**Introduction à Active Directory**

Active Directory a été introduit pour la première fois en 1999 avec la sortie de "Windows 2000 Server".

Active Directory partage plusieurs caractéristiques avec une base de données.

**Les avantages de l'Active Directory**

1. Active Directory permet aux administrateurs de centraliser la gestion des comptes utilisateurs, des groupes, des ordinateurs, des unités d'organisations et des autres objets.
2. Active Directory simplifie l'administration et la maintenance des systèmes.
3. Active Directory assure une authentification sécurisée des utilisateurs et des ordinateurs dans le réseau.

Le schéma de l'Active Directory est similaire à un dictionnaire, il contient les définitions de chaque classe d'objet et de chaque attribut.

Les versions des schémas de l'Active Directory.

Windows Server 2025 Schema version: 90

Windows Server 2022 Schema version: 88

Windows Server 2019 Schema version: 88

Windows Server 2016 Schema version: 87

Windows Server 2012 R2 Schema version: 69

Windows Server 2012 Schema version: 56

Windows Server 2008 R2 Schema version: 47

Windows Server 2008 Schema version: 44

Windows Server 2003 R2 Schema version: 31

Windows Server 2003 Schema version: 30

Windows Server 2000 Schema version: 13

Voici la commande PowerShell qui permet d'afficher la version du schéma de l'Active Directory.

**Get-ADObject (Get-ADRootDSE).schemaNamingContext -Properties objectVersion**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

L'Active Directory a un nombre maximum d'objets qu'il peut gérer.

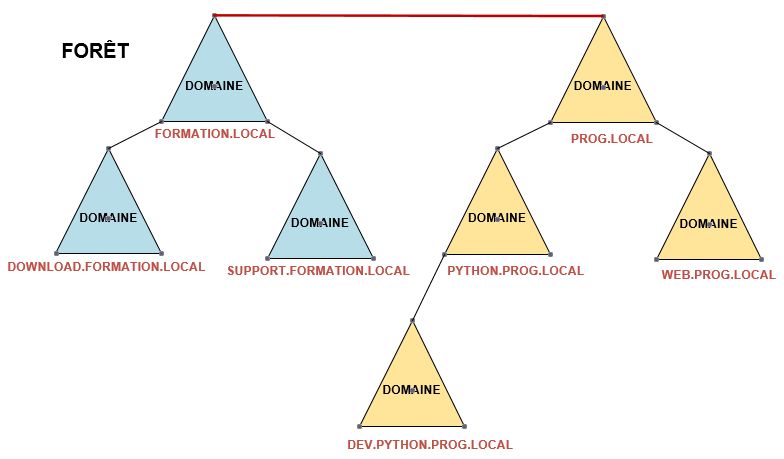
Le nombre d'objet maximum est 231 – 255 = 2 147 483 648 – 255 = 2 147 483 393

**Aperçu d’une structure "Active Directory"**

Active Directory (AD) est une organisation hiérarchisée d'objets.

Les objets sont classés en trois grandes catégories:

* Les ressources (exemple: ordinateurs, imprimantes)
* Les services (exemple: courrier électronique)
* Les utilisateurs et les groupes
* L'AD fournit des informations sur les objets, il organise et contrôle les accès.



Cette forêt est constituée de deux arbres et chaque arbre est constitué de plusieurs domaines.

**Catalogue global**

Le catalogue global est l’ensemble de tous les objets d’une forêt AD DS (Active Directory Domain Services). Un serveur de catalogue global est un contrôleur de domaine qui enregistre une copie complète de tous les objets de l’annuaire pour son domaine hôte et une copie partielle en lecture seule de tous les objets pour tous les autres domaines de la forêt.

Un domaine Active Directory contient au moins un contrôleur de domaine.

**Installation de l'Active Directory en mode graphique**

Dans la console "**Gestionnaire de serveur**" installer le rôle "**Services AD DS**"

* L'installation de l'Active Directory nécessite l'installation du rôle DNS
* L'installation de l'Active Directory exige un redémarrage.
* Après le redémarrage, nous devons compléter la post-installation afin de "promouvoir ce serveur en contrôleur de domaine".
* On doit choisir "Ajouter une nouvelle forêt" si c'est un nouveau domaine

Le répertoire **C:\Windows\NTDS** contient les journaux de transaction, les logs et les fichiers temporaires utiles au fonctionnement de l'Active Directory.

