# Cours - Les bases de l’Active Directory

*BTS SIO - B1/U4 Support et mise à disposition des services informatiques*

*1.2 Répondre aux incidents et aux demandes d’assistance et d’évolution*

# 1. L'annuaire Active Directory et les domaines

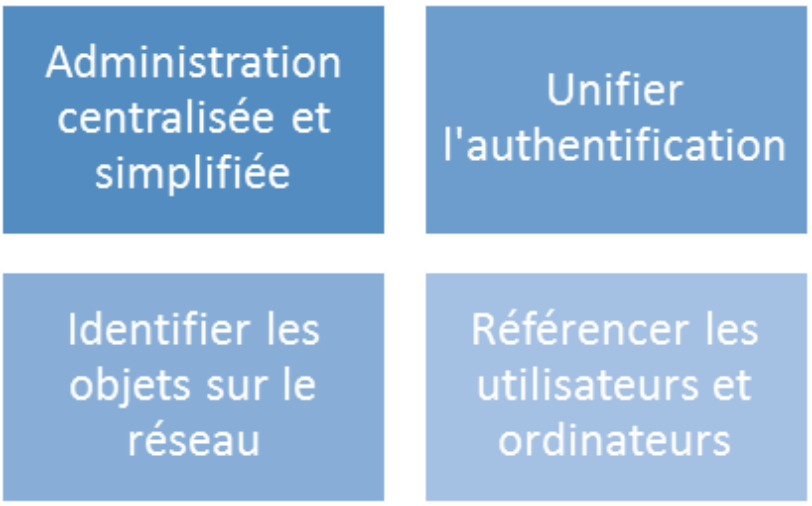
## 1.1. Qu'est-ce que l'Active Directory ?

**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.

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.

## 1.2. Quel est l'intérêt 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 intérêts ?




- **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.
- **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.
- **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.
- **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.

## 1.3. La structure de l'Active Directory

### *1.3.1. 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. Par ailleurs, les unités d'organisation sont des conteneurs 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 qui permettent de ranger les objets à l'intérieur, si cela est plus compréhensible pour vous.

