WINDOWS SERVER 2022

Active Directory, DNS & DHCP

Déploiement du contrôleur de domaine pour l'infrastructure Proxmox

Projet **Infrastructure Proxmox – BTS SIO SISR**

Auteur **Sasiraj GUNARATNARAJAH**

Date **Février 2026**

Doc **3 / 7**

1. CONTEXTE ET OBJECTIFS

Windows Server 2022 constitue la pièce maîtresse de l'infrastructure en matière de gestion des identités et des accès. Déployé sur le réseau LAN-SRV (172.16.1.0/24), ce serveur héberge trois rôles fondamentaux pour le fonctionnement du domaine.

▸ Rôles déployés

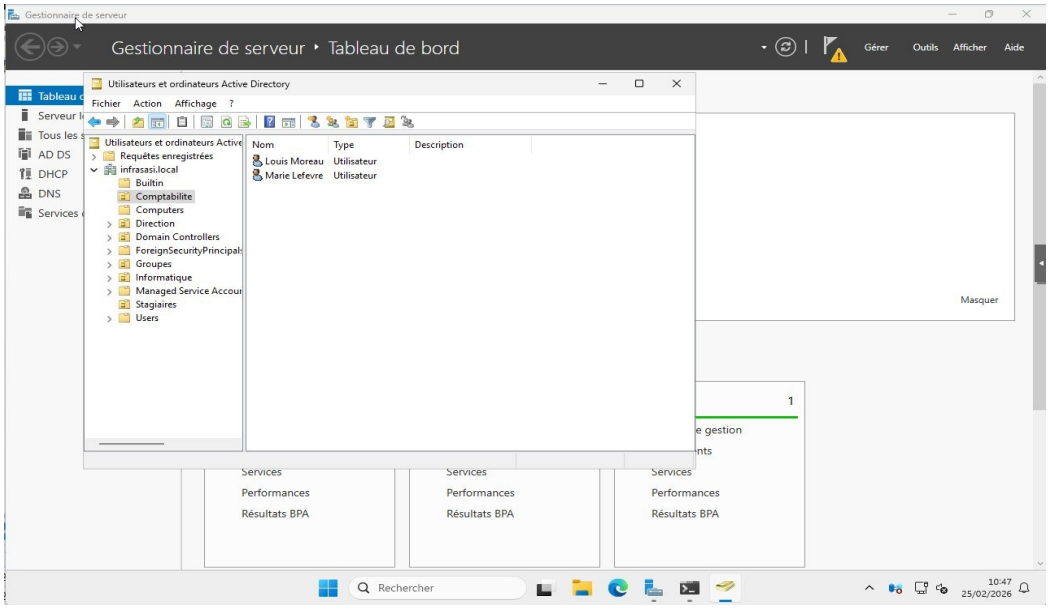
Rôle	Fonction
AD DS	Contrôleur de domaine – gestion centralisée des comptes, groupes et stratégies de sécurité (GPO)
DNS	Résolution de noms pour le domaine interne infrasasi.local et redirection vers les DNS publics
DHCP	Distribution automatique d'adresses IP aux postes du réseau LAN-PDT via un relais pfSense

▸ Pourquoi ces choix ?

Active Directory est la solution standard en entreprise pour la gestion centralisée des identités. Le DNS intégré à AD est indispensable au fonctionnement du domaine : sans lui, les machines ne peuvent pas localiser le contrôleur de domaine. Le DHCP, quant à lui, simplifie l'administration du parc en évitant la configuration manuelle de chaque poste.

2. PRÉREQUIS ET RESSOURCES

Paramètre	Configuration
VM ID (Proxmox)	100
Nom de la VM	Winsrv
Hostname	WS-DC-1
Système d'exploitation	Windows Server 2025 Standard (Desktop Experience)
CPU	4 vCPU (x86-64-v2-AES)
Mémoire vive	4 Go
Stockage	40 Go SATA (LSI 53C895A)
Réseau	Intel E1000 sur vmbr1 (LAN-SRV)
BIOS	OVMF (UEFI) avec TPM

