Windows

Présentation

Types de serveurs

- Contrôleur de domaine – Serveur hébergeant un domaine Active Directory
- Serveur membre -Serveur ne possédant pas la base d'annuaire mais hébergeant des applications client/serveur et des services réseaux
- Contrôleur de domaine en lecture seule – Possède une copie de la base de données AD en lecture seule
- Core server – Il s'agit d'un serveur sans interface graphique

Rôles et fonctionnalités

Un rôle serveur définit la fonction principale du serveur. Chaque rôle peut inclure un ou plusieurs services de rôles, qui correspondent à des éléments facultatifs du rôle.
Une fonctionnalité fournit une fonction auxiliaire au serveur.

DNS

Ce système est repris par Microsoft pour gérer les domaines Windows car il fournit les services de résolution de noms requis par Active Directory.

DNS Dynamique

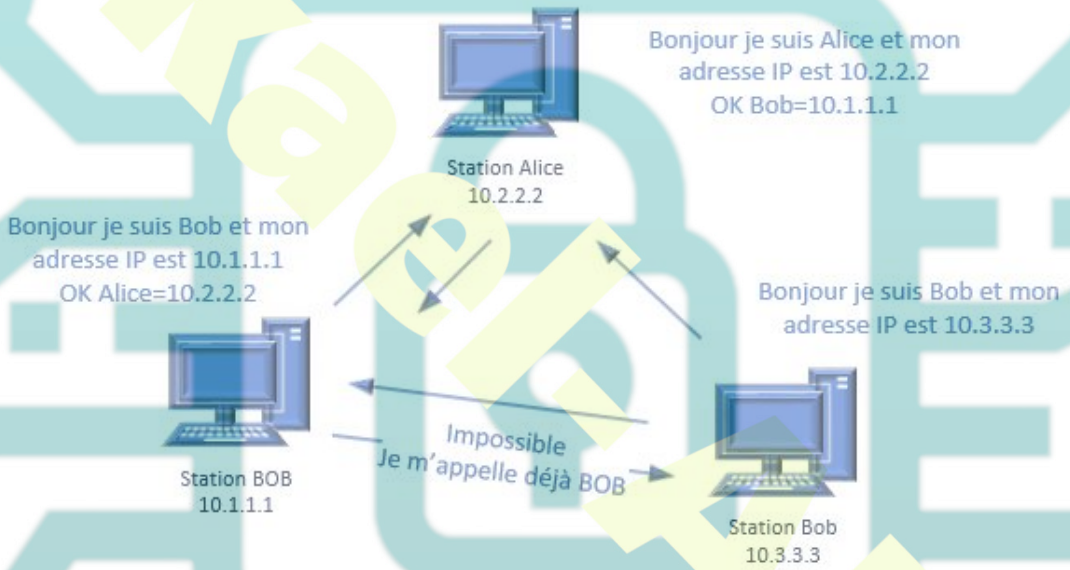
Une des principales composantes du serveur DNS de Windows est de prendre en charge les enregistrements de façon dynamique. Auparavant, les serveurs DNS étaient statiques et toute nouvelle entrée dans le DNS devait se faire manuellement.

Intégrer manuellement toutes les machines Windows du réseau devenait quasi insurmontable et notamment avec la gestion des clients DHCP, c'est pour cela que le DNS dynamique est utilisé dans le cadre des domaines Microsoft.

Gestion des noms sur les réseaux Windows

Dans un domaine MS le principe de base est que toutes les machines doivent être visibles par leur nom. En effet, Lorsque vous installez une machine Windows, vous devez impérativement indiquer un nom **unique** dans le réseau qui servira à repérer la machine sur ce dernier. Ces noms utilisent le protocole NetBios qui permet d'associer l'adresse réseau au nom NetBios en utilisant le principe de la diffusion.

Utiliser 2 noms NetBios identiques créé un conflit comme dans le cas de 2 adresse IP identiques.



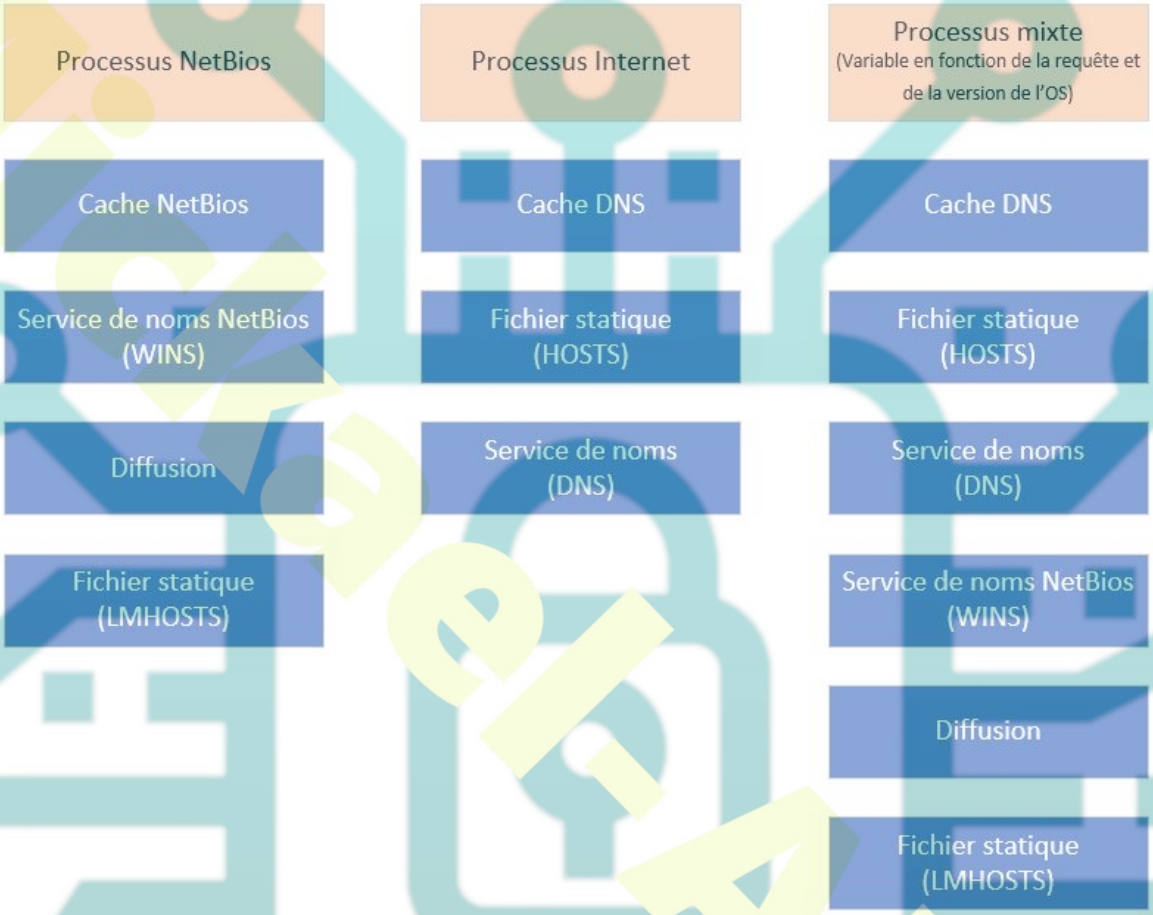
Mais avec l'extension des réseaux et l'apparition des réseaux routés, la diffusion a montré ses limites. La première solution trouvée par MS fût de créer un service de noms NetBios nommé WINS (Windows Internet Name Service) qui est une base de données à plat (non hiérarchique) permettant d'associer l'adresse IP au nom NetBios.

Néanmoins, l'arrivée d'internet et le besoin de devenir compatible full IP a contraint Microsoft à créer un système d'annuaire compatible avec le standard internet.

Dans un premier temps, le choix fût simple : remplacer la gestion des noms NetBios par des noms d'hôtes DNS. Cependant, pour des raisons de compatibilité (gestion des anciens systèmes et des ordinateurs personnels hors domaine), le système de gestion conserve les 2 systèmes de nommage (Netbios et DNS)

La problématique :

1. Avoir un système de nommage sans diffusion compatible avec internet et utilisant les suffixes
2. Conserver un système de nommage avec diffusion compatible avec l'existant



La solution

Utiliser un mixage des deux systèmes de nommage en privilégiant dans un premier temps DNS, puis en s'appuyant (si le DNS n'existe pas) sur le processus NetBios.

Intégration de DNS et Active Directory

Windows prend en charge DNS et Active Directory. Il est possible d'intégrer le DNS en tant qu'objet dans l'annuaire Active Directory. De ce fait, les entrées DNS sont copiées au cours du processus de duplication.

Ce choix peut se décider lors de la création d'une nouvelle zone ou en modifiant une zone existante.

Active Directory

Active Directory est le service d'annuaire proposé avec Windows.

Un service d'annuaire regroupe toutes les informations relatives aux ressources réseaux : utilisateurs, groupes, imprimantes.

Active Directory est un système d'annuaire global et hiérarchisé. Grâce à ce concept, l'utilisateur peut accéder à une ressource sans avoir besoin de connaître l'emplacement physique de cette ressource. Le positionnement physique des ressources devient transparent pour l'utilisateur.

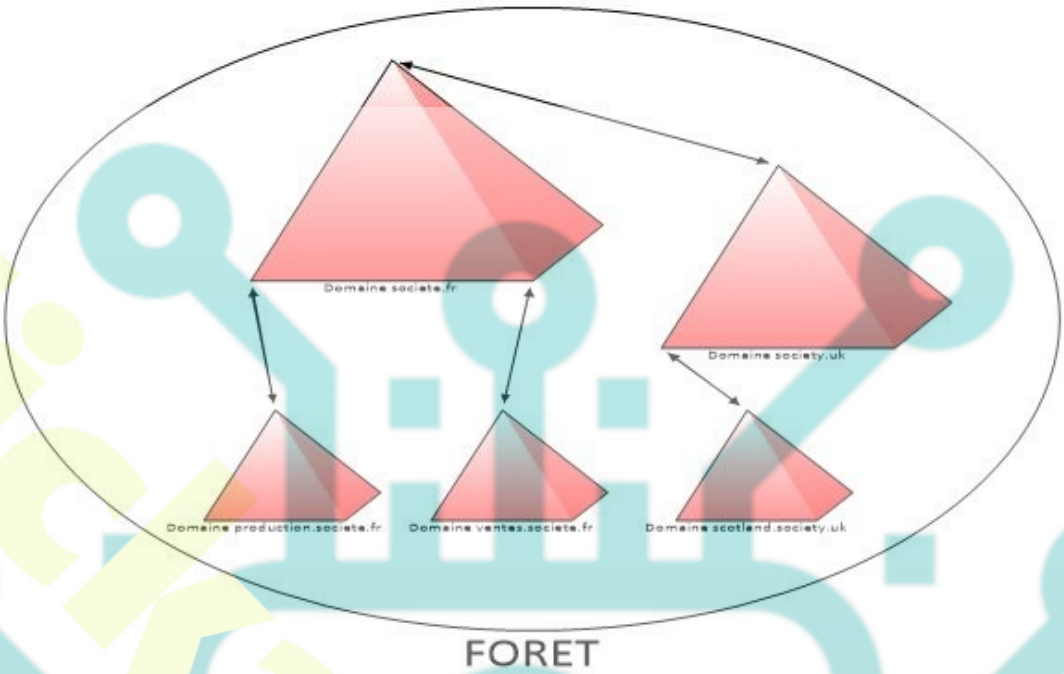
Caractéristiques et fonctionnalités

- Un annuaire distribué : L'annuaire n'est pas centralisé sur un seul ordinateur, ce qui permet d'avoir une tolérance aux pannes et d'accélérer l'accès aux ressources de l'annuaire.
- Active Directory peut contenir plusieurs millions d'objets.
- Une ouverture de session unique pour l'accès à l'ensemble des ressources.
- L'administration d'une partie de l'annuaire peut être déléguée.
- Il est conforme aux recommandations X.500 de l'ISO et prend en charge le protocole LDAP Version 2 et 3.