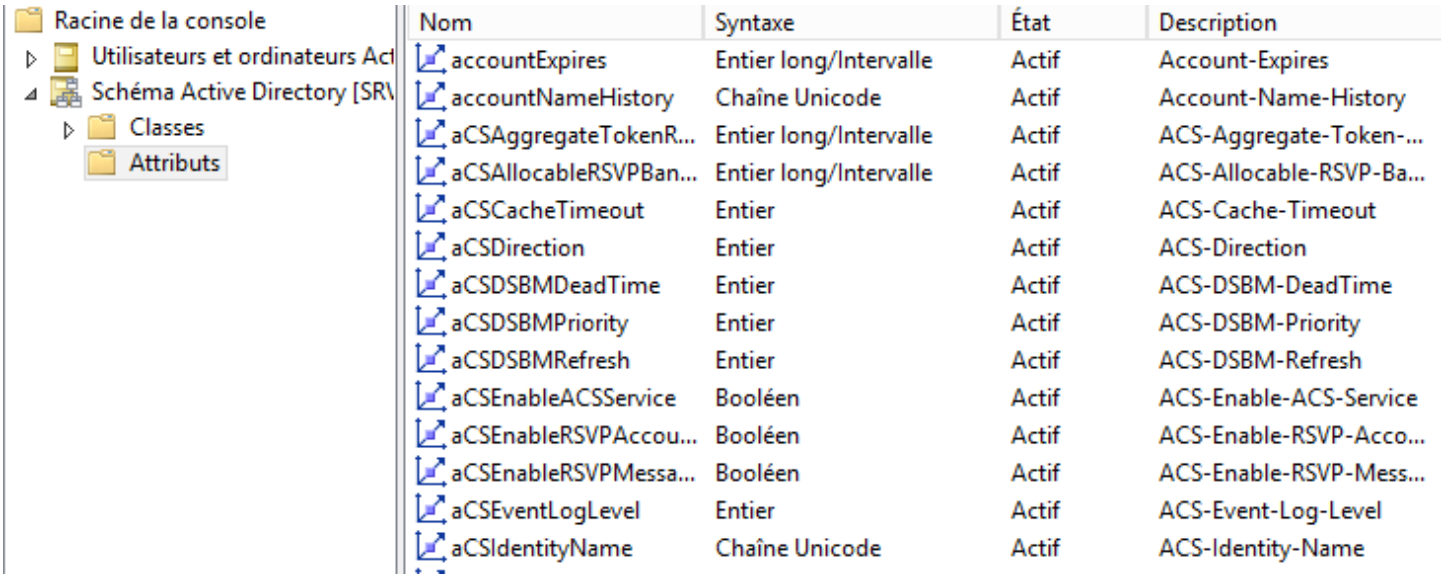
### *1.3.2. Le schéma*

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, voir même pour répondre aux prérequis de certaines applications.

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.




### *1.3.3. 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.
- **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.
- **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.

# 2. Contrôleur de domaine et domaine

## 2.1. Du groupe de travail au domaine

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.

### *2.1.1. 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.
- **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.

### *2.1.2. 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.
- **Administration et gestion de la sécurité centralisée**.

## 2.2. Les contrôleurs de domaine

### *2.2.1. 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.** Nous aborderons la notion de

forêt et de site un peu plus loin. Gardez à l'esprit qu'un contrôleur de domaine est un serveur qui contient une copie de l'annuaire Active Directory.

### *2.2.2. 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.

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.

### *2.2.3. La réplication des contrôleurs de domaine*

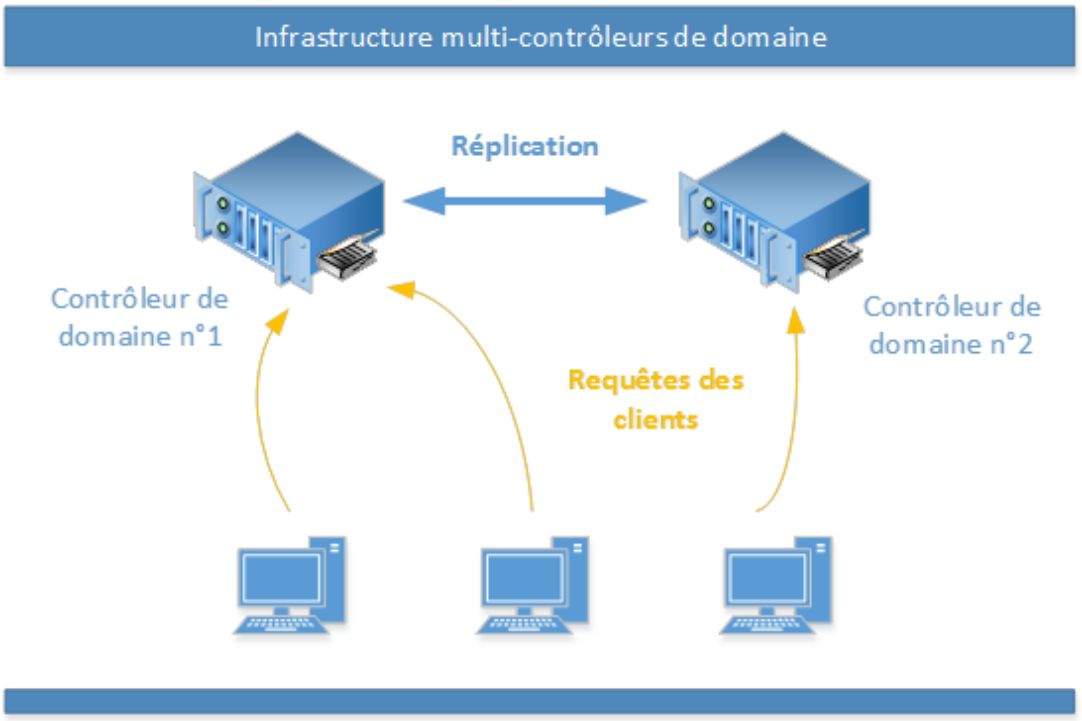
De nos jours, il est indispensable d'avoir au minimum deux contrôleurs de domaine pour assurer la disponibilité et la continuité de service des services d'annuaire. De plus, cela permet d'assurer la pérennité de la base d'annuaire qui est très précieuse. À partir du moment où une entreprise crée un domaine,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

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.

