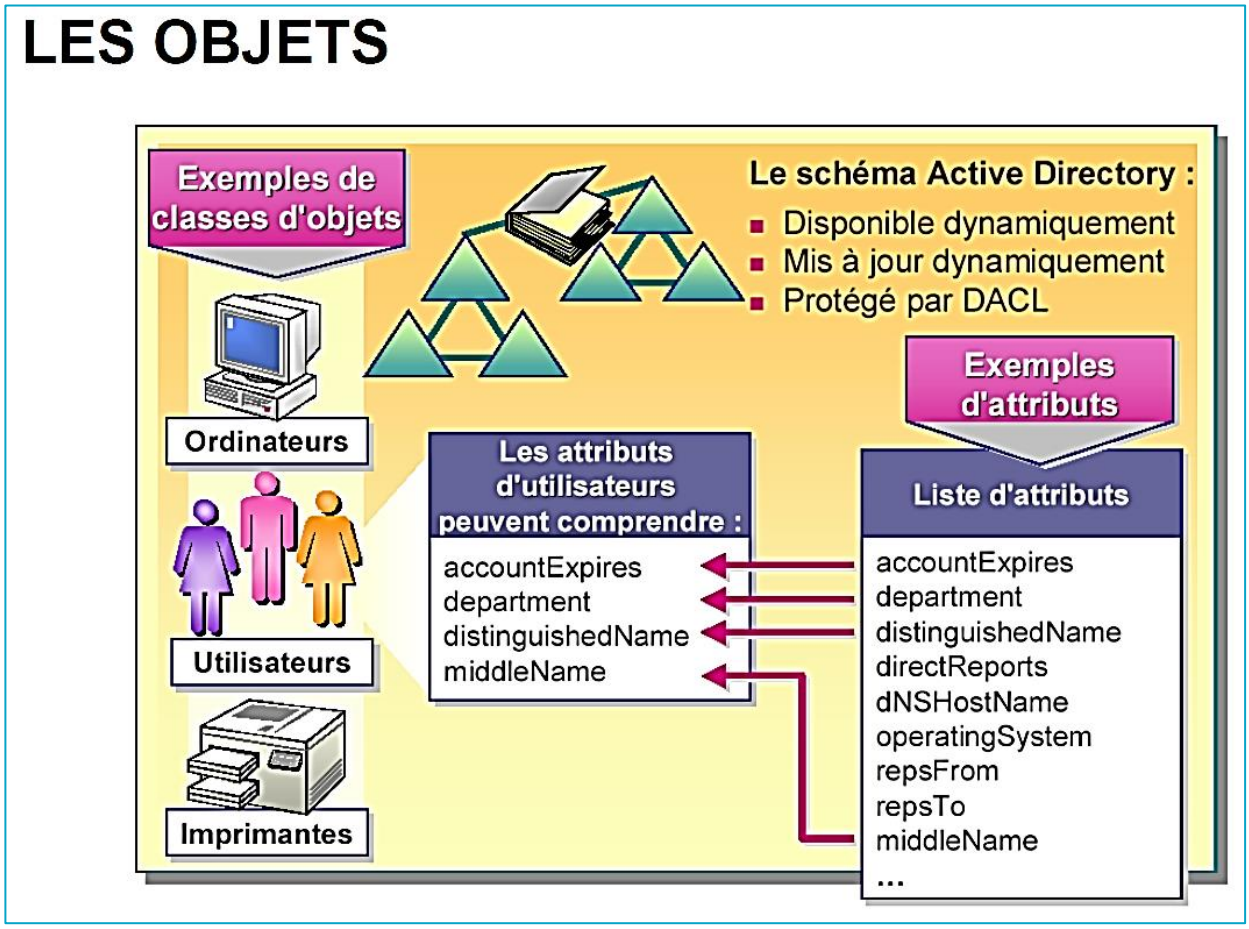


2. LA STRUCTURE DE L'ACTIVE DIRECTORY

A. Les classes et les attributs

Au sein de l'annuaire Active Directory, il y a différents types **d'objets** tels que : les ***utilisateurs***, les ***ordinateurs***, les ***serveurs***, les ***unités d'organisation*** ou encore les ***groupes***. En fait, ces objets correspondent à d**es 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.



