PortailSIO
Réseau • Sysadmin • Cyber • DevOps

TUTORIEL

WINDOWS 2025

Mettre en place la réplication AD DS



SOMMAIRE

1. CONFIGURATION DE L'ADRESSAGE IP DU SECOND SERVEUR
2. RENOMMER LE SERVEUR ET L'INTÉGRER AU DOMAINE
3. INSTALLATION DU RÔLE AD DS
4. PROMOTION DU SERVEUR EN CONTRÔLEUR DE DOMAINE
5. VÉRIFICATION DE LA RÉPLICATION
6. TEST DE LA TOLÉRANCE DE PANNE

© PortailSIO - 11/2026

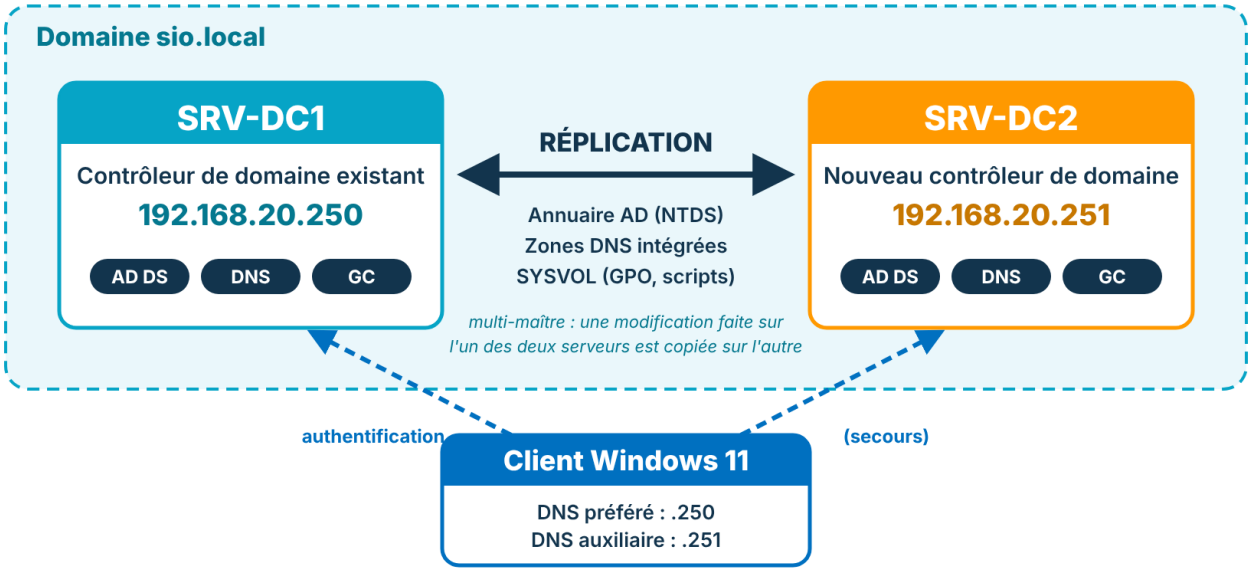
CONFIRME
DIFFICULTE

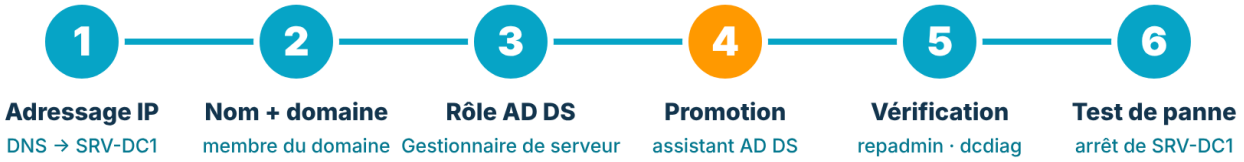
CC BY NC
UTILISATION COMMERCIALE INTERDITE

Ce tutoriel a été réalisé avec l'hyperviseur © Proxmox VE. Il peut être réalisé dans un environnement de virtualisation personnel à l'aide des logiciels © VirtualBox ou © VMware Player et **suppose que vous avez réalisé le tutoriel 2** (installer et configurer le rôle « AD/DS »).

Dans le tutoriel 2, nous avons créé un domaine Active Directory avec **un seul contrôleur de domaine**. Si ce serveur tombe en panne, plus aucun utilisateur ne peut ouvrir de session sur le domaine, la résolution DNS interne ne répond plus et les ressources partagées deviennent inaccessibles : c'est ce que l'on appelle un « point de défaillance unique ».

Pour y remédier, nous allons ajouter un **second contrôleur de domaine** puis vérifier que la **réplication** fonctionne : chaque contrôleur de domaine possède une copie complète de l'annuaire et les deux serveurs se synchronisent automatiquement, dans les deux sens (on parle de réplication « multi-maître »).





Remarque importante :

Un contrôleur de domaine supplémentaire ne crée pas un nouveau domaine : il **rejoint le domaine existant**. **Dans l'assistant, il faudra donc choisir « Ajouter un contrôleur de domaine à un domaine existant » et surtout pas « Ajouter une nouvelle forêt »**.

Dans le cadre de ce tutoriel, nous utilisons deux serveurs Windows Server 2025 dont voici les caractéristiques :

	SRV-DC1 (existant)	SRV-DC2 (à créer)
Rôle	Premier contrôleur de domaine	Contrôleur de domaine supplémentaire
Système	Windows Server 2025	Windows Server 2025 (avec interface graphique)
Adresse IP	192.168.20.250 /24	192.168.20.251 /24
Passerelle	192.168.20.254	192.168.20.254
Domaine	sio.local	sio.local

Pour la machine virtuelle SRV-DC2, prévoyez :

- 2 processeurs virtuels et 4 Go de mémoire vive (8 Go vivement recommandé)
- Un disque système de 60 Go (suffisant pour ce labo informatique)
- Une version **Windows Server 2025** 64 bits (Standard ou Datacenter) installée avec l'interface graphique

Les adresses IP et le nom de domaine **sio.local** sont donnés à titre d'exemple : adaptez-les à votre plan d'adressage et au domaine créé dans le tutoriel 2.

1 – CONFIGURATION DE L'ADRESSAGE IP DU SECOND SERVEUR

Un contrôleur de domaine doit disposer d'une **adresse IP fixe**. Une fois SRV-DC2 installé, ouvrez une session avec le compte « Administrateur » local puis effectuez les manipulations suivantes :

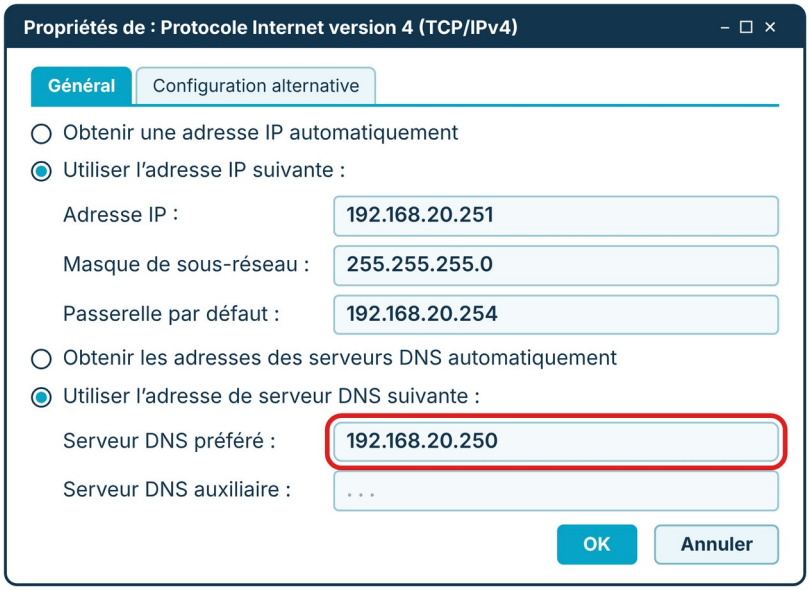
- Ouvrez le « **Gestionnaire de serveur** » et cliquez, dans le volet de gauche, sur « **Serveur local** »
- Dans le volet de droite, cliquez sur le lien situé à droite de « **Ethernet** » (adresse IPv4 attribuée par DHCP) : la fenêtre « Connexions réseau » s'affiche
- Faites un clic droit sur l'icône « **Ethernet** » et cliquez « **Propriétés** » :



- Double-cliquez sur « **Protocole Internet version 4 (TCP/IPv4)** »

- Cochez « **Utiliser l'adresse IP suivante** » et complétez les champs ; **saisissez, comme serveur DNS préféré, l'adresse IP de SRV-DC1** puis cliquez 2 fois le bouton « **OK** » pour valider :

Champ	Valeur à saisir
Adresse IP	192.168.20.251
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	192.168.20.254
Serveur DNS préféré	192.168.20.250 (adresse IP de SRV-DC1)
Serveur DNS auxiliaire	(laisser vide pour le moment)



Le serveur DNS préféré doit pointer vers SRV-DC1, qui héberge déjà la zone DNS du domaine. Sans cela, SRV-DC2 ne pourra pas retrouver le domaine.

Remarque importante :

SRV-DC2 doit utiliser l'adresse IP de SRV-DC1 comme serveur DNS préféré, sinon il sera incapable de trouver le domaine et l'intégration échouera (message « contrôleur de domaine introuvable »).

Vous pouvez aussi réaliser cette configuration en ligne de commande (PowerShell exécuté en tant qu'administrateur) :

```
POWERSHELL
Get-NetAdapter
Set-NetIPInterface -InterfaceAlias "Ethernet" -Dhcp Disabled
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.20.251 -PrefixLength 24 -
DefaultGateway 192.168.20.254
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 192.168.20.250
```

Vérifiez que SRV-DC2 communique bien avec SRV-DC1 :

```
INVITE DE COMMANDES
ping 192.168.20.250
nslookup sio.local
```

✔ **POINT DE CONTRÔLE**

- Le **ping** reçoit des réponses de 192.168.20.250
- **nslookup sio.local** renvoie l'adresse 192.168.20.250 (réponse du DNS de SRV-DC1)

2 – RENOMMER LE SERVEUR ET L'INTÉGRER AU DOMAINE

Lors de l'installation, Windows a attribué un nom aléatoire au serveur (de type WIN-XXXXXXXX). Pour faciliter la gestion de l'infrastructure, nous allons le renommer **SRV-DC2** puis l'intégrer au domaine **sio.local**.

Renommer le serveur :

- Dans le « **Gestionnaire de serveur** », cliquez sur « **Serveur local** » puis cliquez sur le nom de l'ordinateur (lien « **Nom de l'ordinateur** »)
- Dans l'onglet « **Nom de l'ordinateur** », cliquez le bouton « **Modifier…** »
- Saisissez `SRV-DC2` comme nouveau nom et cliquez le bouton « **OK** »
- Cliquez le bouton « **Redémarrer maintenant** » pour valider le changement de nom :



Renommer le serveur avant de l'intégrer au domaine évite de devoir modifier ensuite un compte ordinateur déjà inscrit dans l'annuaire.

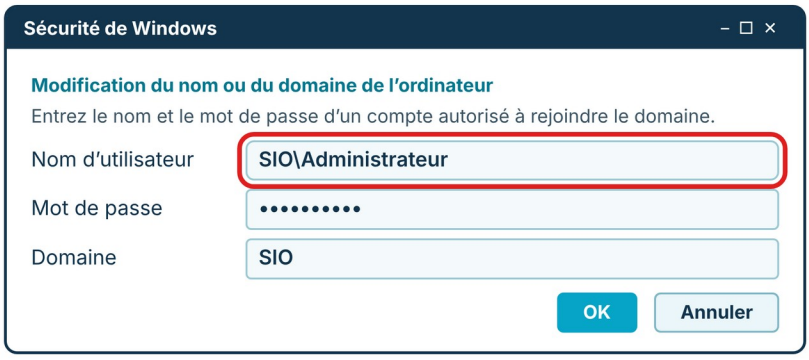
Intégrer le serveur au domaine (une fois le serveur redémarré) :

- Dans le « **Gestionnaire de serveur** », cliquez sur « **Serveur local** » puis sur le lien « **Groupe de travail** »
- Cliquez le bouton « **Modifier…** »
- Une fenêtre s'affiche ; cliquez, dans la rubrique « **Membre d'un** », sur le bouton « **Domaine** », saisissez le nom complet de votre domaine (`sio.local`) et cliquez le bouton « **OK** » :



On indique ici le nom complet du domaine créé dans le tutoriel 2. Si le message « contrôleur de domaine introuvable » s'affiche, vérifiez l'adressage IP et le DNS préféré (étape 1).

- Si le contrôleur de domaine est atteint, une fenêtre d'authentification s'affiche ; complétez-la avec l'identifiant du compte administrateur du domaine (`SIO\Administrateur`) :



Pour l'intégration au domaine, utilisez un compte administrateur du domaine (compte « Administrateur » créé sur SRV-DC1).

- Patientez quelques instants ; si vos paramètres ont été correctement renseignés, le message « **Bienvenue dans le domaine sio.local** » s'affiche (cliquez le bouton « **OK** »)
- Cliquez à nouveau le bouton « **OK** », puis le bouton « **Fermer** » et faites redémarrer le serveur en cliquant « **Redémarrer maintenant** »

Les deux serveurs doivent avoir la même date et la même heure : un écart de plus de 5 minutes provoque un échec de l'authentification (protocole Kerberos). Vérifiez l'heure de SRV-DC2 avant l'intégration.

Au redémarrage, cliquez sur « **Autre utilisateur** » et ouvrez une session avec le compte administrateur du domaine (`SIO\Administrateur`). Cette connexion sera nécessaire pour la suite du tutoriel.

Les deux opérations peuvent également être réalisées en PowerShell :

```powershell
Rename-Computer -NewName "SRV-DC2" -Restart
# après le redémarrage :
Add-Computer -DomainName "sio.local" -Credential (Get-Credential) -Restart
```

✔ **POINT DE CONTRÔLE**

- Dans « Gestionnaire de serveur » > « Serveur local », le champ « **Domaine** » affiche sio.local
- Sur SRV-DC1, dans « Utilisateurs et ordinateurs Active Directory », le conteneur « **Computers** » contient le compte ordinateur SRV-DC2

3 – INSTALLATION DU RÔLE AD DS

Le rôle « **Services AD DS** » installe les fichiers nécessaires pour transformer SRV-DC2 en contrôleur de domaine (même démarche que dans le tutoriel 2). Effectuez les manipulations suivantes :

- Dans le « **Gestionnaire de serveur** », cliquez sur le menu « **Gérer** » puis « **Ajouter des rôles et fonctionnalités** »
- Cliquez « **Suivant** » sur la page « Avant de commencer », sélectionnez « **Installation basée sur un rôle ou une fonctionnalité** » puis cliquez « **Suivant** »
- Vérifiez que le serveur SRV-DC2 est sélectionné et cliquez « **Suivant** »

- Cochez le rôle « **Services AD DS** », cliquez « **Ajouter des fonctionnalités** » dans la fenêtre qui s'affiche puis « **Suivant** » :



Cochez uniquement « Services AD DS ». Le rôle « Serveur DNS » sera ajouté automatiquement lors de la promotion (étape 4).

- Cliquez « **Suivant** » sur les pages « Fonctionnalités » et « AD DS », puis cliquez le bouton « **Installer** »
- Patientez pendant l'installation puis cliquez le bouton « **Fermer** »

Vous pouvez aussi installer le rôle en PowerShell :

```
POWERSHELL
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```

✔ **POINT DE CONTRÔLE**

- Un **drapeau jaune** (notifications) apparaît en haut du Gestionnaire de serveur : le rôle est installé mais le serveur n'est pas encore un contrôleur de domaine

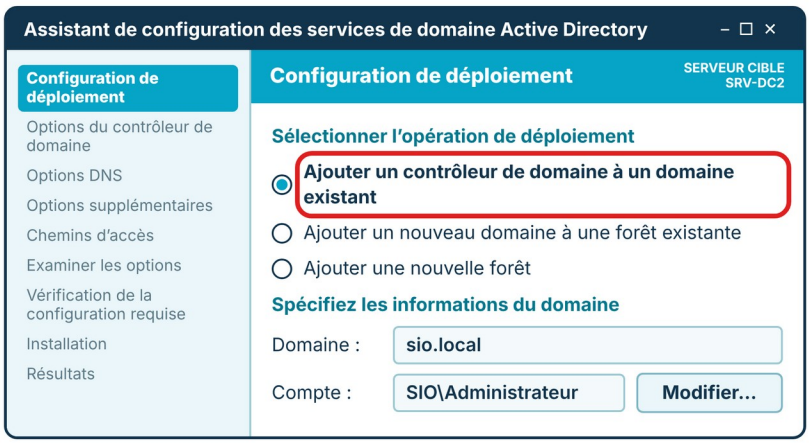
4 – PROMOTION DU SERVEUR EN CONTRÔLEUR DE DOMAINE

C'est l'étape clé du tutoriel : SRV-DC2 va recevoir une copie complète de l'annuaire depuis SRV-DC1 et devenir un contrôleur de domaine à part entière.

- Cliquez sur le drapeau jaune « **Notifications** » puis sur le lien « **Promouvoir ce serveur en contrôleur de domaine** » :

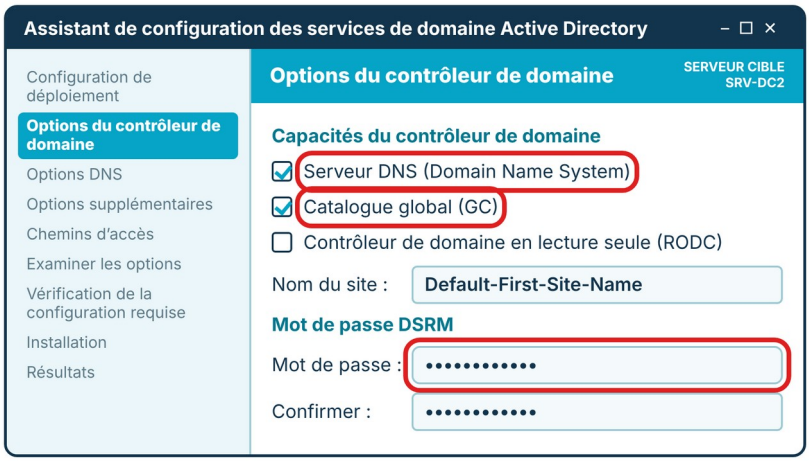


- Page « **Configuration de déploiement** » : sélectionnez « **Ajouter un contrôleur de domaine à un domaine existant** », saisissez le nom du domaine (`sio.local`) puis cliquez « **Modifier…** » pour fournir le compte `SIO\Administrateur` et son mot de passe. Cliquez « **Suivant** » :



Choisissez bien la première option : les deux autres créeraient un nouveau domaine ou une nouvelle forêt.

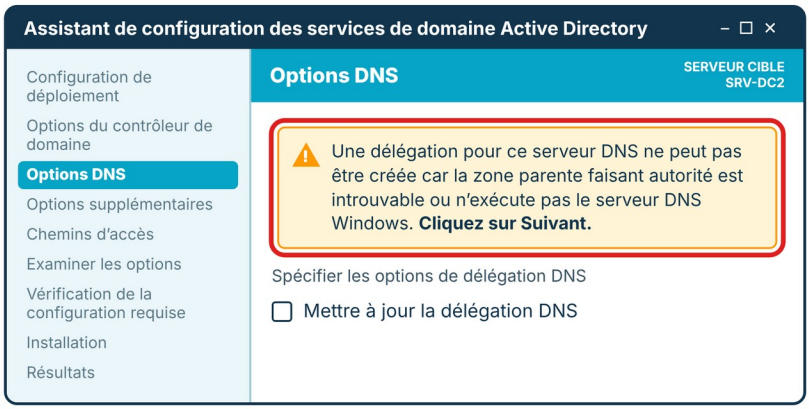
- Page « **Options du contrôleur de domaine** » : laissez cochés « **Serveur DNS (Domain Name System)** » et « **Catalogue global (GC)** », ne cochez pas « Contrôleur de domaine en lecture seule (RODC) », conservez le site « Default-First-Site-Name » et saisissez le **mot de passe DSRM** :



Le mot de passe DSRM (mode de restauration des services d'annuaire) permet de réparer l'annuaire en cas de problème grave. Notez-le et conservez-le précieusement.

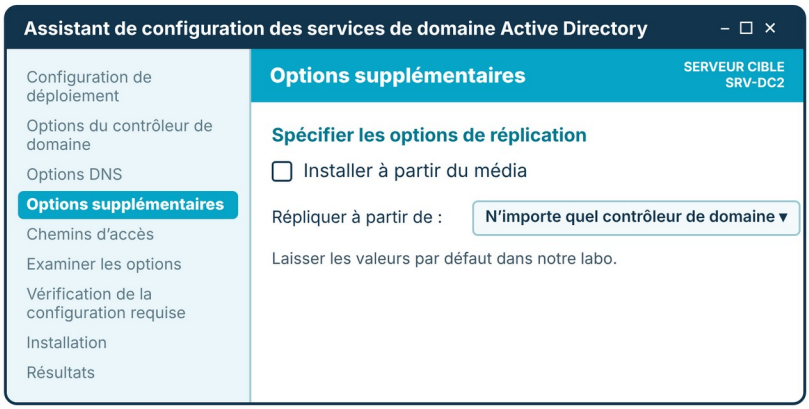
Le catalogue global (GC) permet aux utilisateurs d'ouvrir une session même si SRV-DC1 est indisponible : c'est pourquoi on le conserve sur SRV-DC2.

- Page « **Options DNS** » : un avertissement sur la délégation DNS s'affiche, cliquez « **Suivant** » :



Cet avertissement est normal avec un domaine interne de type « .local » : il n'existe pas de zone DNS parente. Il n'empêche pas la suite de l'installation.

- Page « **Options supplémentaires** » : laissez « **Répliquer à partir de : N'importe quel contrôleur de domaine** » puis cliquez « **Suivant** »
- Page « **Chemins d'accès** » : conservez les dossiers proposés (NTDS et SYSVOL) et cliquez « **Suivant** »



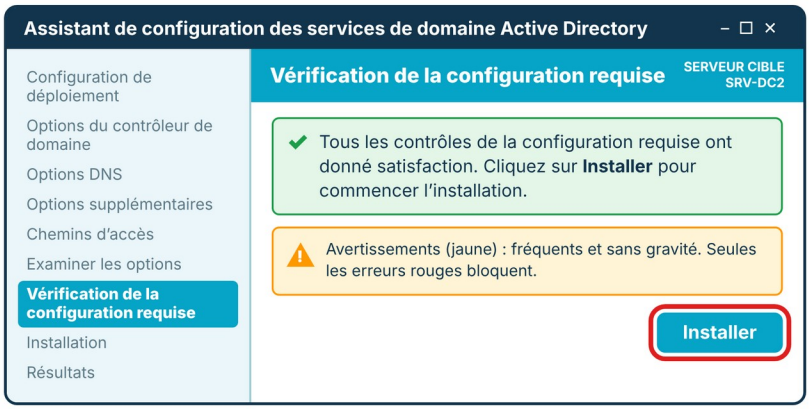
Dans un grand domaine, l'option « Installer à partir du média » (IFM) évite de transférer tout l'annuaire par le réseau. Elle est inutile dans notre labo.

- Page « **Examiner les options** » : vérifiez le récapitulatif puis cliquez « **Suivant** » (le bouton « **Afficher le script** » permet de visualiser la commande PowerShell équivalente) :



« Afficher le script » génère la commande PowerShell correspondant aux choix effectués : pratique pour automatiser ou comprendre ce que fait l'assistant.

- Page « **Vérification de la configuration requise** » : patientez puis cliquez le bouton « **Installer** » :



Des avertissements (en jaune) sont fréquents et sans gravité. Seules les erreurs (en rouge) bloquent l'installation.

Patientez pendant l'installation. À la fin, le serveur **redémarre automatiquement** (un message vous prévient que vous allez être déconnecté). Au redémarrage, l'écran d'authentification affiche désormais le nom du domaine : ouvrez une session avec le compte `SIO\Administrateur`.

La première ouverture de session peut durer plusieurs minutes. Patientez : le dossier SYSVOL (stratégies de groupe et scripts) est répliqué juste après le redémarrage.

Voici la commande PowerShell équivalente à l'assistant :

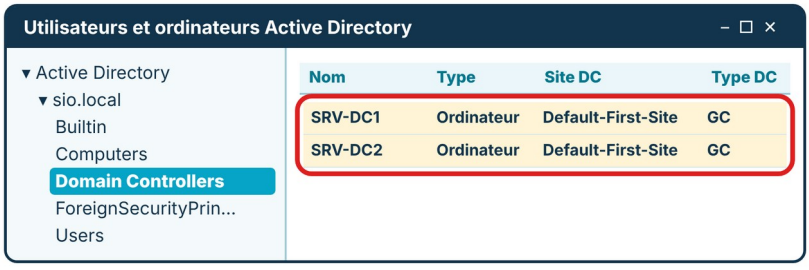
```powershell
Install-ADDSDomainController `
  -DomainName "sio.local" `
  -Credential (Get-Credential "SIO\Administrateur") `
  -InstallDns:$true `
  -SiteName "Default-First-Site-Name" `
  -SafeModeAdministratorPassword (Read-Host -AsSecureString "Mot de passe DSRM") `
  -Force:$true
```

5 – VÉRIFICATION DE LA RÉPLICATION

Une fois SRV-DC2 redémarré et la session ouverte, effectuez les vérifications suivantes (graphiquement puis en ligne de commande).

A – Console « Utilisateurs et ordinateurs Active Directory »

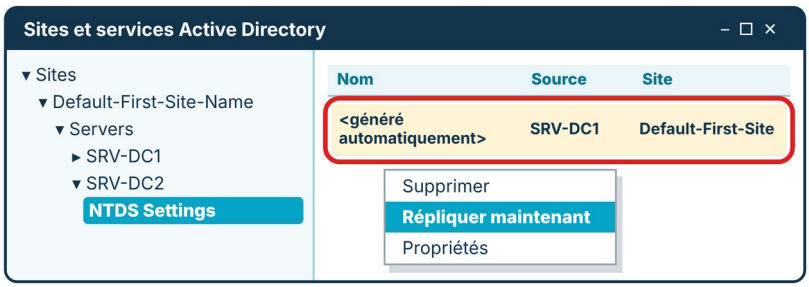
- Dans le « **Gestionnaire de serveur** », cliquez le menu « **Outils** » puis « **Utilisateurs et ordinateurs Active Directory** »
- Développez votre domaine et cliquez sur l'unité d'organisation « **Domain Controllers** » :



Les deux serveurs apparaissent dans l'unité d'organisation « Domain Controllers » : SRV-DC2 est bien devenu un contrôleur de domaine.

B – Console « Sites et services Active Directory »

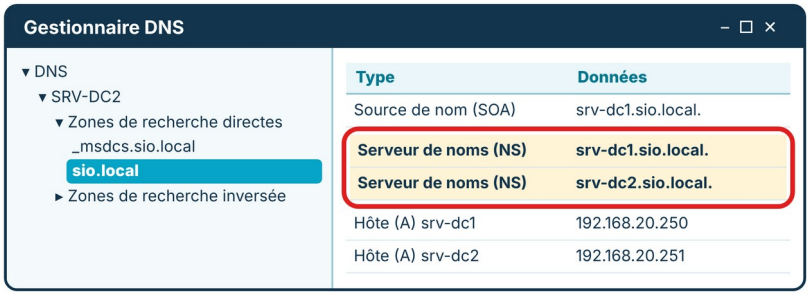
- Cliquez le menu « **Outils** » puis « **Sites et services Active Directory** »
- Développez « **Sites** » > « **Default-First-Site-Name** » > « **Servers** » > « **SRV-DC2** » > « **NTDS Settings** » : une connexion venant de SRV-DC1 a été créée automatiquement
- Faites un clic droit sur cette connexion et cliquez « **Répliquer maintenant** » :



La connexion est créée automatiquement par le KCC. Dans un même site, la réplication se déclenche en quelques secondes après chaque modification ; entre deux sites, l'intervalle par défaut est de 180 minutes.

C – Console « DNS »

- Cliquez le menu « **Outils** » puis « **DNS** » et développez « **Zones de recherche directes** » > « **sio.local** »
- Vérifiez la présence des enregistrements « **Serveur de noms (NS)** » et « **Hôte (A)** » des deux serveurs :



La zone DNS est « intégrée à Active Directory » : elle est répliquée avec l'annuaire, il n'y a rien à copier manuellement sur SRV-DC2.

D – En ligne de commande

Ouvrez PowerShell en tant qu'administrateur sur SRV-DC2 et exécutez les commandes suivantes :

```powershell
Get-ADDomainController -Filter * | Select-Object Name, IPv4Address, Site, IsGlobalCatalog
repadmin /replsummary
repadmin /showrepl
dcdiag /test:replications
net share
```

Commande	Ce qu'il faut observer
Get-ADDomainController	Les deux serveurs sont listés, avec « IsGlobalCatalog » à True
repadmin /replsummary	Aucun échec de réplication (0) et aucune erreur
repadmin /showrepl	Pour chaque partition (Domain, Configuration, Schema...), la dernière tentative de réplication est réussie
dcdiag /test:replications	Le test « Replications » est réussi (passed)
net share	Les partages « NETLOGON » et « SYSVOL » sont présents (SYSVOL répliqué)

E – Test pratique de réplication

- Sur **SRV-DC1**, créez un utilisateur de test : clic droit sur « **Users** » > « **Nouveau** » > « **Utilisateur** » (nom d'ouverture de session : `test.replication`)
- Forcez la réplication si vous ne souhaitez pas attendre (sur SRV-DC1) :

```
POWERSHELL
repadmin /syncall /AdeP
```

- Sur **SRV-DC2**, recherchez l'utilisateur en interrogeant explicitement ce serveur :

```
POWERSHELL
Get-ADUser -Identity test.replication -Server SRV-DC2
```

- L'utilisateur est retrouvé : la réplication fonctionne. Supprimez ensuite l'utilisateur de test (clic droit > « **Supprimer** »)

✔️ **POINT DE CONTRÔLE**

- Les deux contrôleurs de domaine sont visibles dans « Domain Controllers »
- **repadmin /replsummary** n'indique aucun échec
- L'utilisateur créé sur SRV-DC1 est retrouvé sur SRV-DC2

6 – TEST DE LA TOLÉRANCE DE PANNE

A – Déclarer les deux serveurs DNS

SRV-DC2 étant maintenant aussi serveur DNS, chaque machine du domaine doit connaître les deux serveurs. Bonne pratique : sur chaque contrôleur de domaine, le DNS préféré est **l'autre** contrôleur de domaine et le DNS auxiliaire est **lui-même**.

Machine	DNS préféré	DNS auxiliaire
SRV-DC1	192.168.20.251	192.168.20.250
SRV-DC2	192.168.20.250	192.168.20.251
Client Windows 11	192.168.20.250	192.168.20.251

```
POWERSHELL
# sur SRV-DC1
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses
192.168.20.251,192.168.20.250
# sur SRV-DC2
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses
192.168.20.250,192.168.20.251
```

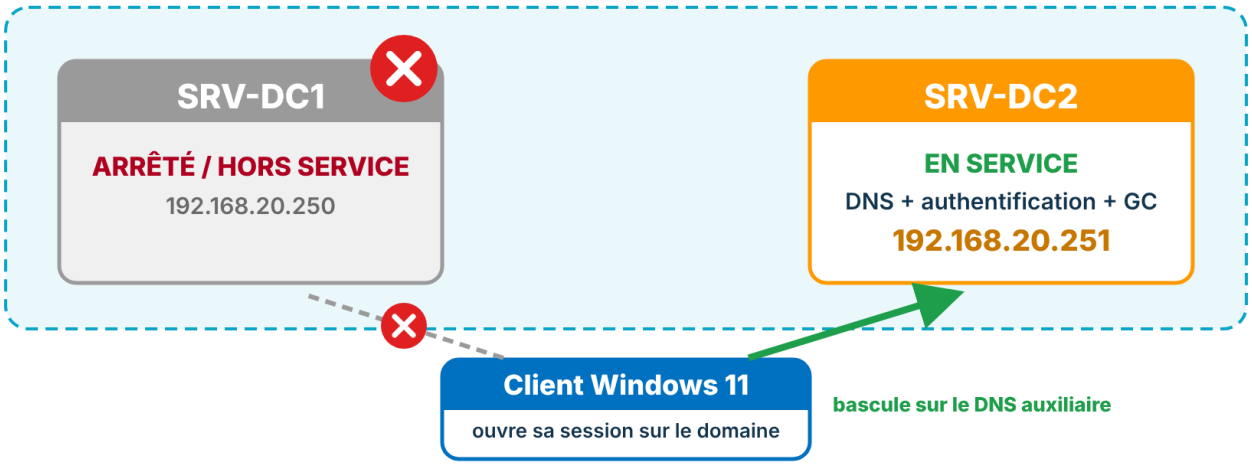
Cette configuration évite qu'un contrôleur de domaine ne s'« isole » en n'interrogeant que lui-même. Pour les postes clients, la configuration manuelle est décrite dans le tutoriel 4 ; si vous utilisez un serveur DHCP, indiquez simplement les deux serveurs DNS dans l'option 006.

B – Simuler la panne de SRV-DC1

- Arrêtez proprement la machine virtuelle SRV-DC1 depuis l'interface de Proxmox VE (ou depuis Windows : « **Démarrer** » > « **Arrêter** »)

- Sur le **client Windows 11**, fermez la session puis ouvrez-la de nouveau avec un compte utilisateur du domaine
- Ouvrez une invite de commandes et exécutez :

INVITE DE COMMANDES (CLIENT WINDOWS 11)
```
echo %LOGONSERVER%
nltest /dsgetdc:sio.local
nslookup sio.local
```



✔ **POINT DE CONTRÔLE**
- La session s'ouvre malgré l'arrêt de SRV-DC1
- **%LOGONSERVER%** et **nltest** affichent **SRV-DC2** (si %LOGONSERVER% affiche le nom du poste lui-même, la session a été ouverte avec des informations d'identification en cache : vérifiez le DNS auxiliaire)
- **nslookup** peut afficher un délai d'attente avant de répondre : le client bascule sur son DNS auxiliaire

C – Redémarrer SRV-DC1 et vérifier le rattrapage

- Pendant que SRV-DC1 est encore arrêté, créez un utilisateur sur **SRV-DC2** (par exemple `test.panne`)
- Redémarrez SRV-DC1, patientez quelques minutes puis exécutez, sur SRV-DC1 :

POWERSHELL
```
repadmin /replsummary
Get-ADUser -Identity test.panne
```

- L'utilisateur créé pendant la panne est présent sur SRV-DC1 : la réplication a rattrapé le retard. Supprimez-le ensuite

Remarque importante :

Les **rôles FSMO** (maîtres d'opérations) restent portés par SRV-DC1 tant qu'on ne les transfère pas. **Si SRV-DC1 est définitivement perdu, il faudra transférer ou saisir ces rôles sur SRV-DC2**. Pour savoir quel serveur les détient :

INVITE DE COMMANDES
```
netdom query fsmo
```

Pour faire de SRV-DC2 le détenteur des cinq rôles (à réaliser uniquement si vous le souhaitez, par exemple avant de décommissionner SRV-DC1) :

```powershell
Move-ADDirectoryServerOperationMasterRole -Identity "SRV-DC2" -OperationMasterRole
SchemaMaster,DomainNamingMaster,PDCEmulator,RIDMaster,InfrastructureMaster
```

Notre domaine dispose maintenant de **deux contrôleurs de domaine qui se répliquent** : la panne d'un seul serveur n'empêche plus les utilisateurs d'ouvrir leur session et d'accéder à leurs ressources.

Pense-bête : commandes de diagnostic Active Directory

Commande	Utilité
repadmin /replsummary	Résumé de la santé de la réplication de tous les contrôleurs de domaine
repadmin /showrepl	Détail de la réplication, partition par partition
repadmin /syncall /AdeP	Force la réplication vers tous les partenaires
dcdiag /test:replications	Teste la réplication du contrôleur de domaine local
dcdiag /test:dns	Teste la configuration DNS du contrôleur de domaine
nltest /dsgetdc:sio.local	Affiche le contrôleur de domaine utilisé par la machine
netdom query fsmo	Affiche les détenteurs des rôles FSMO
Get-ADDomainController -Filter *	Liste les contrôleurs de domaine du domaine