2021

Windows Serveur 2022

Installation et configuration des serveurs

Olivier D.

Table des matières

1 Introduction aux taches d'administration dans WS 2022

Nota : ce cours est complémentaire du cours d'administration des services ADDS. Certaines notions vues ici ne seront pas abordées dans le cours suivant car considérées comme sues.

Rôle serveur

Comparaison des éditions : Comparatif des éditions Standard, Datacenter et Datacenter Azure Edition de Windows Server 2022 | Microsoft Docs

- Edition Standard répandue
- Edition datacenter : nombre illimité de machines virtuelles par hôte
- Licences d'Accès Clients (CAL) : payer pour que les clients accèdent aux services serveur

Rôle de serveur : services rendus à des clients

Serveur de plateforme (accessible par les clients via un logiciel client) :

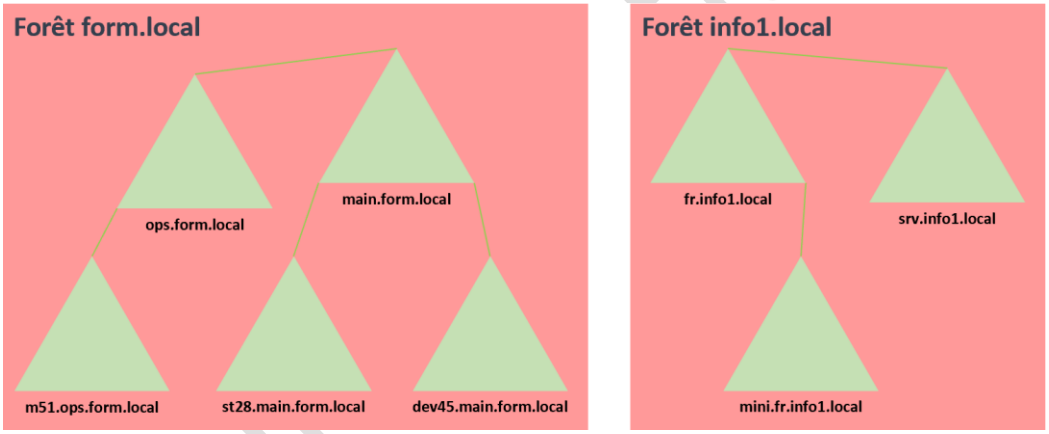
- Installation d'un client local (par exemple Citrix Workspace pour l'accès Citrix ou mstsc pour RDS) et Connexion à RDS ou Citrix (bureau à distance)
- Navigateur web sur les clients et rôle IIS sur le serveur

Rôle de serveur AD :

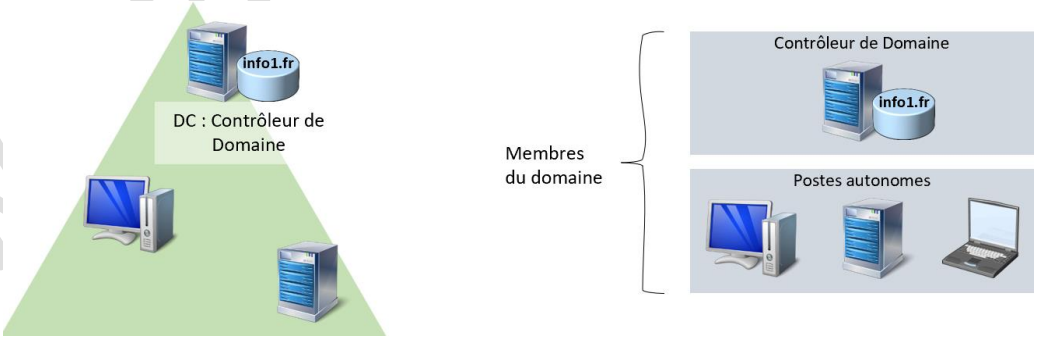
- annuaire, centralisation des comptes, des groupes, des stratégies, etc.
- Il faut ADDS avant de mettre le reste (Active Directory Domain Services = ADDS = AD)

Serveur Core : pas d'interface graphique donc pas de services de déploiement, pas de TSE /Citrix.

Vue d'ensemble d'Active Directory



Relation de confiance entre les différents domaines de la forêt



Membres d'un domaine

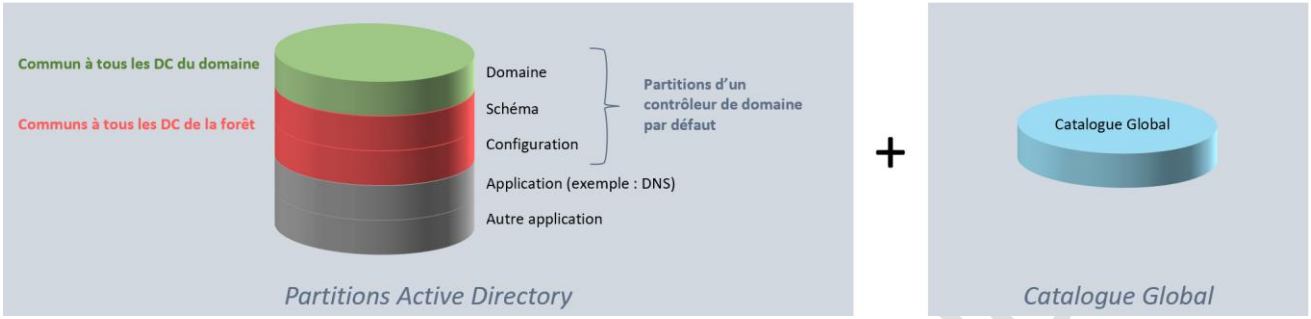
On crée un contrôleur de domaine dans le cas de :

