Annuaire : Active Directory

Un annuaire est une structure hiérarchique qui stocke des informations sur les objets du réseau. Un service d'annuaire, tel qu'Active Directory, fournit des méthodes de stockage des données de l'annuaire et met ces données à la disposition des utilisateurs et des administrateurs du réseau. Par exemple, Active Directory stocke des informations sur les comptes d'utilisateurs, notamment les noms, les mots de passe, les numéros de téléphone, etc. et permet à d'autres utilisateurs autorisés du même réseau d'accéder à ces informations.

I SERVICE D'ANNUAIRE

Le service d'annuaire Active Directory inclut les fonctionnalités suivantes :

✎ Un magasin de données, appelé également annuaire, qui stocke des informations sur les objets Active Directory. Ces objets incluent généralement des ressources partagées, telles que des serveurs, des fichiers, des imprimantes, ainsi que le compte d'utilisateur et le compte d'ordinateur réseau.

✎ Intégration du sous-système de sécurité afin de garantir un processus d'ouverture de session sécurisé sur le réseau, ainsi qu'un contrôle d'accès à la fois sur les requêtes de données de l'annuaire et sur les modifications des données.

✎ Un ensemble de règles, le schéma, qui définit les classes d'objets et d'attributs contenus dans l'annuaire, les contraintes et limites qui s'appliquent aux instances de ces objets et le format de leurs noms.

✎ Un catalogue global qui contient des informations sur chaque objet de l'annuaire. Ceci permet aux utilisateurs et aux administrateurs de retrouver des informations de l'annuaire quel que soit le domaine de l'annuaire qui stocke réellement les données.

✎ Un mécanisme de requête et d'index qui permet aux utilisateurs et aux applications du réseau de publier et de retrouver les objets et leurs propriétés.

✎ Un service de réplication qui distribue les données de l'annuaire sur un réseau. Tous les contrôleurs de domaine d'un domaine participent à la réplication et stockent une copie complète de toutes les informations de l'annuaire concernant leur domaine. Toute modification apportée aux données de l'annuaire est répliquée sur tous les contrôleurs de domaine du domaine.

Pour profiter au maximum des avantages offerts par Active Directory, l'ordinateur qui accède à Active Directory sur le réseau doit exécuter le logiciel client approprié. Sur les ordinateurs qui n'exécutent pas le logiciel client Active Directory, l'annuaire s'affichera simplement comme un annuaire Windows NT.

II VUE D'ENSEMBLE

Un domaine définit une limite de sécurité. L'annuaire inclut un ou plusieurs domaines, chacun avec ses propres stratégies de sécurité et ses propres relations d'approbation avec d'autres domaines. Les domaines présentent plusieurs avantages :

✎ Les stratégies et les paramètres de sécurité (notamment les droits administratifs et les listes de contrôle d'accès) ne traversent pas les domaines.

✎ En déléguant l'autorité administrative à des domaines ou à des unités d'organisation, il n'est plus nécessaire d'avoir un certain nombre d'administrateurs avec des droits d'administration étendus.

✎ Les domaines permettent de structurer votre réseau en fonction de votre organisation.

✎ Chaque domaine stocke uniquement les informations relatives aux objets qu'il contient. En fractionnant l'annuaire de cette façon, Active Directory peut évoluer et stocker de nombreux objets.

Les domaines sont des unités de réplication. Tous les contrôleurs de domaine d'un domaine spécifique peuvent recevoir des modifications et les répliquer sur d'autres contrôleurs de domaine du domaine.

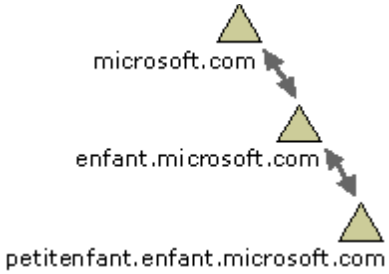
Un domaine unique peut s'étendre sur plusieurs emplacements physiques ou sites L'utilisation d'un domaine unique simplifie considérablement la surcharge administrative.

II.1 ARBORESCENCE DE DOMAINE ET FORÊT

Plusieurs domaines forment une **forêt**. Les domaines peuvent également se regrouper en structures hiérarchiques appelées arborescences de domaine.