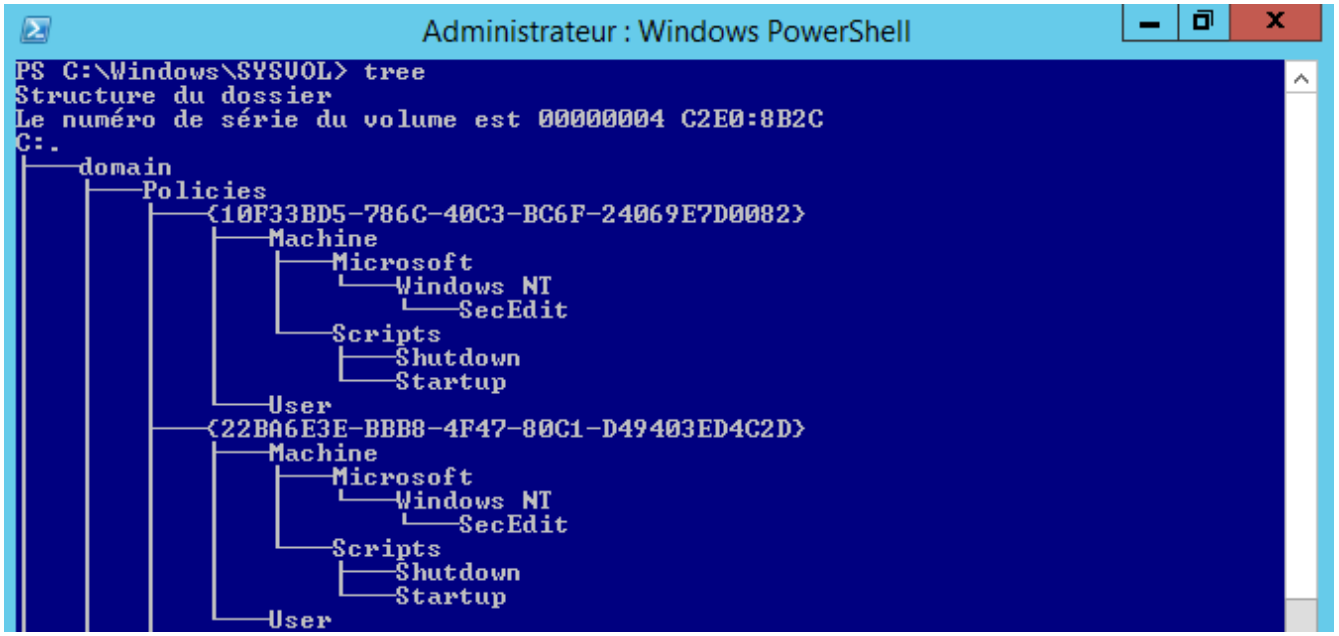
Ainsi, les contrôleurs de domaine répliquent les informations entre eux à intervalle régulier, afin de disposer d'un annuaire Active Directory identique. Sans rentrer dans les détails, un numéro de version est géré par les contrôleurs de domaine, ce qui permet à un contrôleur de domaine de savoir s'il est à jour ou non par rapport à la version la plus récente de l'annuaire.

Sur le schéma ci-dessous, on trouve deux contrôleurs de domaine, présents au sein d'un même domaine et qui répliquent entre eux des informations. Des postes de travail client sont également présents et intégrés dans ce domaine, ils contactent les contrôleurs de domaine pour effectuer différentes actions (authentification d'un utilisateur, demande d'accès à une ressource…).