- CD pour un domaine existant
- CD pour un nouveau domaine dans la forêt
- CD pour un nouveau domaine dans une nouvelle forêt

Les partitions Active Directory

Chaque partition a un rôle particulier :

- Domaine gère les objets du domaine (groupes, partages, utilisateurs, ordinateurs)
- Schéma gère la configuration du schéma de l'ADDS (par exemple le modèle des données stockées)
- Configuration contient les informations de configuration de la forêt (par exemple les sites)
- Le catalogue global contient une partie des attributs de chaque objet du domaine
- D'autres applications peuvent être stockées dans les partitions ADDS, comme les zones DNS pour les DNS intégrés à AD ou des partitions Microsoft Exchange (serveur de messagerie)



Organisation des partitions ADDS

Unité d'organisation (OU ou UO)

Elle se présente sous la forme d'un conteneur dans l'arborescence Active Directory.

Un utilisateur ne peut faire partie que d'une unité d'organisation

Les OU servent à :

- Attribuer des GPO (stratégies de groupe) à conteneur
- Définir des délégations d'organisation (délégation administrative : qui est administrateur sur cette OU)
- Organiser les objets (objectif secondaire)

Forêt

Une forêt est un ensemble de domaines qui s'approuvent mutuellement (domaine de confiance)

Serveur Core

Un serveur Core est un serveur dans interface graphique (sur le modèle de certains serveurs Linux)

- ligne de commande : rendre l'administration faisable que par des personnes qualifiées
- convient aux petites agences dont les personnels seraient tentés d'utiliser le serveur comme un simple poste de travail

Read Only Domain Controller (RODC) :

Contrôleur de Domaine en lecture seule (on n'ajoute donc pas d'objets dedans)

- recopie en lecture seule d'une partie des utilisateurs de l'ADDS pour des sites sensibles (ou la DMZ par exemple). La base étant en lecture seule, il n'y a pas de modification des données non autorisée (piratage)
- convient pour des agences où la sécurité des serveurs est minime.

Utilisation des outils d'administration WS2008

Utilisation de mmc.exe et du Gestionnaire de serveur

Mise en place de l'accès bureau à distance pour l'administration

Permet de se connecter depuis son poste de travail au serveur Windows

Gestionnaire de serveur > Serveur local > Bureau à distance :

- Autoriser les connexions à distance à cet ordinateur
- Sélectionner les utilisateurs (autorisés à se connecter)

2 Création objets utilisateurs et ordinateurs AD

ADDS contient une ancienne SAM en plus de LDAP

Noms associés au compte utilisateur de domaine :

Nom UPN (nom complet) = `guillaume@woodgrovebank.com`
`CN=guillaume,OU=CustomerService,OU=Miami,DC=Woodgrovebank,DC=com` : **du plus près de l'utilisateur au plus loin**

- Verrouillage de compte : en cas de plusieurs mauvais mots de passe (action automatique de la machine)
- Désactivation de compte : action de l'administrateur

Modèle d'objet utilisateur

Copier un compte dans l'OU, le renommer en _ModeleDuConteneur et Désactiver le compte. Permet d'alléger la saisie lors des créations d'objets utilisateurs

Faire une copie de ce compte lorsqu'on veut créer un nouvel utilisateur sans le même conteneur

Utilisation du compte d'ordinateur :

AD gère chaque nom d'ordinateur en lui attribuant un SID. Si deux ordinateurs ont le même nom sur le domaine : l'ancien compte d'ordinateur est supprimé et il faut réparer l'erreur et réintégrer l'ancien ordinateur dans le domaine.

on peut désigner un nom d'utilisateur ayant droit d'intégrer une machine dans le domaine

Automatisation de l'administration des objets ADDS

- Utilisateurs et ordinateurs Active Directory
- Outils de services d'annuaire (`dsadd`, `dsmod`, `dsrm` …)
- outils `csvde` et `ldifde`
- PowerShell

En PowerShell ou Cmd :

`dsadd user "CN=Jean Dupont,OU=RegularUsers,OU=Rebrechien,DC=info1,DC=local"` : crée un utilisateur

`Get-Command -Source ActiveDirectory` : liste de toutes les commandes relatives à Active Directory

`ldifde` : donne les infos utilisateurs de haut en bas

`csvde` : donne les infos utilisateurs ligne par ligne : plus lisible, plus facile pour les exports, etc.

`csvde` sert aussi à récupérer des informations utilisateurs depuis le LDAP

3 Présentation des groupes

Un groupe est défini par son

Type :

- groupe de sécurité (dispose d'un SID) permet de tout faire
- groupe de distribution : utilisés à des fins de messagerie seulement

Étendue (périmètre d'utilisation) :

- groupes Globaux
- groupes de Domaine Local
- groupes Universels

Niveau fonctionnel (ou NF)

Chaque nouveau niveau fonctionnel implique notamment de nouveaux champs qui sont mis à jour automatiquement.

