Microsoft Windows Server : Service d'Annuaire & Active Directory

Notions et concepts liés aux systèmes Microsoft Windows Server

BTS SIO SISR – Bloc n°2 : Administration des systèmes

Sommaire

Présentation générale

Microsoft Windows Server – Généralités

Découverte des systèmes Windows Server : Différents systèmes Windows

- La première version pour serveur apparaît avec Windows NT.
- Voici l'historique des différentes versions de Windows Server accompagnées de leur date de sortie :
  - Windows NT 3.1 Juin 1993
  - Windows NT 3.5 Septembre 1994
  - Windows NT 3.51 Mai 1995
  - Windows NT 4.0 Juillet 1996
  - Windows 2000 Février 2000
  - Windows Server 2003 Avril 2003
  - Windows Home Server Juillet 2007
  - Windows Server 2008 Février 2008
  - Windows Server 2008 R2 Octobre 2009
  - Windows Server 2012 Septembre 2012
  - Windows Server 2012 R2 Octobre 2012
  - Windows Server 2016 Septembre 2016
  - Windows Server 2019 Octobre 2019
  - Windows Server 2022 Août 2021

Les éditions de Windows 2008

- Windows Server 2008 reprend les technologies déjà présentes dans les versions précédentes et apporte un lot d'améliorations utiles aux informaticiens pour la gestion d'une infrastructure serveur.
- Il s'agit par exemple de nouveaux outils de virtualisation, de ressources Web, de fonctions de gestion.
- Windows 2008 possède un ensemble d'outils, dont de nouvelles versions de IIS (Internet Information Services), de Server Manager et des plateformes Hyper-V ou Windows PowerShell.

Les éditions de Windows 2008

- Pour répondre à tous les besoins, Microsoft propose plusieurs éditions de Windows 2008 :
  - Standard
  - Enterprise
  - Datacenter
  - Web
  - Itanium
- Les éditions Standard, Enterprise, Datacenter et Web sont disponibles en versions 32 bits et 64 bits.
- L'édition Itanium n'est disponible qu'en version 64 bits
- Des versions 64 bits uniquement :
  - HPC (high performance computing)
  - Foundation

Découverte des systèmes Windows Server : Les éditions de Windows 2008

- Deux autres éditions sont également disponibles et concernent des petites ou moyennes entreprises :
  - Small Business Server
  - Essential Business Server
- Windows Server 2008 R2 est le premier système d'exploitation de Windows à être disponible uniquement pour les processeurs 64 bits.
- Ces éditions de Windows Server 2008 diffèrent dans leurs capacités de gestion : fonctionnalités, services, nombre de processeurs, etc.

Nouveautés et fonctionnalités de Windows 2008

- Ses fonctionnalités lui octroient des rôles particuliers de serveur en fonction de l'édition utilisée. On peut en avoir un aperçu en consultant le tableau ci-dessous.
- Les lettres F, W, S, E, D et I correspondent respectivement aux éditions de Standard, Enterprise, Web, Datacenter, Foundation et Itanium.

Nouveautés et fonctionnalités de Windows 2008

- Rôles et fonctionnalités en fonction des éditions :

Rôles autorisés du serveur	F	W	S	E	D	I
Web Services (IIS)	X	X	X	X	X	X
Application Server	X		X	X	X	X
Print and Document Services	X		X	X	X	
Hyper-V			X	X	X	
Active Directory Domain Services	X		X	X	X	
Active Directory Lightweight Directory Services	X		X	X	X	
Active Directory Right Management Services	X		X	X	X	
DHCP Server	X		X	X	X	
DNS Server	X	X	X	X	X	
Fax Server	X		X	X	X	
Windows® Deployment Services	O		O	X	X	
Active Directory® Certificate Services	O		O	X	X	
File Services	O		O	X	X	
Network Policy and Access Services	O		O	X	X	
Active Directory® Federation Services	O			X	X	
Windows Server® Update Services (WSUS)	X	X	X	X	X	

Les éditions de Windows 2012

- Windows Server 2012 est un système d'exploitation qui présente :
  - une interface graphique innovante,
  - des outils de gestion variés,
  - et des nouvelles fonctionnalités au niveau réseau, stockage et virtualisation.
- Une fonctionnalité majeure offerte par Windows Server 2012 est le service de « ***Cloud computing*** ».

Les éditions de Windows 2012

- Windows Server 2012 a été développé selon les principes suivants :
  - Modularité des composants du système d'exploitation ;
  - Intégration d'environnements de pré-installation et de pré-démarrage ;
  - Contrôle de compte d'utilisateur (UAC) et élévation de privilèges.