Structure d'Active Directory

Forêt

C'est un groupement de plusieurs arbres qui ont des noms disjoints (par exemple : societe.fr et society.uk) Tous les arbres d'une forêt partagent le même schéma et le même catalogue, mais ont des structures de noms différentes. Les domaines d'une forêt fonctionnent indépendamment les uns des autres, mais les forêts permettent la communication entre domaines.

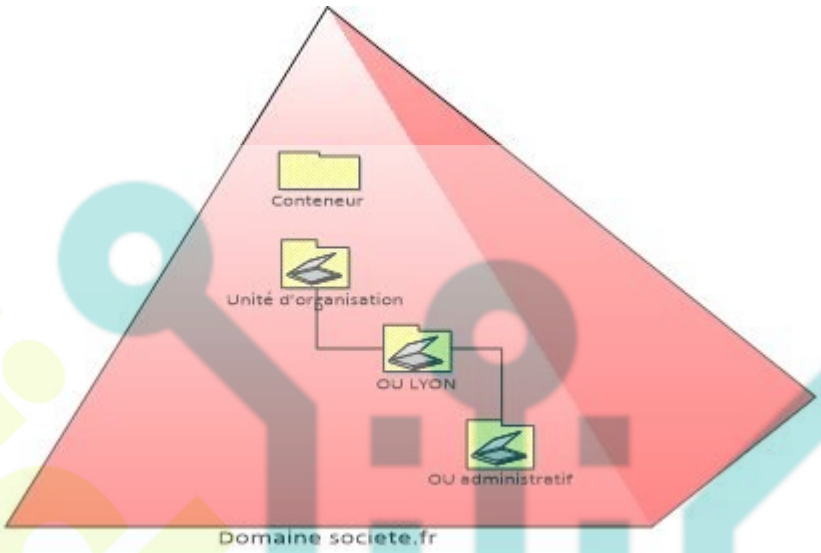


Arbre

C'est un groupement ou un arrangement hiérarchique d'un ou plusieurs domaines Windows qui partagent des espaces de noms contigus (par exemple societe.fr et ventes.societe.fr). Tous les domaines d'un même arbre partagent le même schéma et partagent un catalogue commun.

Domaine

C'est une entité d'administration centralisée contenant des objets (conteneur, unité d'organisation, groupe, utilisateur…) Le domaine regroupe un ensemble d'ordinateurs qui partagent la même base de données d'annuaire. L'administrateur du domaine a les droits nécessaires pour effectuer toutes les tâches d'administration dans le domaine.



Renommer un domaine Active Directory

La procédure suivante vous explique comment renommer un domaine Active Directory.

1. Ouvrir une fenêtre de commande en mode « administrateur » et entrer la commande ci-après qui va générer un fichier Domainlist.xml :.

```
rendom /list
```

2. Éditer le fichier xml, en modifiant votre ancien domaine par le nouveau :

```
<?xml version ="1.0"?>
<Forest>
        <Domain>
                <!-- PartitionType:Application -->
                <Guid>0731e77c-1b86-4dd4-949a-191f75acab61</Guid>
                <DNSname>ForestDnsZones.ais.local</DNSname>
                <NetBiosName></NetBiosName>
                <DcName></DcName>
        </Domain>
        <Domain>
                <!-- PartitionType:Application -->
                <Guid>664c9a1d-a68b-490b-8e6b-f3504998d914</Guid>
                <DNSname>DomainDnsZones.ais.localm</DNSname>
                <NetBiosName></NetBiosName>
                <DcName></DcName>
        </Domain>
        <Domain>
                <!-- ForestRoot -->
                <Guid>30a6dbd6-5032-461b-afd5-afad708ccbca</Guid>
                <DNSname>ais.local</DNSname>
                <NetBiosName>AIS</NetBiosName>
                <DcName></DcName>
        </Domain>
</Forest>
```

Il faut remplacer toutes les occurrences mentionnant l'ancien nom de domaine par le nouveau (ici, on remplace « societe.com » par « ais.local »), puis on enregistre le fichier.

3. Prépare la forêt avec les infos modifiées dans le fichier Domainlist.

```
rendom /showforest
```

4. Prépare les contrôleurs de domaine pour le changement de nom. Chaque contrôleur servant le nom de domaine est contacté et mis en condition.

```
rendom /upload
```

5. Entrer la commande suivante qui va permettre de contacter l'ensemble des contrôleurs de domaine et les préparer au changement.

```
rendom /prepare
```

6. Entrer la commande suivante pour lancer le renommage. Les contrôleurs vont redémarrer automatiquement :

```
rendom /execute
```

7. Réparation des liens des stratégies de groupe (GPO) présents dans Active Directory pour le DNS

```
gpfixup /olddns:societe.com /newdns:ais.local
gpfixup /oldnb:societe.com/newnb:ais.local
```

8. Cette ultime commande est à exécuter **si et seulement si** tous les postes ont pris en compte le changement.
Si cette commande est exécutée trop tôt, elle peut empêcher les postes d'ouvrir une session utilisateur.

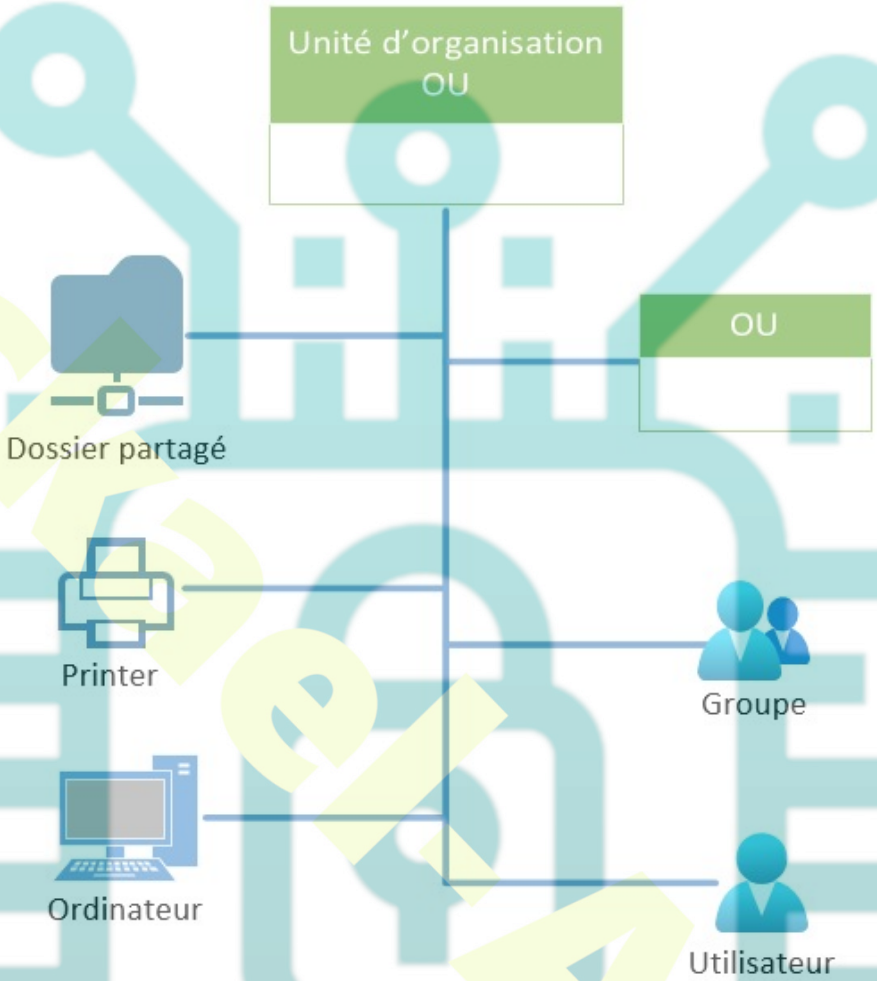
```
rendom /clean
```

Vous pouvez maintenant aller dans la console de gestion DNS pour supprimer l'ancienne zone DNS devenue obsolète.

Site

Combinaison d'une ou plusieurs IP de sous-réseaux connectées par des liens à hauts débits. Ils contiennent les connexions pour configurer la réplication entre sites. Ils permettent d'intégrer la topologie physique du réseau dans Active Directory.