Le fichier **ntds.dit** constitue la base de données de l'Active Directory.

* Ce fichier est présent sur chaque contrôleur de domaine.
* DIT signifie (Directory Information Tree)

**Les partages administratifs (NETLOGON, SYSVOL)**

Après l'installation de l'Active Directory nous avons accès à deux partages

* \\FORMATION.LOCAL\NETLOGON C:\Windows\SYSVOL\sysvol\FORMATION.LOCAL\scripts
* \\FORMATION.LOCAL\SYSVOL C:\Windows\SYSVOL\sysvol

On remarque que le partage NETLOGON est un sous-dossier du partage SYSVOL.

* Le partage NETLOGON est accessible en lecture pour "Tout le monde".
* Le partage NETLOGON est accessible en écriture pour le groupe "FORMATION\Administrateurs".

**L'accès en écriture n'est pas permis si l'accès se fait directement sur le contrôleur de domaine.**

Le partage SYSVOL est répliqué entre les contrôleurs de domaine.

Le partage SYSVOL contient deux dossiers

* \\FORMATION.LOCAL\SYSVOL\FORMATION.LOCAL\**Policies**

**Ce dossier contient les GPO.**

* \\FORMATION.LOCAL\SYSVOL\FORMATION.LOCAL\**scripts**

**Ce dossier contient les scripts de démarrage ou d'ouverture de session.**

**Gestion des utilisateurs, des groupes, des ordinateurs et des unités d'organisation**

* La console "**Utilisateurs et ordinateurs Active Directory**" permet la gestion des utilisateurs, des groupes, des ordinateurs et des unités d'organisation.
* La console "**Centre d'administration Active Directory**" permet la gestion des utilisateurs, des groupes, des ordinateurs et des unités d'organisation.

Cette console est plus récente que la console "Utilisateurs et ordinateurs Active Directory".

**ANNEXE 1**

**"Active Directory" avec deux contrôleurs de domaine**

**Dans le cours, nous n'utiliserons pas deux contrôleurs de domaine.**

Il est préférable d’avoir au minimum deux contrôleurs de domaine pour assurer la disponibilité et la continuité des services de l'Active Directory.