Comme on peut le voir sur le schéma ci-dessous, lorsqu'il y a plusieurs contrôleurs de domaine, les requêtes sont réparties.



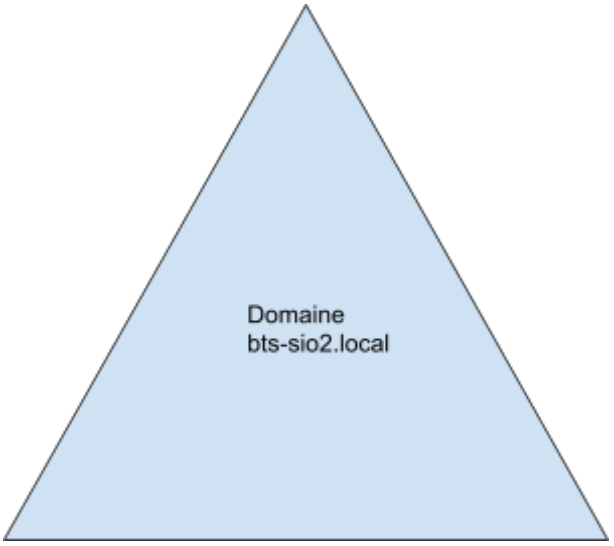

Par ailleurs, les contrôleurs de domaine répliquent le dossier partagé « **SYSVOL** » qui est utilisé pour distribuer les stratégies de groupe et les scripts de connexion.



# 3. Domaine, arbre et forêt

## 3.1. Symbolisation d'un domaine

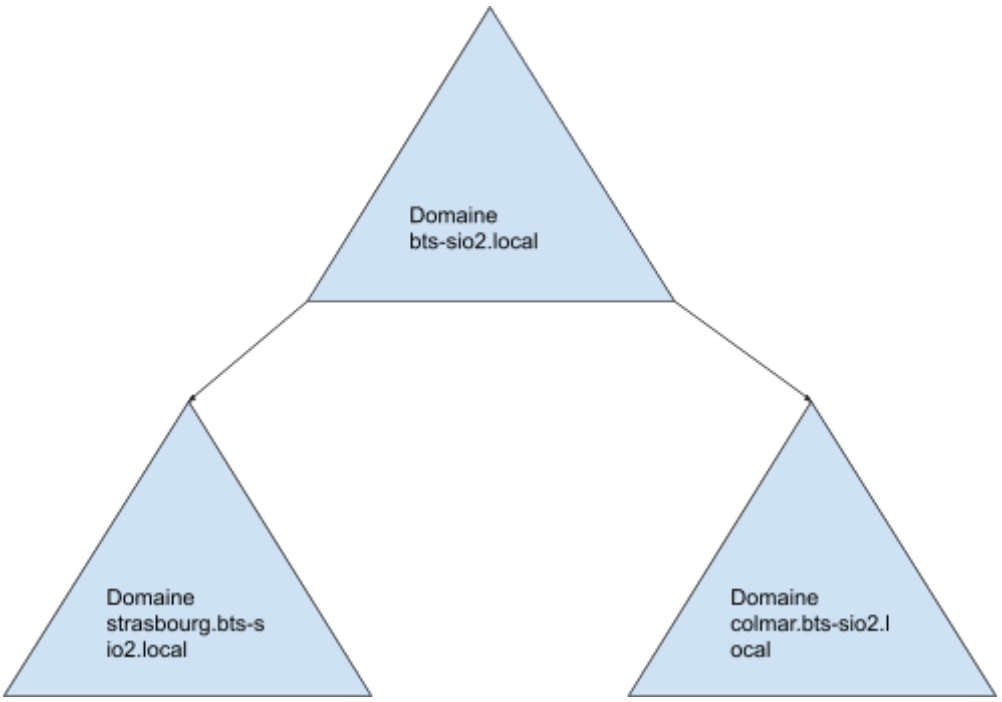
Lorsque vous verrez des schémas d'architecture Active Directory, vous verrez les domaines représentés par des triangles. Ainsi, notre domaine « *bts-sio2.local* » pourrait être schématisé ainsi :