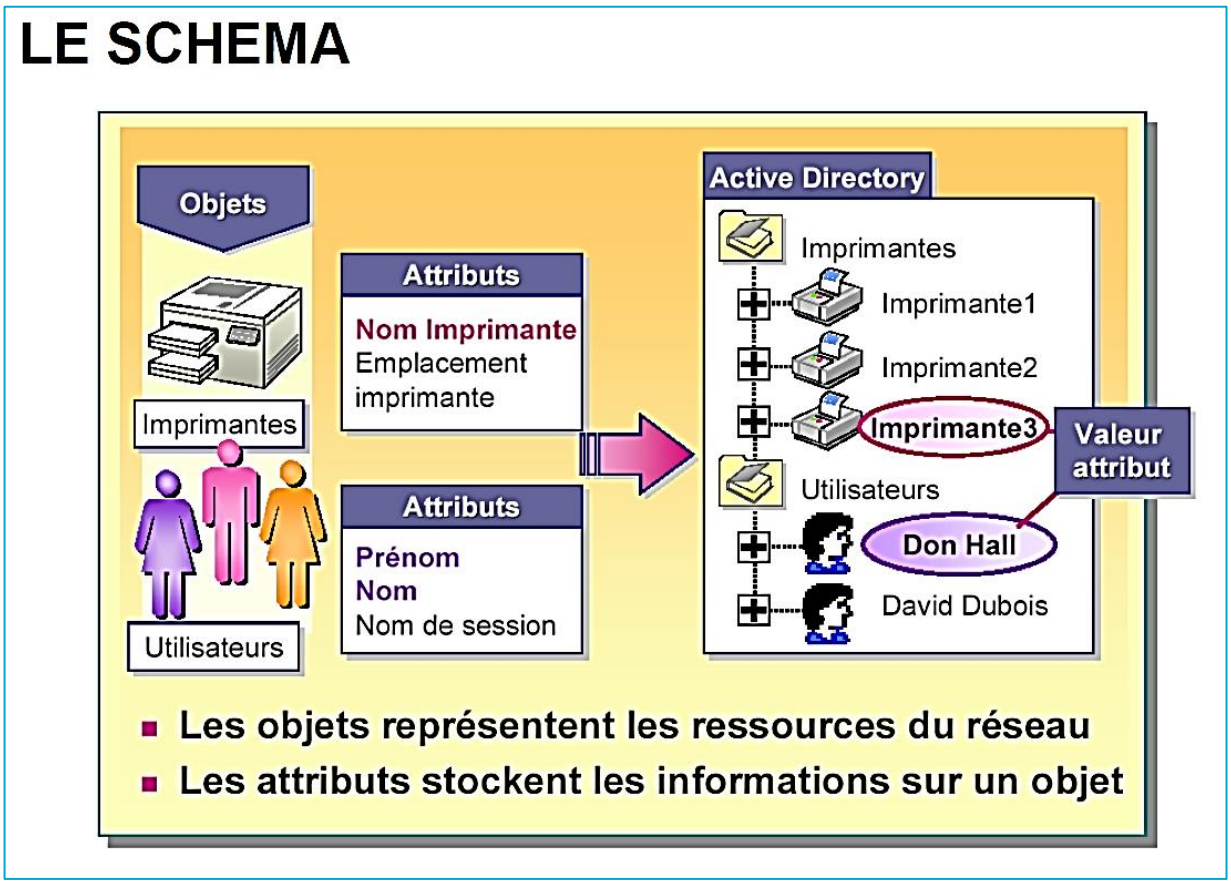
Par ailleurs, les **unités d'organisation (appelées « OU » pour « Organization Unit »)** sont des ***containers d'objets*** afin de faciliter l'organisation de l'annuaire et permettre une organisation avec plusieurs niveaux.

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

Comparez les unités d'organisations à des dossiers dans lesquels vous pouvez créer des sous-dossiers et enregistrer des fichiers.

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 votre annuaire. Il est à noter que le schéma est évolutif, le modèle de base n'est pas figé et peut évoluer selon vos besoins.

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

3. GROUPE DE TRAVAIL ET NOTION DE DOMAINE

Du groupe de travail au domaine

Pour rappel, toutes les machines sous Windows, lorsqu'elles sont installées, sont par défaut intégrées dans un groupe de travail appelé « ***WORKGROUP*** ».

Cela 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.

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.

- **Ce modèle devient très vite inadapté notamment pour la gestion des comptes utilisateurs en nombre**. En effet, chaque utilisateur devra disposer d'un compte sur chaque machine si l'on souhaite mettre en place une authentification.

