Ecole Nationale des Sciences Appliquées El Jadida
Université Chouaib Doukkali El Jadida

Windows Server
Active Directory

ELEMENT DU MODULE : ADMINISTRATION DES SYSTÈMES

FILIÈRE: INGÉNIERIE INFORMATIQUE ET TECHNOLOGIES EMERGENTES (IITE-1)

DÉPARTEMENT : TÉLÉCOMMUNICATIONS, RÉSEAUX ET INFORMATIQUE (TRI)

Prof. Ouaissa Mariyam

Email: ouaissa.mariyam08@gmail.com

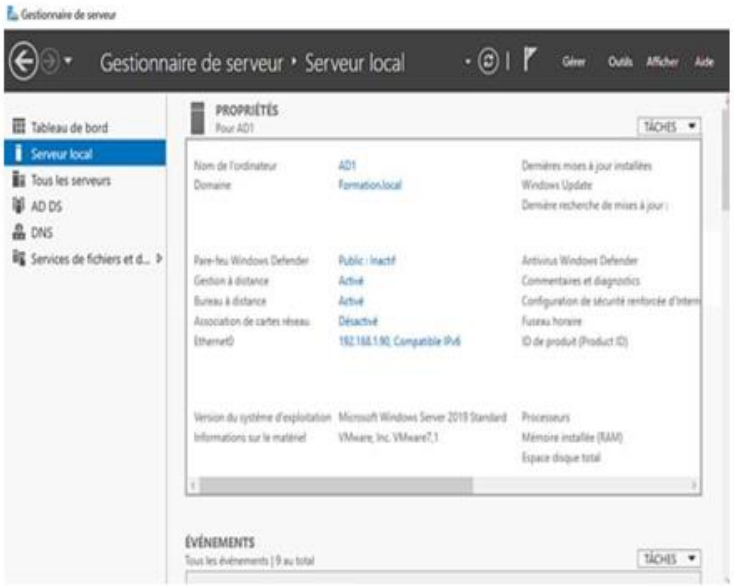
Année Universitaire 2023/2024

Le gestionnaire de serveur

La console **Gestionnaire de serveur** permet la gestion de l'ensemble du serveur (configuration locale, rôle…). On peut y effectuer des opérations de configuration du serveur (adressage IP, nom du serveur…) mais également installer et accéder aux différents rôles (DNS, DHCP…).
Présente depuis Windows Server 2008 et Windows Server 2008 R2, elle a été améliorée avec Windows Server 2012/2012 R2 afin d'offrir une meilleure ergonomie.
Elle permet l'ajout et la suppression de rôles mais également la gestion de serveurs distants. Il est possible de gérer un groupe de serveurs par l'intermédiaire de cette console.

Le gestionnaire de serveur

La gestion du serveur local se fait également par le biais de cette console. Certains paramètres peuvent être modifiées très rapidement. On retrouve le nom de l'ordinateur, le groupe de travail ou le domaine dont la machine est membre. Le bureau à distance ou la gestion à distance sont également configurables.

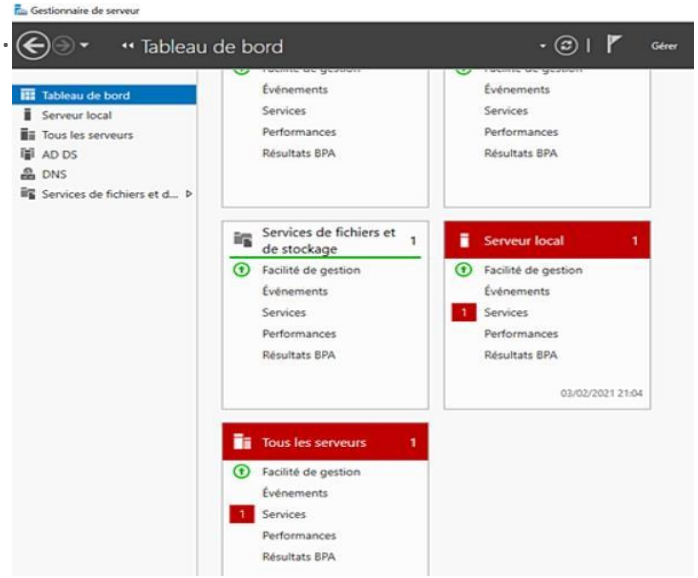


La propriété **Configuration de sécurité renforcée d'Internet Explorer** permet d'activer ou désactiver la sécurité renforcée d'Internet Explorer. Par défaut, l'option est activée.

Le **Tableau de bord** permet pour sa part de s'assurer très rapidement du bon état de santé des services. En cas de service arrêté, l'information s'affiche directement dans la console.