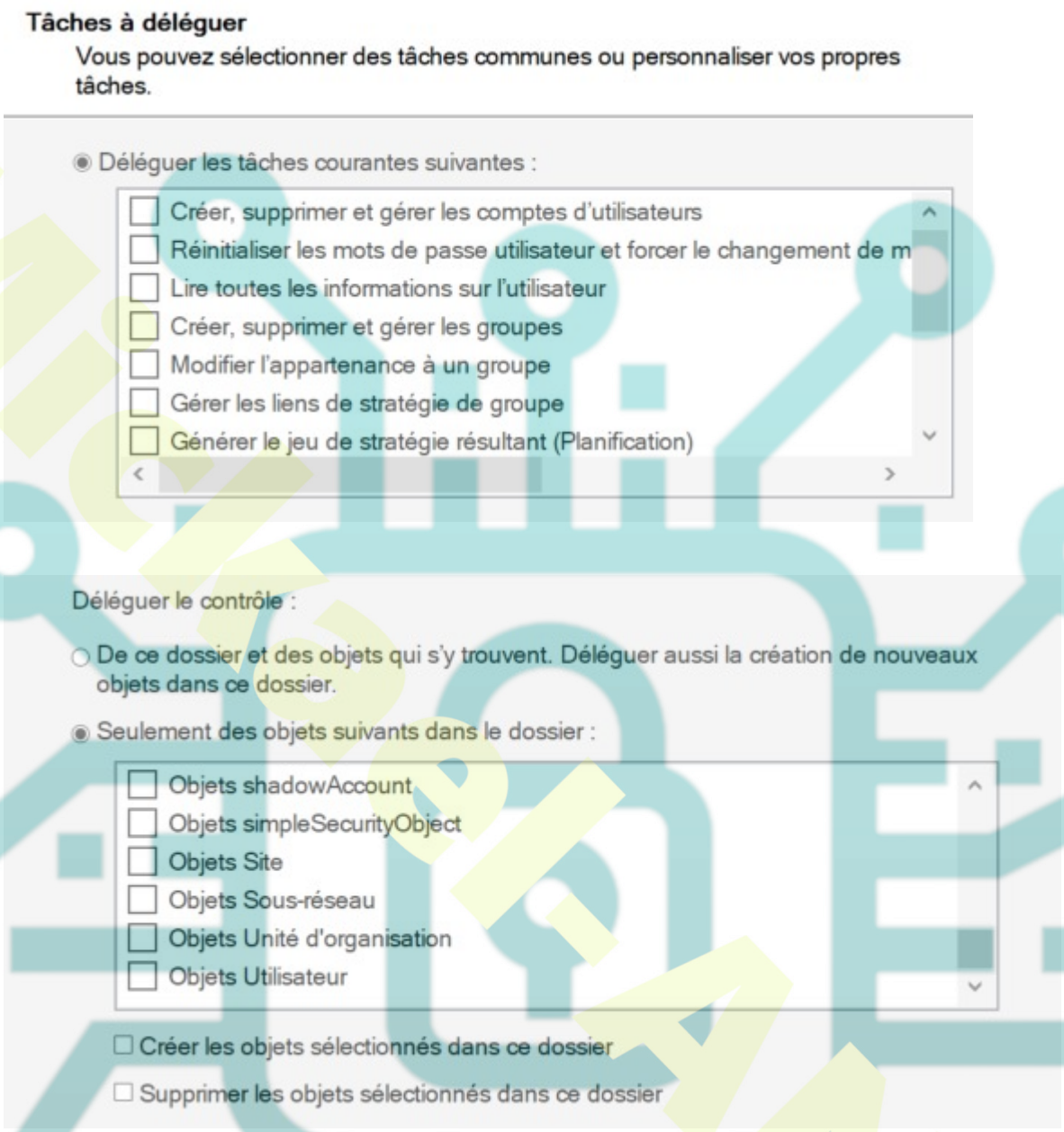
Unité d'organisation



Délégation AD

Gestion des objets Active Directory

Il est possible de contrôler les utilisateurs quant à l'accès aux objets et aux attributs des objets. De plus, la nature hiérarchique d'Active Directory permet de déléguer l'administration de l'annuaire à un utilisateur ou un groupe en lui permettant de gérer un domaine, un ensemble d'unités organisationnelles ou un seul objet.



Contrôleur de domaine

Un ordinateur fonctionnant avec Windows serveur peut fonctionner en tant que serveur membre ou en tant que contrôleur de domaine. Si le serveur a été configuré pour être contrôleur de domaine, il stocke automatiquement une réplique de l'annuaire et duplique les modifications vers les autres contrôleurs de domaine au sein d'un même domaine.
Un domaine peut contenir un ou plusieurs contrôleurs de domaine. Comme tous les contrôleurs d'un même domaine contiennent une copie de l'annuaire en lecture/écriture, il se peut que l'annuaire d'un contrôleur soit différent de celui d'un autre contrôleur tant que la synchronisation ne s'est pas faite.

Serveur de catalogue global

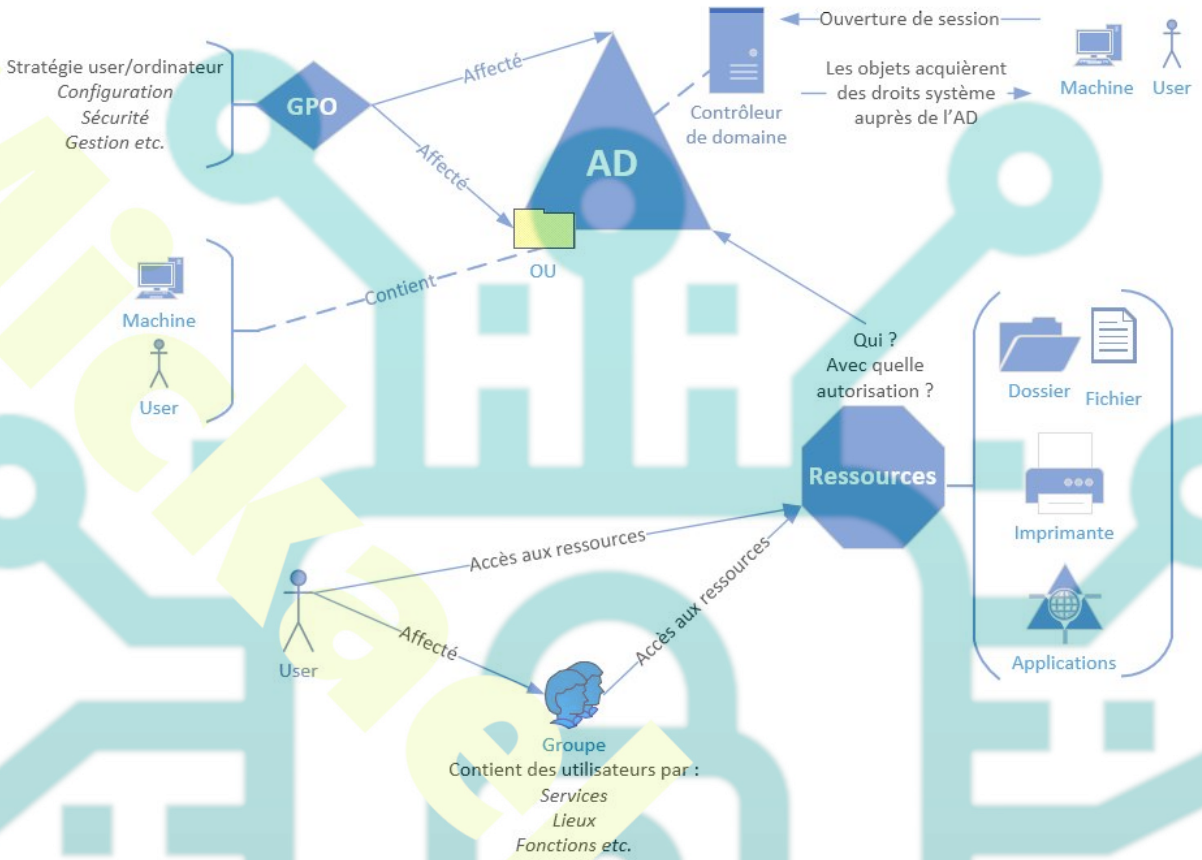
Il permet d'optimiser les recherches effectuées à l'échelle d'une forêt. Si vous souhaitez lister l'ensemble des utilisateurs créés dans Active Directory, c'est le serveur de catalogue global qui se charge de traiter cette requête plutôt que d'interroger chaque domaine de la forêt.
Le premier contrôleur est le serveur de catalogue global. Il est possible de définir d'autres contrôleurs de domaine comme jouant le rôle de serveur de catalogue global (1 par site physique)

Serveur « maître d'opération » rôles FSMO

Le rôle de ces serveurs est de gérer des opérations qui ne doivent pas être effectuées simultanément en plusieurs points du réseau. Dans chaque forêt, on doit avoir un contrôleur de domaine qui remplit un ou plusieurs des cinq rôles de maître d'opération.

Maître de schéma : Contrôle toutes les modifications apportées au schéma. Un seul maître de schéma par forêt.
Pour installer le module du schéma taper (regsvr32 schmmgmt.dll)
Maître de nommage de domaine : Contrôle l'ajout et la suppression de domaine. Un seul maître de nommage de domaine par forêt.
Maître d'identificateur relatif : Alloue des séquences d'identificateurs relatifs (SID) aux différents contrôleurs du domaine. Un seul maître d'identificateur relatif par domaine.
Émulateur de contrôleur principal : En mode mixte, fait le lien entre les contrôleurs Windows AD et les contrôleurs Windows NT. Un seul émulateur de contrôleur principal par domaine.
Maître d'infrastructure : Est responsable de la mise à jour des références groupes/utilisateurs lorsque des ajouts à des groupes sont effectués.

Architecture AD



Gestion des comptes d'utilisateurs et d'ordinateurs

Les utilisateurs

Tout utilisateur qui souhaite accéder à des ressources gérées par des ordinateurs Windows doit posséder un compte utilisateur. Ce compte sert à authentifier l'utilisateur. Avant de créer un compte utilisateur, il faut tout d'abord sélectionner l'unité organisationnelle dans laquelle le compte doit être créé.