Une image contenant conception, prise

Description générée automatiquement avec une confiance moyenne

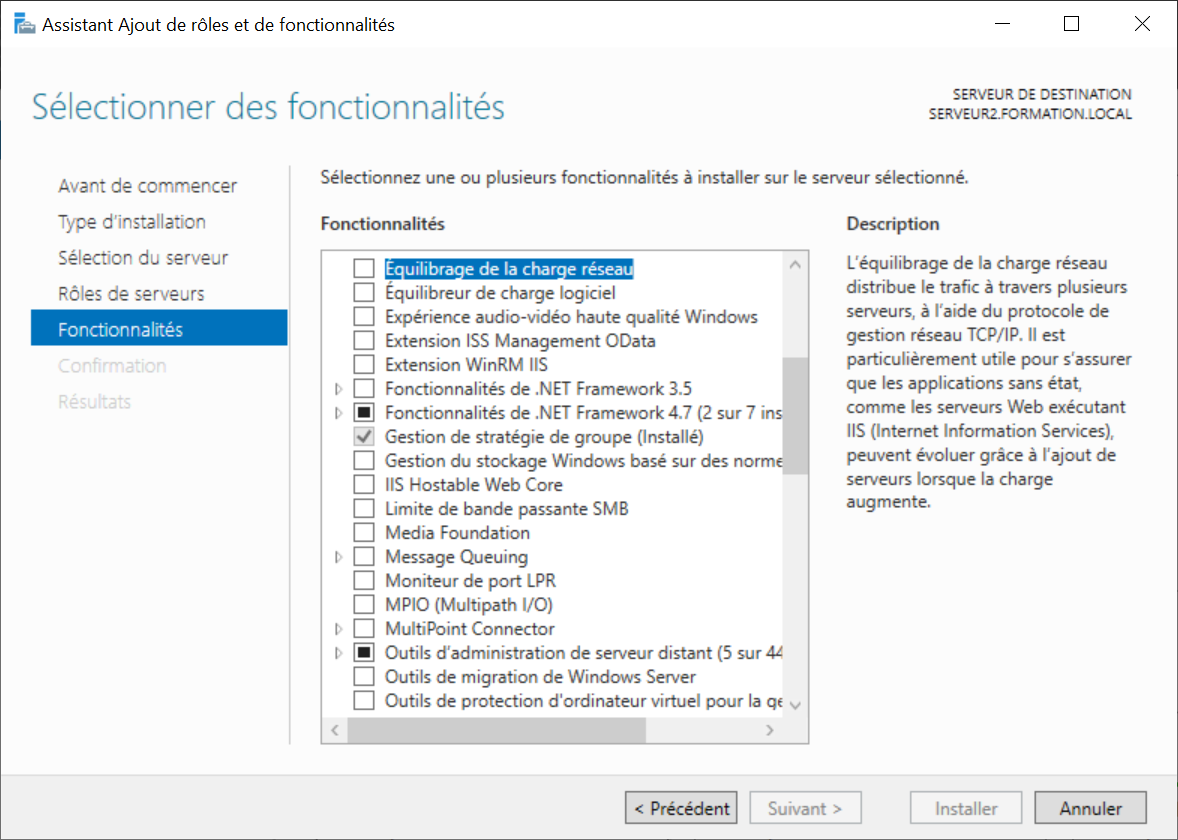
Les contrôleurs de domaine répliquent les informations entre eux à intervalle régulier, afin de disposer d’un annuaire Active Directory identique. En plus, les contrôleurs de domaine répliquent le contenu du dossier "SYSVOL" qui est utilisé pour distribuer les stratégies de groupe et les scripts de connexion.

**ANNEXE 2**

**La fonctionnalité "Équilibrage de la charge réseau"**

**Dans le cours, nous n'utiliserons pas la fonctionnalité "Équilibrage de la charge réseau".**

Voir la description pour comprendre l'utilité de cette fonctionnalité.



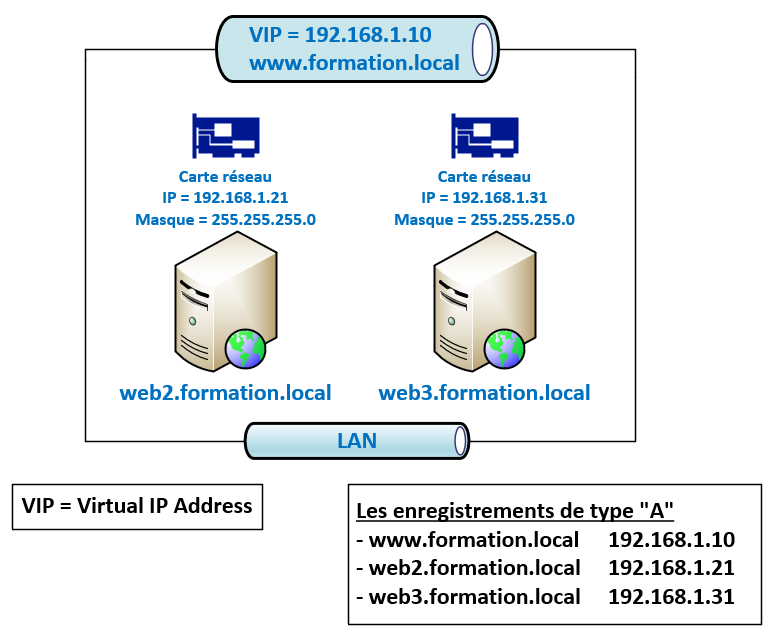
Voici un schéma qui montre deux serveurs qui utilisent la fonctionnalité "**Équilibrage de la charge réseau**".

Chaque serveur héberge un site web dont le contenu est identique.

Sur le premier serveur, l'adresse IP virtuelle 192.168.1.10 est associée à l'adresse IP 192.168.1.20.

Sur le deuxième serveur, l'adresse IP virtuelle 192.168.1.10 est associée à l'adresse IP 192.168.1.21.

Pour avoir accès au site web, on doit utiliser l'adresse IP virtuelle 192.168.1.10.