II.1.1 ARBORESCENCES DE DOMAINE

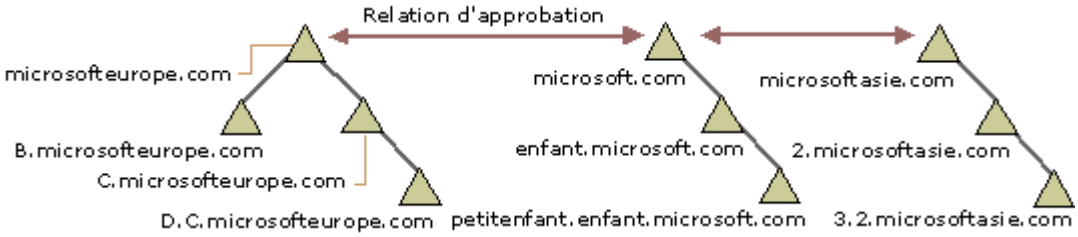
Le premier domaine d'une arborescence de domaine est appelé **domaine racine**. Les autres domaines de la même arborescence de domaine sont appelés **domaines enfants**. Un domaine situé immédiatement au-dessus d'un autre domaine de la même arborescence de domaine est appelé **domaine parent du domaine enfant**.



Tous les domaines qui ont un domaine racine commun forment un ***espace de noms contigu***. Cela signifie que le nom de domaine d'un domaine enfant correspond au nom de ce domaine enfant ajouté au nom du domaine parent. Dans cette illustration, enfant.microsoft.com est à la fois un domaine enfant de microsoft.com et le domaine parent de petitenfant.enfant.microsoft.com. Le domaine microsoft.com est le domaine parent du domaine enfant.microsoft.com. Il est également le domaine racine de cette arborescence de domaine.

II.1.2 FORÊTS

Une forêt se compose de plusieurs arborescences de domaine. Les arborescences de domaine à l'intérieur d'une forêt ne forment pas un espace de noms contigu. Par exemple, même si les deux arborescences de domaine, microsoft.com et microsoftasia.com peuvent avoir chacune un domaine enfant nommé «support », les noms DNS pour ces domaines enfants seraient support.microsoft.com et support.microsoftasia.com. Il n'existe pas d'espace de noms partagé.



Le domaine racine de la forêt est le premier domaine créé dans la forêt. Tous les domaines de toutes les arborescences de domaine situées dans une forêt partagent les caractéristiques suivantes :

- Un schéma commun
- Des informations de configuration communes
- Un catalogue global commun

En utilisant à la fois les arborescences de domaine et les forêts, vous disposez de la flexibilité offerte aussi bien par les conventions d'attribution de noms contigus que par les conventions d'attribution de

noms non contigus. Ceci peut être utile par exemple dans le cas des entreprises qui ont des services indépendants qui doivent conserver leurs propres noms DNS.

II.2 LES OBJETS D'UN DOMAINE

II.2.1 CONTRÔLEUR DE DOMAINE

Un contrôleur de domaine est un ordinateur qui exécute Windows Server, configuré à l'aide de l'Assistant Installation de Active Directory. L'Assistant Installation de Active Directory installe et configure les composants qui fournissent le service d'annuaire Active Directory aux utilisateurs et aux ordinateurs du réseau. Les contrôleurs de domaine stockent les données de l'annuaire et gèrent les interactions entre l'utilisateur et le domaine, y compris les processus d'ouverture de session, l'authentification et les recherches d'annuaire.

Un domaine peut posséder un ou plusieurs contrôleurs de domaine. Une organisation de petite taille qui utilise un réseau local unique peut nécessiter un seul domaine avec deux contrôleurs de domaine afin de garantir une disponibilité élevée et une tolérance de panne. Une organisation de grande taille avec plusieurs emplacements réseau nécessitera un ou plusieurs contrôleurs de domaine sur chaque emplacement afin de garantir une disponibilité élevée et une tolérance de panne.

II.2.2 SERVEURS MEMBRES

Un serveur membre est un ordinateur répondant aux caractéristiques suivantes : Exécute Windows Server, Est un membre de domaine, N'est pas un contrôleur de domaine.

Comme il ne s'agit pas d'un contrôleur de domaine, un serveur membre ne gère pas le processus d'ouverture de session de compte, ne participe pas à la réplication Active Directory et ne stocke pas les informations de stratégie de sécurité du domaine.