Le gestionnaire de serveur

- Plusieurs points sont audités : les événements, les services, les performances et les BPA. Si un chiffre précède une catégorie, cela indique à l'administrateur qu'un ou plusieurs éléments sont à visualiser.
- En cliquant sur **Événements**, une fenêtre présentant les détails de cet événement s'affiche.
- Sur le serveur local, exécutez la commande **net stop spooler**.
- Relancez la console **Gestionnaire de serveur**, une nouvelle analyse est exécutée.
- La console nous indique un problème sur un service.

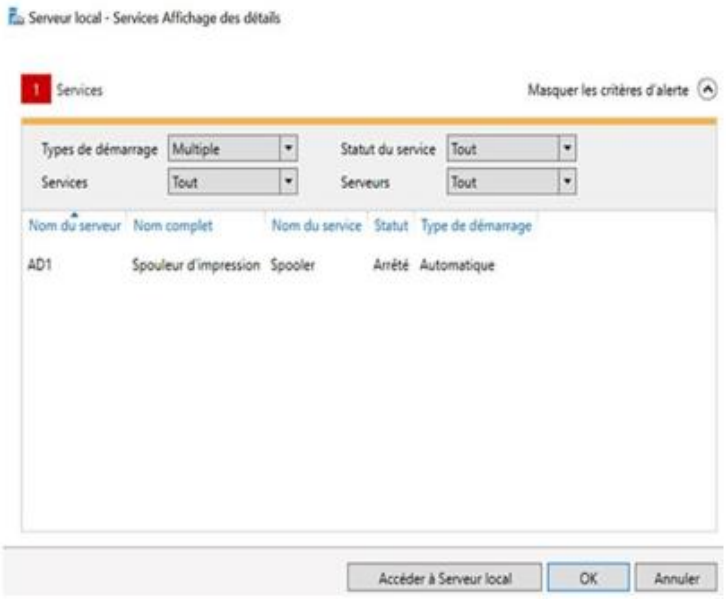


Arrêter le service « spooler » provoque la création d'un nouvel événement. La commande ci- dessus permet d'effectuer l'arrêt de ce service.

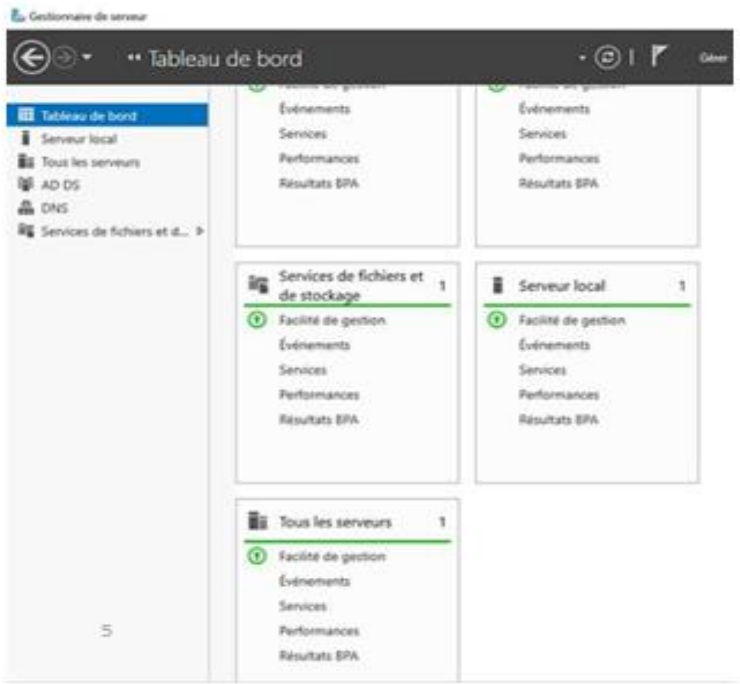
- Cliquez sur le lien **Services** afin d'afficher une nouvelle fenêtre présentant le ou les services qui posent problème

Le gestionnaire de serveur

- Effectuez un clic droit sur le service posant problème puis sélectionnez **Démarrer les services**.
- Cliquez sur **OK** puis cliquez sur le bouton **Actualiser** à droite de **Tableau de bord**.

