# Installation et Migration d'un Domaine Active Directory sous Windows Server 2019





## SOMMAIRE

#### 1... Introduction

- 1.1.... Présentation personnelle
- 1.2.... Présentation du projet

#### 2... Architecture du réseau

- 2.1.... Schéma Réseau
- 2.2.... Liste des serveurs et adresses IP

#### 3... Installation d'Active Directory

- 3.1.... Configuration réseau
- 3.2.... Installation du rôle AD DS
- 3.3.... Promotion en contrôleur de domaine
- 3.4.... Vérification du domaine

#### 4... Gestion des utilisateurs et groupes

- 4.1.... Création des utilisateurs et groupes
- 4.2.... Attribution des droits sur SRV-FILES

#### 5... Configuration des Stratégies de Groupe (GPO)

- 5.1.... Sécurité des mots de passes
- 5.2.... Configuration des accès et restrictions

#### 6... Migration vers le second serveur

- 6.1.... Ajout de SRV-AD02 au domaine
- 6.2.... Promotion en Contrôleur de domaine
- 6.3.... Vérification de la réplication
- 6.4.... Transfert des rôles FSMO
- 6.5.... Suppression du contrôleur SRV-AD01
- 7... Vérifications et tests
- 8... Conclusion et compétences acquises

# 1...Introduction

## 1.1...Présentation personnelle

Je m'appelle Ryan Lapotre, j'ai 22 ans et je suis étudiant au Pôle BTS Alternance de Caen en BTS SIO option SISR (Solutions d'Infrastructures, Systèmes et Réseaux).

Issu d'un BAC STMG option SIG (Systèmes d'Informations et de Gestion), j'ai voulu poursuivre mes études en informatique.

Étant passionné par le développement, je souhaite poursuivre mes études en licence après le BTS en me dirigeant dans une filière plus orientée dans le développement.

Le **BTS SIO SISR** cible l'expertise des infrastructures informatiques, et nous prépare à concevoir, implémenter et gérer des solutions techniques adaptées aux diverses architectures réseau des entreprises. Cette formation est conçue pour nous doter de compétences spécialisées, essentielles à la maitrise des environnements informatiques modernes, comme la configuration de serveurs, qui est primordiale pour assurer le fonctionnement optimal des services et applications d'une entreprise.

La sécurité des réseaux est aussi au programme pour nous former sur la protection des données contre les vulnérabilités et les cyberattaques. Nous développons aussi une expertise en virtualisation qui est la capacité à créer des versions virtuelles de ressources informatiques pour une meilleur flexibilité et efficacité des systèmes.

Une partie du programme est aussi dédiée à la gestion de base de données et au déploiement d'applications, qui permettront d'orchestrer et maintenir les infrastructures critiques.

## 1.2...Présentation du projet

Le projet proposé consiste à mettre en place un contrôleur de domaine (DC) sous Windows Server 2019 (projet 1), puis à le migrer vers une autre machine qui deviendra le DC principal (projet 2).

Il s'agit d'une simulation d'environnement d'entreprise qui me permet d'acquérir des compétences en administration système et gestion de réseau.

Les prérequis pour le projet :

- 4 machines physiques (2 serveurs qui seront DC, 1 serveur de fichier, 1 PC client)
- Une clé USB + l'ISO Windows Server 2019
- Un switch pour connecter les 4 machines entre elles sur un serveur local via RJ-45

# 2...Architecture du réseau

## 2.1...Schéma réseau



## 2.2...Liste des serveurs et adresses IP

| Machine     | Adresse IP    | Rôle                |
|-------------|---------------|---------------------|
| SRV-AD01    | 192.168.10    | Ancien DC           |
| SRV-AD02    | 192.168.1.15  | Nouveau DC          |
| SRV-FILES   | 192.168.1.20  | Serveur de fichiers |
| PC-CLIENT01 | 192.168.1.100 | Machine Client      |

# 3...Installation et configuration d'Active Directory

## 3.1...Configuration réseau



Fixer l'IP Statique du serveur (SRV-AD01) depuis le panneau de configuration



Taper « ipconfig /all » dans CMD pour vérifier la nouvelle IP

Sur la capture d'écran, on voit que l'adresse IP a bien été attribuée à la machine, ainsi que le DNS. Étant un réseau local sans routeur, la passerelle n'est pas nécessaire pour ce projet.

| 1odification du nom ou du domaine de l'ordinateur $~	imes~$ t  | ance      | sécurité > Système v O Rechercher   |
|--|-----------|---|
| /ous pouvez modifier le nom et l'appartenance de cet<br>rdinateur. Ces modifications peuvent influer sur l'accès aux<br>ssources réseau. | votre     | ne générales  |
| lom de l'ordinateur :<br>SRV-AD01  | S" ou     | itandard Evaluation<br>poration. Tous droits Windows Server* 2019   |
| Nom complet de l'ordinateur :<br>RV-AD01   |           |   |
| Autres Membre d'un O Domaine :   | difier    | Pentium(R) Dual-Core CPU E5700 @ 3.00GHz 3.00 GHz<br>VI) : 4,00 Go  |
|  |           | Système d'exploitation 64 bits, processeur x64  |
| Groupe de travail :     WORKGROUP  |           | <ul> <li>e: La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponib<br/>sur cet écran.</li> </ul> |
|  |           | nateur, de domaine et de groupe de travail  |
| OK Annuler   |           | WIN-JBKOQSPL11I SModifier les   |
|  |           | WIN-JBKOQSPL11I paramètres  |
|  |           | teur :  |
| OK Annuler   | Appliquer | WORKGROUP   |

Le PC doit être renommé pour se repérer plus facilement lorsque j'aurais les 4 machines actives.

La deuxième machine (serveur) est connectée au réseau local via le switch, je vais vérifier la communication entre les deux serveurs via la commande « ping » avant de créer le domaine.



Le deuxième serveur (IP : 192.168.1.15, configurée de la même façon que sur le premier serveur) ne reçoit pas les requêtes de ma première machine car le pare-feu bloque les pings par défaut, il faut donc autoriser cette action.

| PS C:\Users\Administr | ateur> New-NetFirewallRule -DisplayName "Autoriser Ping" -Direction Inbound -Protocol ICMPv4 -Action Allow |
|-----------------------|--|
| Name<br>DisplavName   | : {eaa3538e-d117-493f-bb6c-afefb498853c}<br>: Autoriser Ping   |
| Description           |  |
| DisplayGroup          |  |
| Group                 |  |
| Enabled               | : True   |
| Profile               | : Any  |
| Platform              | : {}   |
| Direction             | : Inbound  |
| Action                | : Allow  |
| EdgeTraversalPolicy   | : Block  |
| LooseSourceMapping    | : False  |
| LocalOnlyMapping      | : False  |
| Owner                 |  |
| PrimaryStatus         | : OK   |
| Status                | : La règle a été analysée à partir de la banque. (65536)   |
| EnforcementStatus     | : NotApplicable  |
| PolicyStoreSource     | : PersistentStore  |
| PolicyStoreSourceType | : Local  |



Une fois l'action « ping » autorisée via PowerShell, le nouveau test montre que l'envoi de requêtes fonctionne correctement.

### 3.2...Installation du rôle AD DS (Active Directory Domain Services)

Pour créer le domaine, il faut suivre une procédure :

- → Ouvrir « Gestionnaire de serveur » puis « Ajouter des rôles et fonctionnalités »
- $\rightarrow$  « Installation basée sur un rôle ou une fonctionnalité »
- → Sélection de la machine (SRV-AD01)
- $\rightarrow$  Cocher « Services AD DS »

| 🚘 Assistant Ajout de rôles et de fo   | nctionnalités   | - 🗆   | $\times$ |
|---|---|---|----------|
| Sélectionner des r  | ôles de serveurs  | Assistant Ajout de rôles et de fonctionnalités<br>Ajouter les fonctionnalités requises pour Services AD   | ×        |
| Avant de commencer  | Sélectionnez un ou plusieurs  | DS ?  |          |
| Type d'installation   | Rôles   | Vous ne pouvez pas installer Services AD DS sauf si les services de<br>rôle ou les fonctionnalités suivants sont également installés.   |          |
| Sélection du serveur<br>Rôles de serveurs<br>Fonctionnalités<br>Confirmation<br>Résultats | Accès à distance<br>Attestation d'intégri<br>Hyper-V<br>Serveur de télécopie<br>Serveur DHCP<br>Serveur DNS<br>Serveur Web (IIS)<br>Services Guardian hô<br>Services AD DS<br>Services AD DS<br>Services AD DS<br>Services Bureau à di<br>Services d'activation<br>Services de certificat<br>Services de tédeloier<br>Services de tédeloier | [Outils] Gestion de stratégie de groupe         Outils d'administration de serveur distant         Outils d'administration de rôles         Outils AD DS et AD LDS         Module Active Directory pour Windows PowerShell         Outils AD DS         [Outils] Centre d'administration Active Directory         [Outils] Composants logiciels enfichables et outils         Inclure les outils de gestion (si applicable)         Ajouter des fonctionnalités         Annuler | - e      |
|   |   | < Précédent Suivant > Installer Annule  | r        |

 $\rightarrow$  Confirmer l'installation puis attendre la fin du chargement

## 3.3...Promotion en contrôleur de domaine

Je peux maintenant créer un domaine et promouvoir mon serveur en contrôleur de domaine ; je vais appeler mon domaine « bts.lab ».

| 참 Assistant Configuration des serv  | ices de domaine Active Directory   |           |        | ×        |
|---|--|-----------|--------|----------|
| Assistant Configuration des serv<br>Configuration de déploie<br>Options du contrôleur de<br>Options supplémentaires<br>Chemins d'accès<br>Examiner les options<br>Vérification de la configur | Sélectionner l'opération de déploiement Sélectionner l'opération de déploiement Ajouter un contrôleur de domaine à un domaine existant Ajouter un nouveau domaine à une forêt existante Gajouter une nouvelle forêt Spécifiez les informations de domaine pour cette opération Nom de domaine racine : [bts.lab] |           | SERVEL | JR CIBLE |
| Installation<br>Résultats   | Nom de domaine racine : bts.lab  |           |        |          |
|   |  |           |        |          |
|   | En savoir plus sur les configurations de déploiement   |           |        |          |
|   | < Précédent Suivant >  | Installer | An     | nuler    |

Il est important de sélectionner « Serveur DNS » et « Catalogue Global »

| assistant Configuration des serv  | ices de domaine Active Directory   |   | -    |                  | ×            |
|---|--|---|------|------------------|--------------|
| Options du contrô   | bleur de domaine   |   | SE   | RVEUR C<br>SRV-A | IBLE<br>\D01 |
| Configuration de déploie<br>Options du contrôleur de<br>Options DNS<br>Options supplémentaires<br>Chemins d'accès<br>Examiner les options<br>Vérification de la configur<br>Installation<br>Résultats | Sélectionner le niveau fonctionnel de<br>Niveau fonctionnel de la forêt :<br>Niveau fonctionnel du domaine :<br>Spécifier les fonctionnalités de contré<br>Serveur DNS (Domain Name Syst<br>Catalogue global (GC)<br>Contrôleur de domaine en lectur<br>Taper le mot de passe du mode de re<br>Mot de passe :<br>Confirmer le mot de passe : | la nouvelle forêt et du domaine racine<br>Windows Server 2016   Windows Server 2016   Windows Server 2016   Windows Server 2016   Windows Services d'annuaire (DSRN | A)   |                  |              |
|   | En savoir plus sur les options pour le   | contrôleur de domaine   |      |                  |              |
|   | <  | Précédent Suivant > Insta   | ller | Annule           | er           |

Le nom de domaine sera « **BTS** », il sera affiché sur l'écran de connexion des ordinateurs, et pourra être nécessaire devant l'identifiant pour se connecter à la session. (Ex : **BTS\Administrateur**)

Quand ces conditions sont remplies, je peux procéder à la promotion du domaine.

## 3.4...Vérification du domaine

Une fois la promotion terminée, le serveur va redémarrer. Je vais pouvoir vérifier que le PC « SRV-AD01 » est bien entré dans le domaine « bts.lab »



Ici, la machine est bien dans le domaine.

Je vais pouvoir vérifier que le PC « SRV-AD01 » est bien considéré comme un DC avec la commande « Get-ADDomainController » dans PowerShell.

| PS C:\Users\Administrateur> | Get-ADDomainController -filter *  |
|-----------------------------|---|
| ComputerObjectDN            | : CN=SRV-AD01,OU=Domain Controllers,DC=bts,DC=lab   |
| DefaultPartition            | : DC=bts,DC=lab   |
| Domain                      | : bts.lab   |
| Enabled                     | : True  |
| Forest                      | : bts.lab   |
| HostName                    | : SRV-AD01.bts.lab  |
| InvocationId                | : dd72e06e-9029-4d59-bcf3-85505afa402a  |
| IPv4Address                 | : 192.168.1.10  |
| IPv6Address                 |   |
| IsGlobalCatalog             | : True  |
| IsReadOnly                  | : False   |
| LdapPort                    | : 389   |
| Name                        | : SRV-AD01  |
| NTDSSettingsObjectDN        | : CN=NTDS Settings,CN=SRV-AD01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=bts,DC=lab                                      |
| OperatingSystem             | : Windows Server 2019 Standard Evaluation   |
| OperatingSystemHotfix       |   |
| OperatingSystemServicePack  |   |
| OperatingSystemVersion      | : 10.0 (17763)  |
| OperationMasterRoles        | : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster}  |
| Partitions                  | : {DC=ForestDnsZones,DC=bts,DC=lab, DC=DomainDnsZones,DC=bts,DC=lab, CN=Schema,CN=Configuration,DC=bts,DC=lab,<br>CN=Configuration,DC=bts,DC=lab} |
| ServerObjectDN              | : CN=SRV-AD01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=bts,DC=lab   |
| ServerObjectGuid            | : 1ae9df52-2a79-4175-b09d-ef97283da8df  |
| Site                        | : Default-First-Site-Name   |
| SslPort                     | : 636   |
|                             |   |
|                             |   |



# 4...Gestion des utilisateurs et groupes

4.1...Création des utilisateurs et groupes





| <b>Jtilisateurs et ordinateurs Active</b> | Nom                                      | Type                               | Description  |  |
|---|--|------------------------------------|--|--|
| Requêtes enregistrées                     | Administrateur                           | Utilicateur                        | Comete d'utilisateur d'a   |  |
| bts.lab                                   | Administrateurs clás                     | Groupe de sécurité - Global        | Les membres de ce grou   |  |
| Builtin                                   | Administrateurs clas Enternise           | Groupe de récurité - Universal     | Les membres de ce grou   |  |
| Computers                                 | Administrateurs de l'entreprise          | Groupe de sécurité - Universel     | Administrateurs désigné  |  |
| Domain Controllers                        | Administrateurs du schéma                | Groupe de sécurité - Universel     | Administrateurs désigné  |  |
| ForeignSecurityPrincipal:                 | Admins du domaine                        | Groupe de sécurité - Global        | Administrateurs désigné  |  |
| Managed Service Accour                    | Contrôleurs de domaine                   | Groupe de sécurité - Global        | Tous les contrôleurs de  |  |
| Users                                     | R Contrôleurs de domaine clonables       | Groupe de sécurité - Global        | Les membres de ce arou   |  |
|   | R Contrôleurs de domaine d'entrenris     | Groune de sécurité - Universel     | Les membres de ce grou   |  |
|   | Contrôleurs de domaine en lecture        | Groupe de sécurité - Global        | Les membres de ce grou   |  |
|   | R DorAdminr                              | Groupe de récurité - Domaine local | Groupe der administrate  |  |
|   | R DosllodateProvy                        | Groupe de sécurité - Global        | Les clients DNS qui sont   |  |
|   | R Éditeurs de certificats                | Groupe de sécurité - Domaine local | Les membres de ce arou   |  |
|   | Sectionnaize RH                          | Utilisateur                        | and the second sec |  |
|   | Comune de réplication dont le mot d      | Groune de sécurité - Domaine local | Les mots de nasse des  |  |
|   | R Groupe de réplication dont le mot d    | Groupe de sécurité - Domaine local | Les mots de passe des  |  |
|   | R GRP IT                                 | Groupe de sécurité - Global        |  |  |
|   | R GRP LOG                                | Groupe de sécurité - Global        |  |  |
|   | BR GRP RH                                | Groupe de sécurité - Global        |  |  |
|   | 2. Invité                                | Utilisateur                        | Compte d'utilisateur inv   |  |
|   | R Invités du domaine                     | Groupe de sécurité - Global        | Tous les invités du dom  |  |
|   | R Ordinateurs du domaine                 | Groupe de sécurité - Global        | Toutes les stations de tra   |  |
|   | R Propriétaires créateurs de la stratégi | Groupe de sécurité - Global        | Les membres de ce prou   |  |
|   | R Protected Users                        | Groupe de sécurité - Global        | Les membres de ce grou   |  |
|   | Responsable Logistique                   | Utilisateur                        |  |  |
|   | Serveurs RAS et IAS                      | Groupe de sécurité - Domaine local | Les serveurs de ce proup   |  |
|   | A Technicien Informatique                | Utilisateur                        |  |  |
|   | B Utilisateurs du domaine                | Groupe de sécurité - Global        | Tous les utilisateurs du d   |  |
|   |  |                                    |  |  |

3 groupes créés :

- $\rightarrow$  GRP IT
- $\rightarrow$  GRP RH
- $\rightarrow$  GRP LOG

Avec 1 utilisateur par groupe

4.2...Attribution des droits d'accès sur SRV-FILES (serveur de fichiers)

| C:\Users\Administrateur>ping 192.168.1.10   |
|---|
| Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :<br>Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128<br>Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128<br>Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128<br>Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128 |
| Statistiques Ping pour 192.168.1.10:<br>Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),<br>Durée approximative des boucles en millisecondes :<br>Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms   |

Avant de commencer, je vais vérifier que le serveur de fichier communique bien avec le DC via la commande ping



J'ajoute SRV-FILES dans le domaine via les paramètres système de l'ordinateur, la machine va redémarrer pour appliquer les changements

| néral Partage Sécurité Versions préc  |   |  | × |
|---|---|--|---|
| Partage de fichiers et de dossiers en rése                                  | a Accès réseau  |  |   |
| SHARE<br>Partagé<br>Chemin réseau :<br>\\Srvfiles\share<br>Partager         | Choisir les utilisateurs pouvant accéder<br>Tapez un nom et cliquez sur Ajouter, ou cliquez sur | r à votre dossier partagé<br>la flèche pour rechercher un utilisateur. |   |
| Partage avancé  |   | ✓ Ajouter  |   |
| Définir des autorisations personnalisées, c<br>d'autres options de partage. | Nom   | Niveau d'autorisation  |   |
|   | Administrateur  | Lecture/écriture 🔻   |   |
| 💎 Partage avancé  | Administrateurs   | Propriétaire   |   |
|   | 2 Technicien Informatique   | Lecture 🔻  |   |
|   |   |  |   |
|   | Je rencontre des difficultés pour partager.   |  |   |

Je partage un dossier test sur le réseau avec l'utilisateur « techinfo » créé au préalable pour tester les accès.

Je vais effectuer les mêmes manipulations depuis le PC-CLIENT01 pour vérifier la communication avec le DC ainsi que l'ajout au domaine « bts.lab »

|  |                                   |            |               | Propriétés                           | système  | ×             | Converions re             | 624   |               |   |
|--|-----------------------------------|------------|---------------|--------------------------------------|--|---------------|---------------------------|---|---------------|---|
|  |                                   |            |               | Medifica                             | tion du nom ou du domaine de l'ordinateur - >  | ar à Sistence |                           |   |               | ×   |
| C:\Usans\Administratour\ni                           | ng 102 169 1 10                   |            |               | Yous pour<br>ardinateur<br>ressource | ret notiferie non et l'apparenzace te cel<br>« Cas motifications provent influer sur l'accès aus<br>« Morea. | (with         |                           |   |               | $[\mathbf{v}, \mathbf{\delta}]$ . Redensities dates: Co.PC $\rho$ |
| c. (osers (Administratedrop)                         | ng 192.108.1.10                   |            |               | Nom de l'<br>PC-CLE                  | ordnatour :<br>NTCR  | u ossic       | rs (7)<br>Bersee          | Decamanta                                       | Imagas        |   |
| Envoi d'une requête 'Ping'                           | 192.168.1.10 avec 32 octets de    | données :  |               | Non can<br>PC CLIB                   | gkit de Fordinateur :<br>1991  |               | Musicus                   | Direct 20                                       | Töödersementa |   |
| Réponse de 192.168.1.10 :                            | octets=32 temps<1ms TTL=128       |            |               | Martin                               | Ams.   | jerstenn:     |                           |   |               |   |
| Réponse de 192.168.1.10 :                            | octets=32 temps<1ms TTL=128       |            |               |                                      | ulu  | kr            | 11005                     | Modificación da nom ou da domaine de Fordinatea | ×             |   |
| Réponse de 192.168.1.10 :                            | octets=32 temps<1ms TTL=128       |            |               |                                      | 151  | mph           | Windows (C)               | 🕕 Benarcue descie domaine Mriab.                |               |   |
| Statistiques Ping pour 192                           | .168.1.10:                        |            |               |                                      | CK Annaka  |               | 204 Galillanet kur 200 Ga | 04  |               |   |
| Paquets : envoyés = 4,<br>Dunéo approvimativo dos bo | reçus = 4, perdus = 0 (perte 0%   | 5),        |               |                                      | OK invite  | Animar        |                           |   |               |   |
| Minimum = Oms, Maximum                               | = Oms, Moyenne = Oms              |            |               |                                      |  |               |                           |   |               |   |
|  |                                   |            |               |                                      |  |               |                           |   |               |   |
|  |                                   |            |               |                                      | 9 démentió   |               |                           |   |               | (iii m  |
|  |                                   |            |               |                                      |  |               |                           |   |               |   |
|  |                                   |            |               |                                      |  |               |                           |   |               |   |
|  |                                   |            |               |                                      |  |               |                           |   |               |   |
|  | 📙   🖂 📮   IT                      |            |               |                                      |  |               |                           | - 0   | ;             |   |
|  | Fichier Accueil Partage Affichage |            |               |                                      |  |               |                           |   | $\sim$        |   |
|  | ← → × ↑ 📙 > Réseau > srv-files >  | SHARE > IT |               |                                      |  |               | v Č R                     | echercher dans : IT                             | \$            |   |
|  | N                                 | ^          | 107.7.1       | -                                    | <b>T</b> 10  |               |                           |   |               |   |
|  | Accès rapide                      | IVIO       | diffie le     | iype                                 | laille   |               |                           |   |               |   |
|  | Bureau 💉 📜 test                   | 28/0       | 02/2025 07:06 | Document texte                       | 1 Ko   |               |                           |   |               |   |
|  | Téléchargements #                 |            |               |                                      |  |               |                           |   |               |   |
|  | Documents *                       |            |               |                                      |  |               |                           |   |               |   |
|  | lmages d                          |            |               |                                      |  |               |                           |   |               |   |
|  | h Musique                         |            |               |                                      |  |               |                           |   |               |   |
|  | Vidéos                            |            |               |                                      |  |               |                           |   |               |   |
|  | - Sideos                          |            |               |                                      |  |               |                           |   |               |   |
|  |                                   |            |               |                                      |  |               |                           |   |               |   |

J'ai bien accès au chemin d'accès réseau du serveur de fichiers depuis le PC client

# 5...Configuration des stratégies de groupes

5.1...Sécurité des mots de passe



J'applique des paramètres de stratégie plus strictes pour améliorer la sécurité

5.2...Configuration des accès et restrictions



Ici, pour l'exemple, j'ai créé une GPO (stratégie de groupe) qui empêche les utilisateurs authentifiés et les utilisateurs du groupe « RH » d'effectuer des modifications dans le panneau de configuration de Windows

# 6...Migration vers le second serveur

## 6.1...Ajout du serveur dans le domaine

Comme pour les autres machines, pour ajouter la machine dans le domaine, je passe par les paramètres systèmes et dans « Renommer le PC » puis je tape « bts.lab » dans le domaine à rejoindre, la machine va redémarrer.

## 6.2...Promotion en tant que Contrôleur de domaine

La manipulation pour promouvoir SRV-AD02 en contrôleur de domaine est exactement la même que lorsque j'ai promu SRV-AD01 pour la première fois, en ajoutant bien AD DS lors de la configuration de base.

| 🚡 Assistant Ajout de rôles et de | fonctionnalités  |  |  | -  |                                      | ×            |
|----------------------------------|--|--|--|--|--------------------------------------|--------------|
| Sélectionner le s                | erveur de dest   | ination  |  | SERVEUR DE<br>SR                                       | DESTINAT<br>V-AD02.bts               | ION<br>s.lab |
| Avant de commencer               | Sélectionnez le serveu   | ır ou le disque dur virtu  | el sur lequel installer des rôles  | s et des fonctior                                      | nnalités.                            |              |
| Type d'installation              | Sélectionner un se   | rveur du pool de serve   | urs  |  |                                      |              |
| Sélection du serveur             | O Sélectionner un die  | sque dur virtuel   |  |  |                                      |              |
| Rôles de serveurs                | Pool de serveurs   |  |  |  |                                      |              |
| Fonctionnalités                  |  |  |  |  |                                      |              |
|                                  | Filtre :   |  |  |  |                                      |              |
|                                  | Nom  | Adresse IP   | Système d'exploitation   |  |                                      |              |
|                                  | SRV-AD02.bts.lab   | 192.168.1.15   | Microsoft Windows Server   | 2019 Standard  | Evaluatio                            | n            |
|                                  | 1 ordinateur(s) trouvé   | (s)  |  |  |                                      |              |
|                                  | Cette page présente le<br>ont été ajoutés à l'aid-<br>serveurs hors connexi<br>incomplète ne sont pa | es serveurs qui exécute<br>e de la commande Ajoi<br>on et les serveurs nouv<br>as répertoriés. | nt Windows Server 2012 ou ur<br>iter des serveurs dans le Gesti<br>ellement ajoutés dont la collec | ne version ultéri<br>onnaire de serv<br>cte de données | ieure et q<br>eur. Les<br>est toujoi | ui<br>urs    |
|                                  |  | < Pré  | cédent Suivant >   | Installer  | Annul                                | ler          |



| Assistant Configuration des serv   | ices de domaine Active Directory  |   | -           |                    | ×             |
|--|---|---|-------------|--------------------|---------------|
| Options du contré  | òleur de domaine  |   | SEI<br>SRV- | RVEUR C<br>AD02.bt | IBLE<br>s.lab |
| Configuration de déploie<br>Options du contrôleur de<br>Options supplémentaires<br>Chemins d'accès<br>Examiner les options<br>Vérification de la configur<br>Installation<br>Résultats | Spécifier les capacités du contrôle<br>Serveur DNS (Domain Name S<br>Catalogue global (GC)<br>Contrôleur de domaine en lec<br>Nom du site :<br>Taper le mot de passe du mode d<br>Mot de passe :<br>Confirmer le mot de passe : | sur de domaine et les informations sur le site<br>system)<br>ture seule (RODC)<br>Default-First-Site-Name v<br>e restauration des services d'annuaire (DSRM | )           |                    |               |
|  |   | < Précédent Suivant > Instal  | ler         | Annule             | r             |



## 6.3...Vérification de la réplication

Une fois la promotion et le redémarrage terminés, je dois vérifier la réplication via powershell pour m'assurer que tout s'est bien déroulé.



lci, tout s'est bien passé.

| PS C:\Users\Administrateur.                         | BTS> Get-ADDomainController -Filter *  |
|---|--|
| ComputerObjectDN                                    | : CN=SRV-AD02.QU=Domain Controllers.DC=bts.DC=lab  |
| DefaultPartition                                    | : DC=hts.DC=lab  |
| Domain  | : hts.lab  |
| Enabled   |  |
| Forest  | , http://www.inteliab  |
| HostName  | SRV-AD02 hts lab   |
| InvocationId  | - JNF R022.013.100   |
| TPv4Addrass   |  |
| TPv6Address   |  |
| IsGlobalCatalog                                     | ·<br>· True  |
| TcDeadOnly  | - Falca  |
| IdanPort  | 330  |
| Name  | · 50)  |
| NTDSSettingsObjectDN                                | , SNY ROVE<br>- (NAITOR Settings (N-SDV-AD02 (N-Servers (N-Default-First-Site-Name (N-Sites (N-Configuration DC-bts DC-lab   |
| OperatingSystem                                     | · Under Sarvar 2010 Standard Evaluation  |
| OperatingSystemHotfix                               | · · · · · ·  |
| OpenatingSystemNotrix<br>OpenatingSystemServiceDack |  |
| OpenatingSystemServiceFack                          | · 10 0 (17762)   |
| OpenationMasterPoles                                |  |
| Partitions  | * 15<br>/DC-EncertDreZoner DC-btr DC-lab DC-DomainDerZoner DC-btr DC-lab (N=Schema (N=Configuration DC-btr DC-lab (N=Configuration DC-btr DC-lab )   |
| Fartitions<br>ServerObjectDN                        | : {Ut=FOPEStonscones;Ut=BCS;Ut=BdD, Ut=DomainUnscones;Ut=Bots;Ut=Lab; tw=Schema;tw=ConfigUration;Ut=BtS;Ut=BdD, tw=ConfigUration;Ut=BtS;Ut=BdD, tw=ConfigUration;Ut=BdD, tweConfigUration;Ut=BdD, tweConfigUration;Ut=BdD, tweConfigUration;Ut=BdD, tweConfigUration;Ut=BdD, tweConfigUration;Ut=BdD, tweConfigUration;Ut=BdD, tweConfigUration;Ut=BdD, tweConfigUration;Ut=BdD, tweConfi  |
| Serverobjectow                                      | : CN=SNY=ADZ_CN=SETVETS_CN=DETADIC=FITSCSICE=Name,CN=SICES_CN=CONTIGUEALION,DC=DCS_DC=IAD  |
| Serverobjectadia                                    | : 3037013*0117-4000-0374-40(3/003010)<br>. Dofuls First File New   |
| SalDeat   | : Default=fifSt=Site=wame  |
| SSIPORE   | : 000  |
|   | · CNESRV-4001 OHEDomain Controllers DC=tab   |
| DefaultPartition                                    | · Draha Draha  |
| Domain  | hts lab  |
| Enabled   |  |
| Forest  | , http://www.inteliab  |
| HostName  | · SQLADQ1 hts lab  |
| InvocationId  | . JKY ADJ1.0131.00<br>dd73040.0020./d50.brf3.855053f3/023  |
| TDv/Address   |  |
| TPv6Address   |  |
| IsGlobalCatalog                                     |  |
| TsReadOnly  | False  |
| IdanPort  | 389  |
| Name  | 5 SRV-4001   |
| NTDSSettingsObjectDN                                | : CNENTDS Settings.CN=SRV-AD01.CN=Servers.CN=Default-First-Site-Name.CN=Sites.CN=Configuration.DC=bts.DC=lab   |
| OperatingSystem                                     | - Grand Server 2019 Standard Fuluation   |
| OperatingSystemHotfix                               |  |
| OperatingSystemServicePack                          |  |
| OperatingSystemVersion                              | 10.0 (17763)   |
| OperationMasterRoles                                | <pre>{SchemaMaster, DomainNamineMaster, PDCEmulator, RIDMaster}</pre>  |
| Partitions  | <pre>(DC=EncestDosZones.DC=bts.DC=lab. DC=DomainDosZones.DC=bts.DC=lab. CN=Configuration.DC=bts.DC=lab. CN=Configuration.DC=la</pre> |
| ServerObjectDN                                      | · (NeSRV-ADA) (NeSpverc (NeData) - First-Site-Name (NeSites (NeSite) - Top Filling) (NeSites Del 10), De-Disjo  |
| ServerObjectGuid                                    | Tapedets-Java-Java Servers Jet Volte Art Servers and Se<br>Servers and Servers       |
| Site  | Defaille First-Side Name   |
| SslPort   | - 636  |
|   |  |
|   |  |

On voit bien qu'il y'a maintenant 2 DC, la promotion a bien fonctionnée

## 6.4...Transfert des rôles FSMO

J'ai maintenant 2 DC, mais les rôles principaux sont encore associés au premier DC, il faut donc les transférer sur le second via une commande Powershell.

#### <u>Commande</u> : *netdom query fsmo*



PS C:\Users\Administrateur.BTS> Move-ADDirectoryServerOperationMasterRole -Identity "SRV-AD02" -OperationMasterRole 0,1,2,3,4 Déplacer le rôle de maître d'opérations Voulez-vous déplacer le rôle « PDCEmulator » vers le serveur « SRV-AD02.bts.lab » ? [O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide (la valeur par défaut est « O ») : T

.Je transfère les 5 rôles vers le nouveau DC (SRV-AD02) et je confirme pour tous les rôles en validant avec « T ».

| netdom query fsmo |
|-------------------|
| SRV-AD02.bts.lab  |
| lée.              |
|                   |

Les 5 rôles sont maintenant assignés au serveur SRV-AD02.

Je peux aussi vérifier les rôles un à un pour être sur qu'ils ont bien été transférés (comme le Maître d'infrastructure ou le Contrôleur de schéma). Pour l'exemple je vais essayer avec le Maître d'infrastructure.



Le Maître d'infrastructure est bel et bien assigné à SRV-AD02.bts.lab

## 6.5...Suppression du contrôleur SRV-AD01

Maintenant que tout repose sur le deuxième DC, le premier peut être supprimé sans risque du domaine. Pour ce faire, je vais le rétrograder puis le supprimer



La rétrogradation est en cours et prend quelques minutes



Après la suppression des rôles (AD DS), l'ordinateur va redémarrer et sera sorti du domaine automatiquement.

# 7...Vérifications et tests

Pour terminer la migration, il faut supprimer définitivement SRV-AD01 pour être sûr que le DC SRV-AD02 a bien pris le relais et que la suppression de l'ancien contrôleur n'impacte pas l'architecture actuelle.



Dans Active Directory, SRV-AD01 est encore présent : il faut le supprimer

| Utilisateurs et orainateurs Active<br>Fichier Action Affichage ?  | Ulfectory   |   |                            |   |   |                                   |  | _ | u ^ |
|---|---|---|----------------------------|---|---|-----------------------------------|--|---|-----|
| A Construction of the second sec | Image: Control of the second | See | Type de contrô<br>GC<br>GC | Site<br>Default-First-Si<br>Default-First-Si      | Description   |                                   |  |   |     |
|   |   |   | Se                         | zrvices de domaine /<br>Voulez-vour<br>nommé = SF | Active Directory<br>s vraiment supprimer le type c<br>RV-ADOI = ?<br>Ou | ×<br>robjet « Ordinateur »<br>Non |  |   |     |
| < >>  |   |   |                            |   |   |                                   |  |   |     |

Je n'ai plus qu'à vérifier que la suppression a bien été prise en compte via PowerShell via la même commande que précédemment : « Get-ADDomainController -Filter \* »

|                           | · CN-SBV-AD02 OU-Domain Controllanc DC-btc DC-lab   |
|---------------------------|---|
| lompulerobjectow          | : CN=SKY-AD02,00=00main Controllers,DC=0CS,DC=1aD   |
| lomain                    | : bt=bts_bt=lab   |
| inabled                   |   |
| apact                     | : Intel lab   |
| orest                     |   |
| IOS LINAIME               | : 58V-AU02.015.140  |
| nvocationid               | : 02107408-2005-4004-0201-800205720D/1  |
| PV4Address                | : 192.168.1.15  |
| PV6Address                |   |
| sGlobalCatalog            | : True  |
| sReadOnly                 | : False   |
| dapPort                   | : 389   |
| lame                      | : SRV-AD02  |
| NTDSSettingsObjectDN      | : CN=NTDS Settings,CN=SRV-AD02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configurat<br>on,DC=bts,DC=lab |
| peratingSystem            | : Windows Server 2019 Standard Evaluation   |
| peratingSystemHotfix      |   |
| peratingSystemServicePack |   |
| peratingSystemVersion     | : 10.0 (17763)  |
| perationMasterRoles       | : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster}  |
| artitions                 | : {DC=ForestDnsZones,DC=bts,DC=lab, DC=DomainDnsZones,DC=bts,DC=lab,  |
|                           | CN=Schema,CN=Configuration,DC=bts,DC=lab, CN=Configuration,DC=bts,DC=lab}                                       |
| erverObjectDN             | : CN=SRV-AD02, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=bts, DC=lak               |
| erverObjectGuid           | : 385f0519-61f3-406b-a5f4-4dc37083010f  |
| ite                       | : Default-First-Site-Name   |
| slPort                    | : 636   |

SRV-AD01 n'est plus visible, il a bien été supprimé.

Les tests suivants ont été effectués et ont fonctionnés (pour confirmer la réussite de la migration) :

- $\rightarrow$  Connexion avec les trois utilisateurs sur le domaine
- → GPO Fonctionnelles : l'utilisateur RH n'a pas accès au panneau de configuration
- → Les fichiers partagés depuis le serveur de fichiers (SRV-FILES) sont bien accessibles comme au début

### Problèmes rencontrés et solutions appliquées :

**Problème** : Impossible de joindre une machine au domaine <u>Erreur</u> : « La base de données de sécurité du serveur n'a pas de compte d'ordinateur. » Solution : Mérification et correction des DNS redémorrage du convise notion

Solution : Vérification et correction des DNS, redémarrage du service netlogon

Problème : Mauvaise synchronisation horaire des machines Impact : « Certaines machines ne pouvaient pas communiquer correctement avec le DC. »

Solution : Forcer la synchronisation via la commande « w32tm /resync »

**Problème** : SRV-AD01 toujours visible après rétrogradation <u>Impact</u> : « L'ancien contrôleur de domaine restait dans Active Directory. » <u>Solution</u> : Suppression manuelle et nettoyage des métadonnées AD.

# 8...Conclusion et compétences acquises

### Résumé des étapes réalisées :

Ce projet a permis de mettre en place un domaine Active Directory sous Windows Server 2019, puis de le migrer sur une autre machine également équipée de Windows Server 2019 tout en assurant la continuité du service.

Les étapes principales ont été :

- Installation et configuration de SRV-AD01 comme premier contrôleur de domaine (DC)
- ✓ Création des utilisateurs et groupes Active Directory
- ✓ Configuration des stratégies de groupe (GPO)
- ✓ Ajout du serveur SRV-AD02 et promotion en contrôleur de domaine
- ✓ Vérification de la réplication AD
- ✓ Transfert des rôles FSMO vers SRV-AD02
- ✓ Rétrogradation et suppression de SRV-AD01

Toutes ces étapes ont été validées par des tests fonctionnels tels que la connexion des utilisateurs au domaine, la réplication AD ainsi que l'accès aux ressources réseau.

### Compétences acquises :

Grâce à ce projet, plusieurs compétences techniques ont été développées :

#### Administration Windows Server :

- ✓ Installation et gestion de Windows Server 2019
- Configuration et maintenance d'un contrôleur de domaine Active Directory
- ✓ Gestion des services réseaux DNS

#### Sécurisation et gestion des utilisateurs :

- ✓ Création et gestion des comptes AD + groupes
- ✓ Application de stratégies de groupe (GPO)
- ✓ Sécurisation des accès réseau

#### Migration et maintenance d'Active Directory :

- ✓ Ajout et promotion d'un DC secondaire
- ✓ Transfert des rôles FSMO
- ✓ Rétrogradation et suppression d'un DC

# **Conclusion finale :**

Ce projet m'a permis de découvrir toutes les étapes de mise en place et de migration d'un domaine Active Directory.

J'ai pu manipuler Windows Server, comprendre les enjeux liés aux rôles FSMO et à la réplication AD ainsi que résoudre des problèmes techniques en appliquant des méthodes de diagnostic et de correction adaptées.

La totalité du projet a été recommencée pas moins de trois fois à cause d'erreurs que je ne parvenais pas à résoudre, ce qui impliquait une réinitialisation totale et un retour à zéro, ce qui m'a permis de recommencer pour la dernière fois sans erreur grave puisque j'ai compris précisément comment les éviter.

Il s'agit d'une expérience enrichissante, applicable dans un environnement professionnel pour la gestion d'infrastructure réseau et l'administration système.