Les serveurs membres fonctionnent généralement comme les types de serveurs suivants : Serveurs de fichiers, Serveurs d'applications, Serveurs de bases de données, Serveurs Web, Serveurs de certificats, Pare-feux, Serveurs d'accès distant.

Ces serveurs membres possèdent un ensemble commun de fonctionnalités liées à la sécurité :

- Les serveurs membres sont conformes aux paramètres Stratégie de groupe définis pour le site, le domaine ou l'unité d'organisation.
- Les ressources disponibles sur un serveur membre sont configurées pour le contrôle d'accès.
- Les utilisateurs des serveurs membres sont affectés de droits d'utilisateur.
- Les serveurs membres contiennent une base de données de compte de sécurité locale, le Gestionnaire de compte de sécurité (SAM, Security Account Manager).

II.2.3 POSTE CLIENT

Les ordinateurs peuvent être rattachés à un domaine et affectés à des sites en fonction de leur emplacement dans un sous-réseau ou dans un ensemble de sous-réseaux correctement connectés.

Les sites facilitent l'authentification. En effet, lorsque les clients ouvrent une session sur un domaine en utilisant un compte de domaine, le mécanisme d'ouverture de session recherche tout d'abord les contrôleurs de domaine se trouvant dans le même site que le client. Si vous tentez d'utiliser des contrôleurs de domaine dans le site du client, le trafic de réseau est tout d'abord localisé, ce qui augmente l'efficacité du processus d'authentification.

Les ordinateurs peuvent partager leurs ressources. La gestion des droits d'accès est centralisée sur le contrôleur de domaine Active Directory.

II.2.4 LES UTILISATEURS

Il existe plusieurs types de comptes d'utilisateur, les comptes d'utilisateurs locaux et les comptes d'utilisateurs de domaine. Les comptes d'utilisateurs locaux sont propres à chaque ordinateur et sont stockés en local dans la base SAM.

Un **compte d'utilisateur de domaine** contient les informations propres à un utilisateur, et lui permet d'ouvrir une session sur un **domaine** pour accéder aux ressources réseau. Chaque personne qui se connecte régulièrement au réseau doit disposer d'un compte d'utilisateur de domaine.

Un **compte d'utilisateur de domaine** permet à un utilisateur d'ouvrir une session sur le domaine pour accéder aux ressources réseau. L'utilisateur peut accéder aux ressources réseau à partir de tout ordinateur du réseau, avec un même compte d'utilisateur et un même mot de passe. Ce type de compte d'utilisateur réside dans le **service d'annuaire Active Directory** du **contrôleur de domaine**.

II.2.5 GROUPES

Les groupes sont des objets Active Directory ou des objets d'ordinateur local pouvant contenir des utilisateurs, des contacts, des ordinateurs et d'autres groupes.

Ils permettent de :

- Gérer l'accès des utilisateurs et des ordinateurs aux ressources partagées telles que les objets Active Directory et à leurs propriétés, partages réseau, fichiers, répertoires, files d'attente d'impression, etc.
- Filtrer les paramètres de la stratégie de groupe
- Créer des listes de distribution de courrier électronique

Il existe deux types de groupes, les groupes de sécurité et les groupes de distribution.

Les groupes de sécurité sont utilisés pour regrouper des utilisateurs, des ordinateurs et d'autres groupes en unités faciles à gérer. Lors de l'attribution d'autorisations pour les ressources (partages de fichier, imprimantes et ainsi de suite), les administrateurs doivent les accorder à un groupe de sécurité plutôt qu'à des utilisateurs individuels. Les autorisations sont attribuées une seule fois au groupe, plutôt que de les attribuer une fois à chaque utilisateur individuel. Chaque compte ajouté à un groupe reçoit les droits et les autorisations définis pour ce groupe. Le fait de travailler avec des groupes plutôt qu'avec des utilisateurs individuels **simplifie** considérablement la **maintenance et l'administration du réseau**.

Les groupes de distribution ne peuvent être utilisés qu'en tant que listes de distribution de courrier électronique. Les groupes de distribution n'ont aucune fonction de sécurité.

Lorsque vous utilisez des groupes dans un seul domaine, vous utilisez la stratégie **A G DL P**.

Le principe de la stratégie A G DL P est le suivant : ajoutez des comptes d'utilisateur (**A**) dans des groupes globaux (**G**), placez les groupes globaux dans des groupes de domaine local (**DL**), puis accordez des autorisations (**P**) au groupe de domaine local.