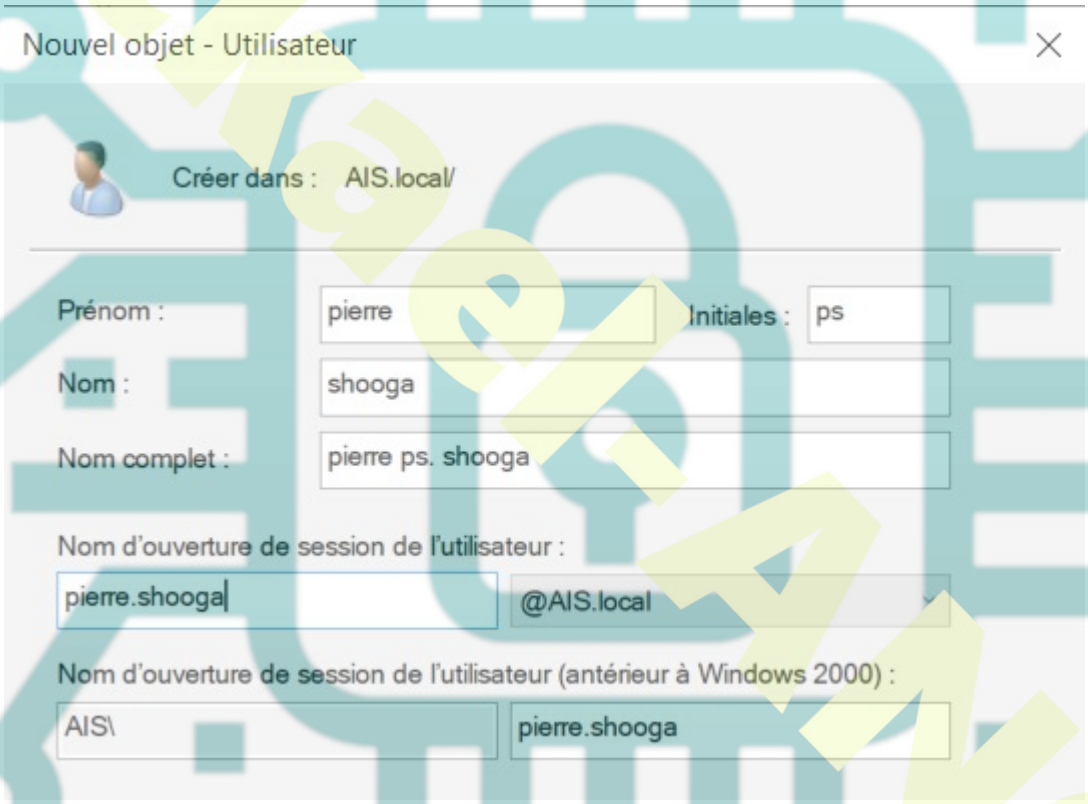
Avant de commencer à créer des objets dans l'annuaire, il est important d'avoir arrêté des conventions de nommage pour les différents types d'objets (Utilisateurs, Groupes, Ordinateurs, Imprimantes, etc.) Un exemple de convention de nommage pour les objets utilisateurs serait de prendre la première lettre du prénom et les x premiers caractères du nom comme nom d'ouverture de session.

Types de comptes

Compte local : les informations de comptes sont stockées localement sur les machines. Si une modification est apportée à un compte, celle-ci devra être répercutée manuellement sur toutes les machines où le compte existe.

Compte de domaine : les informations de comptes sont centralisées dans l'annuaire AD. Si une modification est apportée à un compte, elle sera diffusée à l'ensemble du domaine.

Convention de nommage des comptes utilisateurs
Dans l'annuaire AD, un utilisateur possède plusieurs noms
Le nom d'ouverture de session (login) : MDurand
Le nom d'ouverture de session pré-windows : SOCIETE\MDurand
Le nom d'utilisateur principal : MDurand@societe.fr
Le nom unique LDAP : CN=MDurand, CN=users, DC=societe, DC=fr



Nomenclature de création d'un compte utilisateur
Un login doit obligatoirement être unique dans le domaine. Il faut être capable d'identifier rapidement et sans doute possible le login des employés. Pour cela, il existe plusieurs solutions comme par exemple : initiale prénom+nom, prénom.nom. Cependant, dans le cas où il y a énormément de comptes, on préférera utiliser le numéro de badge, une nomenclature repérant le service, le lieu, le bureau, la filiale etc.

Modèle de comptes utilisateurs
Un modèle de compte est un compte utilisateur temporaire contenant les informations communes à tous les comptes ayant le même rôle dans l'entreprise. Une fois ce modèle de

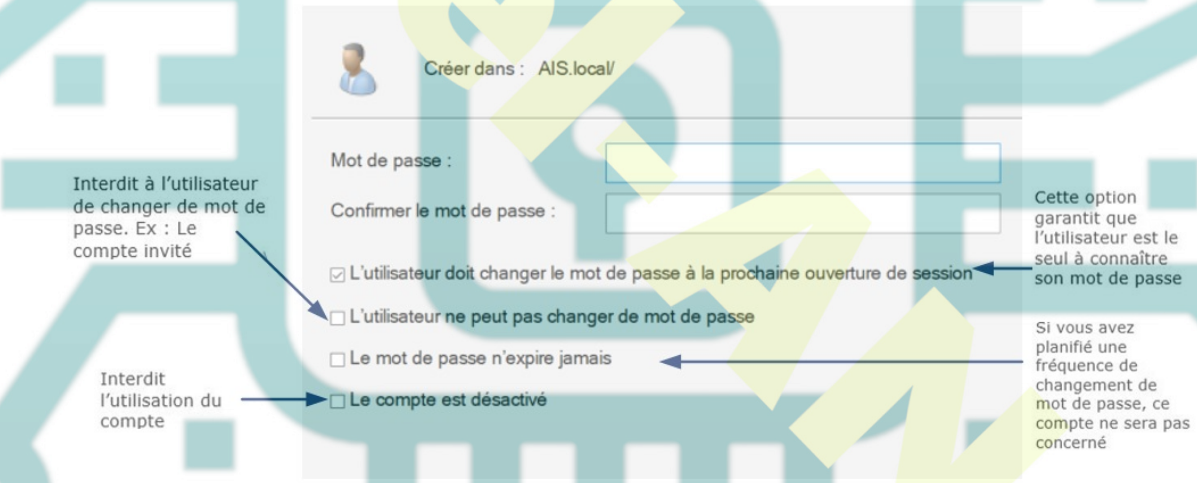
compte créé, il suffit de le dupliquer pour que le nouveau compte hérite des propriétés du modèle (adresse compte, profil, organisation)

Activation et désactivation d'un compte utilisateur

Chaque compte utilisateur possède un identifiant unique interne appelé SID qui est utilisé pour référencer de façon unique cet objet dans l'annuaire.
Lorsque l'on supprime un compte et que l'on recrée ce compte à l'identique, celui-ci se voit affecter un nouveau SID. Il perd ainsi la totalité de son contexte de sécurité. C'est pour cela qu'il est conseillé dans un premier temps de désactiver le compte.
On peut également désactiver un compte pour un employé en congé longue durée (le compte ne pourra plus être utilisé sans réactivation)

Mot de passe utilisateur

Vous pouvez spécifier des options concernant le mot de passe de l'utilisateur. Il y a distinction de casse pour les mots de passe dans Windows alors que ce n'est pas le cas pour les noms des utilisateurs.



Stratégie de mot de passe

Elle se gère au niveau des GPO du domaine, on peut définir la longueur, la complexité, la durée de vie maximale (durée pendant laquelle le mot de passe est valide) et minimale (durée pendant laquelle le mot de passe ne pourra pas être changé)

Stratégie de mot de passe affinée

L'intérêt de ce système c'est qu'il permet de créer plusieurs politiques de complexité des mots de passe et de verrouillages de compte, puis ensuite de les appliquer uniquement sur certains objets.

Stratégie de verrouillage d'un mot de passe
On peut définir au bout de combien de tentatives échouées un compte sera bloqué et si le blocage est permanent ou non.

Horaire d'accès
Permet de définir les heures de connexion autorisées pour un utilisateur.

Limitation au login sur certaines machines
Permet d'indiquer sur quelle machine un utilisateur peut ouvrir une session (par défaut tous les ordinateurs)

Profil
Permet de sauvegarder l'environnement de travail d'un utilisateur (bureau, couleur, raccourcis…) sur un serveur. Ce qui permet à l'utilisateur de travailler sur plusieurs postes tout en gardant son environnement (les modifications effectuées sont enregistrées à la fermeture de session)

Les profils centralisés
Offrent aux utilisateurs la possibilité de garder leur environnement de travail quel que soit le poste sur lequel ils se connectent.
La mise en œuvre d'un profil local est automatique mais la mise en œuvre d'un profil centralisé doit être paramétrée sur le serveur qui stockera les dossiers des utilisateurs.

Script
Permet d'exécuter un programme au démarrage de la session (obsolète, s'utilise via les GPO aujourd'hui)

Répertoire de base
Permet aux utilisateurs de posséder un répertoire personnel sur un serveur (on utilise plus volontiers la redirection de dossiers via les GPO)

Prise de contrôle à distance
Permet de travailler sur une machine distante pour dépanner un poste par exemple.

Comptes d'ordinateurs

Un compte d'ordinateur n'existe que dans un environnement de domaine, il permet d'authentifier chaque ordinateur.
Les comptes d'ordinateurs peuvent être utilisés pour configurer des audits, le déploiement de logiciels, les stratégies de sécurité…

Les groupes

Les groupes sont utilisés dans de nombreux systèmes d'exploitation car ils permettent de simplifier les tâches d'administration. Par exemple, il est plus simple d'accorder des permissions à un groupe d'utilisateurs plutôt qu'aux utilisateurs individuellement.

NB un utilisateur peut faire partie de plusieurs groupes.

On peut trouver les groupes soit dans la base de comptes locale (MMC Utilisateurs et Groupes locaux) soit dans Active Directory (MMC Utilisateurs et Ordinateurs Active Directory)

Pour un groupe donné, on définira deux éléments : Le type de groupe et l'étendue du groupe.

Types de groupes

Les groupes de sécurité : permettent d'affecter des utilisateurs et des ordinateurs à des ressources.
Les groupes de distribution : utilisables par la messagerie MSExchange par exemple. Ne sont pas utilisables pour affecter des permissions sur des ressources aux utilisateurs.

Étendue des groupes

Groupe global : Il a pour rôle d'organiser les utilisateurs par service, fonction, lieu géographique.

Membres	Membres de	Etendue	Autorisations
Comptes d'utilisateurs et groupes globaux du même domaine	Groupes locaux de domaines	Visibles dans toute la forêt	Tous les domaines de la forêt

Groupe de domaine local : Il a pour rôle d'organiser les groupes globaux ayant le même type d'autorisation d'accès à une ressource.

