Présentation des services de l'Active Directory

1. La forêt Active Directory
2. Le domaine et l'arborescence de domaines
3. L'unité d'organisation
4. Les objets
5. Les partitions d'Active Directory
6. Les maîtres d'opération FSMO
7. Le catalogue global
8. Les sites AD
9. La réplication intrasite et la réplication intersites
10. Le niveau fonctionnel du domaine et de la forêt

Remarque sur les niveaux fonctionnels des « Windows Server»

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.

1. 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 : **tpsio.lab**) sera également donné à la forêt. Dans notre exemple, la forêt aura le nom **tpsio.lab**.

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.

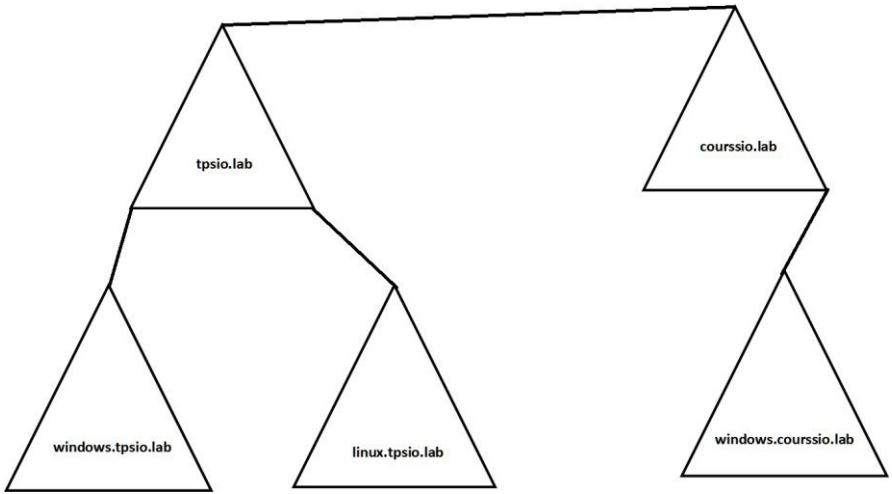
Aucune donnée (compte utilisateur, ordinateur…) n'est répliquée en dehors de la forêt, cette dernière sert donc de frontière de sécurité.

2. 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 **tpsio.lab**. Cette dernière contient un domaine enfant nommé **windows.tpsio.lab.** Le nom **tpsio.lab** est bien identique aux deux domaines.

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 **tpsio.lab** et **courssio.lab** sont deux arborescences différentes dans la même forêt.



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

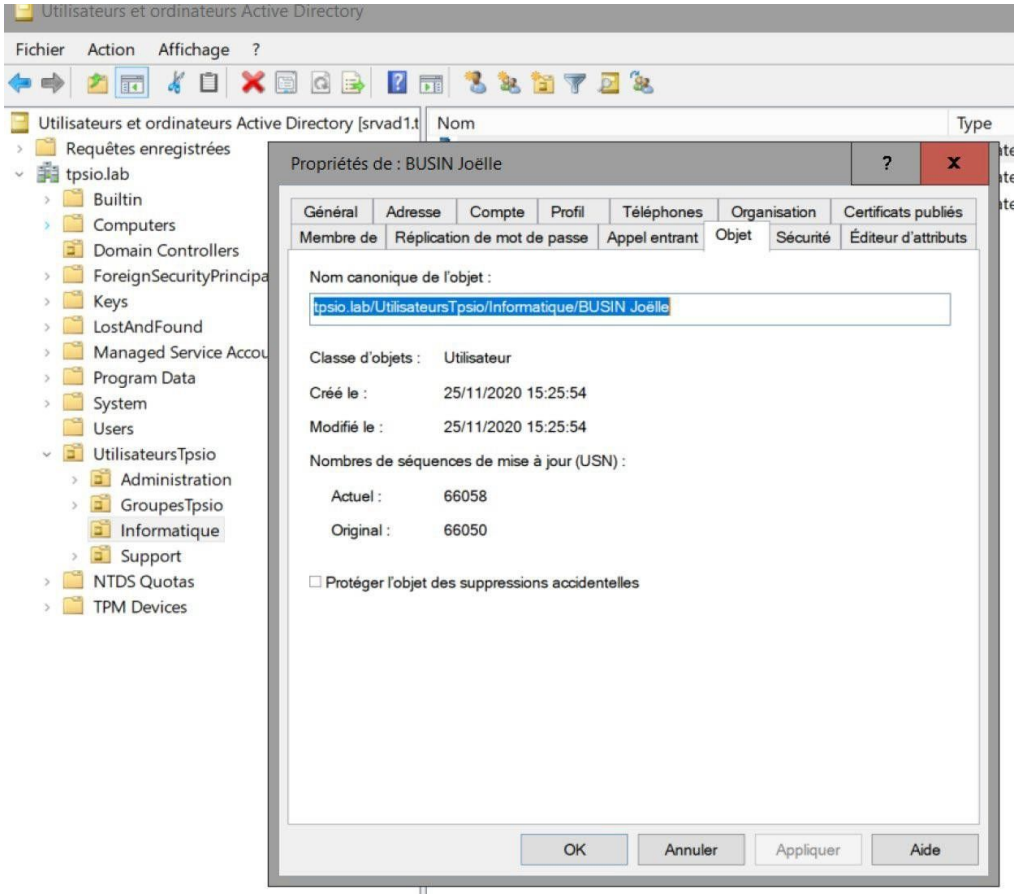
Un domaine contient au moins un contrôleur de domaine. Néanmoins il est recommandé d'en avoir deux afin d'assurer l'authentification en cas de maintenance ou de crash d'un des serveurs d'annuaire. Si plus aucun serveur n'est en ligne, l'authentification ne pourra plus être assurée, ce qui va impliquer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