Si des serveurs avec des versions de système d'exploitation différents existent, il faut s'adapter au plus ancien (il n'est pas possible d'installer un NF 2016 sur un serveur Windows Server 2012).

OS	Niveau fonctionnel disponible						
Windows Server 2008	2000 natif	2003	2008				
Windows Server 2008R2	2000 natif	2003	2008	2008R2			
Windows Server 2012		2003	2008	2008R2	2012		
Windows Server 2012R2		2003	2008	2008R2	2012	2012R2	
Windows Server 2016		2003	2008	2008R2	2012	2012R2	2016
Windows Server 2019			2008	2008R2	2012	2012R2	2016
Windows Server 2022			2008	2008R2	2012	2012R2	2016

Le NF de domaine doit être supérieur ou égal au NF de forêt

Avant de changer de NF :

- sauvegarder
- vérifier sur le site TechNet quelles sont les fonctionnalités disponibles du NF : Niveaux fonctionnels de Windows Server 2016 | Microsoft Docs
- Si ça fonctionne, pourquoi changer ?

Il y a un niveau de **fonctionnel de foret**, et un **niveau fonctionnel de domaine** (les deux peuvent être différents)

Groupes Globaux

- Membres : utilisateurs du même domaine que celui du groupe global
- C'est un conteneur d'utilisateurs ayant des besoins similaires
- Exemple : G_prestataires (liste des prestataires au sein du domaine)

Groupes Universel (beaucoup moins utilisés)

- Membres : pas de restriction, dans la même forêt
- C'est une combinaison de groupes présents sur plusieurs domaines
- Leurs autorisations s'appliquent sur tous les domaines de la forêt

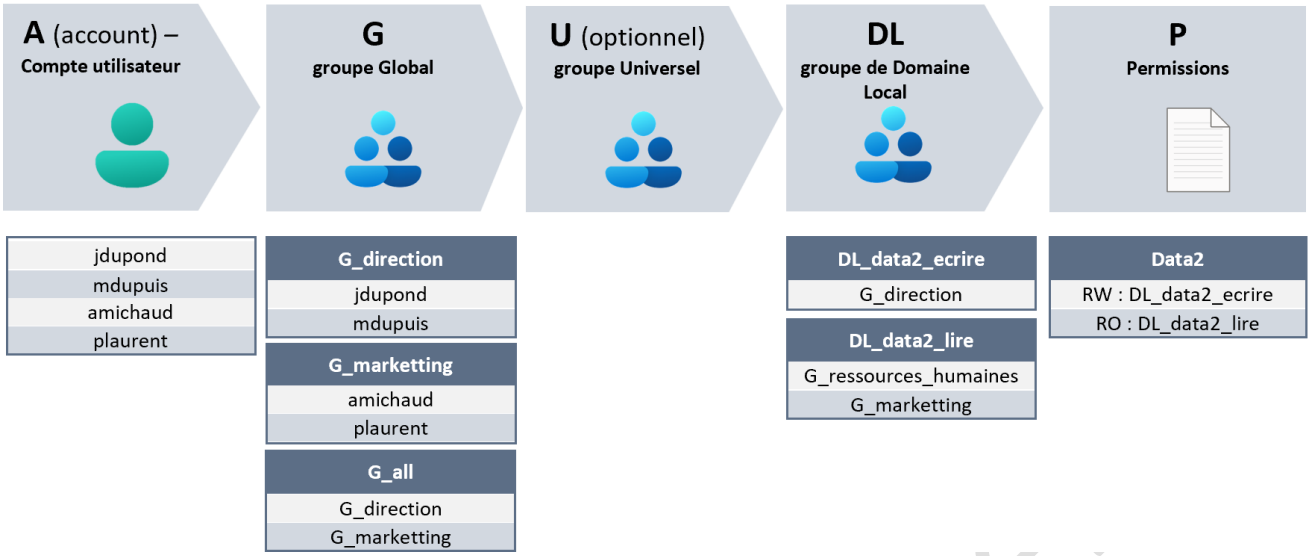
  Dupliqué sur tous les DC des domaines de de la forêt : éviter de les utiliser (pour des raisons de sécurité

- Exemple : U_prestataires (liste des prestataires au sein de la forêt)

Groupes de Domaines Locaux

- Membres : membres faisant partie de la forêt
- Autorisations attribuées au sein du domaine ou existe le groupe de domaine local
- Exemple : DL_partage1_rw, DL_partage1_ro

Imbrication des groupes (très important)



La méthode AG(U)DLP est LA méthode à utiliser

1. On crée les utilisateurs
2. On crée les groupes globaux (G_service paye …)
3. On crée les groupes de domaine local DL_accès en lecture pour SRVFIC1-Partage1
4. On crée les permissions

Administration des groupes

pour modifier l'appartenance à un groupe (soit on fait à partir de l'utilisateur ou à partir du groupe)

Création des unités d'organisation (OU)

On crée d'abord les OU puis, quand on crée un nouvel utilisateur, on le place directement dans une OU