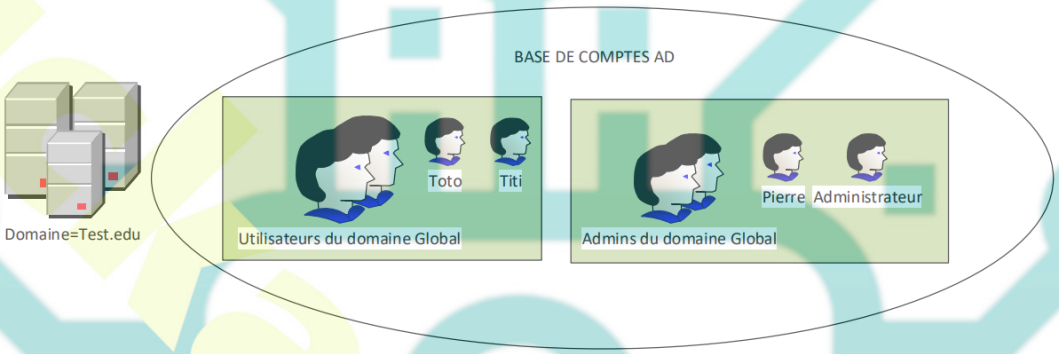
Membres	Membres de	Etendue	Autorisations
Comptes d'utilisateurs, groupes globaux et universels d'un domaine de la forêt, et groupes de domaine local du même domaine	Groupes de domaine local du même domaine	Visibles dans leur propre domaine	Le domaine dans lequel le groupe de domaine local existe

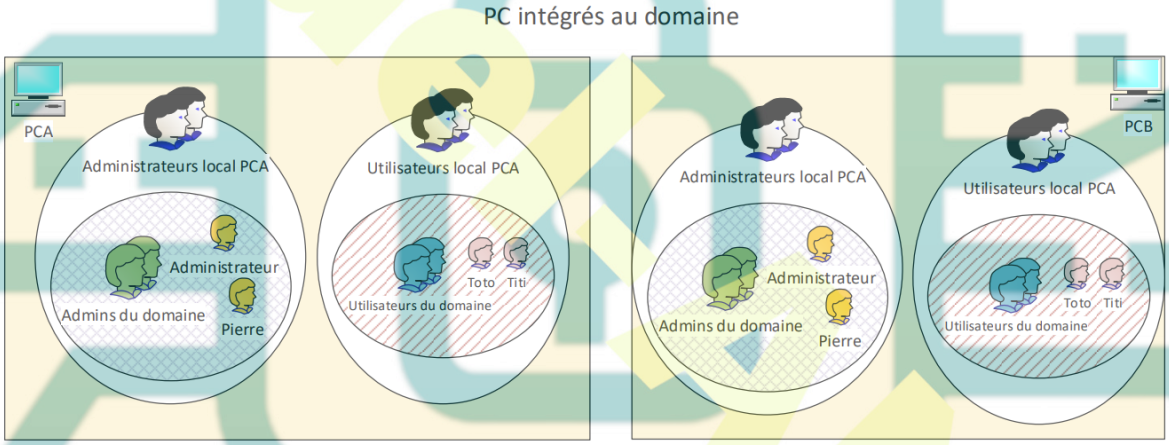
---

Groupe universel : sert dans les multi domaines complexes.

Membres	Membres de	Etendue	Autorisations
Comptes d'utilisateurs, groupes globaux et autres groupes universels d'un domaine de la forêt.	Groupes de domaine local et universels de tout domaine de la forêt	Visibles dans tous les domaines de la forêt	Tous les domaines de la forêt

Gestion des groupes pour les PC intégrant le domaine AD





Gestion des groupes

Gestion des groupes dans un domaine unique simple

Cette stratégie est appelée **A G P**.

- Les utilisateurs doivent être placés dans un groupe Global

- On accorde les permissions au groupe (Ex : regrouper les comptables dans un groupe global COMPTABILITE puis donner à ce groupe l'accès au dossier PAYE)

Gestion des groupes dans un domaine unique complexe

Cette stratégie est appelée **A G G P**

- Les utilisateurs doivent être placés dans un groupe Global.
- On regroupe des groupes globaux dans un seul groupe global pour gérer l'accès aux ressources
  (Ex : regrouper les comptables de Lyon dans un groupe global COMPTALYON, regrouper les comptables de Paris dans un groupe global COMPTAPARIS)
- Insérer les 2 groupes dans un groupe global COMPTAGEN et donner à ce groupe l'accès au dossier PAYE)

Gestion des groupes dans un environnement à domaines multiples simples

Cette stratégie est appelée **A G DL P**

- Dans chaque domaine, les utilisateurs doivent être placés dans un groupe Global.
- Insérer les groupes globaux aux groupes de domaine local pour gérer l'accès aux ressources.
  (Ex : regrouper les comptables du domaine France dans un groupe global COMPTAPARIS, regrouper les comptables du domaine Londres dans un groupe global COMPTALONDRES,
- Insérer les 2 groupes dans un groupe de domaine local ACCESPAYE, puis donner à ce groupe l'accès au dossier PAYE.

Gestion des groupes dans un environnement à domaines multiples complexes

Cette stratégie est appelée **A G U DL P**

- Dans chaque domaine, les utilisateurs doivent être placés dans un groupe Global par service.
- Insérer des groupes globaux dans un groupe universel regroupant les mêmes services de tous les domaines.
- Ajouter les groupes universels aux groupes de domaine local pour gérer l'accès aux ressources.

Groupes par défaut les plus utiles dans Active Directory

- **Utilisateurs du domaine** – Contient tous les utilisateurs du domaine. C'est le groupe principal d'un utilisateur.
- **Administrateurs du domaine** – Contient toutes les personnes devant administrer un domaine.
- **Opérateurs de compte** – Les membres de ce groupe peuvent gérer les comptes utilisateurs.
- **Opérateurs de serveur** – Les membres de ce groupe peuvent administrer les serveurs du domaine.
- **Administrateurs de l'entreprise** – Contient les administrateurs de l'entreprise. Dans le cadre d'un environnement à domaines multiples, un utilisateur placé dans ce groupe peut administrer toute la forêt.
- Utilisateurs du Bureau à distance – Les membres de ce groupe disposent des droits nécessaires pour ouvrir une session à distance

Groupes système

Les groupes système sont des groupes dont les membres sont gérés automatiquement par le système d'exploitation. Ces groupes sont utilisables dans le cas de la mise en place

d'autorisations NTFS.
L'administrateur ne peut pas leur affecter d'utilisateurs.

- **Anonymous Logon** – Représente les utilisateurs non authentifiés.
- **Tout le monde** – Contient tous les utilisateurs y compris le compte invité.
- **Réseau** – Contient les utilisateurs connectés via le réseau.
- **Utilisateurs authentifiés** – Contient les utilisateurs authentifiés.
- **Créateur propriétaire** – Représente l'utilisateur propriétaire d'un l'objet.
- **Interactif** – Tout utilisateur qui ouvre une session localement sera inclus dans ce groupe.

Gestion d'accès aux ressources

Contrôle d'accès

Il est basé sur trois composants qui permettent de définir l'accès à une ressource (fichier, dossier, imprimante…) du système.

Les entités de sécurité (groupe ou utilisateur)
Le SID (identificateur unique des entités)
DACL – Discretionary Access Control List (associées à chaque objet sur lequel on va définir un contrôle d'accès) elles sont composées d'ACE (Access Control Entry) Les ACE contiennent les SID, les informations d'accès (ex : Read, Write, Delete…), l'héritage et l'indicateur (Autoriser ou Refuser)

Administration des autorisations NTFS

Les permissions NTFS permettent de limiter l'accès aux ressources de type fichier ou dossier. Contrairement aux permissions de partage, il est possible de mettre en place des permissions différentes pour un dossier, ses sous dossiers et les fichiers.

Permissions	Codification	Résultat
Contrôle total	RXWDOP	Tous les droits
Modifier	RXWD	Lecture, exécution, écriture, suppression
Lecture et exécution	RX	Lecture et exécution
Lecture	R	Lecture
Ecriture	W	Ecriture, suppression

Autorisations sur les dossiers

Lorsque que sur une même ligne les autorisations sont séparées par un / la première option concerne les dossiers, la deuxième les fichiers.

Objectif

Permettre aux UTILISATEURS de modifier les fichiers existants mais en leur interdisant d'en créer de nouveaux

UTILISATEURS

Solution en mettant en place les permissions à partir du dossier

- Mettre en place les permissions de lecture sur le DOSSIER UNIQUEMENT
- Mettre en place la permission MODIFIER sur les Fichiers UNIQUEMENT

Les permissions sont cumulatives mais **la permission Refuser l'emporte sur toutes les autres.**

Ex : L'utilisateur Alain Robert est membre des groupes locaux Utilisateurs et Dépannage

Utilisateurs et groupes	Permissions	Permissions effectives pour Alain robert
Alain Robert	Contrôle total	Contrôle total + Lecture + Ecriture = Contrôle Total
Groupe Utilisateurs	Lecture et exécution	
Groupe Dépannage	Ecriture	

Ex : L'utilisateur Alain Robert est membre des groupes locaux Utilisateurs et Dépannage.

Utilisateurs et groupes	Permissions	Permissions effectives pour Alain robert
Alain Robert	Refuser Lecture	
Groupe Utilisateurs	Lecture et Exécution	Refuse l'accès
Groupe Dépannage	Ecriture	

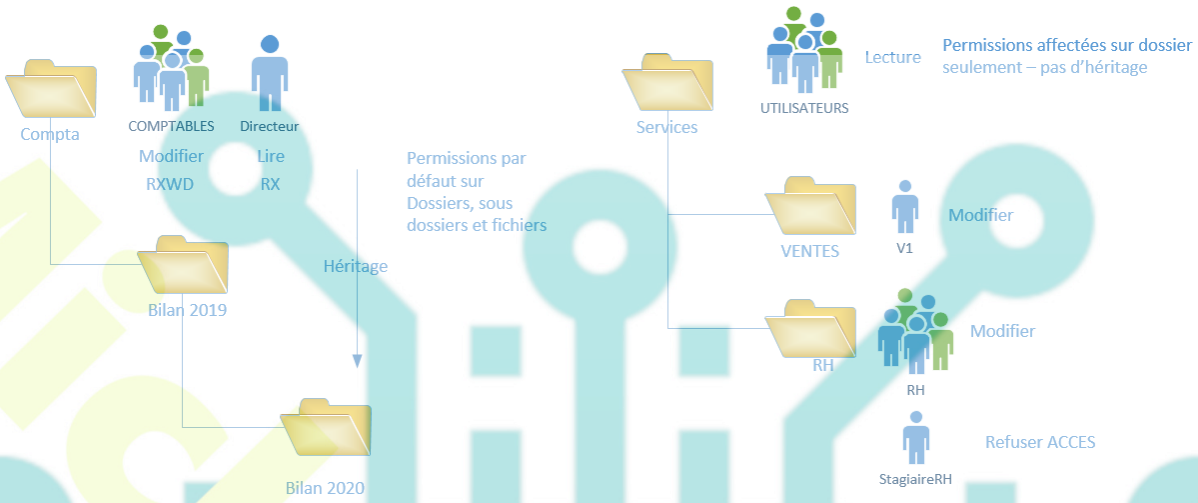
Toutes les opérations de copie héritent des autorisations du dossier cible. Seul le déplacement vers la même partition permet le maintien des autorisations.

Présentation de l'héritage NTFS

Les autorisations affectées à un dossier parent sont héritées par tous les sous-dossiers, et les fichiers qu'il contient. De plus, les nouveaux fichiers et dossiers créés dans ce dossier hériteront aussi de ces permissions.