3. L'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 en utilisant la propriété -**ProtectedFromAccidentalDeletion $true**.


Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active Directory [srvad1.t
Requêtes enregistrées
tpsio.lab
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipa
Keys
LostAndFound
Managed Service Accou
Program Data
System
Users
UtilisateursTpsio
Administration
GroupesTpsio
Informatique
Support
NTDS Quotas
TPM Devices
Nom
Type
Propriétés de : BUSIN Joëlle
Général Adresse Compte Profil Téléphones Organisation Certificats publiés
Membre de Réplication de mot de passe Appel entrant Objet Sécurité Éditeur d'attributs
Nom canonique de l'objet :
tpsio.lab/UtilisateursTpsio/Informatique/BUSIN Joëlle
Classe d'objets : Utilisateur
Créé le : 25/11/2020 15:25:54
Modifié le : 25/11/2020 15:25:54
Nombres de séquences de mise à jour (USN) :
Actuel : 66058
Original : 66050
Protéger l'objet des suppressions accidentelles
OK
Annuler
Appliquer
Aide

4. Les objets

Il est possible de trouver différents types d'objets Active Directory :

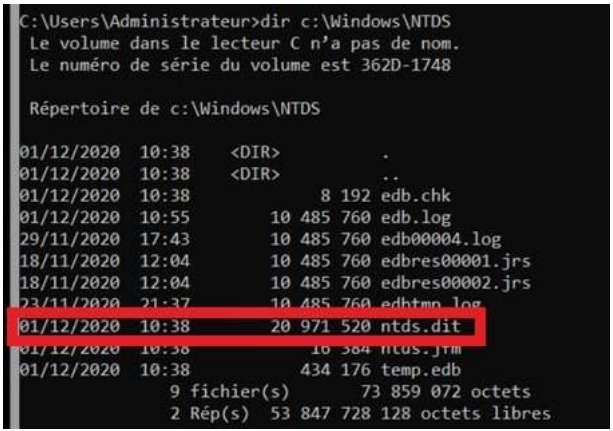
- **Utilisateurs** : permet d'authentifier les utilisateurs physiques qui ouvrent une session sur le domaine. Des droits et permissions sont associés au compte afin de permettre l'accès à une ressource (dossier partagé, boîte aux lettres mail, imprimante…). Ce type d'objet peut également servir de compte 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 desgroupes.
- **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.

5. 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.

Ces partitions sont stockées dans la base de données Active Directory, son emplacement physique sur le serveur d'annuaire est le répertoire **%SystemRoot%\NTDS**.



Le dossier **SYSVOL** stocké à l'emplacement « **C:\Windows\SYSVOL** », « *SYSVOL* » signifie « *System Volume* », et il sert à stocker des données spécifiques qui doivent être répliquées entre les contrôleurs de domaine ou accessibles par les ordinateurs clients.