Exemples d'arborescences :
/nom_de_la_société/Villes/Services/ ou /nom_de_la_société/Services/Villes/

Une OU sert à :

- Attribuer des GPO (stratégies de groupe) à conteneur
- Définir des délégations d'organisation (délégation administrative : qui est administrateur sur cette OU)
- Organiser les objets (objectif secondaire)

Pour supprimer une OU protégée contre la suppression : Gestionnaire de serveur > Affichage > Fonctionnalités avancées

4 Gestion de l'accès aux ressources dans les services de domaine ADDS

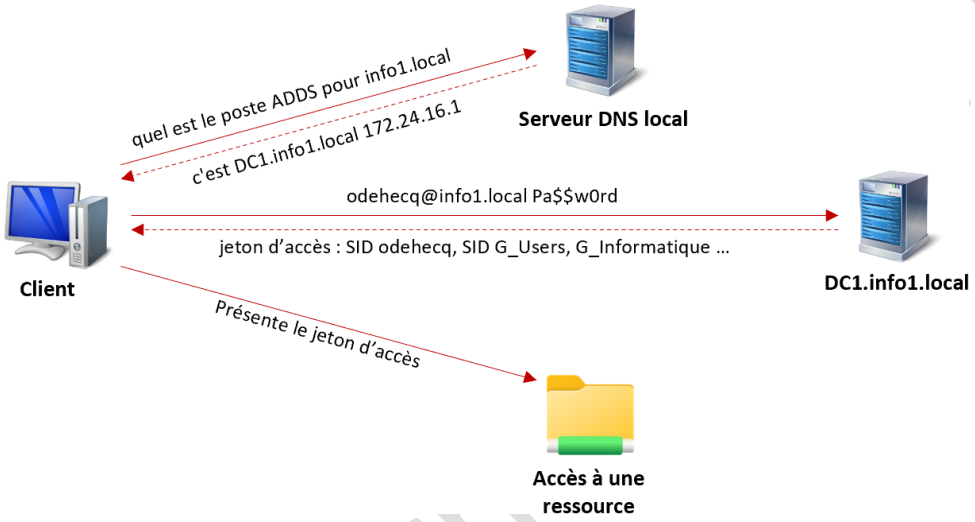
Qu'est-ce qu'une entité de sécurité

S–1–5–21–{Id_de_Domaine} –{Id_de_l'objet_au_sein_du_domaine}

- **S** : SID
- **1** : version du SID
- **5** : Id de l'autorité de certification
- **21** : Domaine AD

Un utilisateur n'aura pas du tout le même SID si on le change de domaine ! Son IdDomaine et son IdObjet seront différents !

Qu'est-ce qu'un Jeton d'Accès



Méthode d'obtention et d'utilisation du jeton d'accès

quand odehecq veut accéder à une ressource, il renvoie l'intégralité des SID contenus dans le jeton d'accès.

En quoi consistent les autorisations

Dossier >> Propriétés > Sécurité > Avancés

- Autorisations : DACL
- Audit : SACL
- Chaque ligne d'une ACL (ACcess List) correspond à une ACE (ACcess Entry)

DL_srv1-partage_ro : accès en lecture sur \\srv1\partage : Membres de DL_srv1-partage_ro : G_marketing

DL_srv1-partage_ct : accès en contrôle total sur \\srv1\partage : Membres de DL_srv1-partage_ct : G_ITAdmins

DL_srv1-partage_refus : refus de lecture sur \\srv1\partage : Membres de DL_srv1-partage_refus : G_BranchManagers

DL_srv1-partage_rw : lecture et écriture sur \\srv1\partage : Membres de DL_srv1-partage_rw : G_Investments

Particularités :

- On fait les droits en fonction des noms du groupes DL
- Les coches grisées ✓ correspondent aux droits hérités par un parent
- Les coches noires ✓ correspondent aux droits définis sur ce dossier (autorisations explicites)
- Désactiver l'héritage : supprime ou convertit les autorisations héritées en autorisations explicites
  - Supprimer les autorisations : plus aucun droit sur le dossier
  - Convertit les autorisations : ajoute les mêmes autorisations que celles du dossier parent
- Accès effectif permet de connaître les autorisations d'un utilisateur en particulier en fonction des autorisations appliquées

Un refus explicite prime sur des autorisations explicites.

Les refus hérités d'un répertoire parents ne priment pas sur les autorisations explicites du dossier courant

Effets de la copie et du déplacement sur les autorisations NTFS

	Sur la même partition	Sur une partition différente
Copie	Hérite des droits du dossier parent	Hérite des droits du dossier parent
Déplacement	Conserve les droits du dossier source	Hérite des droits du dossier parent

Le déplacement sur un même partition est d'ailleurs plus rapide puisqu'il conserve tout.

`robocopy {dossier source} {dossier destination} /E /A /COPYALL /W 0 /R:0 *.*` : garder les droits lors d'une copie pour conserver les droits

Les partages

Le filtrage se fait au plus près de la ressource (filtrage par les droits NTFS).

Les autorisations du partage sont à définir de façon « peu regardantes » car les droits se font au niveau de l'onglet sécurité.