Les éditions de Windows 2012

- Windows Server 2012 est un système d'exploitation 64 bits qui offre quatre éditions répondant à différents besoins :
  - **Datacenter** : cloud computing privé et hybride, virutalisation (1 licence couvrant jusqu'à 2 processeurs),
  - **Standard** : possibilité de virtualisation en fonction de la licence (1 licence couvrant jusqu'à 2 processeurs),
  - **Essentials** : Petites et moyennes entreprises (licence limitée à 25 utilisateurs),
  - **Foundation** : clients recherchant un premier serveur (licence limitée à 15 utilisateurs).

Modes d'installation de Windows 2012

- Dans un objectif d'amélioration de la sécurité, Windows server 2012 propose de trois modes d'installation :
  - **Minimale** qui est l'option par défaut. Elle est analogue à l'option core de WS 2008 tout en augmentant la sécurité. Cette option n'installe pas les éléments d'interface utilisateur et les outils de gestion graphiques ;
  - **Avec une interface graphique** utilisateur qui est l'équivalent de l'installation complète proposée dans WS 2008 ;
  - **Intermédiaire** intitulée « **installation du serveur avec une interface minimale** » qui correspond à une installation serveur complète amputée de l'interpréteur de commandes graphique. L'interface utilisateur est donc minimale.

Rôles et fonctionnalités de Windows 2012

- Certains rôles et certaines fonctionnalités nécessitent une interface graphique et ne peuvent par conséquent n'être installés qu'avec le mode d'installation avec une interface graphique.
- Une installation minimale limite le nombre de rôles pouvant être installés à :
  - AD CS ;
  - AD DS ;
  - AD LDS ;
  - Serveur DHCP ;
  - Serveur DNS ;
  - Services de fichiers ;
  - Hyper-V ;
  - Services multimédia ;
  - Services d'impression et de documents ;
  - Routage et serveur d'accès distant ;
  - Services de diffusion multimédia en continu ;
  - Serveur Web IIS ;
  - Serveur de mise à jour de Windows Server.

Les éditions de Windows 2012 R2

- Il existe plusieurs éditions différentes de Windows Server 2012 R2 sélectionnables.
- Ces éditions permettent aux organisations de sélectionner une version de Windows Server 2012 R2 qui répond au mieux à leurs besoins, plutôt que de payer pour des fonctionnalités dont elles n'ont pas besoin.
- Lors du déploiement d'un serveur pour un rôle spécifique, les administrateurs système peuvent faire des économies substantielles en sélectionnant l'édition appropriée.

Les éditions de Windows 2012 R2

- les éditions Windows Server 2012 R2:
  - **Standard** : fournit l'ensemble des rôles et des fonctionnalités disponibles sur la plateforme Windows Server 2012 R2.
  - **Datacenter** : fonctionnalités qui sont disponibles sur la plateforme Windows Server 2012 R2. Inclut des licences d'ordinateur virtuel illimitées pour les ordinateurs virtuels qui sont exécutés sur le même matériel.
  - **Foundation** : Conçu pour les gérants de PME, prend en charge seulement 15 utilisateurs, ne peut pas être joint à un domaine et inclut des rôles serveur limités.
  - **Essentials :** Édition suivante de Small Business Server. Doit être le serveur racine du domaine. Il ne peut pas fonctionner en tant que serveur Hyper-V , de clustering avec basculement, avec une installation minimale, ni de service de bureau à distance. Il présente des limites pour 25 utilisateurs et 50 périphériques.

Les éditions de Windows 2016

- Windows Server 2016 met plus que jamais l'accent sur la virtualisation en incorporant une nouvelle version d' Hyper-V, son hyperviseur maison, livré en standard :
  - Protection des ressources: une limitation d'utilisation des ressources peut être activée pour éviter qu'une machine virtuelle utilise trop de ressources et dégrade les performances de la machine hôte et des autres VM ;
  - Nested Virtualization (virtualisation imbriquée) : permet d'utiliser Hyper-V dans une machine virtuelle exécutant Windows server 2016 et créer ainsi des machines virtuelles dans la machine virtuelle ;
  - Priorité de redémarrage des VM: permet de redémarrer les VM les plus importantes en premier ;
  - Storage QOS : possibilité d'appliquer des règles QOS sur les disques virtuels ;
  - Ajout/suppression de cartes réseau et mémoire à chaud : évite d'interrompre les services.