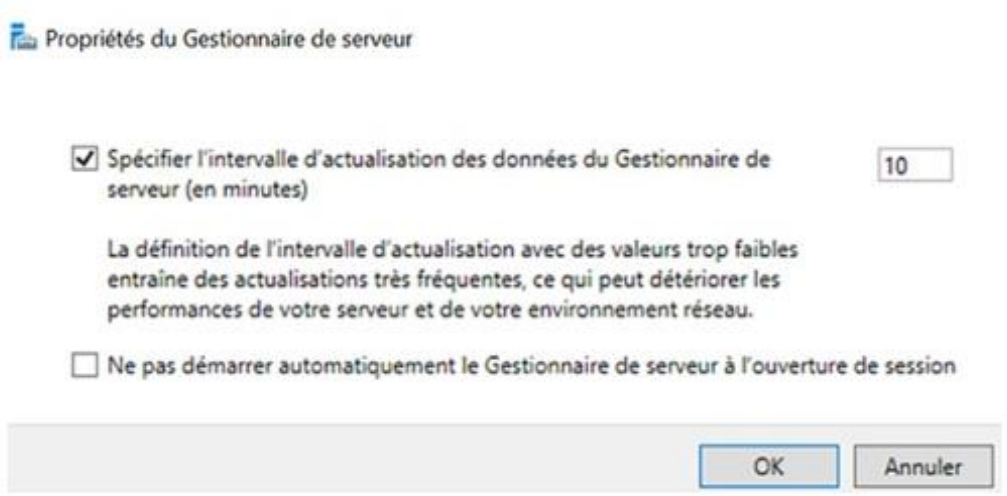


Le problème du service n'apparaît plus. La même opération peut être réalisée pour les serveurs distants. Il est néanmoins obligatoire de créer un groupe comprenant ces serveurs



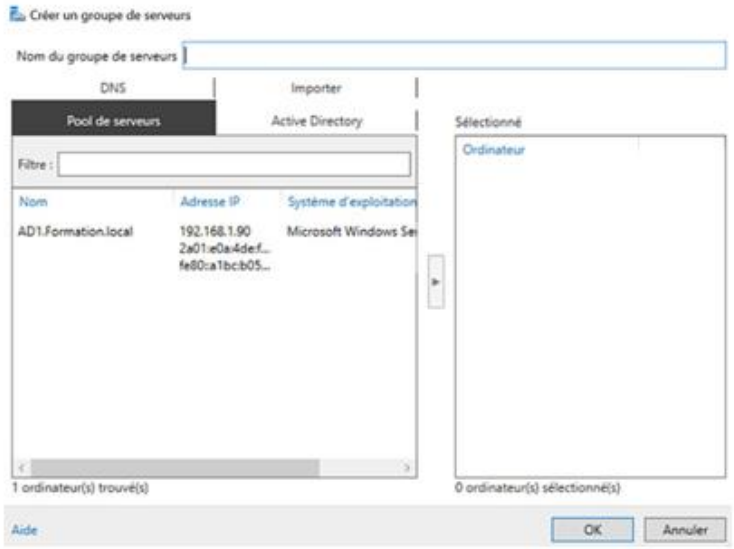
Le gestionnaire de serveur

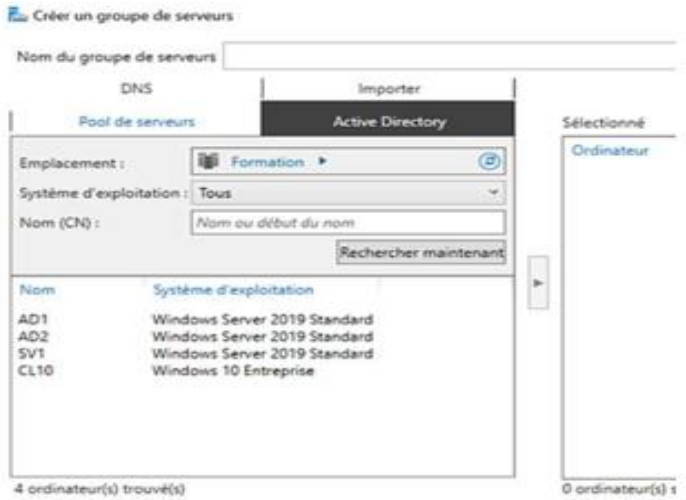
- Le menu **Outils** permet d'accéder à un ensemble de consoles (**Gestion de l'ordinateur**, **Services**, **Pare-feu Windows avec fonctionnalités avancées de sécurité**…) et d'outils (**Diagnostic de mémoire Windows**, **Windows PowerShell**…).
- Lors du clic sur le lien **Gérer**, un menu contextuel s'affiche donnant accès à un ensemble d'options :
- **Propriétés du Gestionnaire de serveur** : il est possible de spécifier un délai d'actualisation des données de la console **Gestionnaire de serveur**. Par défaut, la valeur est configurée à 10 minutes. Le Gestionnaire peut être configuré afin de ne pas se lancer automatiquement lors de l'ouverture de session.