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

Vous n'êtes pas sans savoir que de nombreuses entreprises ont plusieurs succursales, ce qui implique plusieurs sites sur différents emplacements géographiques. Selon l'importance de ces sites, on pourrait envisager de créer un sous-domaine au domaine principal, voire même plusieurs sous-domaines selon le nombre de succursales.

On part du domaine de base « *bts-sio2.local* », auquel on ajoute deux sous-domaines : « *strasbourg.bts-sio2.local* » et « *colmar.bts-sio2.local* » puisque nous avons deux succursales, une à Strasbourg, l'autre à Colmar. Voici la représentation de cette arborescence :



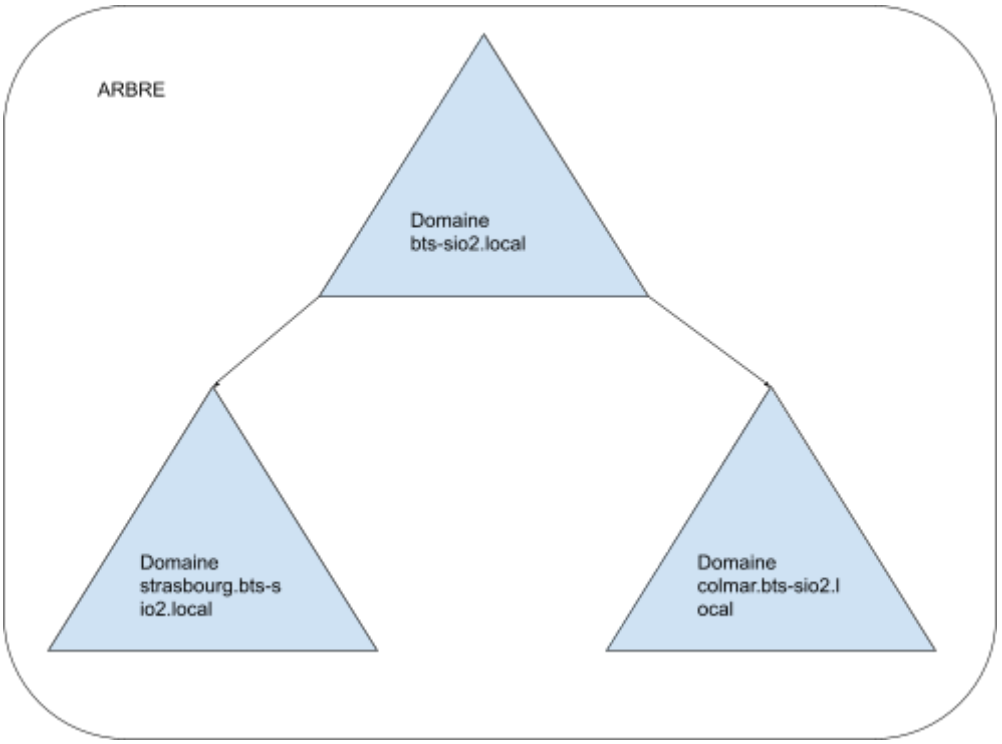

Sur le cas ci-dessus, les domaines « *strasbourg.bts-sio2.local* » et « *colmar.bts-sio2.local* » sont des sous-domaines du domaine racine « *bts-sio2.local* ». On appelle généralement ces domaines, « **des domaines enfants** ».

## 3.2. La notion d'arbre

La notion d'arbre doit vous faire penser à un ensemble avec différentes branches, si c'est le cas, vous êtes sur la bonne voie. 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.**

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




**Les domaines d'un même arbre partagent un espace de nom contigu et hiérarchique, comme c'est le cas avec l'exemple du domaine « *bts-sio2.local* ».**

## 3.3. La notion de forêt

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.

Pour simplifier l'administration, les accès et unifier le système d'information, on peut décider de créer un nouvel arbre dans la même forêt que celle où se situe l'arbre « *bts-sio2* ».

On peut alors affirmer que les différentes arborescences d'une forêt ne partagent pas le même espace de nom et la même structure.

Ainsi, on obtiendra une jolie forêt :

**Mais alors, une forêt pour quoi faire ?**

Vous devez vous dire, c'est bien joli de créer une forêt, de regrouper les domaines entre eux, mais alors qu'est-ce que ça apporte ?

- 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 du domaine « *paris.bts-sio2.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.

## 3.4. Le niveau fonctionnel

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 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.

### *3.4.1. Un niveau fonctionnel, c'est quoi ?*

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.

### *3.4.2. Pourquoi augmenter le niveau fonctionnel ?*

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

Par ailleurs, vous serez 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 », vous ne pourrez pas ajouter un nouveau contrôleur de domaine sous Windows Server 2012 et les versions plus récentes.**

Consulter le tableau des compatibilités sur le TechNet

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.

Augmenter le niveau fonctionnel du domaine via la console "Utilisateurs et ordinateurs Active Directory"

### *3.4.3. 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.

## 3.5. Domaine, arbre, forêt : conclusion

**Il faut garder à l'esprit :**

- **une forêt est un ensemble d'arbres,**
- **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**.

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

# 4. L’unité organisationnelle

Une unité organisationnelle (OU) ou unité d'organisation est un conteneur dans un domaine Microsoft Active Directory qui peut contenir des utilisateurs, des groupes et des ordinateurs.

Il est la plus petite unité par laquelle un administrateur peut affecter des paramètres de stratégie de groupe ou des autorisations de compte.

Une unité d'organisation peut avoir plusieurs sous-OU, mais tous les attributs de l'OU contenant doivent être uniques.

# 5. Les objets

## 5.1. Les différents types d'objets

Il est possible de trouver différents types d'objets Active Directory :

- Utilisateur : permet d'authentifier les utilisateurs physiques qui ouvrent une session sur le domaine. Des droits et permissions sont associés au compte afin de permettre l'accès à une ressource (dossier partagé, boîte aux lettres mail, imprimante...). Ce type d'objet peut également servir de compte de service
- Groupe : permet de rassembler différents objets (utilisateurs ou ordinateurs) qui doivent avoir un accès identique (lecture, modification...) sur une ressource (dossier partagé...). L'administration des permissions est plus aisée en utilisant des groupes.
- Ordinateur : permet d'authentifier des postes physiques ou virtuels connectés au domaine. Il est possible de positionner le compte ordinateur dans une ACL, cela permettra l'accès à une ressource. Si l'authentification ne peut être effectuée, l'ouverture de session sur le domaine est impossible.
- Unité d'organisation : conteneur qui permet l'organisation des objets de façon hiérarchique. Il est possible de lui appliquer une ou plusieurs stratégies de groupe. De plus, cet objet offre la possibilité de mettre en place une délégation.
- Imprimante : une imprimante partagée peut être publiée dans l'AD. Cette action simplifie les étapes de recherches et d'installation pour un utilisateur.

## 5.2. La gestion des objets

### *5.2.1. Le compte utilisateur*

Voir le document dédié à cette partie : Cours - Active Directory - 02 - Focus sur l'objet Utilisateur

### *5.2.2. Les groupes*

Voir le document dédié à cette partie : Cours - Active Directory - 03 - Focus sur les groupes

### *5.2.3. Le compte ordinateur*

Voir le document dédié à cette partie : Cours - Active Directory - 04 - Focus sur l'objet Ordinateur

### *5.2.4. La corbeille AD*

Voir le document dédié à cette partie : Cours - Active Directory - 05 - Focus sur l'objet Corbeille AD