Pour modifier l'héritage, il faut choisir **Paramètres avancés** et désactiver la case à cocher **Permettre aux autorisations héritées du parent de se propager à cet objet et aux objets enfants**.
Deux choix sont ensuite proposés **Copier** (pour conserver les autorisations héritées et les modifier) et **Supprimer** (pour supprimer les autorisations héritées)

Il est possible de vérifier les permissions effectives d'un utilisateur à l'aide de l'onglet **Autorisations effectives** de la fenêtre de sécurité avancée.



Résultat
1-Tous les membres du groupe **COMPTABLES** accèdent aux différents dossiers avec la permission de **Modification**
2-Le **directeur** n'a que l'autorisation de **Lecture** sur les différents dossiers

Résultat
1-tous les membres du groupe **UTILISATEURS** accèdent uniquement au dossier **Services** en **lecture**
2-L'utilisateur **V1** en **lecture** sur le dossier **Services** *car appartenant au groupe* ***UTILISATEURS*** et en **modification** sur le dossier **VENTES**
3-Le groupe **RH** accède au dossier **RH** avec les droits de **modification** à l'exception du **stagiaire qui n'a aucun droit.**

Permissions spéciales

Les permissions spéciales permettent d'affiner les autorisations d'accès au dossier et permettent de spécifier la propagation des autorisations vers les dossiers, sous-dossiers et fichiers.

Administration des dossiers partagés

Partages administratifs

Ces partages ont la particularité de posséder un nom qui se termine par un $.

Ce symbole rend le nom de partage invisible, c'est-à-dire qu'on ne le voit pas lors de l'exploration des ressources à travers le réseau.

ADMIN$: correspond au dossier du système d'exploitation.
C$, D$, E$: Correspond aux racines des disques.
IPC$: permet l'affichage des ressources partagées.

Un utilisateur peut se connecter à un partage administratif à condition qu'il appartienne au groupe administrateurs. Pour pouvoir y accéder, il sera obligatoire de spécifier le chemin UNC complet **\nom_du_serveur\nom_du_partage$.**

Vous pouvez également créer vos propres partages cachés en rajoutant un $ à la fin du nom de partage.

Création de dossiers partagés

Sur des machines clientes ou serveur non contrôleur de domaine, seuls les membres des groupes « Administrateurs » et « Utilisateurs avec pouvoirs » peuvent créer des dossiers partagés.

Sur les contrôleurs de domaine les membres des groupes « Administrateurs » et « Opérateurs de serveurs » peuvent créer des dossiers partagés.

Pour pouvoir créer un partage on peut utiliser l'explorateur et menu contextuel/propriétés sur le dossier puis choisir simple ou partage avancé pour gérer les autorisations d'accès.

Partage simple

L'autorisation est appliquée à la fois au partage et à NTFS.

Partage avancée

Permet que les autorisations d'accès entre NTFS et le partage soient différentes.

Autorisations avancées sur les dossiers partagés

Il existe trois autorisations possibles :
Lecture : Permet d'afficher le contenu du dossier et des sous dossiers, de lire des fichiers et d'exécuter les logiciels.
Modifier : Comme lecture avec en plus la possibilité de créer des fichiers et dossiers, de modifier leurs contenus et de les supprimer.
Contrôle total : comme modifier avec la possibilité de modifier aux travers le réseau les autorisations NTFS des fichiers et dossiers.

Combinaison des permissions de partage et des permissions NTFS

Il n'y a pas de hiérarchie entre les permissions **NTFS** et les permissions de **partage**, lorsque l'on combine les permissions de partage et les permissions NTFS, la permission la plus restrictive est celle qui est efficace.

Pour calculer les permissions effectives lors de la combinaison des permissions, il faut calculer la permission effective au niveau du partage et calculer la permission effective au niveau NTFS, puis prendre **la plus restrictive des deux.**

Ex : Permissions mises en place sur le dossier Application. L'utilisateur Alain Robert est membre des groupes locaux Utilisateurs et Dépannage.

Utilisateurs et groupes	Permissions de partage	Permissions NTFS	Permissions effectives pour Alain robert
Alain Robert	Lire	Modifier	
Groupe Utilisateurs	Contrôle Total	Lecture	Partage = Contrôle Total NTFS = Modifier
Groupe Dépannage	Modifier	Lecture	Combinaison = Modifier

Stratégies de groupe (GPO)

Les stratégies de groupe (Group Policy Object) sont un ensemble de paramètres applicables aux utilisateurs et aux ordinateurs.

Il est possible de configurer l'environnement des utilisateurs, de déployer des applications, d'imposer des stratégies de mots de passe sur le domaine, de paramétrer la sécurité, d'exécuter des scripts, d'imposer certaines règles aux utilisateurs et aux machines du domaine.

On définit les stratégies au niveau du site, du domaine ou de l'unité d'organisation et sont applicables aux objets stockés dans le conteneur.

Lorsqu'une stratégie de groupe est utilisée, un objet est créé et lié au conteneur. Un même objet de stratégie peut être lié à plusieurs conteneurs.

Les objets GPO sont stockés à deux endroits, dans Active Directory et dans le dossier SYSVOL.

Active Directory : contient les informations d'activation des paramètres des stratégies et les informations de version pour garantir la synchronisation.
Dossier SYSVOL : contient des dossiers "temporaires" (les GPT) qui indiquent quelles stratégies sont applicables et sur quels objets les appliquer.

Les GPO se voient affecter un GUID unique qui se présente sous la forme WINNT\SYSVOL\SYSVOL\MASOCIETE.ORG\POLICIES\{A3B2D888-E045-7F5A-00D0FEC00C55}
Les paramètres sont enregistrés dans les fichiers REGISTRY.POL

Permissions

Pour activer ou désactiver une stratégie affectée à un groupe, il faut utiliser l'onglet "sécurité" et préciser sur quel(s) groupe(s) appliquer ou non la stratégie.

On peut aussi indiquer quels sont les groupes qui auront la possibilité de mettre en œuvre des stratégies sur des conteneurs.

Traitement des stratégies

L'ordre de traitement des stratégies au démarrage s'effectue de la façon suivante : application des stratégies d'ordinateur, puis application des stratégies utilisateurs.

> En cas de conflit entre plusieurs stratégies, le système opère de cette façon:
> **Pas de stratégie sur l'objet enfant** : on applique les stratégies de l'objet parent.
> **Stratégie sur l'objet enfant compatible** : on applique les deux stratégies.
> **Stratégie sur l'objet enfant non compatible** : on applique la stratégie la plus proche (c'est-à-dire celle de l'enfant)

L'actualisation des stratégies s'effectue à chaque démarrage, ou toutes les 90 minutes sur les clients et toutes les 5 minutes sur les serveurs.

Héritage des stratégies

Lorsque vous affectez une stratégie, cette dernière est automatiquement mise en place sur tous les objets enfants, sauf si l'option bloquer l'héritage des stratégies est cochée au niveau d'un objet enfant. Cependant, il est possible de passer outre ce blocage et d'imposer une stratégie en cochant l'option aucun remplacement.

Suppression de stratégies

Lorsque l'on supprime une stratégie, les paramètres sont supprimés sur les machines ou les utilisateurs auxquels avait été appliquée cette stratégie.

La suppression de la liaison permet que la stratégie ne soit plus appliquée au conteneur. L'effacement de l'objet permet de supprimer la liaison et l'objet lui-même c'est-à-dire de

tous les conteneurs où l'objet était appliqué.

Pour désactiver une stratégie sans la supprimer, cliquer sur le bouton Options et sélectionner Désactiver.

Délégation de contrôle

Il est possible de déléguer la mise en place des stratégies pour certaines personnes de l'entreprise.

On peut déléguer l'autorisation de modifier un objet GPO existant, déléguer la création d'objets GPO ou déléguer le droit de lier un objet GPO c'est-à-dire affecter une GPO existante à des OU.

Modèles d'administration

L'ensemble de la description des GPO se trouve dans des fichiers dont l'extension est « .admx »
Rien ne vous empêche de créer vos propres modèles d'administration pour gérer des éléments qui ne le sont pas nativement.

Pour administrer l'environnement d'un utilisateur de façon centralisée, vous pouvez par exemple, intervenir sur les éléments suivants :

A. Déployer une application à l'aide de fichiers MSI

Pour déployer des applications, il faut créer un partage accessible aux utilisateurs concernés puis y copier les fichiers MSI.

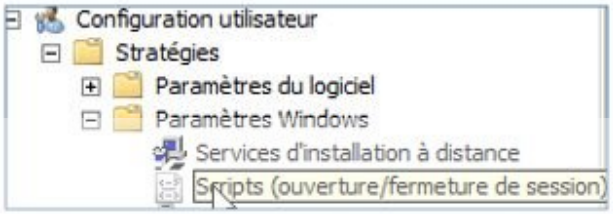
Publication : c'est à l'utilisateur d'aller chercher la nouvelle application dans Programmes du Panneau de Configuration
Attribution : le logiciel s'installe au moment où l'utilisateur clique sur l'icône.

Vous pouvez également désinstaller ou mettre à jour les applications que vous avez déployées par ce biais.

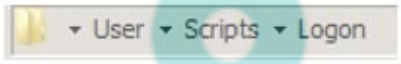
B. Attribution des scripts d'ouverture ou de fermeture de session

Les scripts VBS ou PowerShell permettent de déclencher des instructions à chaque ouverture de session, ce qui est très commode pour lancer automatiquement les tâches répétitives.

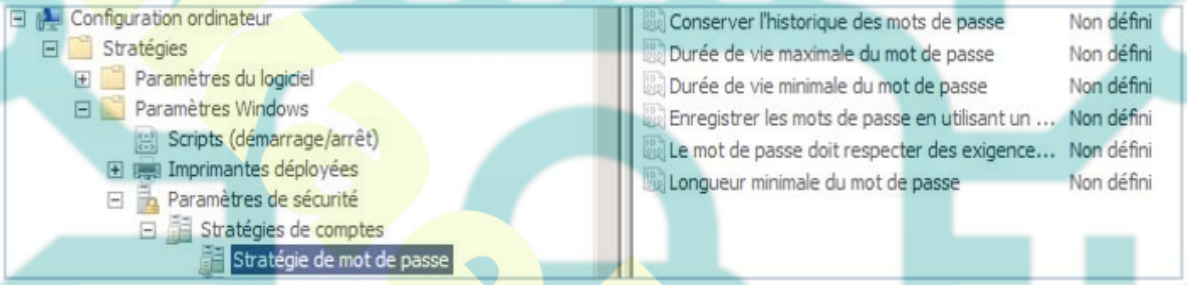
Pour mettre en place un script, vous devez vous placer dans la console de stratégie.