Onglet Partage > Partage avancé > Partager le dossier

- Enlever le groupe Tout le monde et le remplacer par le groupe Utilisateurs authentifiés
- Autorisations possibles pour le partage : lecture, modification, contrôle total

Mise en cache des partages :

Mise en cache : utile pour un partage attribué à **un seul utilisateur** car le fichier le plus récent écrase le plus ancien.

On peut rendre un partage indisponible hors connexion à partir du serveur

Éléments à prendre en compte pour le partage avec NTFS :

- Attribuer les autorisations aux groupes : utiliser la méthode AGuDLP
- Le droit Refuser ne doit être utilisé qu'en cas de nécessité
- Ne jamais refuser l'accès à « Tout le monde »
- Privilégier Contrôle Total au niveau du partage pour le groupe Utilisateurs authentifiés
- Affiner les autorisations au niveau NTFS

Configuration des objets et approbations AD

Utilisateurs et ordinateurs Active Directory > Affichage > Fonctionnalités avancées

Sélection l'OU souhaitée >> Propriété > Sécurité : autorisation au niveau de la gestion d'OU

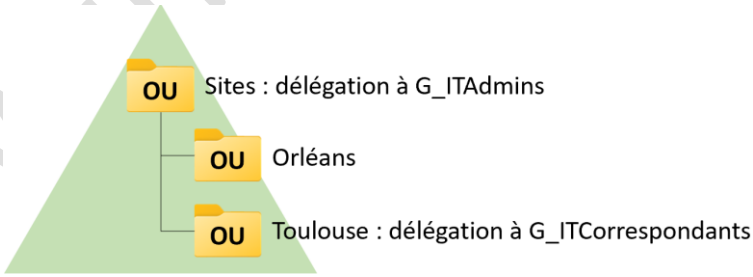


Illustration d'un cas de nécessité de délégation de contrôle, pour un site sans service informatique

Sur une OU, clic-droit > Délégation de contrôle : ouvre l'assistant de délégation de contrôle

C:\Windows\System32\delegwiz.inf : fichier de paramètres à personnaliser si besoin pour ajouter d'autres tâches délégables, telles que l'autorisation de verrouiller un compte Ordinateur

Pour supprimer ou déplacer un OU : en ayant l'affichage Fonctionnalités avancées, sélectionner l'OU >> Propriétés > Objet > décocher « Protéger l'objet des suppressions accidentelles »

Taches administratives depuis un poste client : Utilisation de RSAT

- Sur Windows 10 (avant la mise à jour d'octobre 2018 : à télécharger ici : Download Outils d'administration de serveur distant pour Windows 10 from Official Microsoft Download Center
- Sur Windows 11 : Paramètres > Applications > Fonctionnalités facultatives > RSAT : outils Active Directory …

Pour faire une console ergonomique pour le gestionnaire d'OU :

mmc.exe :

- Fichier > Ajouter ou supprimer un composant … > Utilisateurs et Ordinateurs AD > ajouter
- Sélectionner l'OU choisie > Nouvelle fenêtre à partir d'ici
- Nouvelle vue de la liste des tâches : pour personnaliser l'affichage
- Enregistrer sous… > nommer avec un nom explicite du type « OU miami »

Approbations ADDS

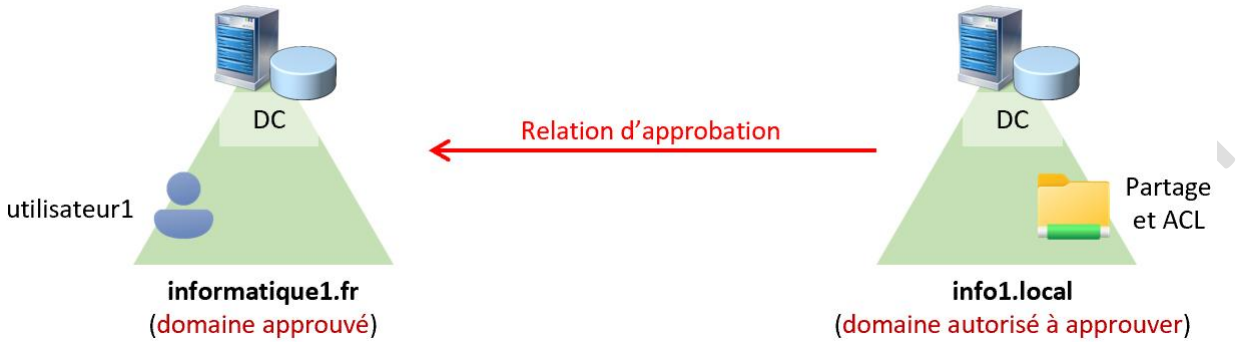
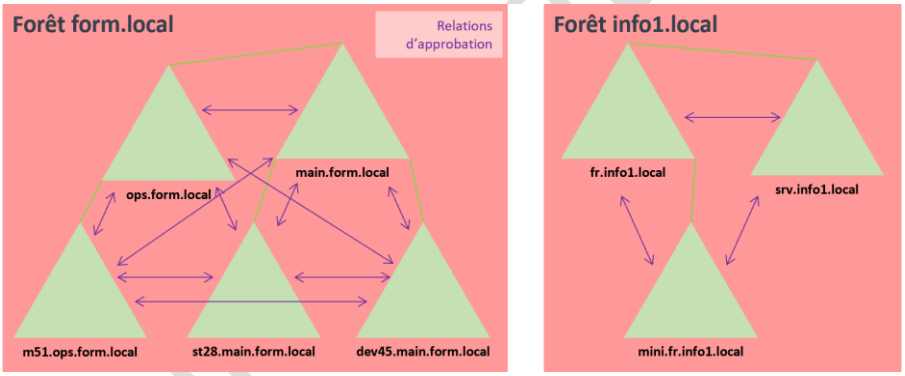


