

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 maîtrise 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 meilleure 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).

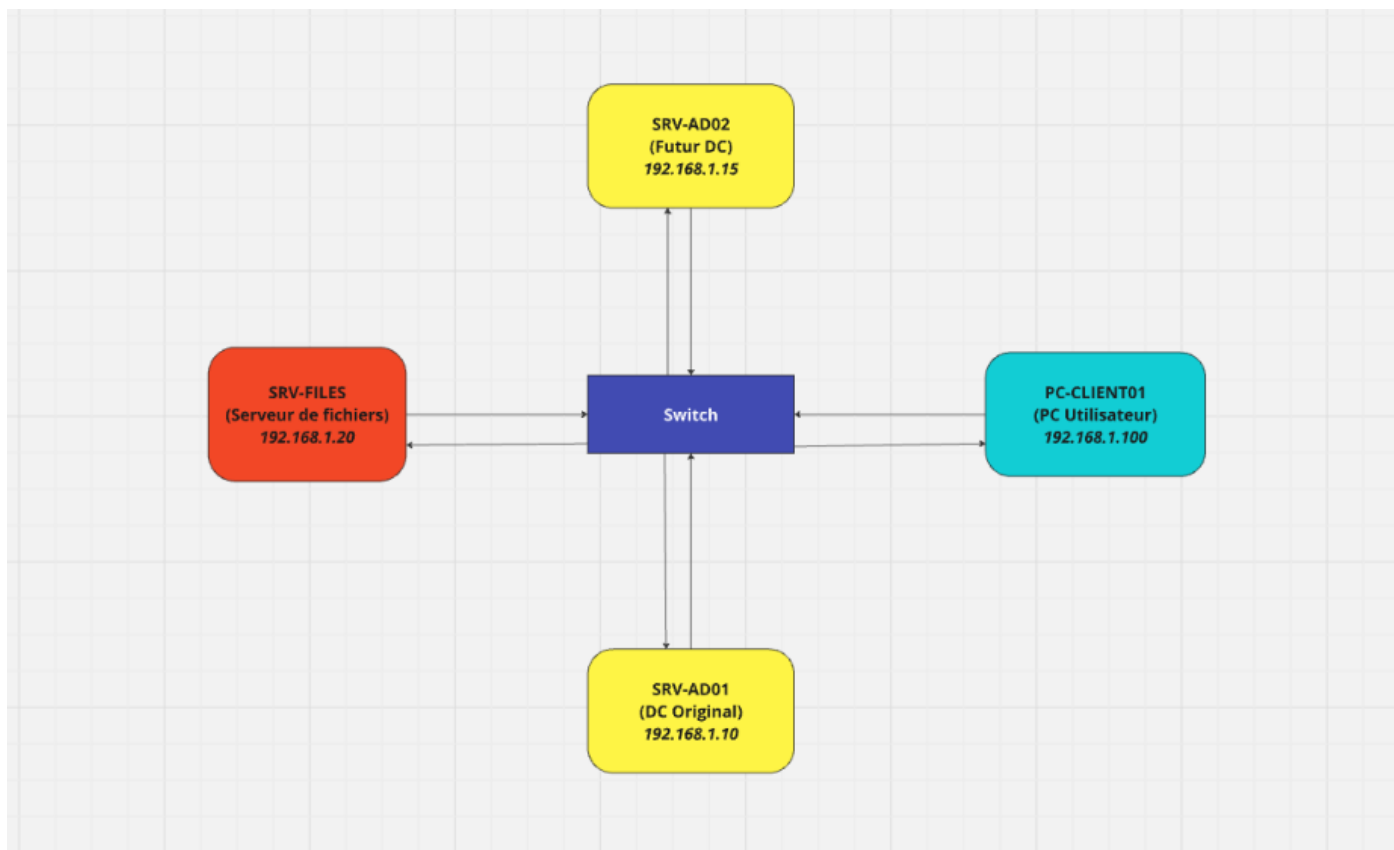
Il s'agit d'une simulation d'environnement d'entreprise qui me permet d'acquérir des compétences en administration système et gestion de réseau.