L'essentiel des informations d'un domaine Active Directory est contenu dans le fichier **ntds.git**. Il est créé lors de l'installation du premier contrôleur de domaine.

```
C:\Users\Administrateur>net share

Nom partage  Ressource                      Remarque

-------------------------------------------------------------------------------
ADMIN$       C:\Windows                     Administration à distance
C$           C:\                            Partage par défaut
H$           H:\                            Partage par défaut
S$           S:\                            Partage par défaut
IPC$                                        IPC distant
GR_Administration
             H:\Commun
GR_Comptabilité
             H:\Commun
GR_Direction H:\Commun
GR_Informatique
             H:\Commun
GR_Secrétariat
             H:\Commun
GR_Support   H:\Commun
NETLOGON     C:\Windows\SYSVOL\sysvol\tpsio.lab\SCRIPTS
                                            Partage de serveur d'accès
SYSVOL       C:\Windows\SYSVOL\sysvol       Partage de serveur d'accès
La commande s'est terminée correctement.


C:\Users\Administrateur>
```

Plus précisément, voici les éléments principaux que l'on trouvera dans le partage SYSVOL :

Scripts de connexion | Stratégie de groupe (GPO)

Pour rappel, les scripts de connexion s'exécutent à l'ouverture de session de l'utilisateur, ils sont généralement écrits en BATCH et comporte des commandes qui permettent de créer des lecteurs réseau sur les machines clientes (commande « net use »). Quant aux stratégies de groupe, elles sont récupérées par les clients puis appliquées, dans le but d'appliquer une stratégie de personnalisation de l'espace de travail de l'utilisateur.

De ce fait, si le partage SYSVOL est en erreur, vous aurez de gros problèmes ! Plus de réplication des GPOs et scripts de connexion entre les contrôleurs de domaine, plus possible pour les clients de récupérer les dernières mises à jour de GPO et les scripts… Bref, vous imaginez la galère… D'où l'intérêt de prendre connaissance de l'existence du partage SYSVOL.

Attention, **il ne faut pas utiliser ce partage pour stocker d'autres sortes de données, ce n'est pas du tout recommandé !** Non seulement, car le partage SYSVOL n'est pas fait pour ça, mais aussi, car les processus de réplication seront plus longs (plus de données à répliquer).

Le répertoire « *C:\Windows\SYSVOL* » est composé de plusieurs sous-dossiers :

```
C:\Users\Administrateur>dir c:\Windows\SYSVOL\DOMAIN
 Le volume dans le lecteur C n'a pas de nom.
 Le numéro de série du volume est 362D-1748

 Répertoire de c:\Windows\SYSVOL\DOMAIN

18/11/2020  12:11    <DIR>          .
18/11/2020  12:11    <DIR>          ..
18/11/2020  12:04    <DIR>          Policies
22/11/2020  16:55    <DIR>          scripts
               0 fichier(s)                0 octets
               4 Rép(s)  53 848 113 152 octets libres
```

-**domain** : ce répertoire contient toutes les données à jour (GPO et scripts), réparties en deux sous dossiers : « Policies » et « scripts ».

-**Policies** : ce répertoire est stocké sous « *domain* » et stocke toutes les GPOs du domaine, que l'on crée au sein de la console « *Gestion des stratégies de groupe* ». Un sous-dossier par GPO est créé où le nom du dossier correspond au GUID de l'objet GPO.

```
 Répertoire de c:\Windows\SYSVOL\DOMAIN\Policies

18/11/2020  12:04    <DIR>          .
18/11/2020  12:04    <DIR>          ..
18/11/2020  12:04    <DIR>          {31B2F340-016D-11D2-945F-00C04FB984F9}
18/11/2020  12:04    <DIR>          {6AC1786C-016F-11D2-945F-00C04fB984F9}
               0 fichier(s)                0 octets
               4 Rép(s)  53 847 793 664 octets libres
```

Répertoire "Policies" stocké dans SYSVOL

-**scripts** : ce répertoire est stocké sous « domain » et contient les différents scripts, notamment les scripts de connexion.

-**staging areas** : ce répertoire est utilisé pour créer une file d'attente (queue) des données en attente de réplication à destination des autres contrôleurs de domaine. **C**es dossiers sont utilisés par le système de réplication DFS-R(*Distribution File System Replication*) .

6. Les maîtres d'opération FSMO

Cinq rôles **FSMO** (*Flexible Single Master Operation*) existent dans une forêt Active Directory. Ils possèdent chacun une fonction au sein de l'annuaire et la perte de certain de ces rôles peut être problématique.

Deux rôles sont présents uniquement sur un des contrôleurs de domaine de la forêt, ils sont généralement présents au niveau du domaine racine (premier domaine de la forêt).

- **Rôle maître de schéma** : comme nous l'avons vu, le schéma est en lecture seule sur les contrôleurs de domaine. Néanmoins il est parfois nécessaire de procéder à sa mise à jour. Pour cela, un contrôleur de domaine dans la forêt dispose du rôle Maître de schéma.
- **Maître de dénomination de domaine** : lors d'une opération au niveau du domaine (ajout/suppression,...), le serveur qui possède ce rôle permet d'assurer une cohérence des noms de domaine.

Les trois autres rôles sont présents sur chaque domaine de la forêt.

- **Maître RID** : ce rôle est donné à un des contrôleurs de domaine. Son rôle est l'attribution de **blocs d'identificateur relatifs (RID)** aux différents contrôleurs de domaine de son domaine qui en font la demande. Le RID est utilisé lors de la création d'un objet pour créer le **SID (identifiant de sécurité)**. Ce dernier est construit en associant le RID à l'identificateur de domaine (SID du domaine identique à l'ensemble des objets).

- **Maître infrastructure** : le serveur possédant ce rôle est responsable de la surveillance des objets des autres domaines de la forêt. Lors de la présence dans une ACL d'un objet étranger à son domaine, il a pour fonction la prise en charge de la vérification de l'état de ces objets (désactivé, renommé, supprimé…).
- **Maître émulateur PDC** : ce rôle a une importance capitale dans une forêt Active Directory. En effet il a pour rôle de synchroniser son horloge avec un serveur de temps. Par la suite les différents contrôleurs de domaine viendront effectuer la même opération en le prenant comme maître de temps. Ainsi l'ensemble des contrôleurs de domaine auront une horloge synchronisée. La gestion du temps est également importante pour les postes et serveurs. Ces derniers sont également synchronisés à l'aide des contrôleurs de domaine.

7. 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.

8. Les sites AD

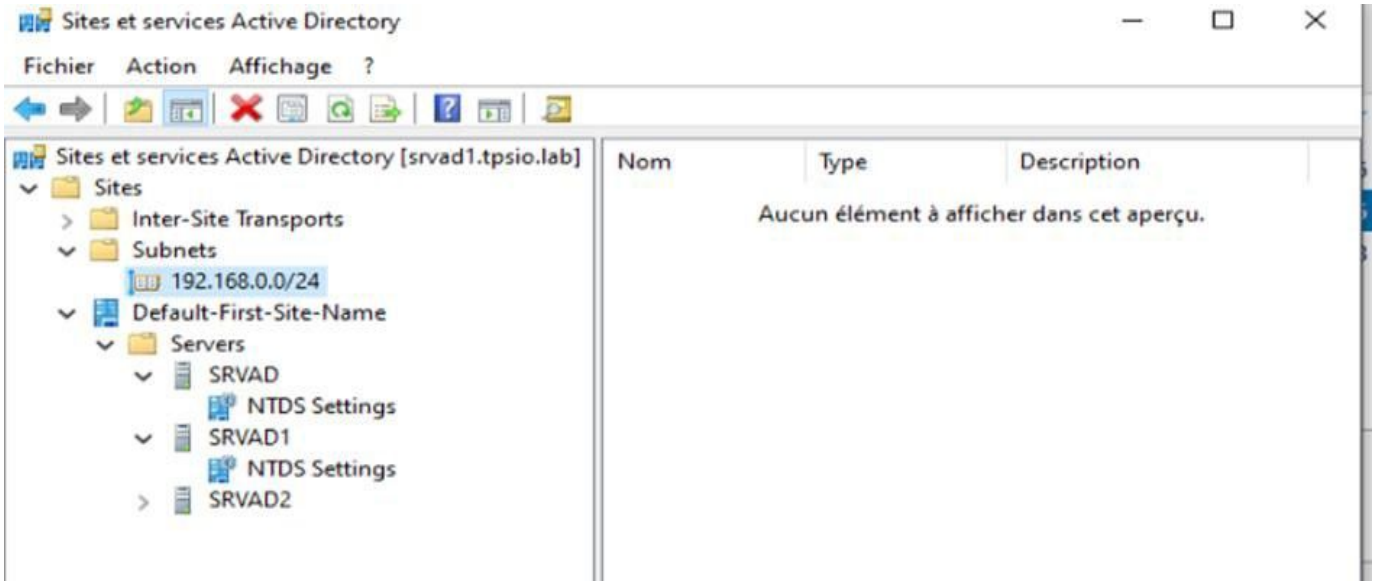
Afin de réduire l'utilisation des lignes reliant les différentes entités physiques (siège et sites distants), les domaines sont découpés de manière logique en sites AD. Ces derniers représentent généralement la topologie physique de l'entreprise. Dans un site AD, la connectivité réseau est considérée 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.

9. La réplication intrasite et la réplication intersites

La réplication permet de s'assurer qu'une modification effectuée sur un contrôleur de domaine est transmise à ses paires. Cette opération s'effectue à l'aide d'objets de type « connexion ». Elles sont de type unidirectionnels (réplication entrante uniquement).


Sites et services Active Directory
Fichier Action Affichage ?
Sites et services Active Directory [srvad1.tpsio.lab]
Sites
Inter-Site Transports
Subnets
192.168.0.0/24
Default-First-Site-Name
Servers
SRVAD
NTDS Settings
SRVAD1
NTDS Settings
SRVAD2
Nom
Type
Description
Aucun élément à afficher dans cet aperçu.

Ces chemins de réplication (objet connexion), vont permettre la création de la topologie de réplication. La vérification de la cohérence des données (**KCC**, *Knowledge Consistency Checker*) pourra être également assurée.

La topologie permet également d'avoir une continuité au niveau de la réplication et ce même en cas de défaillance d'un contrôleur de domaine. Il est donc **très important** de ne pas modifier les liens de connexion. L'ISTG effectue la création de la topologie et l'adapte en fonction des pannes des serveurs d'annuaire ou coupure réseau. Si les liens ont été modifiés manuellement, cette opération de mise à jour de la topologie ne s'effectue plus. Il est donc recommandé de laisser travailler l'ISTG sans intervenir.

Il existe deux types de réplications :

- Intrasite
- intersites

La réplication intrasite permet une réplication des modifications pour les contrôleurs de domaine d'un même site.

À la suite d'une modification d'une des partitions Active Directory, une notification est effectuée au bout de 15 secondes par le contrôleur de domaine à son premier partenaire. Cette opération de notification a pour but de donner l'information du changement.

Trois secondes plus tard, une notification est envoyée aux autres contrôleurs de domaine. Ces délais dans les notifications permettent d'assurer une réduction du trafic réseau.

Suite à la notification, le serveur partenaire demande la modification. L'agent de réplication d'annuaire (**DRA**, *Directory Replication Agent*) peut par la suite opérer le transfert.

Dans le cas où aucune modification n'est effectuée, la méthode de scrutation est utilisée.

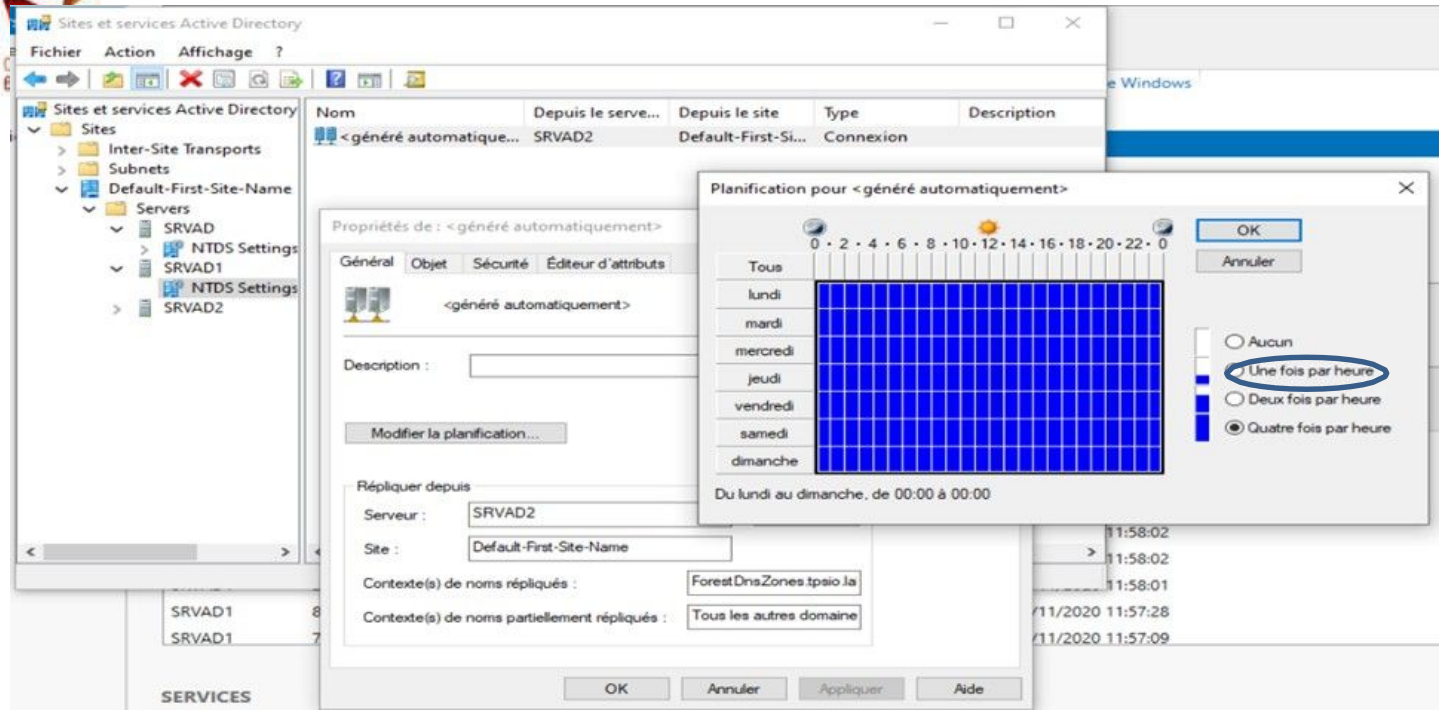
Cette méthode consiste à interroger un serveur afin de connaître une éventuelle modification sur une des partitions de l'Active Directory. L'intervalle de scrutation pour une réplication intrasite est d'une heure. Cette valeur est celle par défaut.

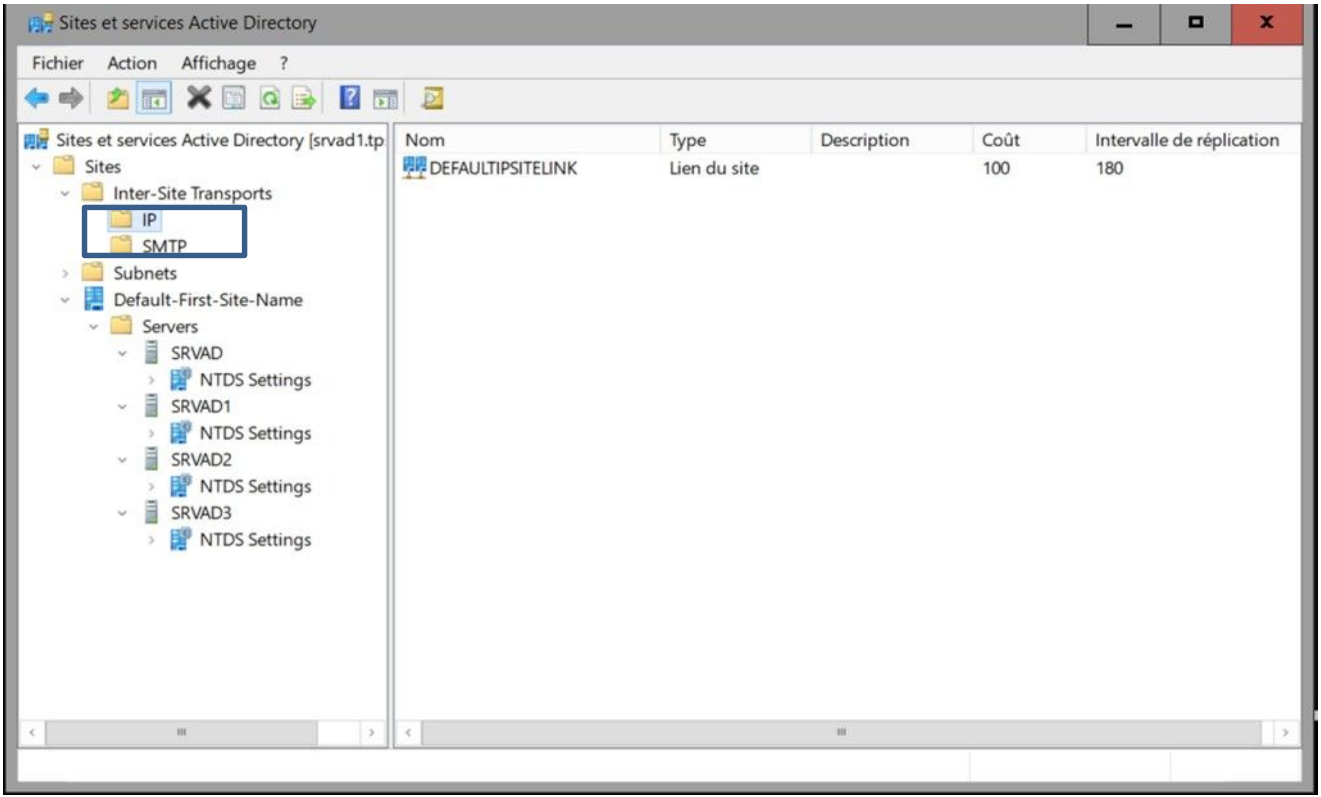
La réplication de type intersites consiste à effectuer des réplications sur des serveurs d'annuaire présent dans des sites AD différents.

L'**ISTG** (*Intersite Topology Generator*, générateur de topologie intersites) effectue la création d'objets
de connexion entre les serveurs de chaque site. Cela permet la réplication intersites.

Pour les raisons évoquées plus haut, il est préférable de ne pas modifier ses liens de connexion.

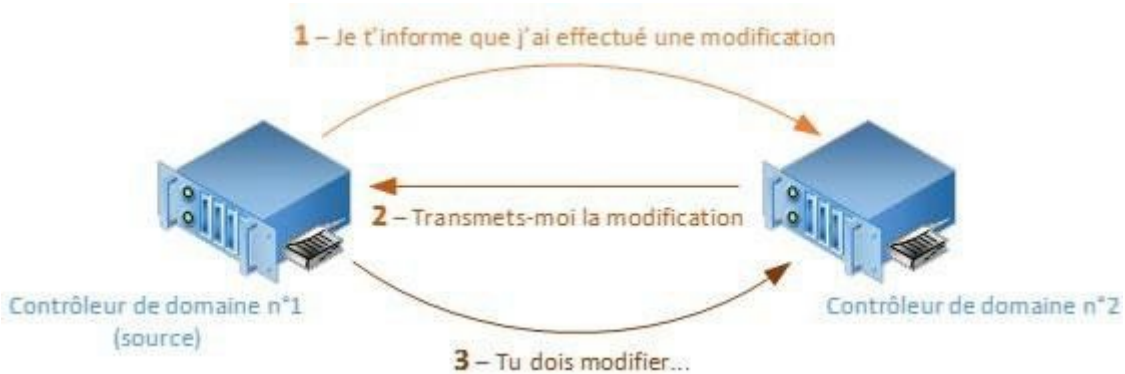
Dans chaque site, un contrôleur de domaine est sélectionné afin d'obtenir le rôle de tête de pont. Ce dernier a la responsabilité de répliquer ou récupérer d'éventuelles modifications d'un autre serveur tête de pont. Par la suite une réplication de type intrasite s'opère. Cette élection est effectuée automatiquement. Pour les mêmes raisons que les liens de connexion, il est préférable de ne pas faire d'élection manuelle.


Sites et services Active Directory
Fichier Action Affichage ?
Sites et services Active Directory
Sites
Inter-Site Transports
Subnets
Default-First-Site-Name
Servers
SRVAD
NTDS Settings
SRVAD1
NTDS Settings
SRVAD2
Nom
Depuis le serve...
Depuis le site
Type
Description
<généré automatique...
SRVAD2
Default-First-Si...
Connexion
Propriétés de : <généré automatiquement>
Général
Objet
Sécurité
Éditeur d'attributs
<généré automatiquement>
Description :
Modifier la planification...
Répliquer depuis
Serveur :
SRVAD2
Site :
Default-First-Site-Name
Contexte(s) de noms répliqués :
ForestDnsZones.tpsio.la
Contexte(s) de noms partiellement répliqués :
Tous les autres domaine
OK
Annuler
Appliquer
Aide
Planification pour <généré automatiquement>
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0
Tous
lundi
mardi
mercredi
jeudi
vendredi
samedi
dimanche
Du lundi au dimanche, de 00:00 à 00:00
OK
Annuler
Aucun
Une fois par heure
Deux fois par heure
Quatre fois par heure
SRVAD1
SRVAD1
SERVICES


Sites et services Active Directory
Fichier Action Affichage ?
Sites et services Active Directory [srvad1.tp
Sites
Inter-Site Transports
IP
SMTP
Subnets
Default-First-Site-Name
Servers
SRVAD
NTDS Settings
SRVAD1
NTDS Settings
SRVAD2
NTDS Settings
SRVAD3
NTDS Settings
Nom
Type
Description
Coût
Intervalle de réplication
DEFAULTIPSITELINK
Lien du site
100
180

Pour effectuer la réplication intersites, deux protocoles sont utilisés :

- **IP** : utilisé pour toutes les réplications intrasites et intersites. Ce protocole est très souvent utilisé.
- **SMTP** : utilisé principalement en cas de connexions non fiables. Une CA (autorité de certification) est nécessaire, ce qui alourdit l'administration. Ce protocole est très peu utilisé pour la réplication.



10. Niveau fonctionnel du domaine et de la forêt

Un niveau fonctionnel permet l'activation d'une ou plusieurs fonctionnalités pour un domaine ou une forêt. Plusieurs niveaux sont disponibles, néanmoins toute modification de niveau est irréversible (il est par la suite impossible de descendre d'un niveau).

Ceci a un impact sur le domaine et/ou la forêt mais principalement sur les contrôleurs de domaine. Il est nécessaire d'avoir au minimum tous les contrôleurs de domaine qui exécutent le système d'exploitation correspondant à celui du niveau fonctionnel choisi. Si le niveau choisi est Windows Server 2012, les contrôleurs de domaine doivent au minimum exécuter Windows Server 2012. Il est intéressant de noter que Windows Server 2019, n'apporte pas de nouveau niveau fonctionnel.

Niveau fonctionnel Windows Server 2008

Le niveau fonctionnel Windows Server 2008 offre les fonctionnalités suivantes :

- Activation de la réplication du système de fichiers **DFS** (*Distributed File System*) pour le dossier **SYSVOL**.
- Protocole AES (*Advanced Encryption Services*) 128 et 256 bits pour l'authentification Kerberos.
- Mise en place de la stratégie de mot de passeaffinée.

Au niveau de la forêt, aucune nouvelle fonctionnalité n'est apportée.

Niveau fonctionnel Windows Server 2008 R2

Le niveau fonctionnel permet l'utilisation de la **corbeille AD**. Cette dernière assure la restauration d'un objet Active Directory (unité d'organisation, compte utilisateur…). L'ensemble des propriétés sont restaurées.

Niveau fonctionnel Windows Server 2012

Une nouveauté est apportée avec le niveau fonctionnel du domaine, avec le protocole Kerberos Armoring. Aucune nouveauté n'est apportée avec le niveau fonctionnel de la forêt.

Niveau fonctionnel Windows Server 2012 R2

Aucune nouveauté apportée par le niveau fonctionnel de la forêt. Concernant celui du domaine la sélection du niveau fonctionnel 2012 R2 permet d'obtenir les fonctionnalités suivantes :

- **Silos de stratégies d'authentification** : cette fonctionnalité permet l'application de stratégie d'authentification pour certains comptes (utilisateurs, ordinateurs, services).
- **Stratégies d'authentification** : appliquées aux comptes utilisateur, elles permettent d'indiquer sur quelle machine un utilisateur peut ouvrir une session. Cette fonctionnalité utilise un contrôle d'accès basé sur des conditions.

Niveau fonctionnel Windows Server 2016

Aucune nouveauté offerte par le niveau fonctionnel.

Niveau fonctionnel Windows Server 2025

Le niveau fonctionnel de domaine de Windows Server 2025 inclut toutes les fonctionnalités disponibles dans les niveaux fonctionnels de domaine antérieurs, mais inclut également les nouvelles fonctionnalités suivantes :

Fonctionnalité optionnelle de pages de base de données 32k. Pour en savoir plus sur l'utilisation de la taille de page de base de données 32 000, consultez les pages Database 32k pour Active Directory.
Pour en savoir plus sur les nouvelles fonctionnalités, consultez Nouveautés de Windows Server 2025.

. Structure Logique d'Active Directory

La structure logique d'Active Directory offre une méthode efficace pour concevoir une hiérarchie. Les composants logiques de la structure d'Active Directory sont les suivants :

Les Domaines

Les Unités d'Organisation.

A.Les Arborescences : Le premier domaine installé est le domaine racine de la forêt. Au fur et à mesure que des domaines lui sont ajoutés, cela forme la structure de l'arborescence ou la structure de la forêt, selon les exigences pour les noms de domaine. Une arborescence est un ensemble de domaines partageant un nom commun. Par exemple : « **tpsio.lab** » est le domaine parent du domaine « **linux.tpsio.lab** ».

Structure Physique d'Active Directory

La structure physique permet d'optimiser les échanges d'informations entre les différentes machines en fonction des débits assurés par les réseaux qui les connectent.

On distingue :

- Les contrôleurs de Domaine Un contrôleur de domaine est un ordinateur exécutant Windows Server qui stocke un répliqua de l'annuaire. Il assure la propagation des modifications faites sur l'annuaire. Il assure l'authentification et l'ouverture des sessions des utilisateurs, ainsi que les recherches dans l'annuaire.
- Les Sites et Liens de Sites Un site est une combinaison d'un ou plusieurs sous réseaux connectés entre eux par une liaison à haut débit fiable (liaison LAN). Définir des sites permet à Active Directory

Il s'agit donc de gérer et d'optimiser le trafic du réseau. Pour concevoir une structure physique cohérente, il faut maitriser le fonctionnement de la réplication entre contrôleurs de domaine et les rôles des maîtres d'opérations.