Illustration de la relation d'approbation entre domaines

Dans le cas de ressources (partages, imprimantes, etc.) et de comptes (utilisateurs) sur des domaines différents, la relation d'approbation va de la ressource vers les comptes. On dit que les ressources **approuvent** les comptes

Au sein d'une forêt, tous les domaines s'approuvent mutuellement (relation bidirectionnelle transitive)



Dans une forêt, les domaines s'approuvent mutuellement (relation bidirectionnelle et transitive)

5 Les GPO (stratégies de groupe)

Documentation officielle : https://docs.microsoft.com/fr-fr/troubleshoot/windows-server/group-policy/group-policy-overview

Les GPO (Group Policy Objects), permettent de diminuer la charge d'administrative en exécutant des paramètres automatiquement. Cela réduit donc les mises à jour et le dépannage (dans le cas de fausses manipulations).

Le TCO (cout total de possession) diminue, le ROI (retour sur investissement) augmente.

Une GPO permet d'automatiser la gestion des ordinateurs et des utilisateurs (pas de gestion des groupes)

On peut récupérer les modèles d'administration de logiciels non prévus dans les GPO (.ADMX)

Fichiers ADMX

(!) attention aux paramètres de l'OS plus nombreux que ceux du DC quand on utilise adminpak

A chaque nouvelle version de Windows, un nouveau fichier ADMX est mis à disposition par Microsoft. Il suffit de faire la recherche. Exemple « admx Windows 11 21H2 » : https://www.microsoft.com/en-us/download/details.aspx?id=103507

- Installez le fichier téléchargé
- Ouvrez C:\Program Files (x86)\Microsoft Group Policy\Windows 11 October 2021 Update (21H2)\PolicyDefinitions
- Copiez les fichiers .admx et les dossiers fr-fr\ et en-US\ dans le dossier PolicyDefinitions. Ce dossier ce trouve ici : \\info1.local\SYSVOL\info1.local\Policies\PolicyDefinitions (créer le dossier PolicyDefinitions si besoin)
- Les Modèles d'administration se trouvent dans : Configuration ordinateur\Stratégies\Modèles d'administration

Pour les ADMX de Google Chrome : https://support.google.com/chrome/a/answer/187202?hl=fr#zippy=%2Cwindows

Configuration de l'étendue des GPO

Les GPO peuvent être liées à un domaine ou à des OU

Une GPO ne s'applique par pour les groupes présents dans l'OU mais pour les ordinateurs ou les utilisateurs présents

- Sur l'OU : bloquer l'héritage permet de ne pas faire s'appliquer les GPO des OU supérieures
- Sur la GPO appliquée : forcer la GPO la fait s'appliquer aux objets enfants, même en bloquant l'héritage

Créer une GPO

1. Gestion de stratégie de groupe ou `gpmc.msc` > Sélectionner l'OU concernée >> Créer un objet GPO …
2. Donner un nom clair à la GPO puis cliquer sur OK
3. Clic droit sur la nouvelle GPO >> Modifier
4. Stratégies > Modèles d'admin > Tous les paramètres (filtres + options des filtres)
5. Cliquer/glisser la GPO là où on veut qu'elle s'applique

(!) En dernier recours : Filtrage de sécurité d'une GPO sélective :

- Ne s'appliquant qu'à G_Compta : ajouter le groupe G_Compta + supprimer le groupe Utilisateurs Authentifiés
- S'appliquant à tout le monde sauf au G_Directeurs : ajouter le groupe G_Directeurs et mettre un refus explicit, laisser Utilisateurs Authentifiés

Mettre en pause une GPO : dans le dossier « Objets de stratégies de groupe » >> Etat GPO :

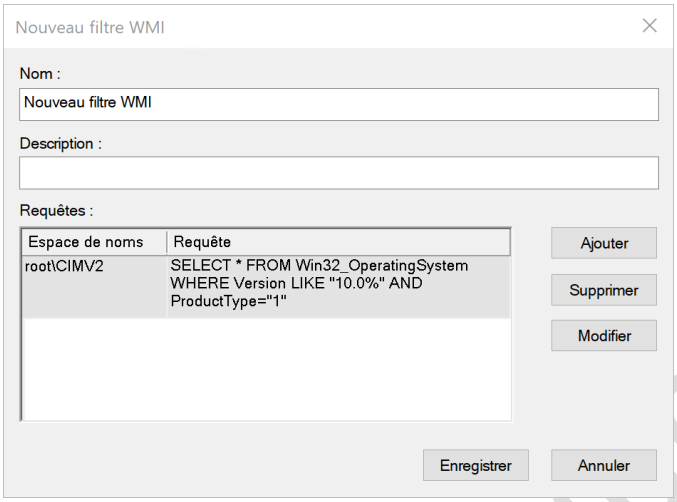
Il est possible de désactiver entièrement la GPO, de désactiver juste la partie ordinateurs ou juste la partie utilisateurs

Filtrage WMI

Le filtrage WMI permet d'appliquer ou non la GPO en fonction de caractéristiques internes de l'ordinateur.