Le gestionnaire de serveur

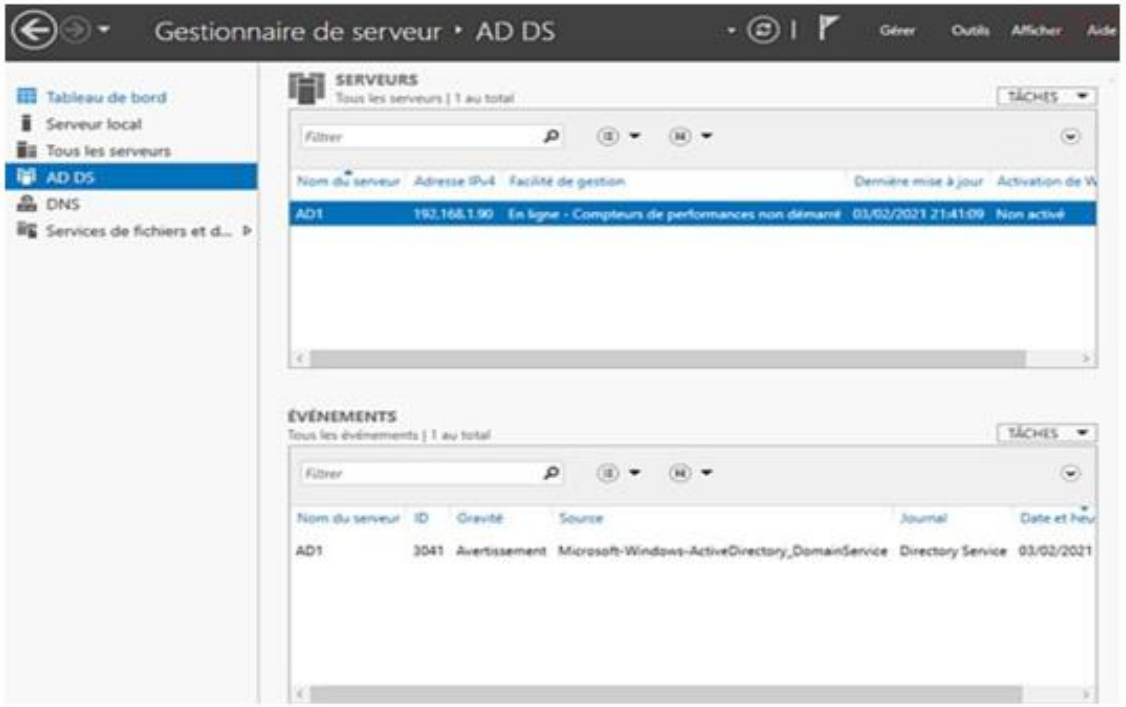
- **Créer un groupe de serveurs** : afin de pouvoir gérer plusieurs serveurs depuis cette machine, il convient de créer un groupe de serveurs. Par la suite, il est possible d'installer/supprimer des rôles ou simplement d'en effectuer la surveillance. L'ajout peut se faire par la saisie d'un nom ou d'une adresse IP dans l'onglet **DNS**.
- La recherche du poste peut également être effectuée à l'aide d'Active Directory, en sélectionnant l'emplacement (racine du domaine, unité d'organisation…) ou en saisissant le nom de la machine.
- **Ajouter/supprimer des rôles et fonctionnalités** : les opérations d'ajout ou de suppression peuvent être effectuées sur le serveur local ou sur une machine distante.





Le gestionnaire de serveur

Lors de l'ajout d'un nouveau rôle, un nouveau nœud apparaît dans la colonne de gauche de la console **Gestionnaire de serveur**. En cliquant dessus, le panneau central donne accès aux événements du rôle ...

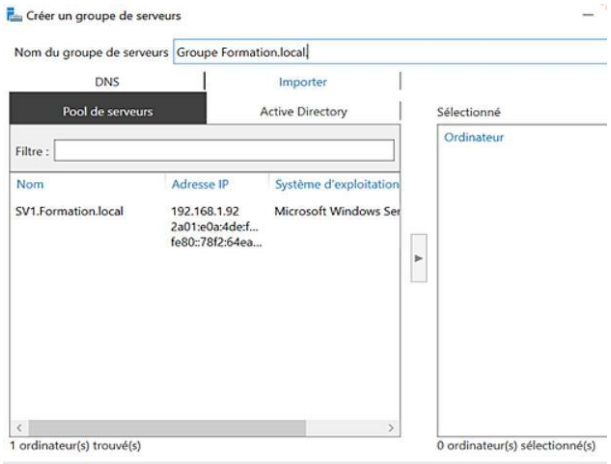


Le gestionnaire de serveur

Création d'un groupe de serveur

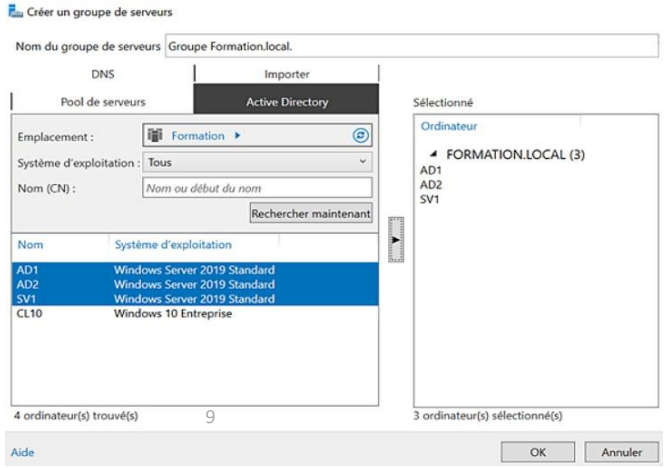
Comme nous avons pu le voir, la création d'un groupe nous permet d'effectuer l'administration à distance.

- Si ce n'est pas déjà effectué, joignez la machine **SV1** au domaine. Au redémarrage, lancez la console **Gestionnaire de serveur** si celle-ci ne s'affiche pas toute seule. Cliquez sur **Gérer** puis sélectionnez **Créer un groupe de serveur**.
- Dans le champ **Nom du groupe de serveurs**, saisissez **Groupe Formation.local**.



- Cliquez sur l'onglet **Active Directory**.
- Cliquez sur le bouton **Rechercher maintenant**.
- Sélectionnez **AD1**, **AD2** puis **SV1** et cliquez sur le bouton

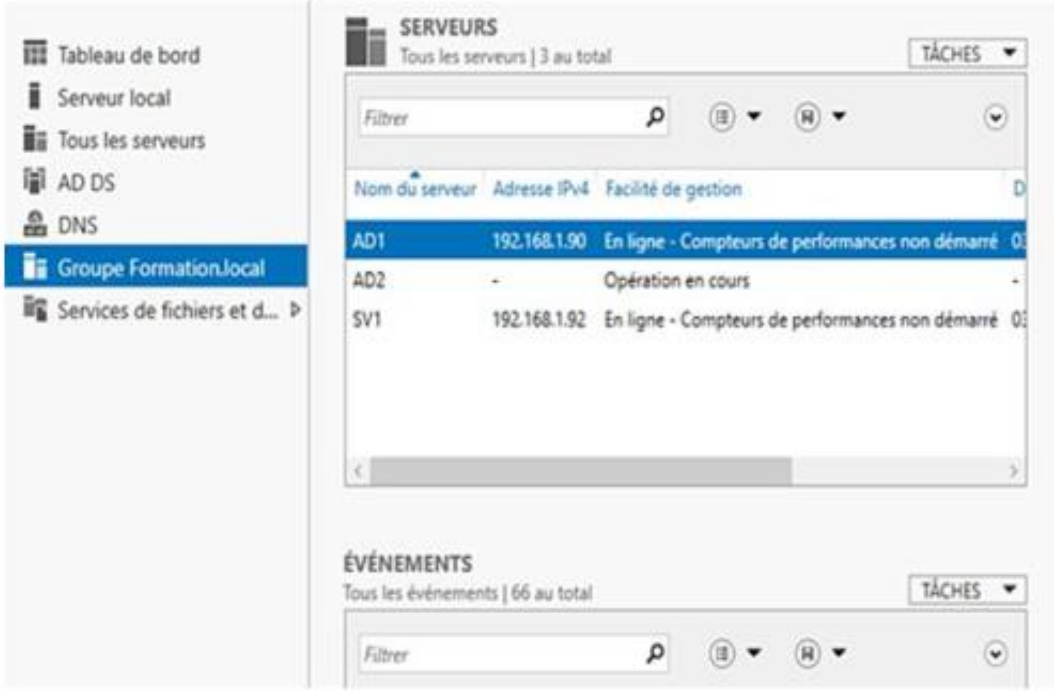
  présent entre les champs de sélection et la liste **Selectionné** dans le but de les insérer dans le groupe.
- Cliquez sur **OK** afin de valider la création du groupe.



Le gestionnaire de serveur

Création d'un groupe de serveur

Le nouveau groupe est présent dans la console **Gestionnaire de serveur**.



Service de domaine Active Directory

Introduction

- 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.
- L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows, macOS ou encore Linux. Il permet également l'attribution et l'application de stratégies ainsi que l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés (en), les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

Service de domaine Active Directory

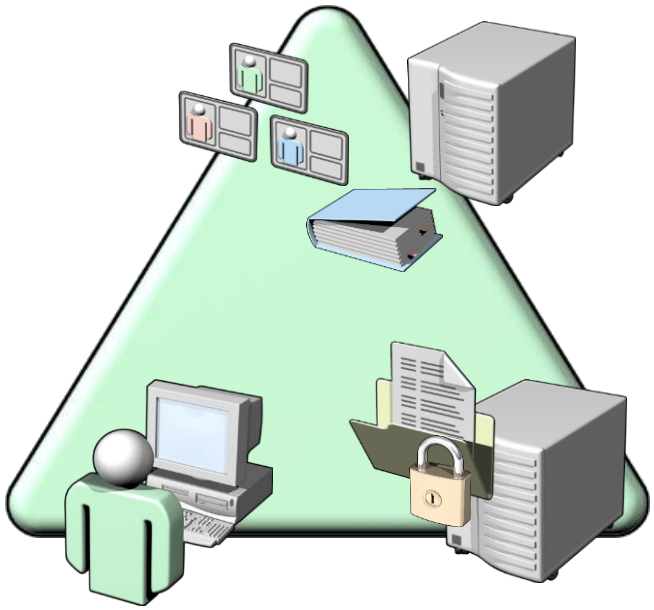
AD DS se compose à la fois de composants physiques et logiques

Composants physiques	Composants logiques
• Magasin de données • Contrôleurs de domaine • Serveur de catalogue global • Contrôleur de domaine en lecture seule	• Partitions • Schéma • Domaines • Arborescences de domaines • Forêts • Sites • Unités d'organisation

Service de domaine Active Directory

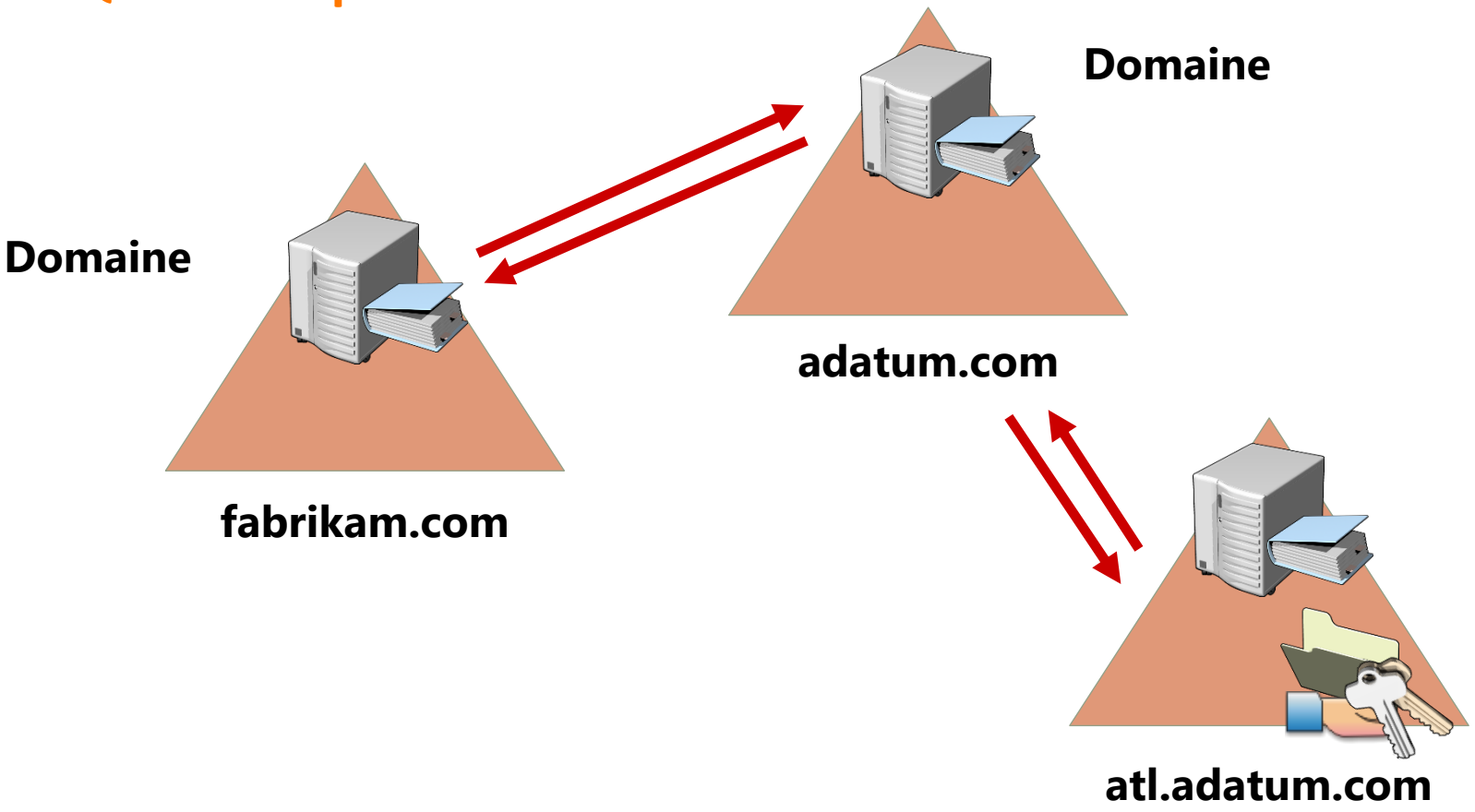
Que sont les domaines AD DS ?