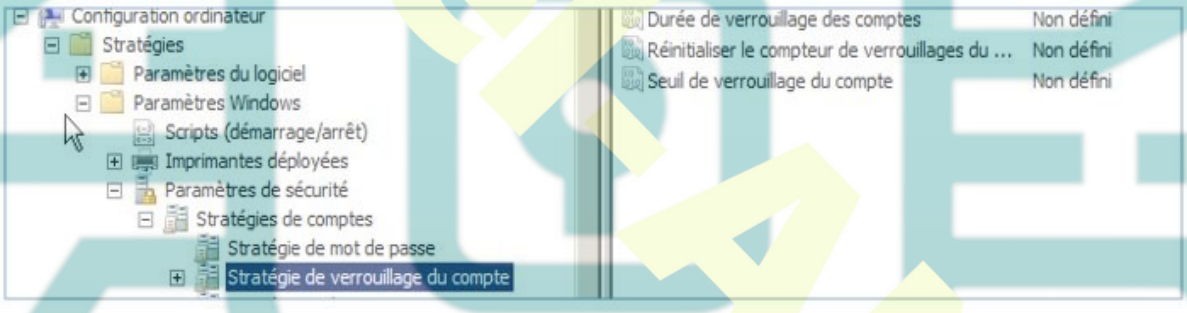


Puis placer le fichier VBS dans le dossier suivant



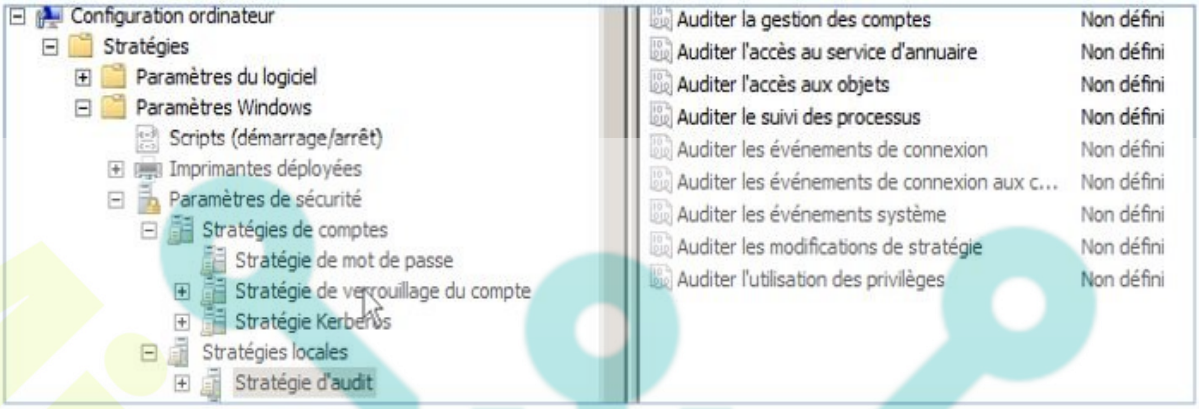
C. Mettre en place stratégie de sécurité des mots de passe et de verrouillage du compte (Stratégie de domaine uniquement)





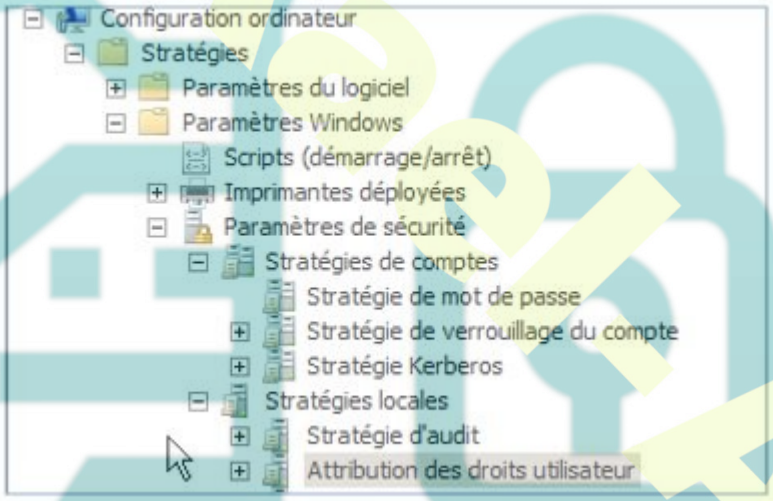
D. Mettre en place stratégie d'audit

Cet outil permet de consigner dans le journal de sécurité des évènements ou des activités effectués par le système ou les utilisateurs. Il va donc tracer ce que vous avez choisi de surveiller.



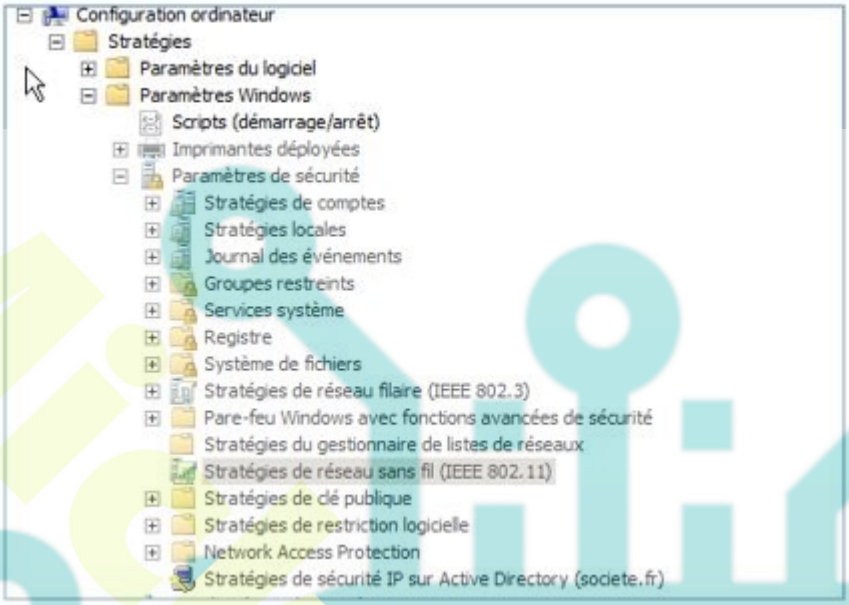
E. Changer les droits système des utilisateurs

Pour affecter plus de droits à certains utilisateurs, il est possible de modifier ces derniers via les stratégies.



F. Stratégie de sécurité

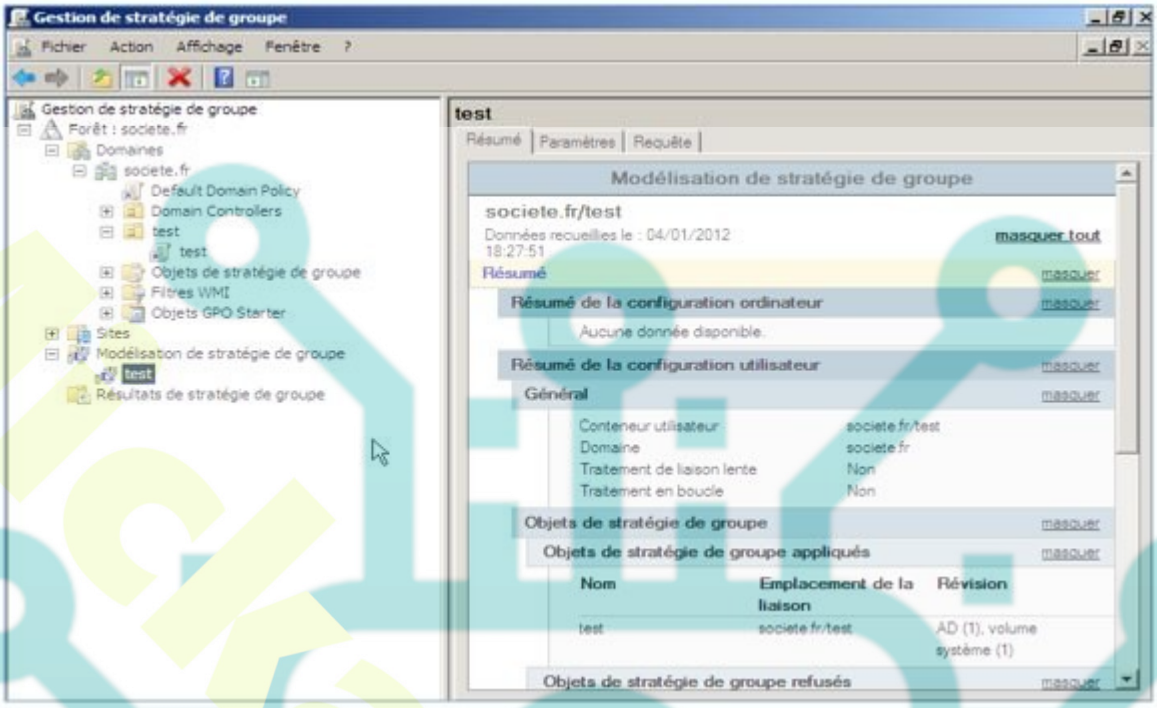
Vous pouvez également gérer de nombreuses options liées à la sécurité via les objets de stratégies (accès sans fils, IP, pare feux…)



Outils d'administration des GPO

Console de gestion des stratégies

Elle regroupe les différentes options de gestion (création, modification, suppression, simulation, audit…)



GPUpdate

Outil en ligne de commande qui permet de forcer la mise à jour des GPO et l'application des stratégies de groupes.

Par défaut, les ordinateurs effectuent cette réactualisation toutes les 90 minutes et les contrôleurs de domaine sont réactualisés eux toutes les 5 minutes.

Rapport de stratégie de groupe

Ce rapport au format HTML/XML permet de visualiser uniquement les paramètres qui ont été modifiés.

Simulation de déploiement de GPO, génère un rapport de test.

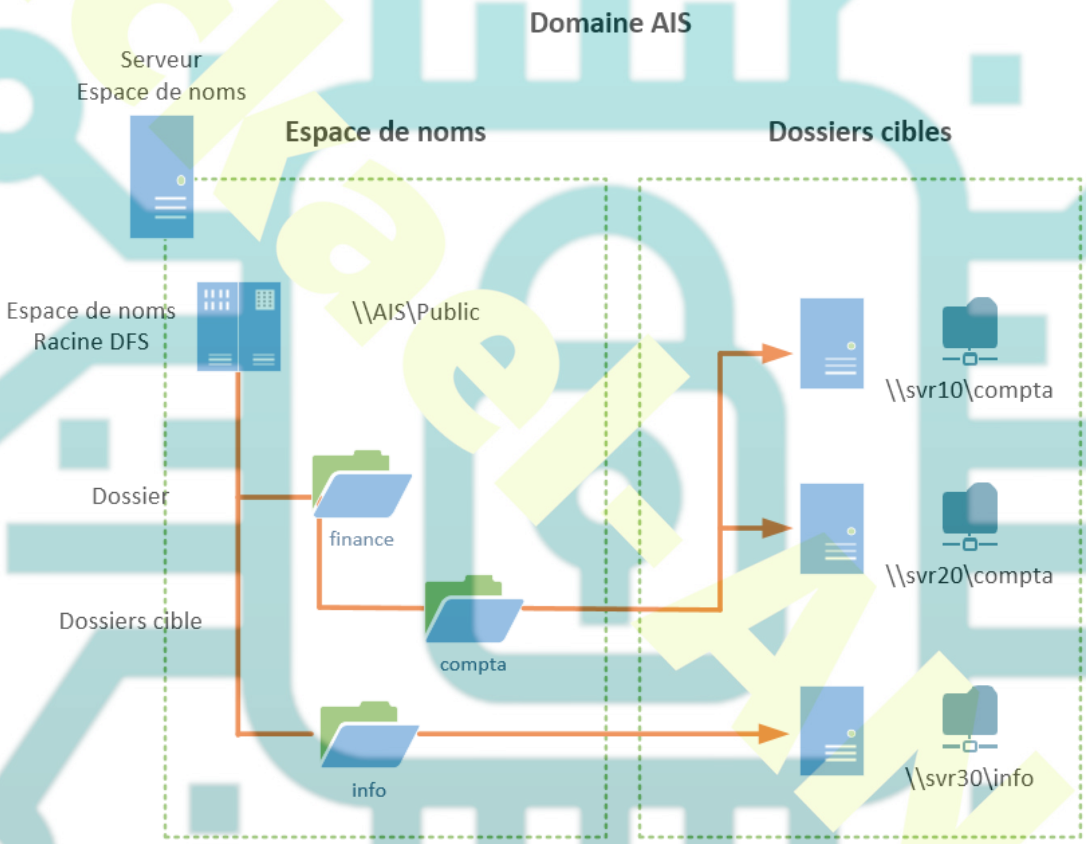
https://gpsearch.azurewebsites.net/

Outil de recherche de GPO

DFS

DFS est un système de fichier hiérarchisé qui permet de structurer les fichiers partagés sur différents serveurs du réseau de façon logique. Il permet de centraliser un ensemble de partages qu'il faudra rendre accessibles de manière uniforme.

Avec le DFS, l'utilisateur final ne visualise pas le nom du serveur sur lequel il accède pour lire les données et en cas de panne ou de changement de serveur, le chemin d'accès reste le même.



- **Serveur d'espace de noms** : un serveur d'espace de noms héberge un espace de noms. Le serveur d'espace de noms peut être un serveur membre ou un contrôleur de domaine.
- **Racine de l'espace de noms** : la racine de l'espace de noms est le point de départ de l'espace de noms. Dans la figure précédente, le nom de la racine est Public et le chemin d'espace de noms est \\AIS\Public. Ce type d'espace de noms est un espace de noms basé sur un domaine, car il commence par un nom de domaine (par exemple, AIS) et ses métadonnées sont stockées dans Active Directory Domain Services (AD DS). Un

espace de noms basé sur un domaine peut être hébergé sur plusieurs serveurs d'espaces de noms pour augmenter la disponibilité de l'espace de noms.

- **Dossier** : les dossiers sans cibles de dossier ajoutent une structure et une hiérarchie à l'espace de noms, et les dossiers avec des cibles de dossier fournissent aux utilisateurs du contenu réel.
- **Cibles de dossier** : une cible de dossier représente un chemin d'accès UNC (Universal Naming Convention) d'un dossier partagé. Le dossier cible est l'emplacement où les données et le contenu sont stockés.
  Un utilisateur qui accède à \\AIS\Public\finance\compta sera redirigé soit sur \\srv10\compta soit sur \\srv20\compta en fonction de sa localisation géographique.

La gestion des disques

Les commandes disque

FSUTIL – Afficher les infos d'un lecteur
fsutil fsinfo drives
Obtenir le type d'un lecteur donné avec la commande
fsutil fsinfo drivetype D:
Déterminer la quantité d'espace libre sur un lecteur, utilisez la commande
fsutil volume diskfree C:
Désactiver les noms de fichiers courts pour accélérer Windows
fsutil behavior set disable8dot3 1
Remettre les noms courts
fsutil behavior set disable8dot3 0

CHKDSK – Vérifie un disque et affiche un rapport de l'état du disque

DISKPART (mode console)
Crée ou supprime des partitions sur un disque dur.
diskpart [/add | /delete] [nom_du_peripherique | nom_du_lecteur | nom_de_la_partition] [taille]

FIXBOOT (mode console)
Écrit un nouveau secteur de démarrage sur la partition système.
fixboot [lecteur]

FIXMBR (mode console)
Répare le Master Boot Record (MBR) sur le disque spécifié.
fixmbr [nom_de_peripherique]

FORMAT – Formate le lecteur spécifié avec le système de fichier spécifié.
format [lecteur:] [/q] [/fs:systeme-de-fichier]

Protection des fichiers

Cryptage

Le cryptage d'un fichier ou d'un dossier s'appuie sur le système EFS qui utilise des clés publiques. Ce système est transparent pour l'utilisateur, le chiffrement et le déchiffrement s'effectuant à la volée.
De plus, les fichiers chiffrés ne sont jamais paginés sur disque pour des raisons de sécurité.
Cependant, si l'on n'est plus en mesure de déchiffrer un fichier (personne ayant démissionné etc.) l'administrateur a la possibilité d'ouvrir les fichiers chiffrés (un administrateur est considéré comme agent de récupération)

NB. Un fichier ou dossier chiffré ne peut être partagé, de même il n'est pas possible de copier ou déplacer un fichier si l'on ne possède pas la clé privée.

Active Directory Rights Management Services

AD RMS est une technologie de protection des documents numériques. Elle propose le chiffrement des données et la mise en place de restrictions de droits d'accès sur des documents (mail, document Word, feuille Excel…)

Le principe est de mettre une protection sur le fichier lui-même ce qui permet de garder cette protection même si le fichier est transporté hors de l'entreprise. Les droits d'accès permettent de contrôler qu'un utilisateur à accès restreint ne puisse pas transférer, copier, modifier, imprimer un fichier. Il ne peut également pas utiliser l'Impression écran.

Il est également possible de gérer l'expiration des fichiers afin que le contenu des documents ne s'affiche plus après un certain délai.

Cependant, pour ouvrir le fichier il faut être doté d'applications compatibles comme la suite Office, Office 365, Adobe Acrobat, XPS, internet Explorer, Edge.

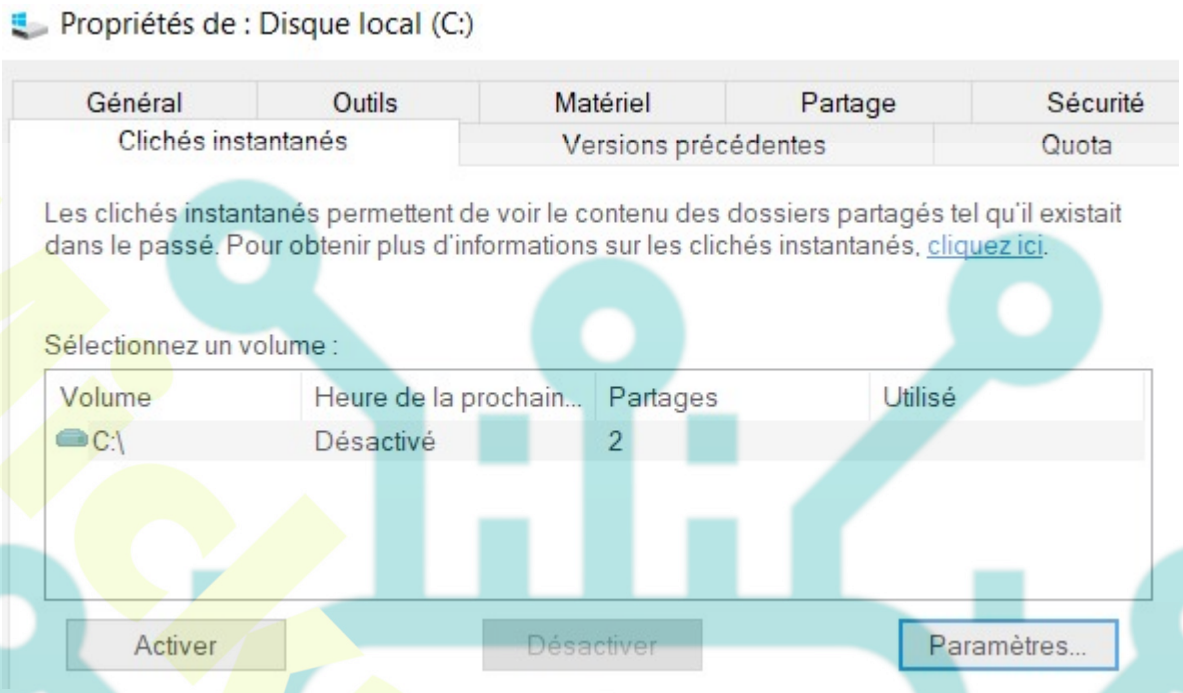
Clichés instantanés

Le cliché instantané s'appuie sur la technologie Volume Shadow Copy Service. Ce système permet de disposer de plusieurs versions d'un fichier sur un volume donné et les rendre accessibles aux utilisateurs par le biais de répertoires partagés. Un utilisateur aura donc la possibilité de visualiser les différentes versions d'un fichier ou d'un dossier pour le comparer, le copier ou le restaurer selon les cas.

L'activation des clichés instantanés ne peut se faire que sur un volume dans son intégralité. Il n'est pas possible de sélectionner des dossiers ou fichiers spécifiques.
Si vous supprimez un volume, désactivez les clichés instantanés sous peine d'engendrer des erreurs par la suite.

Configurer les clichés instantanés

Vous pouvez accéder aux propriétés des clichés instantanés en ouvrant l'explorateur Windows, faire un clic droit sur un volume et sélectionner **Configurer les clichés instantanés**.



Paramètres

Volume : indique le volume concerné par le paramétrage.

Zone de stockage : indique sur quel volume seront stockés les clichés. Les clichés sont situés dans le dossier système *System Volume Information*.

Planification : Deux tâches quotidiennes par défaut sont planifiées pour la réalisation de clichés (à 7 Heures et à 12 Heures, du lundi au vendredi)

Depuis le serveur vous aurez également la possibilité de visualiser, de copier ou de restaurer un fichier ou un dossier.

Pour cela, réalisez un clic droit sur le volume, le dossier ou le fichier voulu et sélectionnez l'option « Restaurer les versions précédentes »