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

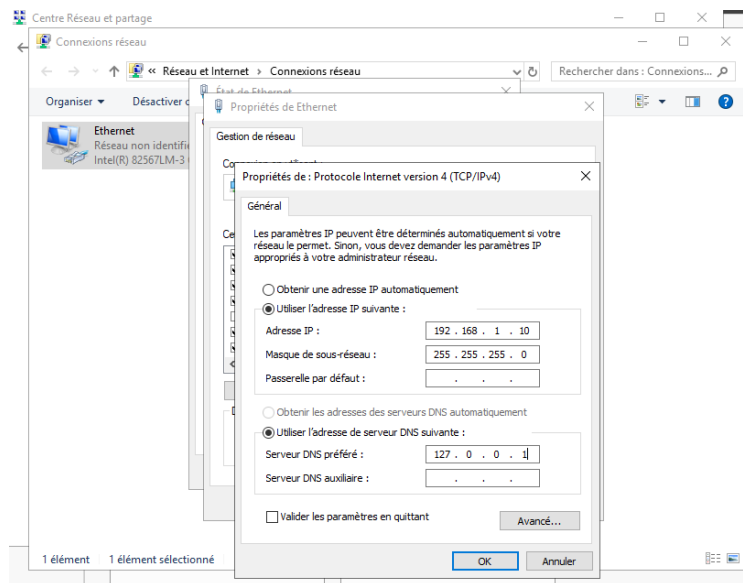


2.2...Liste des serveurs et adresses IP

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

```
Administrateur: C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig /all

Configuration IP de Windows

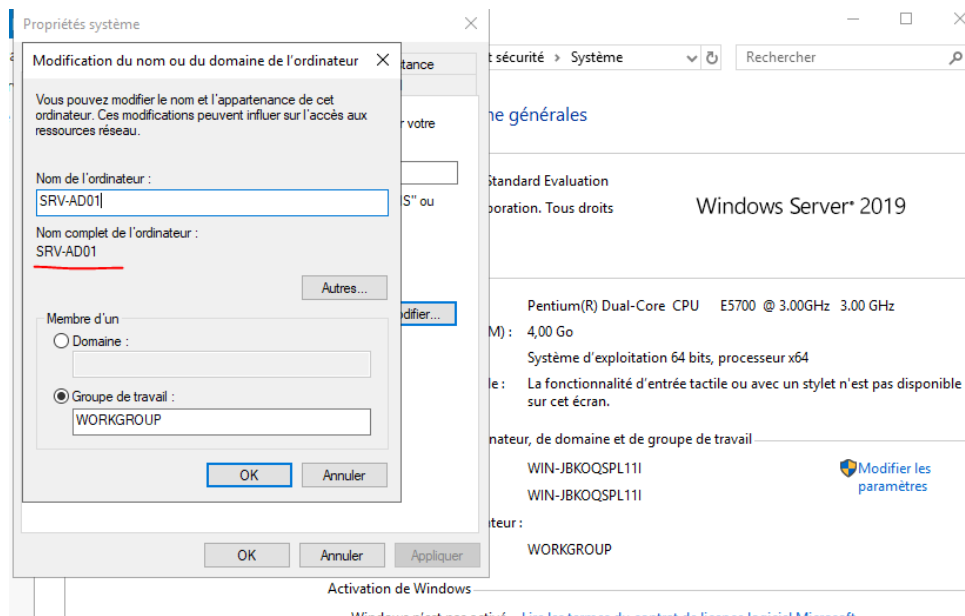
  Nom de l'hôte . . . . . : WIN-JBKOQSP11I
  Suffixe DNS principal . . . . . :
  Type de noeud . . . . . : Hybride
  Routage IP activé . . . . . : Non
  Proxy WINS activé . . . . . : Non

Carte Ethernet Ethernet :

  Suffixe DNS propre à la connexion. . . :
  Description. . . . . : Intel(R) 82567LM-3 Gigabit Network Connection
  Adresse physique . . . . . : F0-4D-A2-37-65-4A
  DHCP activé. . . . . : Non
  Configuration automatique activée. . . : Oui
  Adresse IPv6 de liaison locale. . . . . : fe80::d354:4521:be8d:5ab5%6(préfééré)
  Adresse IPv4. . . . . : 192.168.1.10(préfééré)
  Masque de sous-réseau. . . . . : 255.255.255.0
  Passerelle par défaut. . . . . :
  IAID DHCPv6 . . . . . : 116411810
  DUID de client DHCPv6. . . . . : 00-01-00-01-2F-52-60-61-F0-4D-A2-37-65-4A
  Serveurs DNS. . . . . : 127.0.0.1
  NetBIOS sur Tcpip. . . . . : Active
```

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.



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.

```
C:\Users\Administrateur>ping 192.168.1.15

Envoi d'une requête 'Ping' 192.168.1.15 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
```

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\Administrateur> New-NetFirewallRule -DisplayName "Autoriser Ping" -Direction Inbound -Protocol ICMPv4 -Action Allow

Name                : {eaa3538e-d117-493f-bb6c-afeb498853c}
DisplayName         : 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
```

```
C:\Users\Administrateur>ping 192.168.1.15
Envoi d'une requête 'Ping' 192.168.1.15 avec 32 octets de données :
Réponse de 192.168.1.15 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.15 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.15 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.15 : octets=32 temps<1ms TTL=128

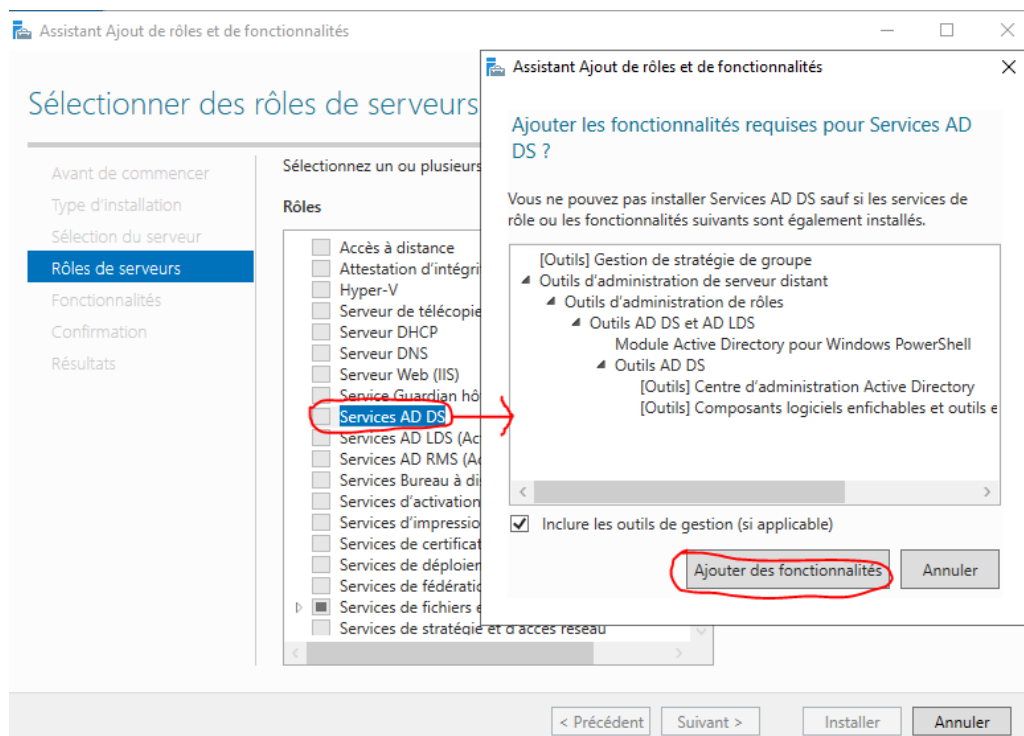
Statistiques Ping pour 192.168.1.15:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

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 :

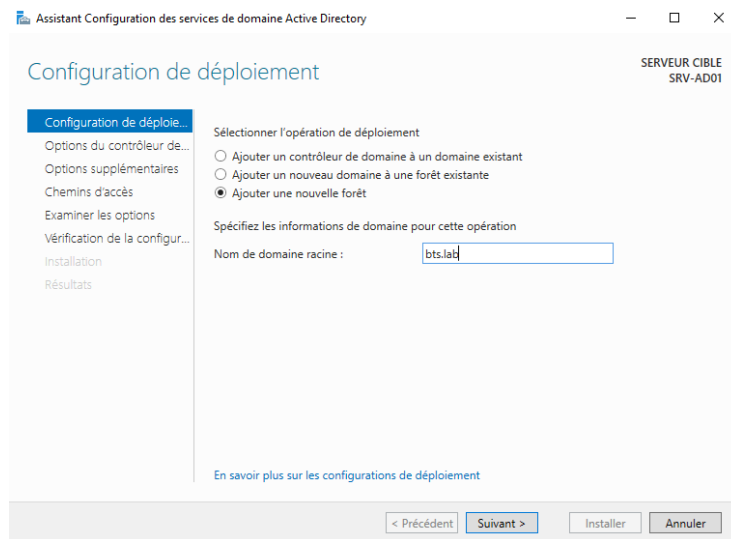
- Ouvrir « Gestionnaire de serveur » puis « Ajouter des rôles et fonctionnalités »
- « Installation basée sur un rôle ou une fonctionnalité »
- Sélection de la machine (SRV-AD01)
- Cocher « Services AD DS »



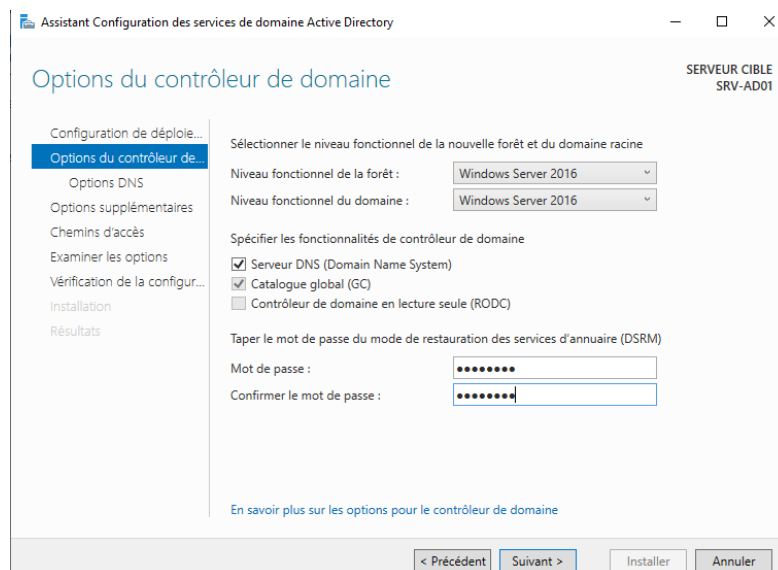
→ Confirmer l'installation puis attendre la fin du chargement

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 ».



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



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 »

```
Administrateur: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> Get-ADDomain

AllowedDNSSuffixes           : {}
ChildDomains                 : {}
ComputersContainer           : CN=Computers,DC=bts,DC=lab
DeletedObjectsContainer      : CN=Deleted Objects,DC=bts,DC=lab
DistinguishedName            : DC=bts,DC=lab
DNSRoot                       : bts.lab
DomainControllersContainer    : CN=Domain Controllers,DC=bts,DC=lab
DomainMode                   : Windows2016Domain
DomainSID                     : S-1-5-21-1899828923-3349229793-1986631637
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=bts,DC=lab
Forest                       : bts.lab
InfrastructureMaster          : SRV-AD01.bts.lab
LastLogonReplicationInterval : (CN=(3182f348-016d-11d2-945f-00c04f8984f9),CN=Policies,CN=System,DC=bts,DC=lab)
LinkedGroupPolicyObjects      : CN=LostAndFound,DC=bts,DC=lab
LostAndFoundContainer        : ManagedBy
Name                          : bts
NetBIOSName                  : bts
ObjectClass                   : domainDNS
ObjectGUID                    : 88788727-a0f3-4b5d-8908-b26324177b64
ParentDomain                  :
PDCemulator                   : SRV-AD01.bts.lab
PublicKeyRequiredPasswordRolling : True
QuotasContainer               : CN=NTDS Quotas,DC=bts,DC=lab
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers       : (SRV-AD01.bts.lab)
RIDMaster                     : SRV-AD01.bts.lab
SubordinateReferences         : (DC=ForestDnsZones,DC=bts,DC=lab, DC=DomainDnsZones,DC=bts,DC=lab,
CN=Configuration,DC=bts,DC=lab)
SystemContainer               : CN=System,DC=bts,DC=lab
UsersContainer                 : CN=Users,DC=bts,DC=lab
```

```
PS C:\Users\Administrateur> Get-ADForest

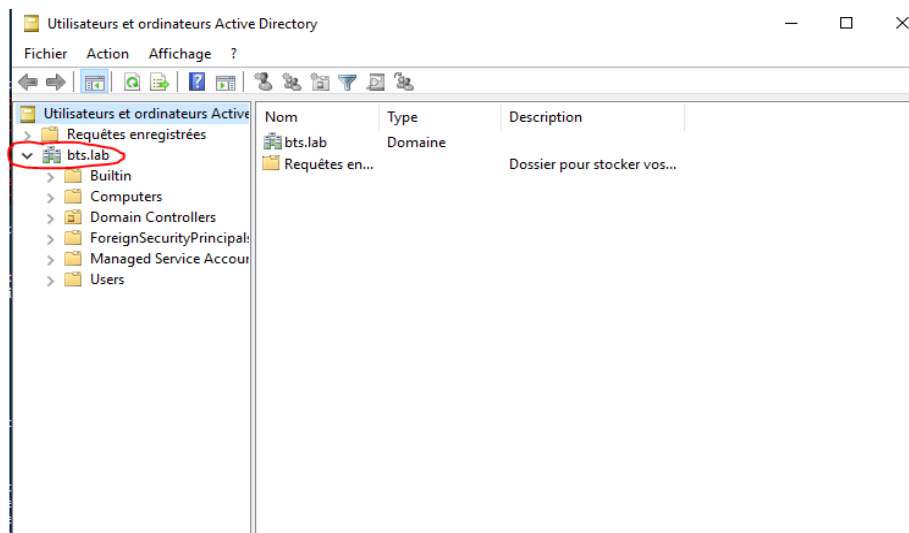
ApplicationPartitions : {DC=ForestDnsZones,DC=bts,DC=lab, DC=DomainDnsZones,DC=bts,DC=lab}
CrossForestReferences : {}
DomainNamingMaster    : SRV-AD01.bts.lab
Domains                : {bts.lab}
ForestMode             : Windows2016Forest
GlobalCatalogs        : {SRV-AD01.bts.lab}
Name                   : bts.lab
PartitionsContainer    : CN=Partitions,CN=Configuration,DC=bts,DC=lab
RootDomain             : bts.lab
SchemaMaster           : SRV-AD01.bts.lab
Sites                  : {Default-First-Site-Name}
SPNSuffixes            : {}
UPNSuffixes            : {}
```

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.

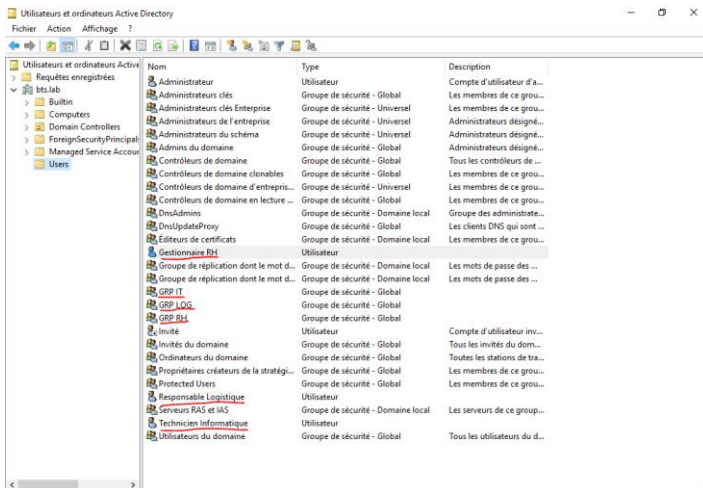
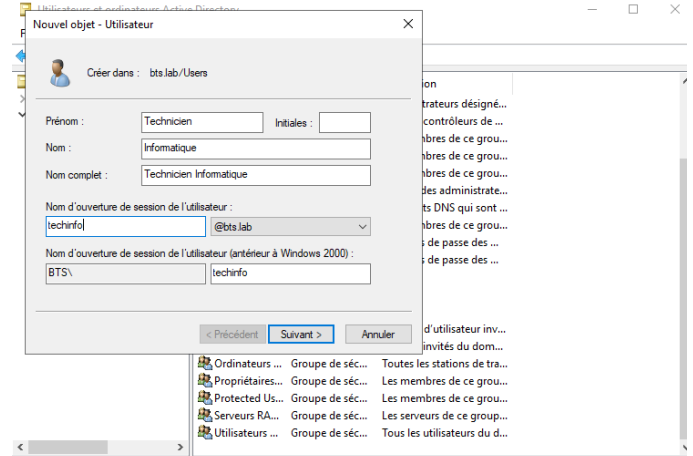
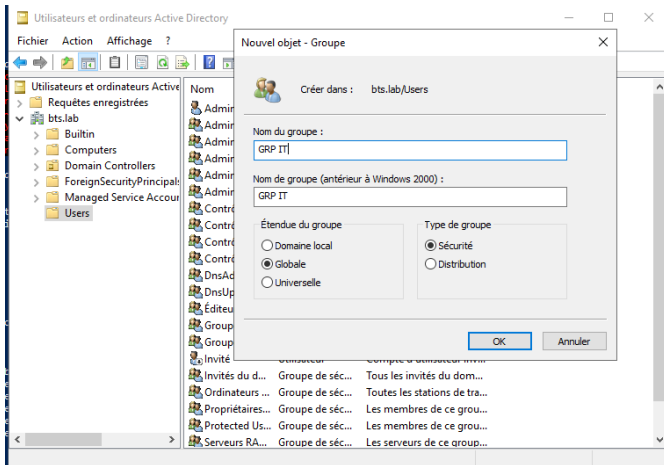
```
PS C:\Users\Administrateur> Get-ADDomainController -filter *

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,
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-ef97283db8df
Site                       : Default-First-Site-Name
SslPort                     : 636
```



4...Gestion des utilisateurs et groupes

4.1...Création des utilisateurs et groupes



3 groupes créés :

- GRP IT
- GRP RH
- GRP LOG

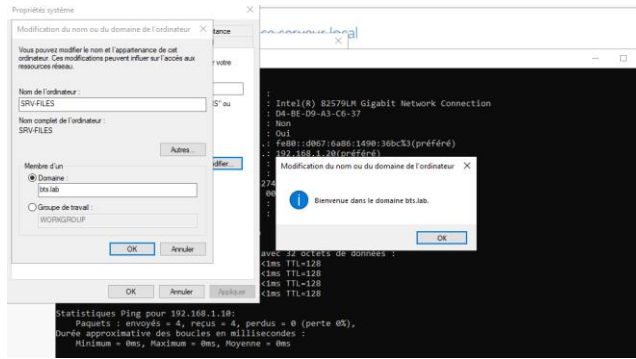
Avec 1 utilisateur par groupe

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

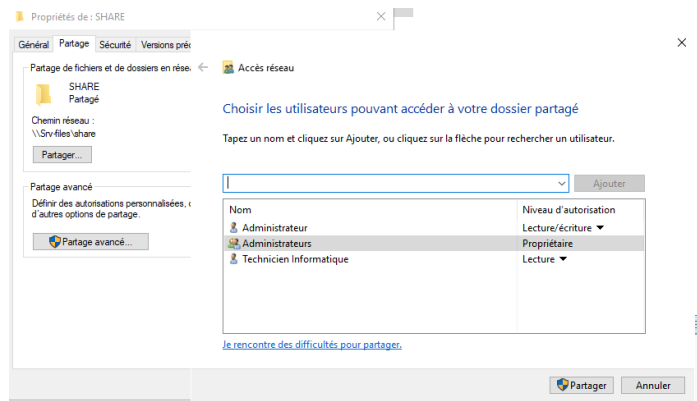
```
C:\Users\Administrateur>ping 192.168.1.10
Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        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



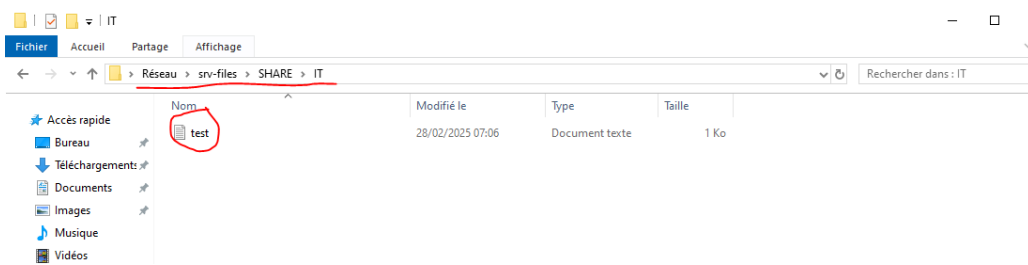
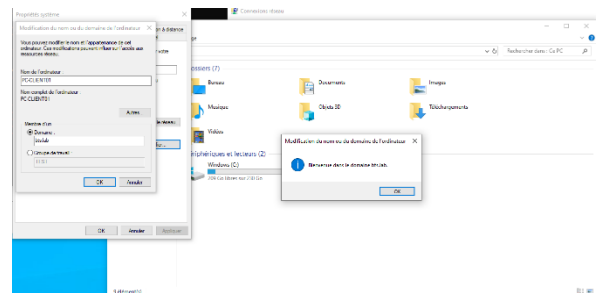
Je partage un dossier test sur le réseau avec l'utilisateur « techinfo » créé au préalable pour tester les accès.

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 »

```
C:\Users\Administrateur>ping 192.168.1.10

Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.10 : octets=32 temps<1ms TTL=128

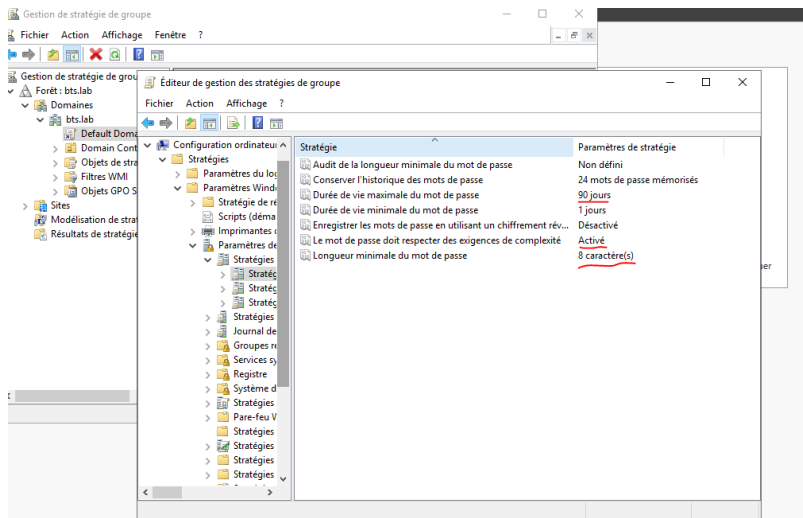
Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```



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

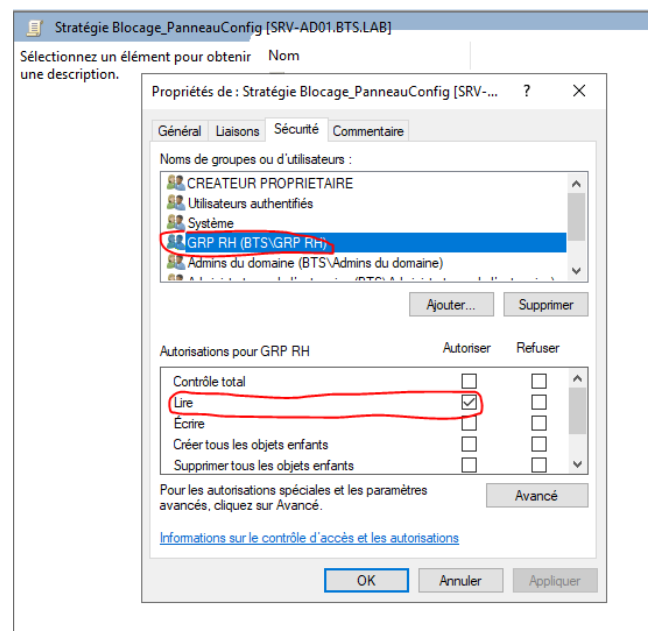
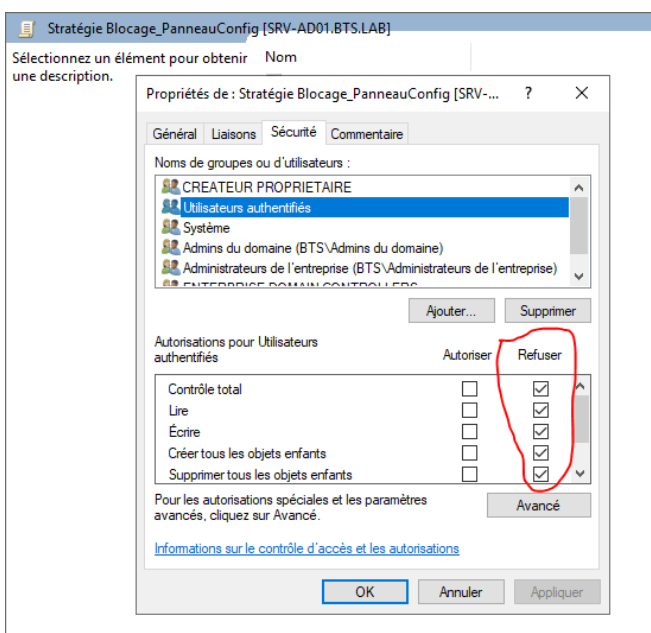
5... Configuration des stratégies de groupes

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

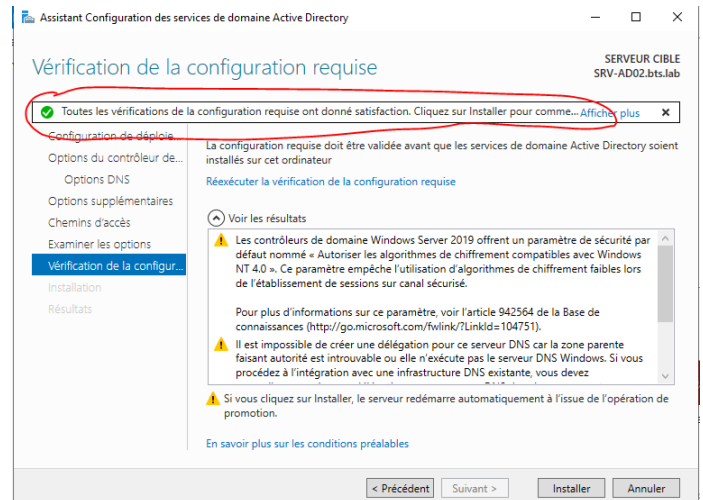
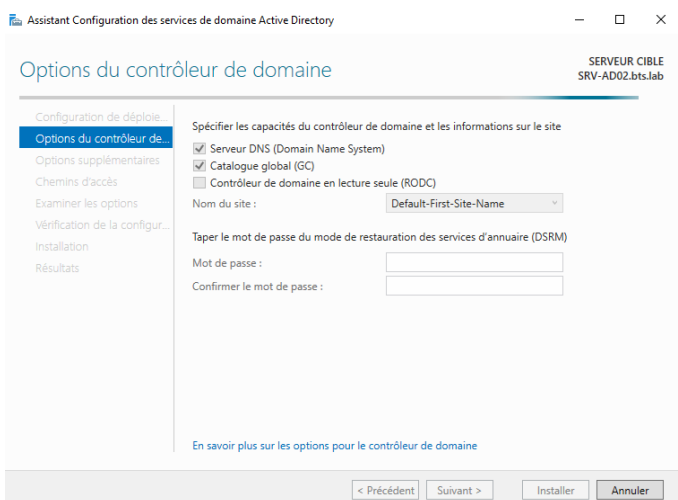
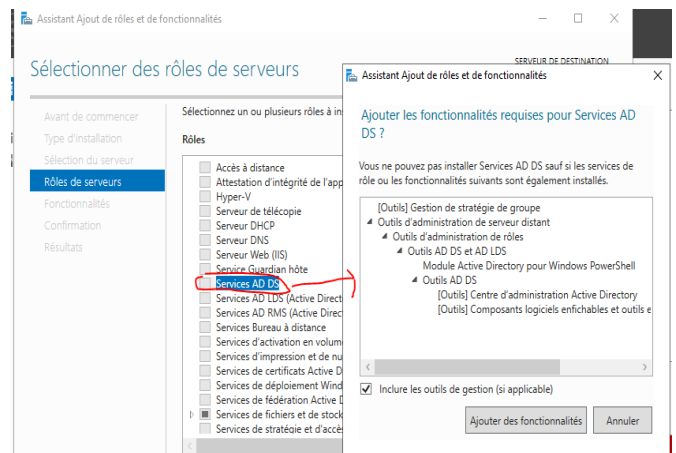
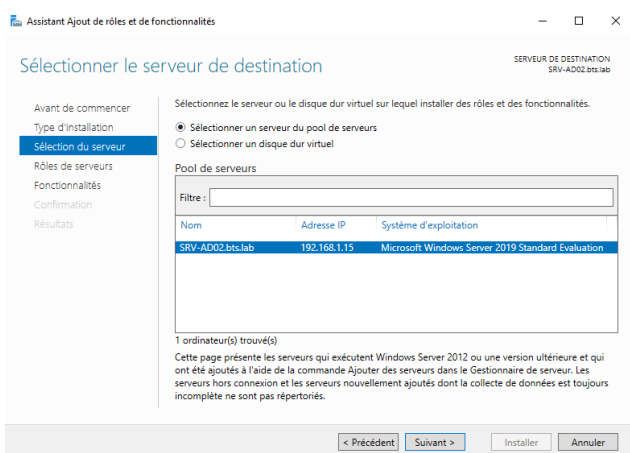
6...Migration vers le second serveur

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.



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.

```
PS C:\Users\Administrateur.BTS> repadmin /showrepl

Repadmin : exécution de la commande /showrepl sur le contrôleur de domaine complet localhost
Default-First-Site-Name\SRV-AD02
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : 1b7e6695-2fbc-4c43-ac80-291ad28c84d0
ID de l'invocation DSA : d21ef468-2bc8-40b4-b261-8db205f2db71

=== INSTANCES VOISINES ENTRANTES ===

DC=bts,DC=lab
  Default-First-Site-Name\SRV-AD01 via RPC
  GUID de l'objet DSA : dd72e06e-9029-4d59-bcf3-85505afa402a
  La dernière tentative, le 2025-02-28 16:52:54, a réussi.

CN=Configuration,DC=bts,DC=lab
  Default-First-Site-Name\SRV-AD01 via RPC
  GUID de l'objet DSA : dd72e06e-9029-4d59-bcf3-85505afa402a
  La dernière tentative, le 2025-02-28 16:37:40, a réussi.

CN=Schema,CN=Configuration,DC=bts,DC=lab
  Default-First-Site-Name\SRV-AD01 via RPC
  GUID de l'objet DSA : dd72e06e-9029-4d59-bcf3-85505afa402a
  La dernière tentative, le 2025-02-28 16:26:16, a réussi.

DC=DomainDnsZones,DC=bts,DC=lab
  Default-First-Site-Name\SRV-AD01 via RPC
  GUID de l'objet DSA : dd72e06e-9029-4d59-bcf3-85505afa402a
  La dernière tentative, le 2025-02-28 16:51:46, a réussi.

DC=ForestDnsZones,DC=bts,DC=lab
  Default-First-Site-Name\SRV-AD01 via RPC
  GUID de l'objet DSA : dd72e06e-9029-4d59-bcf3-85505afa402a
  La dernière tentative, le 2025-02-28 16:37:46, a réussi.
```

Ici, tout s'est bien passé.

```
PS C:\Users\Administrateur.BTS> Get-ADDomainController -Filter *

ComputerObjectDN      : CN=SRV-AD02,OU=Domain Controllers,DC=bts,DC=lab
DefaultPartition      : DC=bts,DC=lab
Domain                 : bts.lab
Enabled                : True
Forest                 : bts.lab
HostName               : SRV-AD02.bts.lab
InvocationId           : d21ef468-2bc8-40b4-b261-8db205f2db71
IPv4Address            : 192.168.1.15
IPv6Address            :
IsGlobalCatalog       : True
IsReadOnly             : False
LdapPort               : 389
Name                   : SRV-AD02
NTDSSettingsObjectDN  : CN=NTDS Settings,CN=SRV-AD02,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   : {}
Partitions              : (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...)
ServerObjectDN         : CN=SRV-AD02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=bts,DC=lab
ServerObjectGuid       : 385f0519-61f3-406b-a5f4-4dc37083010f
Site                   : Default-First-Site-Name
SslPort                : 636

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, 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
```

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.

Commande : `netdom query fsmo`

```
PS C:\Users\Administrateur> netdom query fsmo
Contrôleur de schéma          SRV-AD01.bts.lab
Maître des noms de domaine   SRV-AD01.bts.lab
Contrôleur domaine princip.  SRV-AD01.bts.lab
Gestionnaire du pool RID      SRV-AD01.bts.lab
Maître d'infrastructure      SRV-AD01.bts.lab
L'opération s'est bien déroulée.
```

Tous les rôles sont associés au contrôle de domaine d'origine.

(SRV-AD01)

```
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 « 0 ») : T
```

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

```
PS C:\Users\Administrateur> netdom query fsmo
Contrôleur de schéma          SRV-AD02.bts.lab
Maître des noms de domaine   SRV-AD02.bts.lab
Contrôleur domaine princip.  SRV-AD02.bts.lab
Gestionnaire du pool RID      SRV-AD02.bts.lab
Maître d'infrastructure      SRV-AD02.bts.lab
L'opération s'est bien déroulée.
```

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

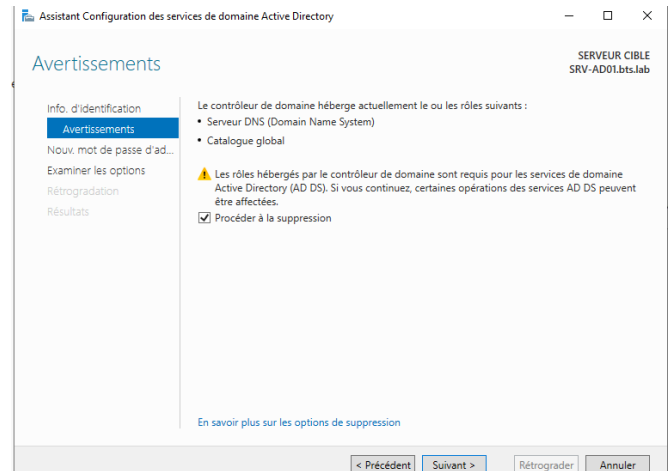
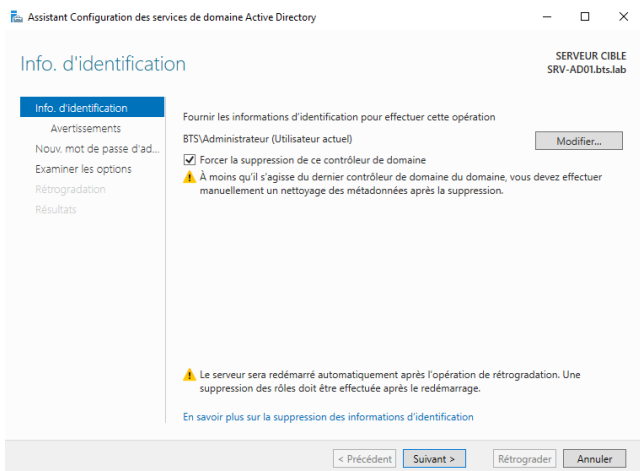
Je peux aussi vérifier les rôles un à un pour être sûr qu'ils ont bien été transférés (comme le Maître d'infrastructure ou le Contrôleur de schéma). Pour l'exemple je vais essayer avec le Maître d'infrastructure.

```
PS C:\Users\Administrateur.BTS> Get-ADDomain | Select-Object InfrastructureMaster
InfrastructureMaster
-----
SRV-AD02.bts.lab
```

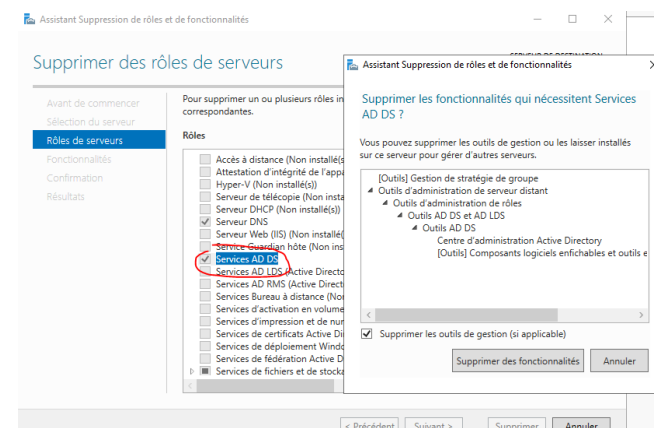
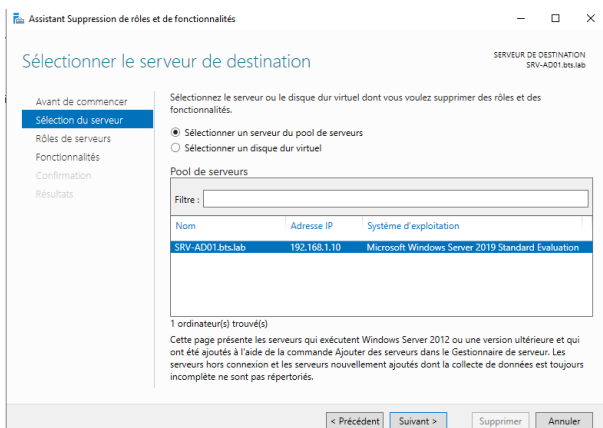
Le Maître d'infrastructure est bel et bien assigné à SRV-AD02.bts.lab

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



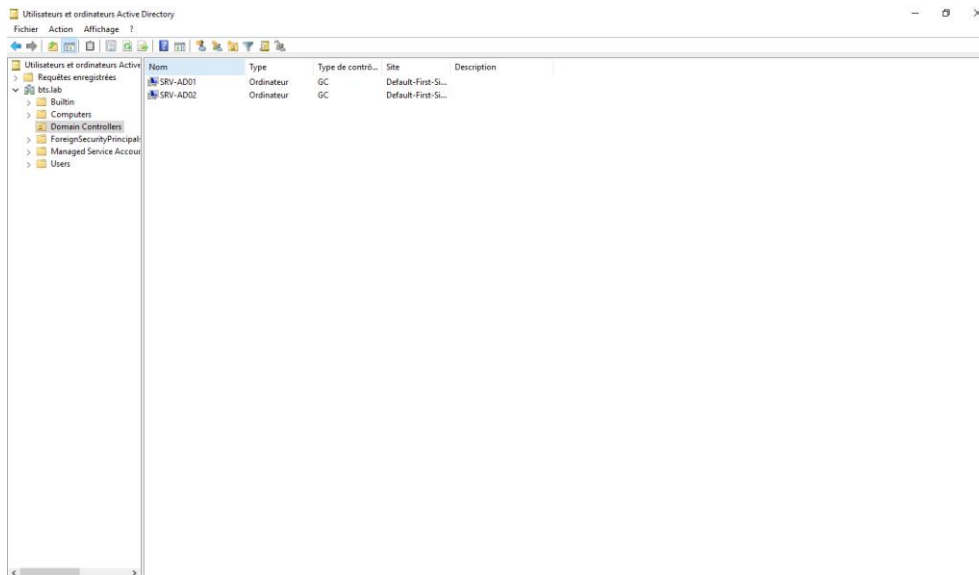
La rétrogradation est en cours et prend quelques minutes



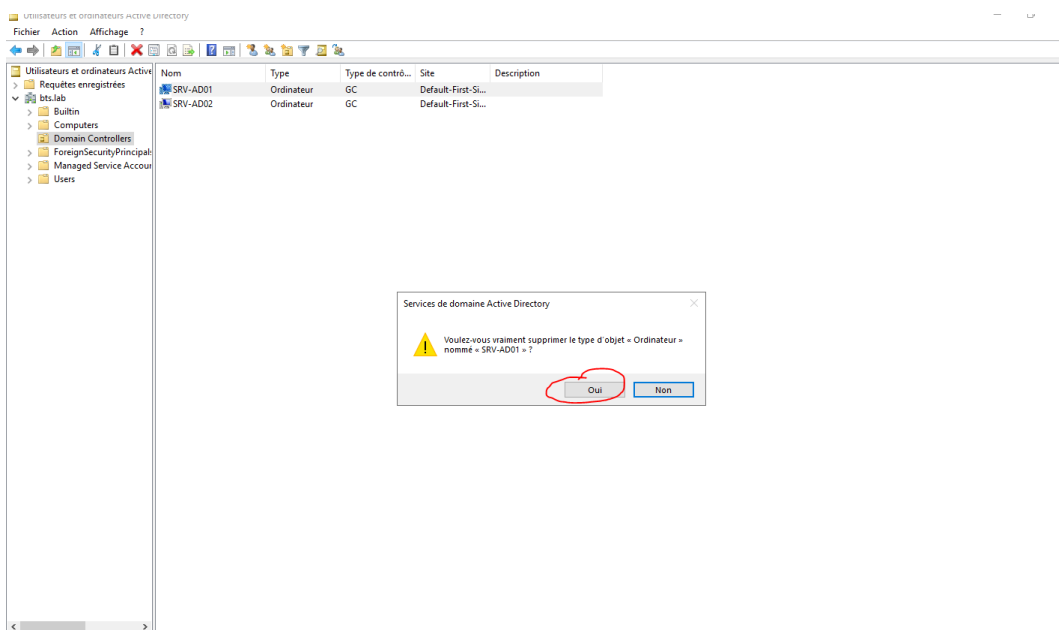
Après la suppression des rôles (AD DS), l'ordinateur va redémarrer et sera sorti du domaine automatiquement.

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



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 * »

```
PS C:\Users\Administrateur.BTS> Get-ADDomainController -Filter *

ComputerObjectDN      : CN=SRV-AD02,OU=Domain Controllers,DC=bts,DC=lab
DefaultPartition      : DC=bts,DC=lab
Domain                : bts.lab
Enabled               : True
Forest                : bts.lab
HostName              : SRV-AD02.bts.lab
InvocationId          : d21ef468-2bc8-40b4-b261-8db205f2db71
IPv4Address           : 192.168.1.15
IPv6Address           :
IsGlobalCatalog       : True
IsReadOnly            : False
LdapPort              : 389
Name                  : SRV-AD02
NTDSSettingsObjectDN  : CN=NTDS Settings,CN=SRV-AD02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configurati
on,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, CN=Configuration,DC=bts,DC=lab...}
ServerObjectDN       : CN=SRV-AD02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=bts,DC=lab
ServerObjectGuid      : 385f0519-61f3-406b-a5f4-4dc37083010f
Site                  : Default-First-Site-Name
SslPort              : 636

PS C:\Users\Administrateur.BTS>
```

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) :

- 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

Erreur : « La base de données de sécurité du serveur n'a pas de compte d'ordinateur. »

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

Impact : « L'ancien contrôleur de domaine restait dans Active Directory. »

Solution : 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.