- Les services AD DS requièrent un ou plusieurs contrôleurs de domaine
- Tous les contrôleurs de domaine maintiennent une copie de la base de données du domaine synchronisée en permanence
- Le domaine est le contexte dans lequel des comptes d'utilisateurs, des comptes de groupes et des comptes d'ordinateurs sont créés
- Le domaine est une limite de réplication
- Un centre d'administration pour configurer et gérer des objets
- N'importe quel contrôleur de domaine peut authentifier n'importe quelle connexion au domaine



Service de domaine Active Directory

Qu'est-ce qu'une forêt AD DS ?



Service de domaine Active Directory

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 partition configuration et 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.

Service de domaine Active Directory

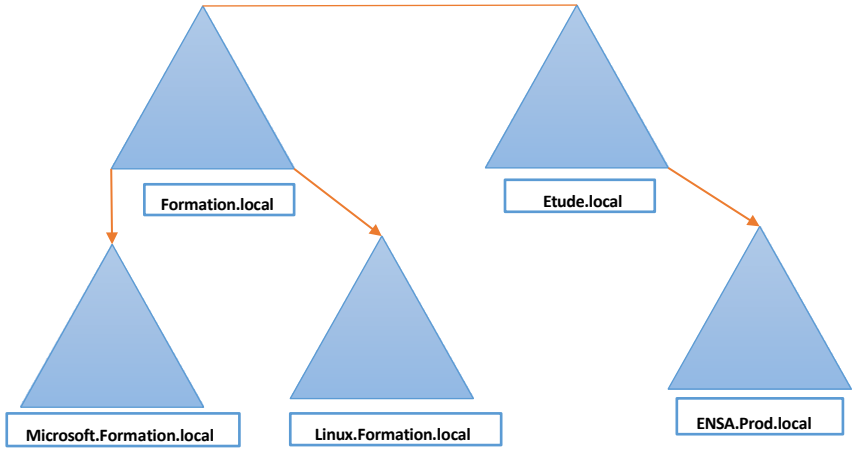
Contrôleurs de domaine

- Des serveurs qui hébergent la base de données Active Directory (NTDS.DIT) et SYSVOL
- Le service d'authentification Kerberos et les services KDC effectuent l'authentification
- Meilleures pratiques
  - Disponibilité : Au moins deux contrôleurs de domaine dans un domaine
  - Sécurité : Contrôleur de domaine en lecture seule et BitLocker

Service de domaine Active Directory

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**. Le nom **Formation.local** est bien identique aux deux domaines (**Microsoft.local** et **Linux.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 Etude.local** sont deux arborescences différentes dans la même forêt.



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

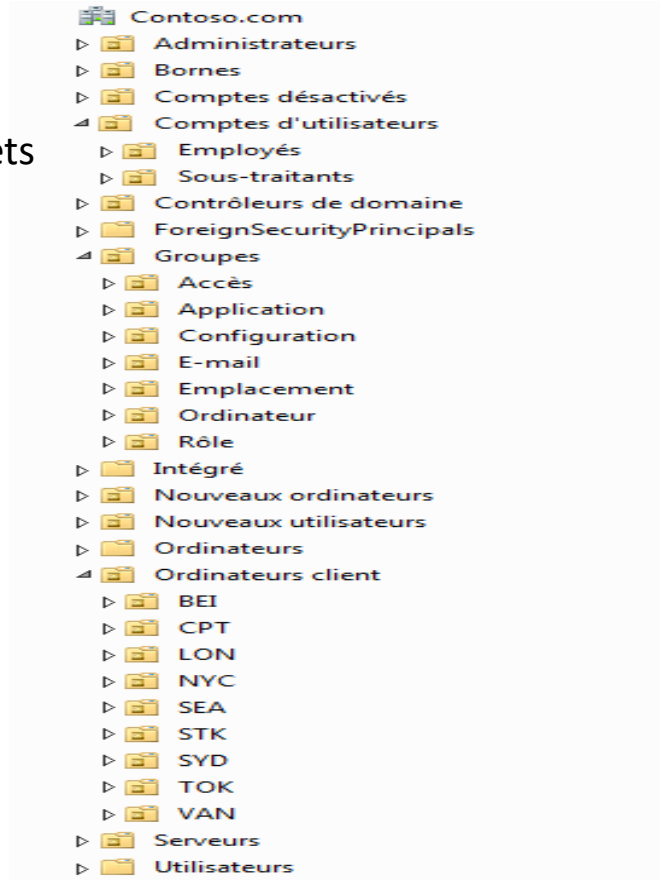
Un domaine contient au moins un contrôleur de domaine. Néanmoins il est recommandé d'en avoir deux afin d'assurer l'authentification en cas de maintenance ou de crash d'un des serveurs d'annuaire. Si plus aucun serveur n'est en ligne, l'authentification ne pourra plus être assurée, ce qui va impliquer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

