

Chapitre 4

Services de domaine

Active Directory

1. Présentation des services de l'Active Directory

Active Directory est un annuaire implémenté sur les systèmes d'exploitation depuis Windows 2000 Server. Depuis cette première version de l'annuaire, de nombreuses améliorations ont été apportées.

1.1 La forêt Active Directory

Une forêt est une collection d'un ou plusieurs domaines Active Directory, le premier installé étant appelé domaine racine. Son nom DNS (exemple : Formation.local) sera également donné à la forêt. Dans notre exemple, la forêt aura le nom Formation.local. Dans une forêt, l'ensemble des domaines utilise la même configuration ainsi que le même schéma. Le système de partition est détaillé à la section Les partitions d'Active Directory.

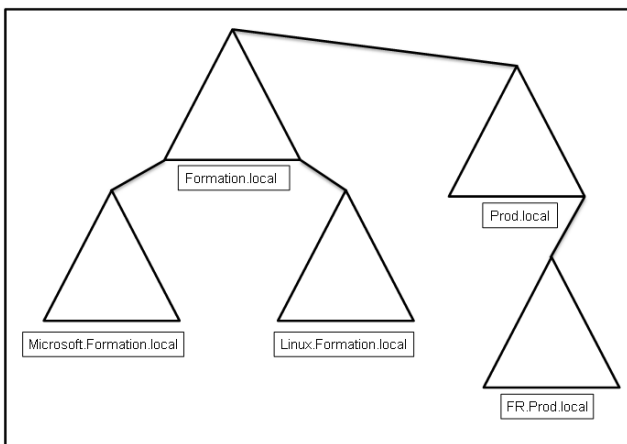
Aucune donnée (compte utilisateur, ordinateur...) n'est répliquée en dehors de la forêt, cette dernière sert donc de frontière de sécurité.

1.2 Le domaine et l'arborescence de domaines

Une arborescence de domaines est une suite de domaines qui partagent un espace de noms contigu. Ainsi dans l'exemple ci-après nous pouvons voir l'arborescence de domaines Formation.local. Cette dernière contient un domaine enfant nommé Microsoft.Formation.local. La racine Formation.local est bien identique à la racine du domaine (Microsoft.Formation.local).

La relation d'approbation entre **les domaines d'une même arborescence** est de type parent/enfant. Lors de l'ajout d'un domaine enfant, une relation d'approbation de type bidirectionnelle et transitive est créée automatiquement.

Si l'espace de noms est différent, nous parlerons dans ce cas d'une nouvelle arborescence. Les domaines Formation.local et Prod.local sont deux arborescences différentes dans la même forêt.



Le domaine représente une limite de sécurité où les utilisateurs sont définis.

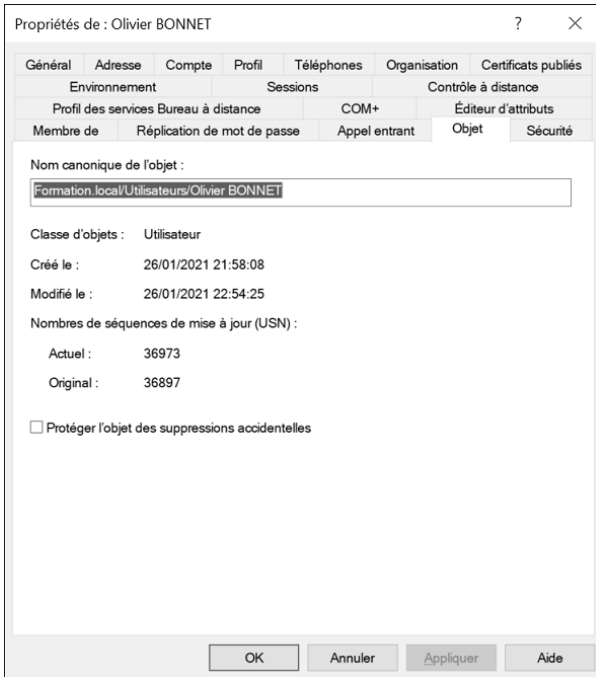
Un domaine contient au moins un contrôleur de domaine. Néanmoins il est recommandé d'en avoir deux afin d'assurer l'authentification en cas de maintenance ou de crash d'un des serveurs d'annuaire. Si plus aucun serveur n'est en ligne, l'authentification ne pourra plus être assurée, ce qui va impliquer une perte de production pour l'ensemble des utilisateurs.

Un serveur ayant le rôle de contrôleur de domaine a la responsabilité de l'authentification des comptes utilisateurs et ordinateurs.