Documentation officielle : Créer des filtres WMI pour l'Windows - Windows security | Microsoft Docs

Dans le dossier Filtres WMI >> Nouveau



La requête permet de définir quels sont les postes concernés par le filtre. Ici les Windows 10

Exemples de filtrages :

- `SELECT * FROM Win32_Processor WHERE AddressWidth = "64"` : tous les ordinateurs avec un OS 64bits
- `SELECT Name FROM Win32_ComputerSystem WHERE Name LIKE "PC-PORTABLE-%"` : tous les ordinateurs dont le nom commence par "PC-PORTABLE-"

Une fois crée, pensez à appliquer le filtre à la GPO. Il n'est possible d'appliquer qu'un filtre WMI par GPO

Résultats de la stratégie de groupe

Dossier « Résultat de stratégie de groupe » : permet de récupérer des informations de GPO (il faut que la session soit active). Pensez à `gpupdate /force` sur le poste à tester

Modélisation de la stratégie de groupe

Dossier « Modélisation de stratégie de groupe » : simulation du résultat (on peut changer l'OU, les groupes, l'utilisateur, l'ordinateur …)

Délégations

Selon l'objet sélectionné, les possibilités ne sont pas les mêmes

- Objet de stratégies de groupes : la délégation donne le droit de créer des GPO
- Sur la GPO elle-même : la délégation permet de modifier le domaine d'application de la GPO
- Sur une OU : la délégation permet de lier des GPO, lancer des analyses, lire les résultats

6 Configuration des environnements des utilisateurs et ordinateurs à l'aide de GPO

Scripts

Modification de la GPO dans `gpmc.msc`

Ordinateur > Stratégies > Paramètres Windows > Scripts (ne s'applique qu'aux ordinateurs de l'OU) : de démarrage / d'arrêt

Utilisateur > Stratégies > Paramètres Windows > Scripts (ne s'applique qu'aux utilisateurs de l'OU) : de démarrage de session/ de fermeture de session

Redirection de dossiers

On peut rediriger certains dossiers ciblés vers un lecteur réseau : AppData, Bureau, Docs

Utilisateur > Stratégies > Paramètres Windows > Redirection de dossiers : vers un dossier partagé

- Il faut que le groupe Utilisateurs authentifiés ait le droit Contrôle Total sur le partage \\WS2022AD1.info1.local\users$
- Paramètre de la cible = de base : chemin d'accès à la racine : \\WS2022AD1.info1.local\users$
- Paramètre de la cible = avancé : gérer les sécurités soi même

Installation de logiciels

Documentation officielle : https://docs.microsoft.com/fr-fr/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software

- Le logiciel à installer doit-être au format .msi et sur un partage réseau accessible en lecture
- Testez l'installation automatique avant (et utilisez un fichier de réponses si besoin)
- Utilisateur > Stratégies > Paramètres du logiciel > Installation de logiciel :
    - Si le mode de déploiement est « publié » : laisse le choix à l'utilisateur d'installer ou non
    - Le logiciel doit-être sur un partage accessible à l'utilisateur

Personnellement, je préfère l'exécution d'un script avec chocolatey ou winget.

Si vous installez des logiciels avec chocolatey, pensez à `choco update all` au démarrage de la session

Configuration des préférences des GPO

Sous-dossier Préférences : permet de changer des paramètres de GPO (ex. : installation d'imprimantes réseau) mais l'utilisateur peut aller à l'encontre de ces préférences.

Résolution des problèmes de GPO

S'il y a un souci sur un paramètre qui est dans une GPO récupérée et traitée : une autre GPO va à l'encontre de celle-ci, un paramètre n'est pas pris en charge, etc.

S'il y a un souci de GPO non traitée : l'objet est non concerné par la GPO, il y a un filtrage de sécurité, un filtre WMI, etc.

7 Implémentation de la sécurité à l'aide d'une GPO

La stratégie de compte/mot de passe se fait dans la GPO **Default Domain Policy** car c'est une GPO liée au domaine ET d'ordre des liens de niveau 1 (sous-entendu, elle a la priorité sur les autres GPO)

Verrouillage de mots de passe fait par la GPO **Default Domain Contrôler Policy** car c'est le DC qui gère les objets ordinateurs du domaine.