Service de domaine Active Directory

Unités d'organisation

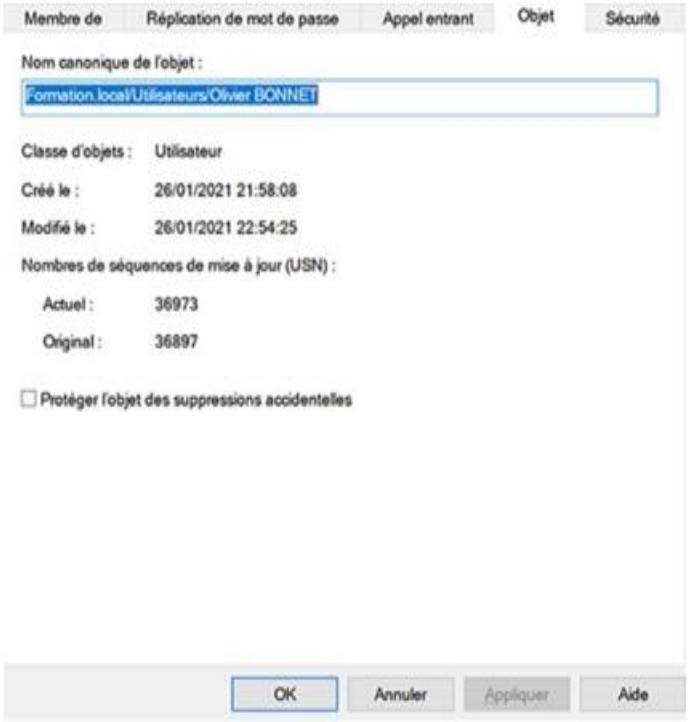
- Conteneurs permettent de regrouper des objets dans un domaine
- Créer des unités d'organisation pour
  - Déléguer des autorisations administratives
  - Appliquer la stratégie de groupe



Service de domaine Active Directory

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.



Service de domaine Active Directory

Qu'est-ce que le schéma AD DS ?

Le schéma d'Active Directory agit en tant que modèle pour Active Directory DS en définissant les attributs et les classes d'objets, comme :

- Attributs
  - objectSID
  - sAMAccountName
  - emplacement
  - manager
  - service
- Classes
  - Utilisateur
  - Groupe
  - Ordinateur
  - Site

Service de domaine Active Directory

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.

Service de domaine Active Directory

Les partitions d'Active Directory

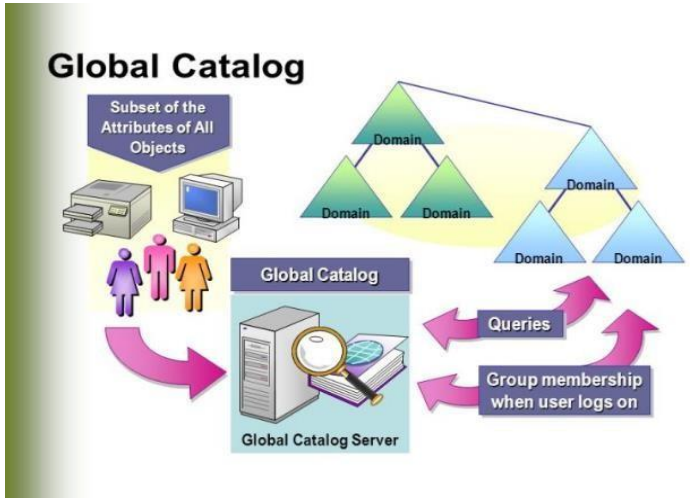
Active Directory utilise quatre types de partitions d'annuaire, toutes partagées par les contrôleurs de domaine. La création est effectuée lors de l'étape de promotion. Les partitions de configuration et de schéma sont partagées par l'ensemble des contrôleurs de domaine.

- **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.

Service de domaine Active Directory

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.



Service de domaine Active Directory

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 réplications 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.