Par exemple, une salle avec 10 machines nécessitera de créer le compte de l'utilisateur sur chacune des 10 machines si l'on veut qu'il conserve à chaque fois le même identifiant et le même mot de passe ! Donc pour 10 utilisateurs, il faudra créer 10 utilisateurs par machine x 10 soit 100 manipulations !

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.

- **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.

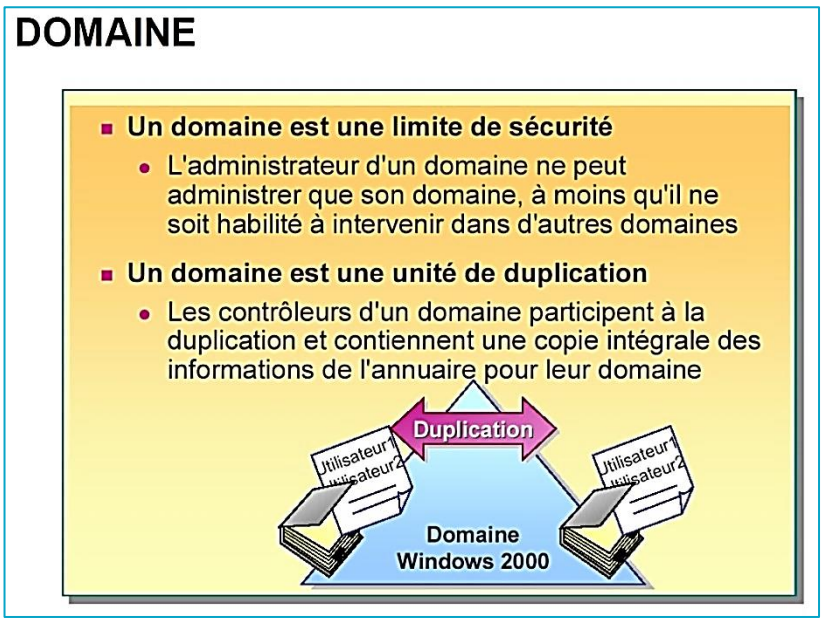
4. NOTION DE CONTROLEUR DE DOMAINE

A. Qu'est-ce qu'un contrôleur de domaine ?

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.



De plus, lorsque vous créez le premier contrôleur de domaine dans votre organisation, vous créez également le premier domaine, la première forêt, ainsi que le premier site.

B. Le 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.

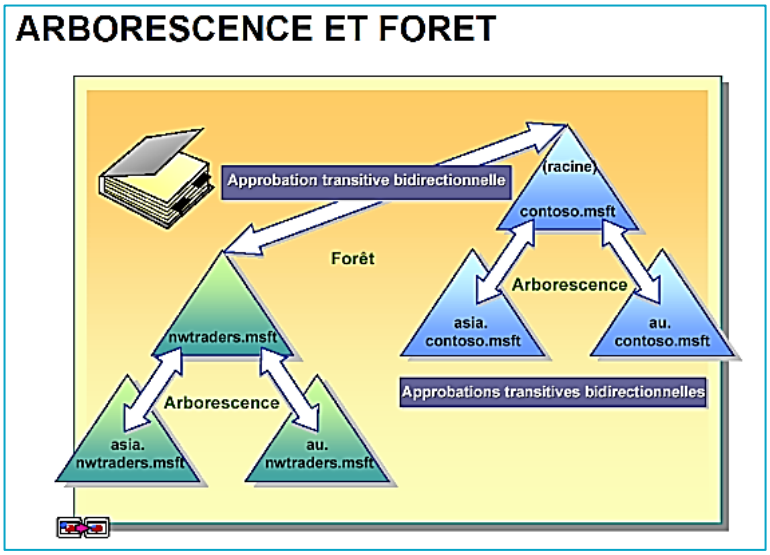
C. La réplication des contrôleurs de domaine

Afin d'assurer une haute disponibilité et d'éviter tout problème, il est vivement recommandé 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.

5. NOTION D'ARBRE ET DE FORET



Au sein du domaine schématisé par des triangles généralement, on retrouvera **tout un ensemble d'Unités d'Organisation remplies d'objets de différentes classes** : utilisateurs, ordinateurs, groupes, contrôleurs de domaine, etc…

De 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, voir même plusieurs sous-domaines selon le nombre de succursales.

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.**

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.

Mais alors qu'apporte la création d'une forêt ?

- Tous les arbres d'une forêt partagent un schéma d'annuaire commun.

- Tous les domaines d'une forêt partagent un « catalogue global commun ».

- 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.

- Simplification de l'administration et flexibilité. Un utilisateur d'un domaine pourra accéder à des ressources situées dans un autre domaine ou se connecter sur une machine du domaine si les autorisations le permettent.

6. NOTION DE NIVEAU FONCTIONNEL DU DOMAINE

Le ***niveau fonctionnel*** est une notion également à connaître lors de la mise en œuvre d'une infrastructure Active Directory. ***À la création d'un domaine, un niveau fonctionnel est défini*** et il correspond généralement à la version du système d'exploitation serveur depuis lequel on crée le domaine.

Par exemple, si l'on effectue la création du domaine depuis un serveur sous Windows Server 2012, le niveau fonctionnel sera « *Windows Server 2012* ». Dans un environnement existant, on est souvent amené à faire évoluer notre infrastructure, notamment les systèmes d'exploitation, ce qui implique le déclenchement d'un processus de migration. Une étape incontournable lors de la migration d'un Active Directory vers une version plus récente et le changement du niveau fonctionnel. Ainsi, il est important de savoir à quoi il correspond et les conséquences de l'augmentation du niveau.

Plus le niveau fonctionnel est haut, plus vous pourrez bénéficier des dernières nouveautés liées à l'Active Directory et à sa structure. Par exemple, **si le niveau fonctionnel est « Windows Server 2003 », vous ne pourrez pas ajouter un nouveau contrôleur de domaine sous Windows Server 2012 et les versions plus récentes.**

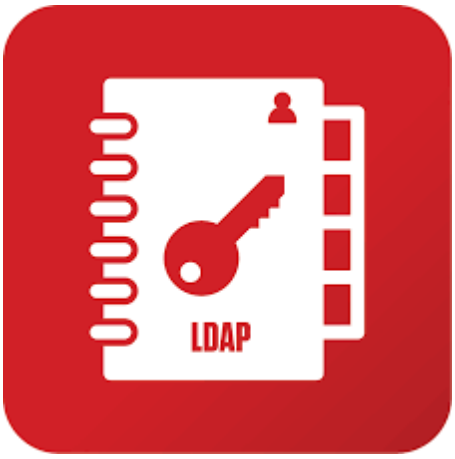
À l'inverse, si le niveau fonctionnel est « *Windows Server 2012* », **il sera impossible d'intégrer de nouveaux contrôleurs de domaine qui utilisent un système d'exploitation plus ancien que Windows Server 2012.**

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

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.

7. LE PROTOCOLE LDAP

A. Qu'est-ce que le protocole LDAP ?



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*) est qui apporte une couche de sécurité supplémentaire avec du chiffrement.

B. Que contient l'annuaire LDAP ?

L'annuaire LDAP correspond directement à l'Active Directory. Il contient 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, 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...).

C. Comment est structuré 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 (clé primaire) dans les bases de données pour identifier rapidement une ligne.

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).

COMPRENDRE L'ECRITURE LDAP

Par exemple, le chemin d'accès suivant, correspondant à un objet « *utilisateur* » nommé « *prof* », du domaine « laboprof.fr » et étant stocké dans une unité d'organisation (OU) nommée « *btssio* » : l**aboprof.fr,btssio,prof**

En « langage » LDAP, on traduira ainsi : **cn=prof,ou=btssio,dc=laboprof,dc=fr**

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

Dans un chemin LDAP vers un objet, on trouve toujours la présence du domaine sous la forme : « *dc=laboprof,dc=fr* » (ne pas mettre d'espace)

D. A quel moment a-t-on besoin d'utiliser le protocole LDAP ?

Le protocole LDAP permet de créer des liaisons entre une application et l'annuaire des utilisateurs.

Prenons pour exemple un helpdesk de type GLPI. Lorsque les utilisateurs du domaine souhaitent se connecter à l'interface GLPI pour saisir un ticket de maintenance, il est souhaitable que l'identifiant de connexion et le mot de passe soient les mêmes que ceux utilisés pour la connexion au domaine. On évite ainsi les erreurs et une accumulation d'identifiants avec des mots de passe nombreux.

Le protocole LDAP permet donc d'effectuer une liaison entre GLPI (par exemple) et l'Active Directory de manière à **importer les utilisateurs de l'annuaire AD** dans l'application GLPI. Ainsi, les utilisateurs ne seront pas à créer dans l'application puisqu'ils existent déjà dans l'annuaire et l'authentification de ces derniers restera identique.