Implémentation de stratégies de mots de passe affinées

Réservé aux administrateurs « qui s'y connaissent ». But : modifier les stratégies de mots de passe pour des groupes

1. Créer la stratégie de mots de passe affinée

   Modifications ADSI > Nouveau … (Domaine) > System > Password Setting Configuration > Nouveau … Rentrer les paramètres (!) Durée = JJ:HH:mm:ss

2. Lier la stratégie à un groupe

   Utilisateurs et Ordinateurs AD > (affichage avancé) System > Password Setting Container > Propriétés > Sécurité > Choisir les groupes concernés

3. Lier un groupe AD à un groupe type SAM

   Dans GPO > Ordinateur > Stratégies > Paramètres Windows > Groupes restreints : chercher un groupe dans BuiltIn, ajouter le groupe du domaine ciblé

Stratégie de restriction logicielle

1. Ajouter une stratégie : nouvelle stratégie de sécurité logicielle ; niveau de sécurité :
   - tout autoriser sauf …
   - tout refuser sauf … (**non recommandé**)
2. Définir les exceptions selon : règle de certificat, règle de hachage, chemin d'accès

Modèles de sécurité

Des modèles existent, mais ils sont surtout utiles pour UN rôle particulier → rare
Création assistée de modèle → tester avant !

8 Configuration de la conformité des serveurs en matière de sécurité

Il faut appliquer la sécurité à tous les niveaux afin de bloquer le niveau supérieur si un niveau est passé (livre 9-5)

EFS

Permet de crypter le système de fichiers (documentation : Protection des données avec le système EFS (Encrypting File System) | Microsoft Docs)

Le certificat utilisé contient une clé privée (à garder en sécurité) et une clé publique (qui peut être partagée)

A partir du fichier non crypté, si on utilise la clé publique : on obtient le fichier crypté

Inconvénient de l'EFS : ne permet pas de chiffrer les données du système d'exploitation (pour ça on utilise BitLocker)

EFS : si on réinitialise le mot de passe utilisateur : on ne peut plus utiliser ses clés, il faut définir un agent de récupération

Configuration d'une stratégie d'audit

Traçabilité : utile sur une OU=Serveurs

Ordinateur > Stratégies > Paramètres Windows > Sécurité > Stratégie d'audit

Doit être ciblé :

- quelle ressource auditer
- quels évènements auditer
- durée de l'audit

Exemple : tracer des utilisateurs qui suppriment des fichiers dans un répertoire partagé

- GPO : accès aux objets, réussite
- Dossier : tout le monde, suppression de dossiers
- CMD : `auditpol /?`
- aller consulter les évènements d'audit

WSUS (9-21 ; 9-23)

Serveur de mises à jour Windows update. Utile derrière un pare-feu et pour réduire la bande passante et les mises à jour autorisées

Gestionnaire de serveur > Gérer > Ajouter des rôles > Service WSUS

Console d'administration : Service WSUS

Commandes PowerShell : `get-command | where-object Source -eq UpdateServices`

- Liste des clients WSUS : `Get-WsusComputer`
- Supprimer les mises à jour obsolètes de la BDD [1]: `Invoke-WsusServerCleanup -CleanupObsoleteUpdates`

Exemple :

1 groupe de client « WsusTest », 1 groupe « WsusPreprod » et plusieurs groupes « WsusProdXX » : cela permet de tester les éventuels effets de bord des mises à jour avant de les déployer en production.

C'est le client qui doit aller chercher les mises à jour sur le serveur WSUS : il faut configurer cela par GPO : Configuration Ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update > Gérer les mises à jour proposées par Windows Server Update Services :

- Spécifier l'emplacement intranet du service de mise à jour Microsoft : activé et http://{serveur wsus}:8530

`wuauclt.exe` : force la recherche des mises à jour sur le serveur WSUS

[1] BDD : Base de Données

9 Configuration et gestion des technologies de stockage

La gestion du stockage fait partie des rôles de l'administrateur du serveur :

- Il faut assurer un suivi (évolution de la consommation pour prévoir les besoins)
- Il faut garder un historique de données : attention au seuil critique
- Il faut surveiller l'augmentation du volume de données. Augmentation justifiée ou non ? Informer les utilisateurs de la nature des documents à stocker

FSRM[2]

FSRM Permet de faire de l'analyse des données : capacité, coût, migration des données, quotas

Documentation : Vue d'ensemble des outils de gestion de ressources pour serveur de fichiers (FSRM) | Microsoft Docs

Installation : Fonctionnalités > Outils d'administration de rôles > Outils de services de fichiers > Outils du Gestionnaire de ressources du serveur de fichiers

Console : Gestionnaire de ressources du serveur de fichiers

Les quotas servent à :

- analyser qui occupe quoi sans limiter l'espace disque
- limiter l'espace disque (attention aux potentiels effets de bords). L'outil de base (sans FSRM) se limite aux partitions

Gestionnaire de Ressources de Serveur de Fichiers

Mise en place des quotas :

- sur les dossiers : un quota sur l'ensemble des données contenues
- automatique : un quota égal par sous-dossier, par exemple pour les dossiers personnels des utilisateurs

Rapport sur l'utilisation du disque : planifiables ou exécutables à la main.

Réseaux SAN

Un réseau NAS est un ensemble de disques dur avec partage de ressources intégré. Ne coute pas cher

Un réseaux SAN est un réseau dédié de stockage. Les possibilités sont élevées et cela coute très cher : plusieurs dizaines de milliers d'euros minimum.

Pour se faire une idée : NAS Expert, vente en ligne de solution de stockage et mémoire

- Nota : la capacité brute est la capacité avant mise en place du RAID. La capacité utile est donc bien plus faible

[2] FSRM : File Server Resource Management