Les éditions de Windows 2016

- Windows Server 2016 met plus que jamais l'accent sur la virtualisation en incorporant une nouvelle version d' Hyper-V :
  - Microsoft ne pouvait pas passer à coté de la technologie des conteneurs qui constitue une nouveauté essentielle de 2016.
  - Il est possible d'utiliser des conteneurs compatibles docker ou Hyper-V
  - Le déploiement d'environnement de test, de développement ou même de production se fait plus facilement et rapidement.

Les éditions de Windows 2016

- Azure stack :
  - c'est le service cloud Microsoft ;
  - Azure stack permet d'installer un cloud Azure au sein de son datacenter.
- C'est un système de cloud hybride qui travaille indépendamment du cloud public Azure et du cloud privé sur le réseau local mais qui peut échanger des données avec les deux.

Les éditions de Windows 2016

- les éditions Windows Server 2016 :
  - Standard, Datacenter et Essentials
  - La version Essentials est réservée aux petites entreprises de maximum 25 personnes et 50 machines.
- Le prix dépend du nombre de cœurs présents dans le serveur.
- A cela, il faut ajouter les licences d'accès client (CAL), une licence par poste client (pour les versions Standard et Datacenter).

Les éditions de Windows 2019

- Nouveautés et fonctionnalités importantes :
  - L'hyper-convergence : Hyper-Convergant Infrastructure (HCI) est un framework IT rassemblant traitement (calcul), stockage, mise en réseau et virtualisation dans un seul système ;
  - Cela permet de combiner le meilleur de l'infrastructure cloud et locale grâce au logiciel Azure Stack HCI.
  - Cloud hybride : permet de combiner les environnements auto-hébergés (serveurs Windows 2019) et cloud (Azure).
  - Windows 2019 intègre un sous-système Linux (comme Windows 10) pour lequel, on va pouvoir installer une distribution Linux (Debian, Kali, ...)
    - Cela permettra de taper des commandes en bash et d'administrer, par exemple, des serveurs Web Linux comme Apache

Les éditions de Windows 2019

- Nouveautés et fonctionnalités importantes :
  - Containers : Microsoft ne pouvait pas passer à coté de la technologie des conteneurs qui est largement utilisée :
    - Il est possible d'utiliser des conteneurs compatibles docker ou Hyper-V
  - Le déploiement d'environnement de test, de développement ou même de production se fait plus facilement et rapidement.
  - A noter que Windows Server 2019 supporte Kubernetes, la solution containers de Google.

Les éditions de Windows 2019

- les éditions Windows Server 2019 :
  - Standard et Datacenter
- Le prix dépend du nombre de cœurs présents dans le serveur.
- A cela, il faut ajouter les licences d'accès client (CAL), une licence par poste client (pour les versions Standard et Datacenter).

Les éditions de Windows 2019

- La configuration matérielle minimale requise :
  - Architecture du processeur : x64
  - Cadence du processeur : 1,4 à 2 gigahertz (GHz)
  - Mémoire vive (RAM) : 512 Mo à 2 Go
  - Espace disponible sur le disque dur : 32 à 64 Go, et plus si le serveur a plus de 16 Go de RAM

Présentation générale

Microsoft Windows Server et le service d'annuaire Active Directory

Windows Server : Outils et protocoles réseau

- Windows Server implémente un ensemble d'outils d'administration du réseau tels que le centre réseau et Partage et les diagnostics réseau.
- Il offre 3 types d'identification réseau :
  - **Domaine** : les ordinateurs sont connectés au réseau d'entreprise ;
  - **Groupe de travail** : réseau privé dans lequel les ordinateurs appartiennent à un groupe de travail sans être directement connecté à Internet (partage réseau, partage d'imprimantes réseaux, ...);

Windows Server : Outils et protocoles réseau

- Il offre 3 types d'identification réseau (suite) :
  - **Réseau public** : réseau situé dans un lieu public (MAN).

- A « *chaque type de réseau* » est associé « *un profil de réseau* » qui possède notamment des ***paramètres de sécurité différents***.

Windows Server : Contrôleur de domaine, serveur membre et serveur

- L'installation d'un serveur ayant un système d'exploitation Windows Server 2012 nécessite une réflexion en amont qui définit en général l'assignation du serveur à un groupe de travail ou à un domaine.
- Un **groupe de travail** permet de gérer un ordinateur de **manière individuelle (peer-to-peer)**.
- Un **domaine** permet la gestion d'un ensemble d'ordinateurs de **manière collective** grâce à des **contrôleurs de domaine**.

Windows Server : Contrôleur de domaine, serveur membre et serveur

- Lors d'une installation de Windows Server 2012 sur un nouveau système, il est possible de configurer le serveur en tant que :
  - **Serveur membre** : il appartient à un domaine mais ne stocke pas d'informations d'annuaire ;
  - **Contrôleur de domaine** : il appartient à un domaine, stocke les informations d'annuaire, offre des services d'authentification et d'annuaire du domaine ;
  - **Serveur autonome** : il n'appartient à aucun domaine.

Windows Server : Annuaire (Active Directory)

- Windows Server 2012 offre un modèle de réplication dite « **multimaitre** » qui permet de répliquer automatiquement les modifications d'annuaire sur d'autres contrôleurs de domaine.
- Il permet de distribuer un annuaire complet d'informations appelé « **magasin de données** » est un ensemble d'objets représentant les **comptes utilisateur**, les **comptes de groupes**, les **comptes d'ordinateurs**, les **ressources partagées** (serveurs, fichiers, imprimantes…).

Windows Server : Annuaire (Active Directory)

- Depuis Windows Server 2008, la fonctionnalité d'annuaire a été regroupée et une famille de services connexes a été créée. Elle comprend notamment :
  - Active Directory Certificate Services (AD CS) : permet de déployer des autorités de certification et les services de rôle associés ;
  - Active Directory Domain Services (AD DS) : banque centralisée d'informations sur les objets réseau, y compris les comptes d'utilisateur et d'ordinateur. Utilisé pour l'authentification et l'autorisation ;

Windows Server : Annuaire (Active Directory)

- Depuis Windows Server 2008, la fonctionnalité d'annuaire a été regroupée et une famille de services connexes a été créée. Elle comprend notamment :
  - Active Directory Federation Services (AD FS) : fournit la prise en charge de l'authentification unique (SSO) via le Web et de la fédération des identités sécurisée (équivalent Linux RADIUS);
  - Active Directory Lightweight Directory Services (AD LDS) : prend en charge le stockage des données pour les applications orientées annuaire qui ne requièrent pas l'infrastructure complète des services de domaine Active Directory ;
  - Active Directory Rights Management Services (AD RMS) : permet d'appliquer des stratégies de gestion des droits pour empêcher tout accès non autorisé à des documents sensibles.

Windows Server : Annuaire (Active Directory)

- Les services de domaine Active Directory (AD DS) et les services associés constituent :
  - une **base** pour les **réseaux d'entreprise** qui exécutent **des systèmes d'exploitation Windows**.
  - une **base de données AD DS** est le **magasin central** de **tous les objets de domaine**, tels que les comptes d'utilisateur, les comptes d'ordinateur et les groupes.
  - **AD DS fournit un répertoire hiérarchisé interrogeable** et **une méthode pour l'application de la configuration** et **des paramètres de sécurité aux objets** de l'entreprise.

Windows Server : Annuaire (Active Directory)

- Les contrôleurs de domaine AD DS hébergent également le service qui authentifie les comptes d'utilisateur et d'ordinateur quand ils se connectent au domaine :
  - Comme AD DS stocke des informations sur tous les objets inclus dans le domaine et que tous les utilisateurs et ordinateurs doivent se connecter aux contrôleurs de domaine AD DS lorsqu'ils se connectent au réseau,
  - AD DS constitue le principal moyen vous permettant de configurer et gérer les comptes d'utilisateur et d'ordinateur dans votre réseau.

Windows Server : Annuaire (Active Directory)

- AD DS se compose à la fois de **composants physiques** et **logiques**.
- Vous devez comprendre la manière dont les composants d'AD DS fonctionnent ensemble de façon à pouvoir gérer efficacement votre réseau et contrôler à quelles ressources vos utilisateurs peuvent accéder.
- En outre, vous pouvez utiliser de nombreuses autres options AD DS, y compris l'installation et la configuration du logiciel et des mises à jour, la gestion de l'infrastructure de sécurité, l'activation de l'accès à distance et de DirectAccess, ainsi que la gestion des certificats.

Windows Server : Annuaire (Active Directory)

- Une des fonctionnalités d'AD DS est la fonctionnalité **Stratégie de groupe** qui permet de configurer des stratégies centralisées que vous pouvez utiliser pour gérer la plupart des objets dans AD DS.
- La compréhension des divers composants AD DS est importante pour pouvoir utiliser correctement la fonctionnalité **Stratégie de groupe**.

Active Directory : composants physiques et logiques

- Les composants physiques : les informations relatives à AD DS sont stockées dans un fichier unique sur le disque dur de chaque contrôleur de domaine :
  - **Contrôleurs de domaine** : contiennent des copies de la base de données AD DS.
  - **Magasin de données** : un fichier sur chaque contrôleur de domaine qui stocke les informations AD DS.
  - **Serveurs de catalogue global** : hébergent le catalogue global, lequel est une copie partielle, en lecture seule, de tous les objets dans la forêt. Un catalogue global accélère les recherches d'objets susceptibles d'être stockés sur des contrôleurs de domaine d'un domaine différent de la forêt.

Active Directory : composants physiques et logiques

- Les composants physiques : les informations relatives à AD DS sont stockées dans un fichier unique sur le disque dur de chaque contrôleur de domaine :
  - **Contrôleurs de domaine en lecture (RODC) :** installation spéciale d'AD DS dans une forme en lecture seule. Elle est souvent utilisée dans les filiales où la sécurité et l'assistance informatique sont souvent moins avancées que dans les centres d'affaires principaux.

Active Directory : composants physiques et logiques

- Les composants logiques AD DS sont des structures utilisées pour l'implémentation d'une conception Active Directory appropriée à une organisation.
- Voici certains types de structures logiques qu'une base de données Active Directory peut contenir.
  - **Partition :** une section de la base de données AD DS - la base de données AD DS est représentée en un seul fichier nommé « NTDS.DIT », elle est affichée, gérée et répliquée comme si elle était composée de sections ou d'instances distinctes. Celles-ci sont appelées partitions ou encore contextes d'appellation.

Active Directory : composants physiques et logiques

- Voici certains types de structures logiques qu'une base de données Active Directory peut contenir.
  - **Schéma :** définit la liste des types d'objets et d'attributs que tous les objets dans AD DS peuvent avoir.
  - **Domaine** : limite d'administration logique pour les utilisateurs et les ordinateurs.
  - **Arborescence de domaine** : collection des domaines qui partagent un domaine racine commun et un espace de noms DNS (Domain Name System).

Active Directory : composants physiques et logiques

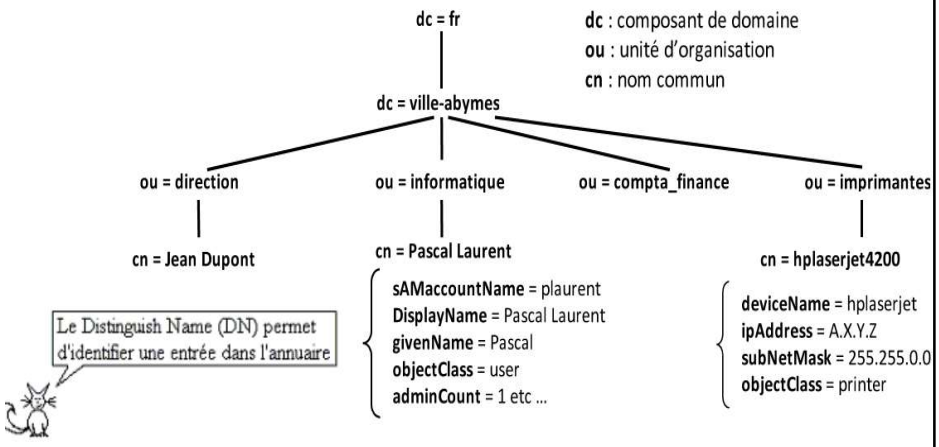
- Voici certains types de structures logiques qu'une base de données Active Directory peut contenir.
  - **Forêt :** collection des domaines qui partagent un service AD DS commun.
  - **Site** : collection d'utilisateurs, de groupes et d'ordinateurs, tels qu'ils sont définis par leurs emplacements physiques. Les sites sont utiles dans des tâches d'administration de la planification telles que la réplication des modifications apportées à la base de données AD DS.
  - **Unité d'organisation** : les unités d'organisation (OU) sont des conteneurs dans AD DS qui fournissent une infrastructure pour déléguer des droits d'administration et pour lier des objets de stratégie de groupe (GPO).

Active Directory : protocole LDAP et service d'annuaire

- La structure d'un annuaire LDAP est une arborescence (un arbre) hiérarchique appelée **DIT** (Directory Information Tree – Arbre d'information de l'annuaire).
- Le protocole **LDAP** (Lightweight Directory Access Protocol – Protocole léger d'accès à un annuaire) 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, **Active Directory** est **un annuaire LDAP**.
  - **Remarque :** les communications LDAP s'effectuent sur le port 389.

Active Directory : protocole LDAP et service d'annuaire

- La structure d'un annuaire LDAP :



Active Directory : Distinguished Name et le GUID

- Un ***Distinguished Name*** correspond à une entrée de l'annuaire :
  - Un annuaire est un ensemble d'entrées.
  - Ces entrées étant elles-mêmes constituées de plusieurs attributs.
  - 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.

Active Directory : Distinguished Name et GUID

- L'identifiant unique d'un objet est appelé GUID « 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 qu'un chemin complet pour accéder à cet objet dans l'annuaire.
  - **Exemple - DN : cn=Pascal laurent, ou=informatique, dc=ville-abymes, dc=fr**

Active Directory : classes d'objets et attributs

- Les différentes classes d'objet que nous retrouvons dans cet annuaire LDAP sont :
  - Des comptes utilisateurs, des unités d'organisation et des périphériques.
  - Mais un annuaire LDAP peut aussi contenir des groupes, des ordinateurs et des contacts.
- Pour chaque classe d'objets, l'annuaire LDAP stocke des 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 email etc …)

Active Directory : structure d'un annuaire LDAP

- Sachez que nous pouvons structurer un annuaire LDAP selon la société et sa répartition géographique ou ses secteurs d'activités.
- Mais aussi partir sur une structure basée sur les objets (utilisateurs, groupes, imprimantes, …).
  - **Remarques :**
    - En règle général, en termes de performance, il vaut mieux avoir un arbre le plus plat possible (très peu de niveaux).
    - Par contre, en termes de facilité d'administration, il vaut mieux introduire des branches par type d'objet ou par organisation ; cela facilite les mises à jour de données ou la mise en place des droits d'accès spécifiques. Si l'organisation change souvent et que le personnel est très mobile, le branchage par organisation est à proscrire.

Active Directory : rôle d'un service d'annuaire

- Un 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.
- Il présente les avantages (intérêts) suivants :
  - **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.

Active Directory : rôle d'un service d'annuaire

- Il présente les avantages (intérêts) suivants :
  - **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). Un seul compte peut permettre un accès à tout le système d'information, ce qui est fortement intéressant pour les collaborateurs, surtout que de nombreuses applications sont capables de s'appuyer sur l'Active Directory pour l'authentification.
  - **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.

Active Directory : rôle d'un service d'annuaire

- Il présente les avantages (intérêts) suivants :
  - **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…

Active Directory : un service DNS indispensable

- Sans le service DNS l'Active Directory ne fonctionnera pas.
- C'est d'ailleurs pour ça que lors de la mise en place d'un domaine, l'installation du serveur DNS est proposée.
- **Le protocole DNS est utilisé pour la résolution des noms,** ce qui permet aux postes clients de localiser les contrôleurs de domaine au sein de votre système d'information.
- De la même manière, lorsque l'on souhaite joindre un client au domaine, on utilise un nom comme « ***ville-abymes.fr*** », ce qui implique une requête DNS pour savoir quelle est l'adresse IP correspondante à ce nom, vous serez alors redirigé vers votre contrôleur de domaine qui traitera la requête.

Active Directory : un service DNS indispensable

- Le serveur DNS crée une zone correspondante à votre domaine et stocke de nombreux enregistrements.
- Il y a bien sûr un enregistrement (de type A) pour chaque contrôleur de domaine
- **Remarques :**
  - 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.

Active Directory : différence « domaine » et « 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*** » :
  - 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.

Active Directory : différence « domaine » et « groupe de travail »

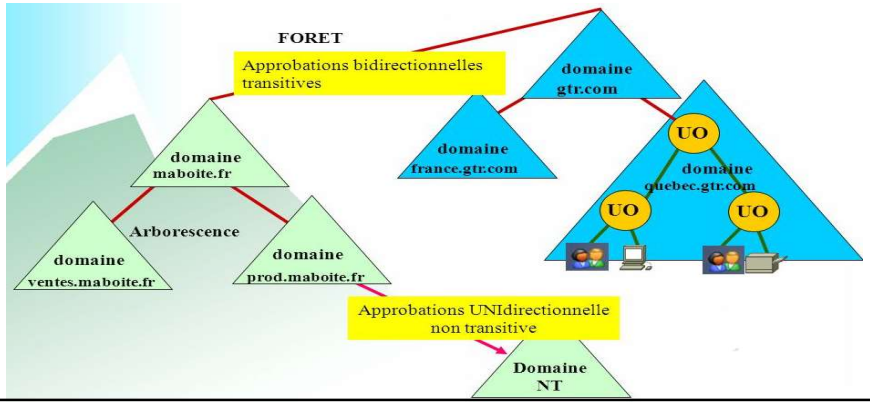
- **Modèle « Groupe de travail » :**
  - **Une base d'utilisateurs par machine** : appelée « **base SAM** », cette base est unique sur chaque machine et non partagée, ainsi, chaque machine contient sa propre base d'utilisateurs indépendante les unes des autres.
  - **Très vite inadapté dès que le nombre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

Active Directory : différence « domaine » et « groupe de travail »

- **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**.

Active Directory : principaux concepts – relations entre domaine, arbre et forêt

- Structure logique d'Active Directory : domaine, arbre et forêt



Active Directory : principaux concepts – relations entre domaine, arbre et forêt

- 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.
- Activité : Identifier et relever les domaines principaux (domaines de base), et les sous-domaines (domaines enfants) de la structure logique proposée ci-dessus.

Active Directory : principaux concepts – relations entre domaine, arbre et forêt

- La **notion d'arbre** doit vous faire 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.**
- Les domaines d'un même arbre partagent un espace de nom contigu et hiérarchique, comme c'est le cas avec l'exemple du domaine « *gtr.com* ».
- Activité : Identifier les arbres qui composent la structure logique proposée ci-dessus.

AD : principaux concepts – relations entre domaine, arbre et forêt

- Une **forêt** c'est **un ensemble d'arbres**.
  - 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.

AD : principaux concepts – relations entre domaine, arbre et forêt

- Imaginons maintenant que nous rachetons la société « *ma boite* », dont le siège est à Paris, et que nous décidons de créer un domaine racine « *maboite.fr*», avec deux fonctions de la société « ventes » et « production » pour lesquelles l'activité est décentralisée. On obtiendra : **ventes.maboite.fr prod.maboite.fr**, un arbre avec la racine «*maboite.fr* ».
- Pour simplifier l'administration, les accès et unifier le système d'information, on peut décider de créer cet arbre «*ma boite* » dans la même forêt que celle où se situe l'arbre « *gtr* ».
- On peut alors affirmer que les différentes arborescences d'une forêt ne partagent pas le même espace de nom et la même structure.
- Activité : Identifier la ou les forêt(s) qui compose(nt) la structure logique proposée ci-dessus.

AD : principaux concepts – forêt et relation d'approbation

- **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.

AD : principaux concepts – forêt et 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.
  - Une ***multinationale***, qui scindera son infrastructure en plusieurs domaines, on peut imaginer un par zone géographique (Europe, Asie, Amérique, etc), il faudra là aussi créer des relations de confiance pour faciliter l'accès aux ressources.
  - 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).
- 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.

AD : principaux concepts – forêt et relation d'approbation

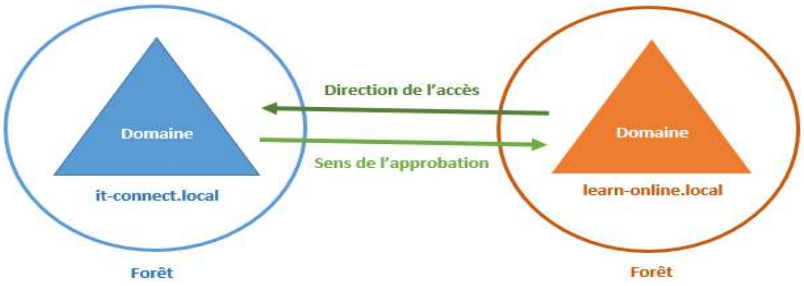
- Lorsque l'on parle de relations d'approbations, on ne peut pas échapper aux notions de ***direction*** et de ***transitivité*** :
- **Direction** : Dans le cadre d'une relation d'approbation, la direction peut être **unidirectionnelle** c'est-à-dire uniquement dans un sens, ou **bidirectionnelle** 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.

AD : principaux concepts – forêt et relation d'approbation

- Lorsque l'on parle de relations d'approbations, on ne peut pas échapper aux notions de ***direction*** et de ***transitivité.***
- **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.
  - 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.

AD : principaux concepts – forêt et relation d'approbation

- Les relations d'approbation : schéma récapitulatif des notions de ***direction*** et de ***transitivité***



AD : contrôleur de domaine

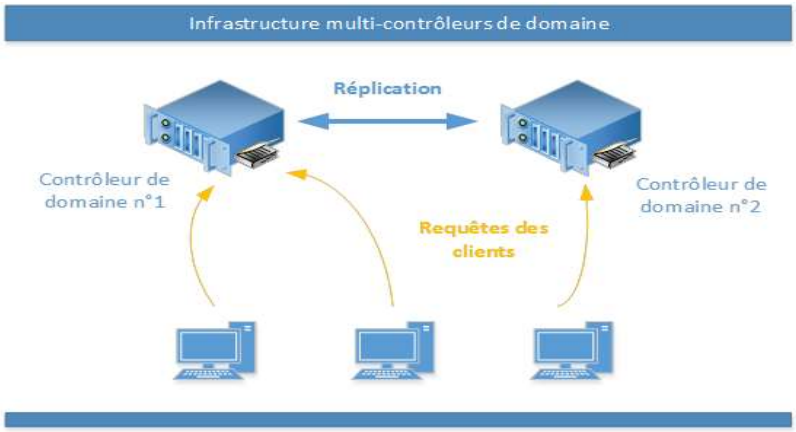
- Lorsque l'on crée un domaine, le serveur depuis lequel on effectue cette création est promu au rôle de « contrôleur de domaine » du domaine créé.
  - Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine.
  - De ce fait, il devra vérifier 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.

AD : contrôleur de domaine

- **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.**
  - Gardez à l'esprit qu'un contrôleur de domaine est un serveur qui contient une copie de l'annuaire Active Directory.
- De nos jours, il est inévitable d'avoir **au minimum deux contrôleurs de domaine** pour assurer **la disponibilité et la continuité 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.

AD: contrôleur de domaine

- Infrastructure multi-contrôleurs de domaine :



Windows Server : les notions de « groupes » et de « portée (étendue) »

- Il existe deux types de groupe : **sécurité** et **distribution**
- **Le type « sécurité » :** les groupes de sécurité sont les plus utilisés et ceux que vous manipulerez 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 ».

Windows Server : les notions de « groupes » et de « portée (étendue) »

- Il existe deux types de groupe : **sécurité** et **distribution**
- **Le type « 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 ».

Windows Server : les notions de « groupes » et de « portée (étendue) »

- Il existe deux types de groupe : **sécurité** et **distribution**
- **Le type « 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 ».

Windows Server : les notions de « groupes » et de « portée (étendue) »

- 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 pour les groupes : **domaine local, globale et universelle**
- **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.

Windows Server : les notions de « groupes » et de « portée (étendue) »

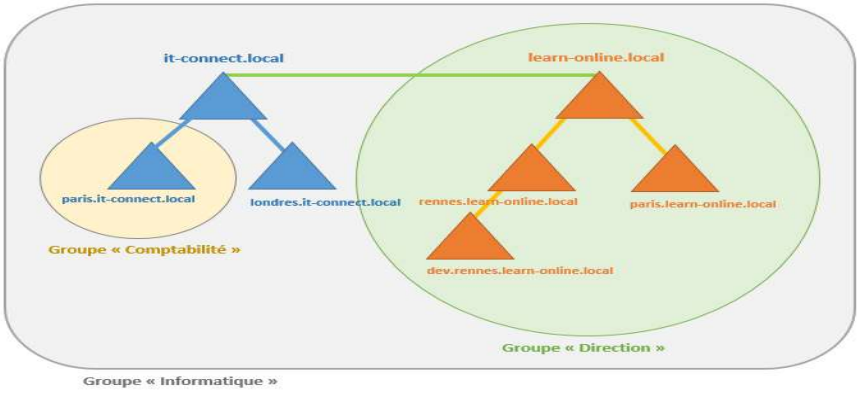
- Il existe trois étendues pour les groupes : domaine local, globale et universelle
- **Globale** : un groupe ayant une étendue « globale » pourra être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés par le domaine de base. Ainsi, si un « domaine A » approuve via une relation 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.

Windows Server : les notions de « groupes » et de « portée (étendue) »

- Il existe trois étendues pour les groupes : domaine local, globale et universelle
- **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.

Windows Server : les notions de « groupes » et de « portée (étendue) »

- Activité : identifier et relever les 3 groupes qui ont été créés dans cette arborescence et indiquer leur portée. Justifier votre classement !



Microsoft Windows Server et le service d'annuaire Active Directory

FIN