1.3 L'unité d'organisation

Une **unité d'organisation (OU, Organizational Unit)** est un objet de type conteneur. Il permet d'effectuer une hiérarchisation dans l'annuaire Active Directory. Les objets (utilisateurs, ordinateurs) sont ainsi regroupés pour l'application d'une GPO (*Group Policy Object* - stratégie de groupe) ou pour faciliter l'administration. Il est possible également de déléguer l'administration des objets présents dans ce conteneur. Cette dernière action permet de donner à un utilisateur la possibilité d'effectuer une action (réinitialiser le mot de passe de l'utilisateur, ajouter des objets...) sans nécessiter de droits d'administrateur du domaine.

Depuis Windows Server 2008, il est possible de se protéger contre la suppression accidentelle d'une unité d'organisation. Par défaut lors de la création d'une OU, cette protection est activée. Il faudra décocher la case **Protéger l'objet des suppressions accidentelles** dans l'onglet **Objet** des propriétés pour pouvoir supprimer une OU. Notez que beaucoup d'autres objets peuvent être protégés mais nécessite d'activer manuellement (ou par script) la protection.



1.4 Les 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, etc.). L'administration des permissions est plus aisée en utilisant des groupes.

- **Ordinateur** : permet d'authentifier les 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 Active Directory. Cette action simplifie les étapes de recherche et d'installation pour un utilisateur.

1.5 Les partitions d'Active Directory

Active Directory utilise quatre types de partitions d'annuaire, toutes partagées par les contrôleurs de domaine. La création est effectuée lors de l'étape de promotion. Les partitions de configuration et de schéma sont partagées par l'ensemble des contrôleurs de domaine.

- **Partition de domaine** : contient les informations sur les objets qui ont été créés dans un domaine (attributs de compte utilisateur et d'ordinateur...). Ces informations sont présentes uniquement sur l'ensemble des serveurs d'annuaire du domaine concerné.
- **Partition de configuration** : permet de décrire la topologie de l'annuaire (liste complète des domaines, arborescences et forêt). L'ensemble des contrôleurs de domaine de la forêt se partagent les informations contenues dans cette partition.
- **Partition de schéma** : contient tous les attributs et classes de tous les objets qui peuvent être créés. Lors de la création d'un compte utilisateur, l'objet et ses propriétés sont dupliqués depuis le schéma. Lors de l'ajout d'un nouveau service (Exchange, sccm...), il est nécessaire de procéder à la mise à jour de cette partition. Il est intéressant de noter qu'un seul serveur dans la forêt contient le droit d'écriture sur le schéma, les autres étant uniquement en lecture seule.
- **Partition DNS** : contient la ou les bases de données DNS. Les enregistrements DNS, etc. y sont stockés.

Ces partitions sont stockées dans la base de données Active Directory, son emplacement physique sur le serveur d'annuaire est le répertoire **%systemroot%\NTDS**.

1.6 Les maîtres d'opération FSMO

Cinq rôles **FSMO** (*Flexible Single Master Operation*) existent dans une forêt Active Directory. Ils possèdent chacun une fonction au sein de l'annuaire et la perte de certain de ces rôles peut être problématique.

Deux rôles sont présents uniquement sur un des contrôleurs de domaine de la forêt, ils sont généralement présents au niveau du domaine racine (premier domaine de la forêt).

- **Rôle maître de schéma** : comme nous l'avons vu, le schéma est en lecture seule sur les contrôleurs de domaine. Néanmoins il est parfois nécessaire de procéder à sa mise à jour. Pour cela, un contrôleur de domaine dans la forêt dispose du rôle Maître de schéma.
- **Maître de dénomination de domaine** : lors d'une opération au niveau du domaine (ajout/suppression...), le serveur qui possède ce rôle permet d'assurer une cohérence des noms de domaine.

Les trois autres rôles sont présents sur chaque domaine de la forêt.

- **Maître RID** : ce rôle est donné à un des contrôleurs de domaine. Son rôle est l'attribution de **blocs d'identificateur relatifs (RID)** aux différents contrôleurs de domaine de son domaine qui en font la demande. Le RID est utilisé lors de la création d'un objet pour créer le **SID (identifiant de sécurité)**. Ce dernier est construit en associant le RID à l'identificateur de domaine (SID du domaine identique à l'ensemble des objets).
- **Maître infrastructure** : le serveur possédant ce rôle est responsable de la surveillance des objets des autres domaines de la forêt. Lors de la présence dans une ACL d'un objet étranger à son domaine, il a pour fonction la prise en charge de la vérification de l'état de ces objets (désactivé, renommé, supprimé...).
- **Maître émulateur PDC** : ce rôle a une importance capitale dans une forêt Active Directory. En effet il a pour rôle de synchroniser son horloge avec un serveur de temps. Par la suite les différents contrôleurs de domaine viendront effectuer la même opération en le prenant comme maître de temps. Ainsi l'ensemble des contrôleurs de domaine auront une horloge synchronisée. La gestion du temps est également importante pour les postes et serveurs. Ces derniers sont également synchronisés à l'aide des contrôleurs de domaine.