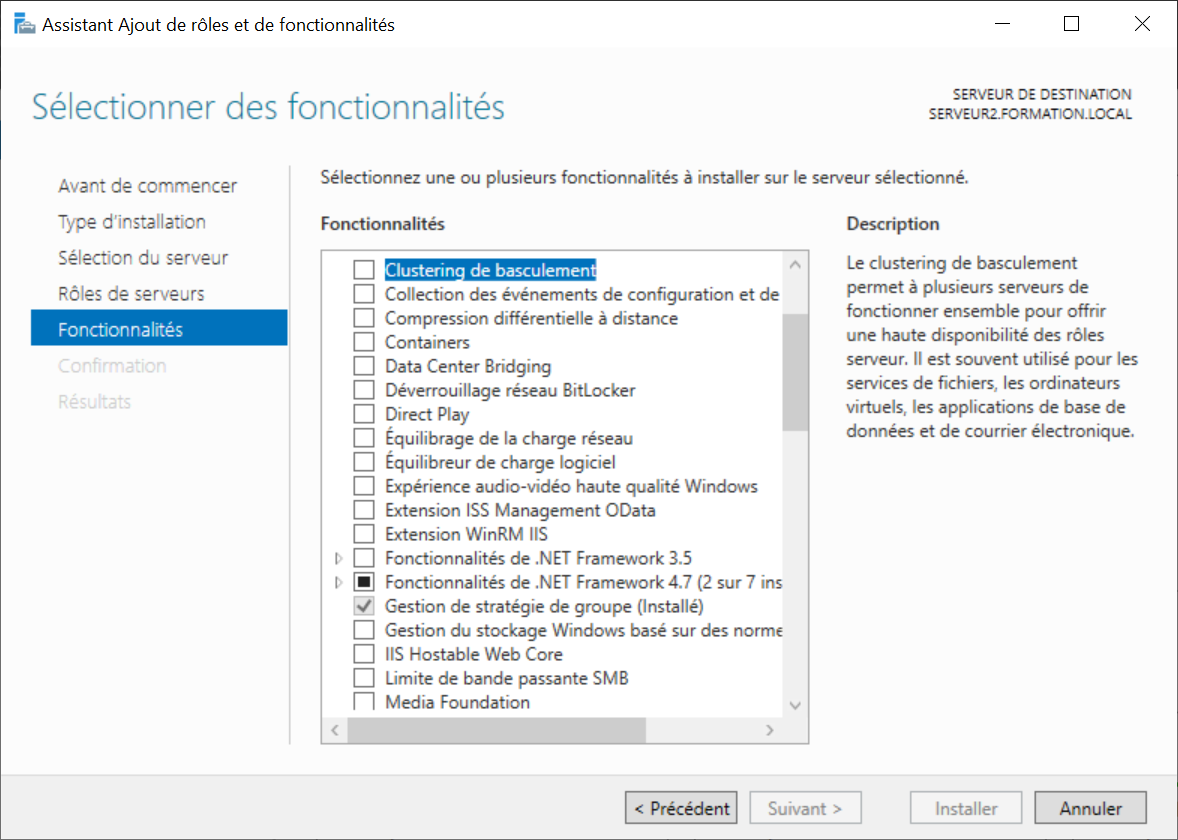


**ANNEXE 3**

**La fonctionnalité "Clustering de basculement"**

**Dans le cours, nous n'utiliserons pas la fonctionnalité "Clustering de basculement".**

Voir la description pour comprendre l'utilité de cette fonctionnalité.



Voici un schéma d'un cluster de basculement.

Chaque serveur a trois cartes réseau.

Une image contenant diagramme, capture d’écran, ligne, conception

Description générée automatiquement

**ANNEXE 4**

**"Active Directory" et Linux**

**Dans le cours, nous ne joindrons pas de distribution Linux à l'Active Directory.**

"Ubuntu 21.04" apporte l'intégration native de Microsoft Active Directory.

Ce n'est pas nouveau que de pouvoir joindre un ordinateur Linux à l'Active Directory, ce qui est nouveau avec "Ubuntu 21.04" c'est qu'il est possible de le faire pendant l'installation.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement