

TP Active Directory

Création du domaine enfant tssr1.sete.local

Objectif

Créer un domaine enfant nommé tssr1.sete.local, intégré à la forêt Active Directory sete.local, en réseau VPN local via Tailscale.

Définitions de base

Notion	Définition débutant
Forêt Active Directory	C'est le plus grand ensemble logique dans AD. Elle regroupe plusieurs domaines. Ici, la forêt est sete.local .
Domaine enfant	C'est un domaine qui dépend d'un autre, comme une sous-partie. Ici, c'est tssr1.sete.local , enfant de sete.local.
Contrôleur de domaine (DC)	Serveur qui gère l'authentification et les ressources du domaine.
DNS (Domain Name System)	Service qui traduit les noms des machines (comme sete.local) en adresses IP.
Tailscale	VPN qui connecte plusieurs machines entre elles, comme si elles étaient sur le même réseau local.
Promotion AD DS	Action de transformer un serveur Windows normal en contrôleur de domaine .
DSRM (Directory Services Restore Mode)	Mode spécial de récupération d'Active Directory, protégé par un mot de passe à noter.

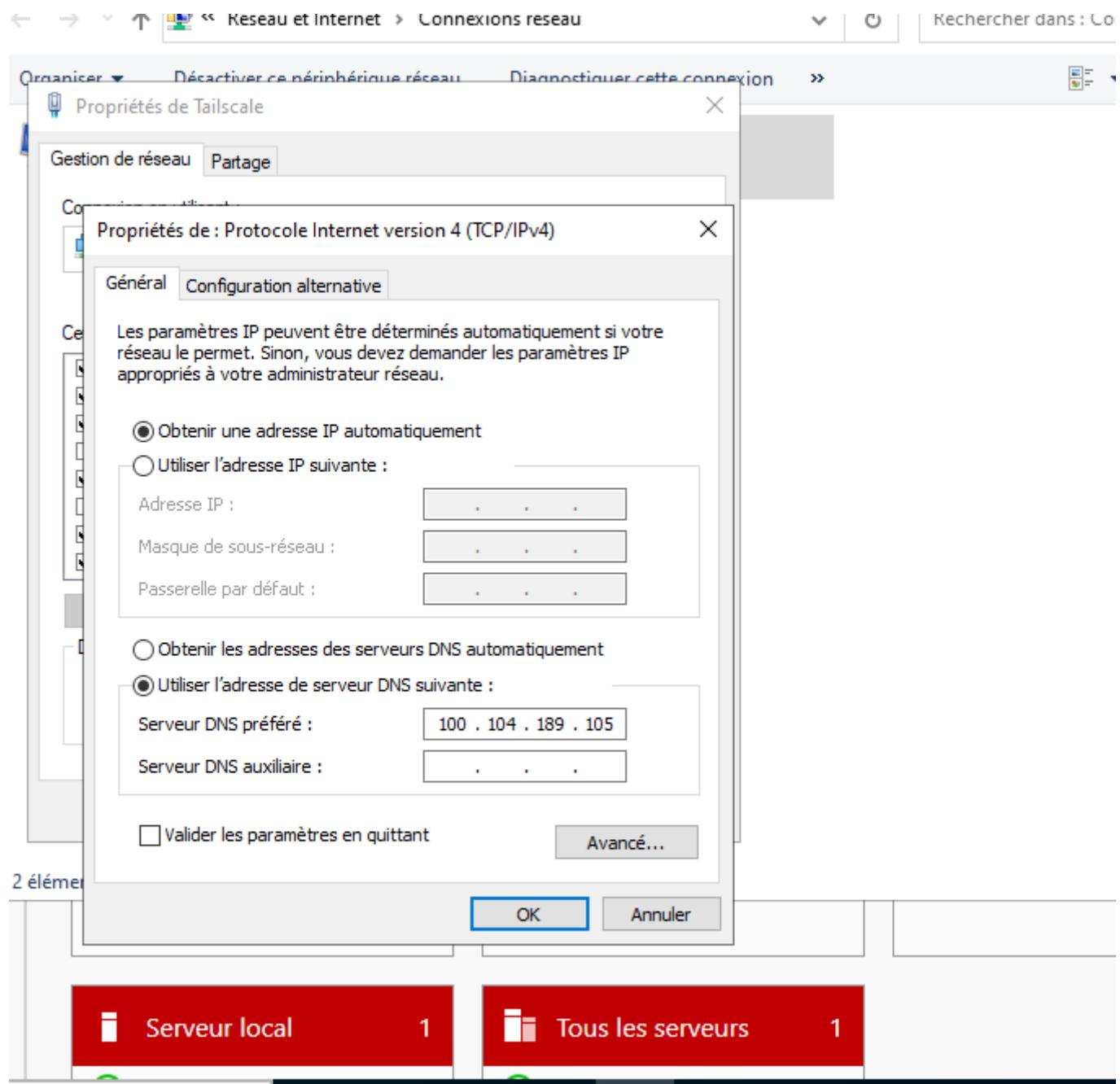
Mon environnement

Machine	Domaine	Rôle	IP Tailscale
DC1 (Chafik)	sete.local	Forêt racine	100.104.189.105
DC2 (moi)	tssr1.sete.local	Domaine enfant	100.71.113.76
DC3 (Yousef)	dev.sete.local	Domaine enfant	100.68.151.23

Galère DNS au démarrage des VM des domaines enfants

À chaque redémarrage de nos VM, il fallait reconfigurer la carte réseau Tailscale dans Windows, car l'adresse IP DNS ne restait pas enregistrée.

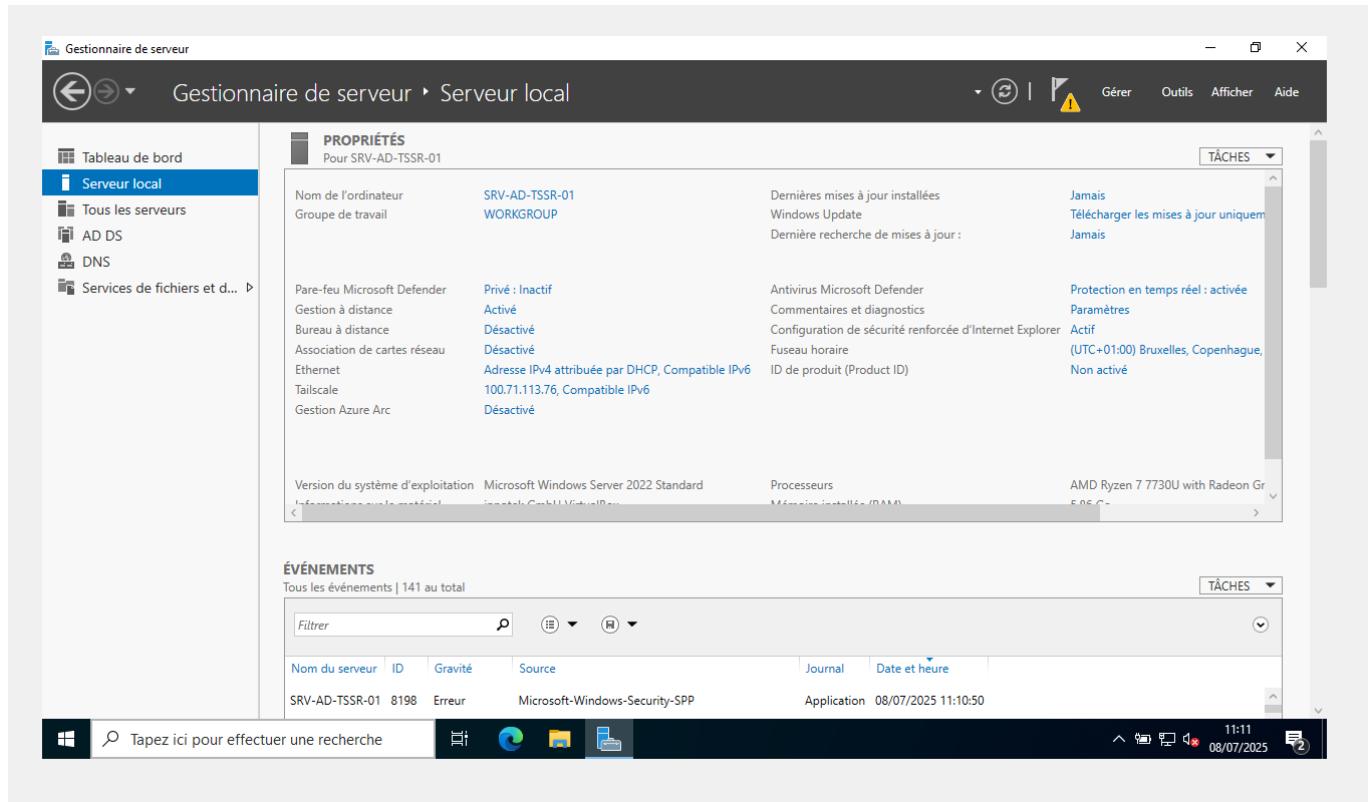
Il fallait remettre 100.104.189.105 (IP Tailscale du DC1 sete.local) comme DNS préféré sur ma carte Tailscale.



Étapes de la configuration

Étape 1 : Préparer mon serveur Windows

- J'ai renommé ma machine en SRV-TSSR1.
- Je l'ai mise à jour.
- J'ai vérifié qu'elle ping bien le serveur DC1 (sete.local).
- J'ai récupéré les identifiants admin de la forêt (Administrator / mot de passe).



Étape 2 – Installer le rôle AD DS

Dans Gestionnaire de serveur, j'ai installé Services de domaine Active Directory (AD DS).

Pas de redémarrage requis ici.

Étape 3 – (**Échec**) Première tentative avec tssr.sete.local

Lors de ma première promotion, j'ai voulu créer le domaine enfant tssr.sete.local. La promotion a planté au milieu du processus :

- Le DNS n'était pas bien configuré.

Résultat : machine en vrac, impossible de finaliser la promotion.

Solution choisie : plutôt que réparer, j'ai recommencé à zéro, avec un nouveau nom de domaine enfant → tssr1.sete.local (comme ça pas de conflit).

Étape 4 – Promouvoir le serveur en domaine enfant tssr1.sete.local

J'ai relancé l'assistant de promotion AD DS.

Cette fois-ci, j'ai bien configuré :

- Type : Domaine enfant
- Domaine parent : sete.local
- Nom enfant : tssr1
- Domaine complet : tssr1.sete.local

J'ai mis un mot de passe DSRM que j'ai noté.

Problème DNS rencontré

Le serveur sete.local (DC1) avait :

DNS Tailscale : 100.104.189.105 ✓ (normal)

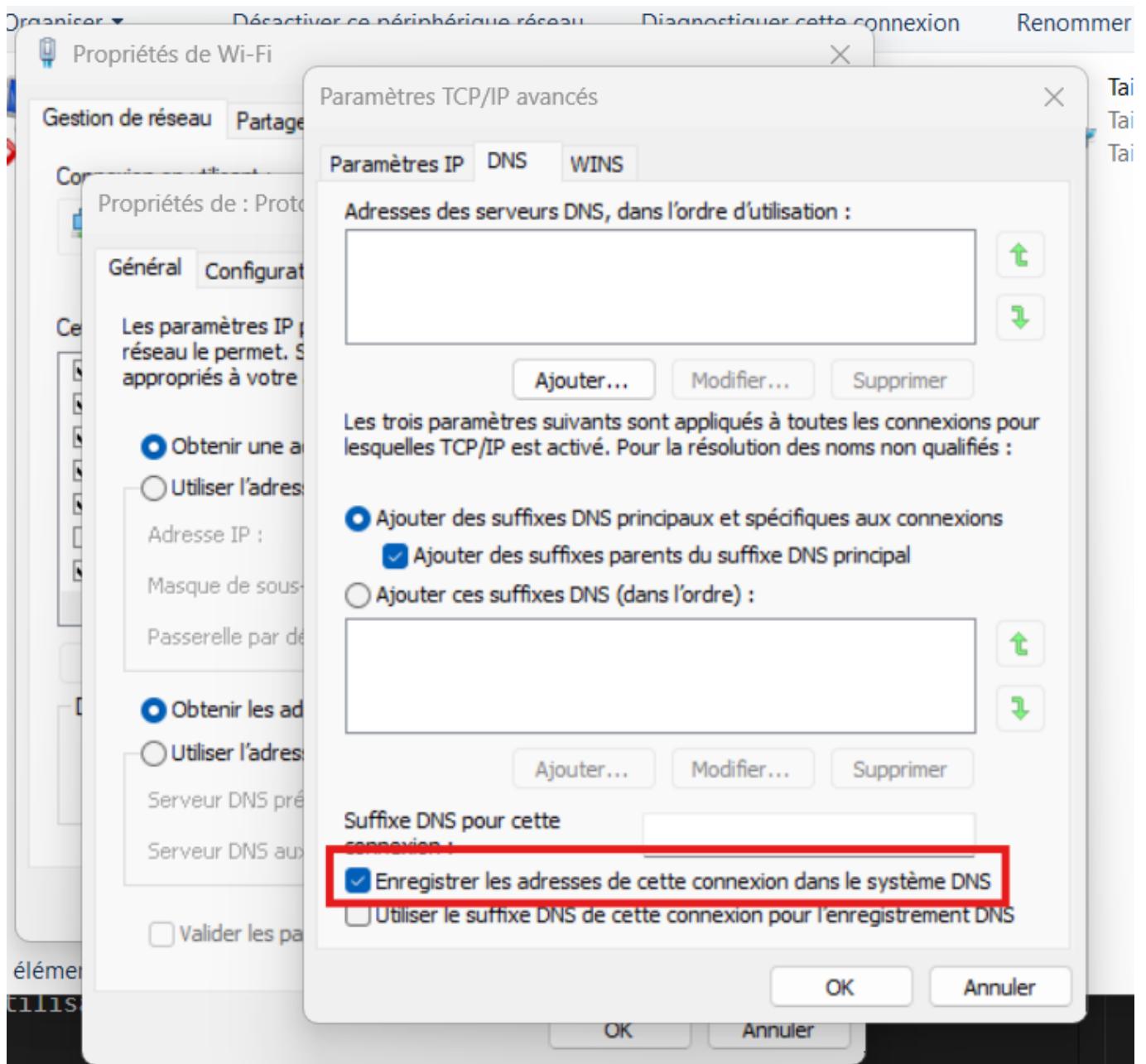
MAIS aussi un DNS en 192.x.x.x ✗ (de sa carte réseau locale Windows).

Résultat : quand mon serveur tssr1 essayait de le joindre, il tombait parfois sur cette IP 192.x.x.x inaccessible pour moi.

Solution trouvée :

Sur sete.local, Chafik a désactivé l'enregistrement DNS automatique de la carte réseau locale.

Propriétés de la carte réseau locale > Onglet DNS > Déscocher "Enregistrer cette connexion dans DNS".



Et là, tout passait uniquement par Tailscale.

Étape 5 – Vérifications et redémarrage

Après promotion, mon serveur a redémarré.

Je me suis connectée avec le compte tssr1\Administrateur.

En allant sur Utilisateurs et ordinateurs Active Directory, j'ai accès à la gestion centralisée des comptes utilisateurs, des groupes, des ordinateurs et des unités organisationnelles (OU) au sein du domaine, ce qui me permet de créer, modifier, supprimer et organiser ces objets pour administrer efficacement l'environnement réseau.

The screenshot shows the Windows Server Management Console with the 'Utilisateurs et ordinateurs Active Directory' snap-in open. The left pane displays the domain structure under 'tssr1.sete.local'. The right pane lists various users and groups with their type and descriptions:

Nom	Type	Description
Administrateur	Utilisateur	Compte d'utilisateur d'a...
Administrateurs clés	Groupe de séc...	Les membres de ce grou...
Admins du domaine	Groupe de séc...	Administrateur désigné...
Contrôleurs de domaine	Groupe de séc...	Tous les contrôleurs de ...
Contrôleurs de domaine clonables	Groupe de séc...	Les membres de ce grou...
Contrôleurs de domaine en lecture seule	Groupe de séc...	Les membres de ce grou...
DnsAdmins	Groupe de séc...	Groupe des administrat...
DnsUpdateProxy	Groupe de séc...	Les clients DNS qui sont ...
Éditeurs de certificats	Groupe de séc...	Les membres de ce grou...
Groupe de réplication dont le mot de passe RODC est autorisé	Groupe de séc...	Les mots de passe des ...
Groupe de réplication dont le mot de passe RODC est refusé	Groupe de séc...	Les mots de passe des ...
Invité	Utilisateur	Compte d'utilisateur inv...
Invités du domaine	Groupe de séc...	Tous les invités du doma...
Ordinateurs du domaine	Groupe de séc...	Toutes les stations de tra...
Pauline Augquier	Utilisateur	
Propriétaires créateurs de la stratégie de groupe	Groupe de séc...	Les membres de ce grou...
Protected Users	Groupe de séc...	Les membres de ce grou...
Serveurs RAS et IAS	Groupe de séc...	Les serveurs de ce group...
Utilisateurs du domaine	Groupe de séc...	Tous les utilisateurs du d...

Pour tester le bon fonctionnement j'ai crée un utilisateur :

Nom	Type	Description
Administrateur	Utilisateur	Compte d'utilisateur d'a...
Administrateurs clés	Groupe de séc...	Les membres de ce grou...
Admins du domaine	Groupe de séc...	Administrateurs désigné...
Contrôleurs de domaine	Groupe de séc...	Tous les contrôleurs de ...
Contrôleurs de domaine clonables	Groupe de séc...	Les membres de ce grou...
Contrôleurs de domaine en lecture seule	Groupe de séc...	Les membres de ce grou...
DnsAdmins	Groupe de séc...	Groupe des administrat...
DnsUpdateProxy	Groupe de séc...	Les clients DNS qui sont ...
Éditeurs de certificats	Groupe de séc...	Les membres de ce grou...
Groupe de réplication dont le mot de passe RODC est autorisé	Groupe de séc...	Les mots de passe des ...
Groupe de réplication dont le mot de passe RODC est refusé	Groupe de séc...	Les mots de passe des ...
Invité	Utilisateur	Compte d'utilisateur inv...
Invités du domaine	Groupe de séc...	Tous les invités du doma...
Ordinateurs du domaine	Groupe de séc...	Toutes les stations de tra...
Pauline Augquier	Utilisateur	
Propriétaires créateurs de la stratégie de groupe	Groupe de séc...	Les membres de ce grou...
Protected Users	Groupe de séc...	Les membres de ce grou...
Serveurs RAS et IAS	Groupe de séc...	Les serveurs de ce group...
Utilisateurs du domaine	Groupe de séc...	Tous les utilisateurs du d...

Vérifications finales

Depuis sete.local, Chafik nous a envoyé les captures des commandes :

```
Get-ADForest  
Get-ADDomain
```

On a bien vu dans les résultats que les 3 domaines étaient listés dans la forêt :

sete.local (racine) tssr1.sete.local (mon domaine enfant) dev.sete.local (domaine enfant de Youcef)

```
PS C:\Users\Administrateur.SRV-AD01> get-ADForest

ApplicationPartitions : {DC=ForestDnsZones,DC=sete,DC=local, DC=DomainDnsZones,DC=sete,DC=local}
CrossForestReferences : {}
DomainNamingMaster    : SRV-AD01.sete.local
Domains              : {dev.sete.local, sete.local, tssr1.sete.local}
ForestMode            : Windows2016Forest
GlobalCatalogs       : {SRV-AD01.sete.local}
Name                 : sete.local
PartitionsContainer  : CN=Partitions,CN=Configuration,DC=sete,DC=local
RootDomain           : sete.local
SchemaMaster         : SRV-AD01.sete.local
Sites               : {Default-First-Site-Name}
SPNSuffixes          : {}
UPNSuffixes          : {}
```

```
PS C:\Users\Administrateur.SRV-AD01> get-ADDomain
```

```
AllowedDNSSuffixes      : {}
ChildDomains            : {dev.sete.local, tssr1.sete.local}
ComputersContainer      : CN=Computers,DC=sete,DC=local
DeletedObjectsContainer : CN=Deleted Objects,DC=sete,DC=local
DistinguishedName       : DC=sete,DC=local
DNSRoot                : sete.local
DomainControllersContainer : OU=Domain Controllers,DC=sete,DC=local
DomainMode              : Windows2016Domain
DomainSID               : S-1-5-21-1920055850-1989876339-3061935551
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=sete,DC=local
Forest                 : sete.local
InfrastructureMaster     : SRV-AD01.sete.local
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=sete,DC=local}
LostAndFoundContainer   : CN=LostAndFound,DC=sete,DC=local
ManagedBy               : 
Name                   : sete
NetBIOSName            : SETE
ObjectClass             : domainDNS
ObjectGUID              : 9984d166-5043-4134-99c0-f4e65d13a093
ParentDomain            : 
PDCEmulator             : SRV-AD01.sete.local
PublicKeyRequiredPasswordRolling : True
QuotasContainer         : CN=NTDS Quotas,DC=sete,DC=local
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers : {SRV-AD01.sete.local}
RIDMaster               : SRV-AD01.sete.local
SubordinateReferences  : {DC=dev,DC=sete,DC=local, DC=tssr1,DC=sete,DC=local,
                        DC=ForestDnsZones,DC=sete,DC=local, DC=DomainDnsZones,DC=sete,DC=local...}
SystemsContainer        : CN=System,DC=sete,DC=local
UsersContainer          : CN=Users,DC=sete,DC=local
```

Vérifications réseau

Depuis mon serveur tssr1.sete.local :

Ping vers sete.local → OK via Tailscale.

```
*C:\Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.20348.3807]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.SRV-AD-001>ping sete.local

Envoi d'une requête 'ping' sur sete.local [100.104.189.105] avec 32 octets de données :
Réponse de 100.104.189.105 : octets=32 temps=34 ms TTL=128
Réponse de 100.104.189.105 : octets=32 temps=91 ms TTL=128
Réponse de 100.104.189.105 : octets=32 temps=32 ms TTL=128
Réponse de 100.104.189.105 : octets=32 temps=94 ms TTL=128

Statistiques Ping pour 100.104.189.105:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 32ms, Maximum = 94ms, Moyenne = 62ms

C:\Users\Administrateur.SRV-AD-001>

C:\Users\Administrateur.SRV-AD-001>ping 100.104.189.105

Envoi d'une requête 'Ping' 100.104.189.105 avec 32 octets de données :
Réponse de 100.104.189.105 : octets=32 temps=152 ms TTL=128
Réponse de 100.104.189.105 : octets=32 temps=74 ms TTL=128
Réponse de 100.104.189.105 : octets=32 temps=67 ms TTL=128
Réponse de 100.104.189.105 : octets=32 temps=112 ms TTL=128

Statistiques Ping pour 100.104.189.105:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 67ms, Maximum = 152ms, Moyenne = 101ms

C:\Users\Administrateur.SRV-AD-001>
```

nslookup sete.local → OK, réponse DNS correcte.

```
*C
C:\Users\Administrateur.SRV-AD-001>nslookup sete.local
DNS request timed out.
    timeout was 2 seconds.
Serveur :     UnKnown
Address: 100.104.189.105

Nom :      sete.local
Addresses: 2a01:cb1d:8158:f600:8d80:9d04:bf5:b0bc
           100.104.189.105

C:\Users\Administrateur.SRV-AD-001>
```

ipconfig /all → DNS principal = 100.104.189.105.

Carte inconnue Tailscale :

```
Suffixe DNS propre à la connexion. . . : tail8c0f31.ts.net
Description. . . . . : Tailscale Tunnel
Adresse physique . . . . . :
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . : Oui
Adresse IPv4. . . . . : 100.71.113.76(préféré)
Masque de sous-réseau. . . . . : 255.255.255.255
Passerelle par défaut. . . . . :
Serveurs DNS. . . . . : 100.104.189.105
NetBIOS sur TCPIP. . . . . : Désactivé
Liste de recherche de suffixes DNS propres à la connexion :
                                tail8c0f31.ts.net
```

Carte Ethernet Ethernet 3 :

```
Suffixe DNS propre à la connexion. . . : lan
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter #3
Adresse physique . . . . . : 08-00-27-39-6F-F3
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . : Oui
Adresse IPv4. . . . . : 192.168.1.68(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : mardi 8 juillet 2025 15:46:13
Bail expirant. . . . . : mercredi 9 juillet 2025 15:47:34
Passerelle par défaut. . . . . : 192.168.1.254
Serveur DHCP . . . . . : 192.168.1.254
Serveurs DNS. . . . . : 127.0.0.1
                                         192.168.1.254
NetBIOS sur Tcpip. . . . . : Activé
```

Bilan

Sincèrement, la partie la plus compliquée, c'était le DNS, car on était sur un VPN Tailscale et qu'il fallait jongler entre plusieurs réseaux. La première tentative de promotion m'a permis de comprendre où ça bloque, et repartir sur tssr1.sete.local a simplifié les choses. Finalement, on a réussi à avoir une forêt stable, et on a bien appris à résoudre les conflits d'IP et d'enregistrements DNS.