1.7 Le catalogue global

Un serveur catalogue global est un contrôleur de domaine qui possède une copie des attributs de tous les objets Active Directory de son domaine. Par défaut seuls certains attributs sont répliqués, il est néanmoins possible d'inclure d'autres attributs en fonction de votre besoin.

La console **Schéma Active Directory** permet de sélectionner les attributs à répliquer. Lors de l'authentification de l'utilisateur, le serveur catalogue global est interrogé, ceci afin de récupérer la liste des groupes universels dont l'utilisateur est membre.

1.8 Les sites AD

Afin de réduire l'utilisation des lignes reliant les différentes entités physiques (siège et sites distants), les domaines sont découpés de manière logique en sites AD. Ces derniers représentent généralement la topologie physique de l'entreprise. Dans un site AD, la connectivité réseau est considérée comme très bonne. On parlera de réplication intrasite (réplication entre les contrôleurs de domaine du site).

En créant ce découpage, avec les sites AD, l'administration des réplifications entre les sites est facilitée. Ainsi on économise la bande passante des liaisons WAN. La réplication sera de type intersites.

Lors d'une ouverture de session, le contrôleur de domaine du site AD sur lequel l'utilisateur est présent sera préféré. Néanmoins dans le cas où aucun serveur d'authentification n'est présent, le contrôleur de domaine d'un autre site sera utilisé.

1.9 La réplication intrasite et la réplication intersites

La réplication permet de s'assurer qu'une modification effectuée sur un contrôleur de domaine est transmise à ses paires. Cette opération s'effectue à l'aide d'objets de type « connexion ». Elles sont de type unidirectionnels (réplication entrante uniquement).

Ces chemins de réplication (objet connexion), vont permettre la création de la topologie de réplication. La vérification de la cohérence des données (**KCC**, *Knowledge Consistency Checker*) pourra être également assurée.

La topologie permet également d'avoir une continuité au niveau de la réplication et ce même en cas de défaillance d'un contrôleur de domaine. Il est donc **très important** de ne pas modifier les liens de connexion. L'ISTG effectue la création de la topologie et l'adapte en fonction des pannes des serveurs d'annuaire ou coupure réseau. Si les liens ont été modifiés manuellement, cette opération de mise à jour de la topologie ne s'effectue plus. Il est donc recommandé de laisser travailler l'ISTG sans intervenir.

Comme nous l'avons vu, il existe deux types de réplifications :

- Intrasite
- Intersites

La réplication intrasite permet une réplication des modifications pour les contrôleurs de domaine d'un même site.

À la suite d'une modification d'une des partitions Active Directory, une notification est effectuée au bout de 15 secondes par le contrôleur de domaine à son premier partenaire. Cette opération de notification a pour but de donner l'information du changement.

Trois secondes plus tard, une notification est envoyée aux autres contrôleurs de domaine. Ces délais dans les notifications permettent d'assurer une réduction du trafic réseau.

Suite à la notification, le serveur partenaire demande la modification. L'agent de réplification d'annuaire (**DRA**, *Directory Replication Agent*) peut par la suite opérer le transfert.

Dans le cas où aucune modification n'est effectuée, la méthode de scrutation est utilisée. Cette méthode consiste à interroger un serveur afin de connaître une éventuelle modification sur une des partitions de l'Active Directory. L'intervalle de scrutation pour une réplication intrasite est d'une heure. Cette valeur est celle par défaut.

La réplication de type intersites consiste à effectuer des réplifications sur des serveurs d'annuaire présent dans des sites AD différents.

L'**ISTG** (*Intersite Topology Generator*, générateur de topologie intersites) effectue la création d'objets de connexion entre les serveurs de chaque site. Cela permet la réplification intersites.

Pour les raisons évoquées plus haut, il est préférable de ne pas modifier ses liens de connexion.

Dans chaque site, un contrôleur de domaine est sélectionné afin d'obtenir le rôle de tête de pont. Ce dernier a la responsabilité de répliquer ou récupérer d'éventuelles modifications d'un autre serveur tête de pont. Par la suite une réplication de type intrasite s'opère. Cette élection est effectuée automatiquement. Pour les mêmes raisons que les liens de connexion, il est préférable de ne pas faire d'élection manuelle.

Pour effectuer la réplication intersites, deux protocoles sont utilisés :

- **IP** : utilisé pour toutes les réplifications intrasites et intersites. Ce protocole est très souvent utilisé.
- **SMTP** : utilisé principalement en cas de connexions non fiables. Une CA (autorité de certification) est nécessaire, ce qui alourdit l'administration. Ce protocole est très peu utilisé pour la réplication.