II.3 LA RÉPLICATION

Active Directory utilise une **réplication multimaître**, ce qui permet à un contrôleur de domaine de la forêt d'effectuer des requêtes, y compris des modifications apportées à l'annuaire par les utilisateurs.

Les informations sur l'annuaire sont répliquées à la fois dans et parmi les sites. Active Directory réplique des informations dans un site précis plus régulièrement qu'à travers plusieurs sites. Cela permet d'équilibrer le besoin en informations sur l'annuaire à jour grâce aux limites imposées par la bande-passante du réseau disponible.

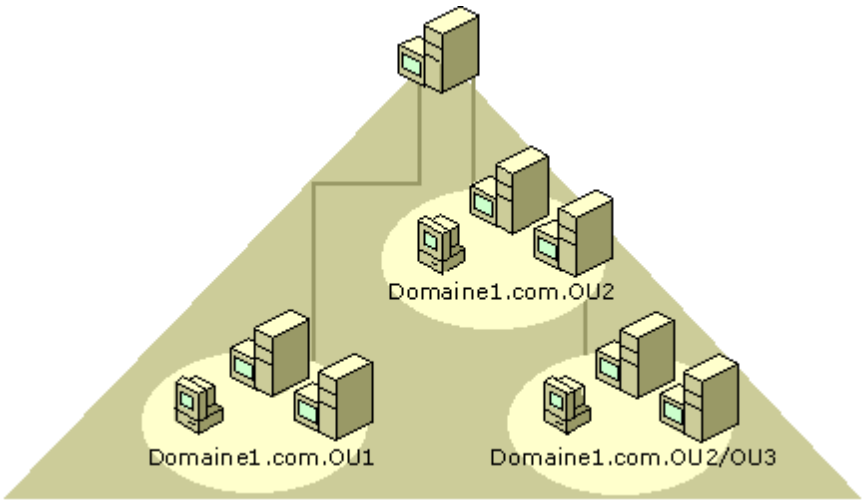
Vous pouvez personnaliser la façon dont Active Directory réplique des informations à l'aide de liaisons de sites pour spécifier le mode de connexion de vos sites. Vous pouvez fournir des informations sur le

coût d'une liaison de sites, sur les heures de disponibilité de la liaison et sur la fréquence d'utilisation de la liaison. Active Directory utilise ces informations pour définir quelle liaison de sites sera utilisée pour répliquer les informations. Le fait de personnaliser les calendriers de réplication afin que la réplication se produise à des heures précises, par exemple lorsque le trafic de réseau est faible, rend la réplication plus efficace.

II.4 UNITÉS D'ORGANISATION

Un type d'objet annuaire particulièrement utile contenu dans les domaines est l'unité d'organisation. Les **unités d'organisation** sont des **conteneurs** Active Directory dans lesquels vous pouvez placer des **utilisateurs**, des **groupes**, des **ordinateurs** et **d'autres unités d'organisation**. Une unité d'organisation ne peut pas contenir des objets d'autres domaines.

Une unité d'organisation est l'étendue ou l'unité la plus petite à laquelle vous pouvez attribuer des paramètres de Stratégie de groupe ou déléguer une autorité administrative. Avec les unités d'organisation, vous pouvez créer des conteneurs à l'intérieur d'un domaine afin de représenter les structures hiérarchiques et logiques de votre organisation. Ceci vous permet de gérer la configuration et l'utilisation des comptes et des ressources en fonction de votre modèle d'organisation.



Tel qu'il apparaît dans l'illustration, les unités d'organisation peuvent contenir d'autres unités d'organisation. Vous pouvez développer une hiérarchie de conteneurs selon vos besoins afin de traduire la hiérarchie de votre organisation à l'intérieur d'un domaine. Avec les unités d'organisation vous pouvez minimiser le nombre de domaines requis pour votre réseau.

Vous pouvez utiliser des unités d'organisation pour créer un modèle administratif auquel vous pourrez appliquer une échelle quelconque. Un utilisateur peut recevoir des droits d'administration pour toutes les unités d'organisation d'un domaine ou pour une seule unité d'organisation. Un administrateur d'une unité d'organisation ne requiert pas des droits d'administration pour les autres unités d'organisation du domaine.