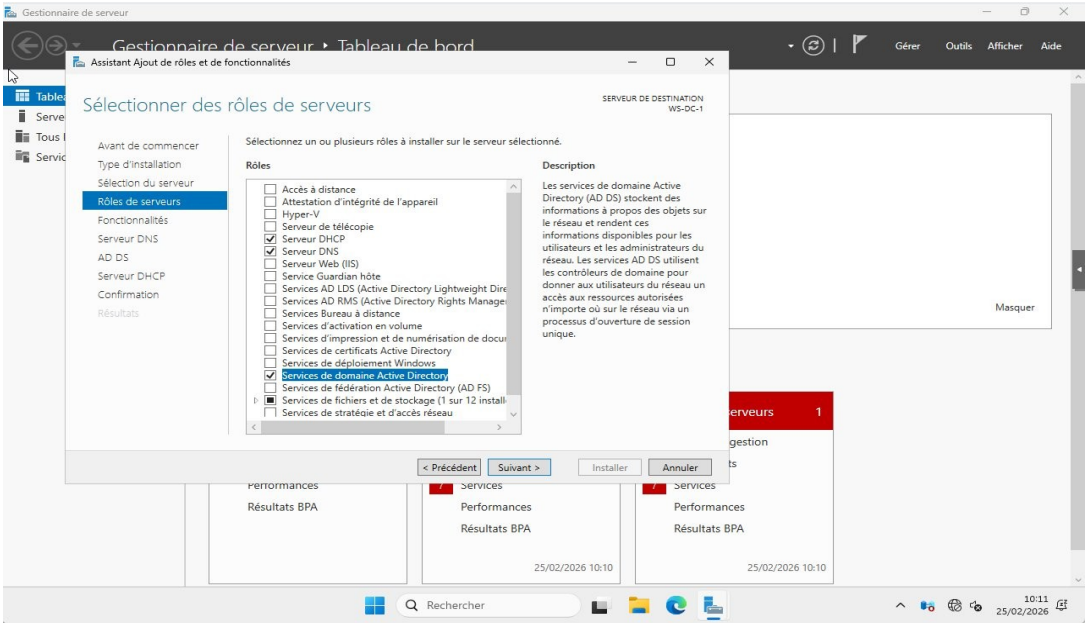


Le contrôleur SCSI LSI 53C895A et la carte réseau Intel E1000 ont été choisis pour leur compatibilité native avec Windows, évitant l'installation de drivers VirtIO supplémentaires.

3. CONFIGURATION RÉSEAU

Avant d'installer les rôles serveur, il est essentiel de configurer une adresse IP statique. Un contrôleur de domaine ne doit jamais recevoir son adresse via DHCP, car les clients doivent pouvoir le localiser de manière fiable.

La configuration réseau a été effectuée dans les propriétés de la carte Intel PRO/1000, via le protocole TCP/IPv4 :



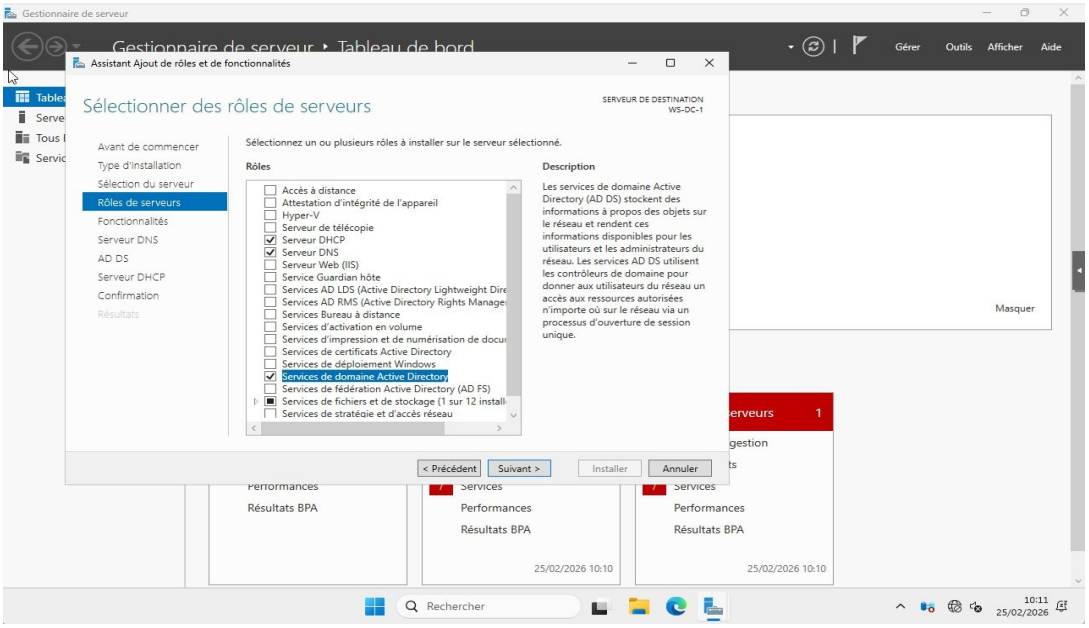
Paramètre	Valeur
Adresse IP	172.16.1.10
Masque	255.255.0.0 (/16)
Passerelle	172.16.1.254 (pfSense LAN)
DNS préféré	172.16.1.10 (lui-même, car il hébergera le DNS)

> *Le serveur DNS préféré pointe vers lui-même (127.0.0.1 ou 172.16.1.10). C'est une bonne pratique pour un contrôleur de domaine : il interroge d'abord son propre service DNS pour résoudre les enregistrements du domaine.*

4. INSTALLATION DES RÔLES SERVEUR

L'installation des rôles s'effectue depuis le Gestionnaire de serveur, via l'assistant « Ajouter des rôles et fonctionnalités ». Trois rôles ont été sélectionnés :

- Services de domaine Active Directory (AD DS)
- Serveur DNS
- Serveur DHCP



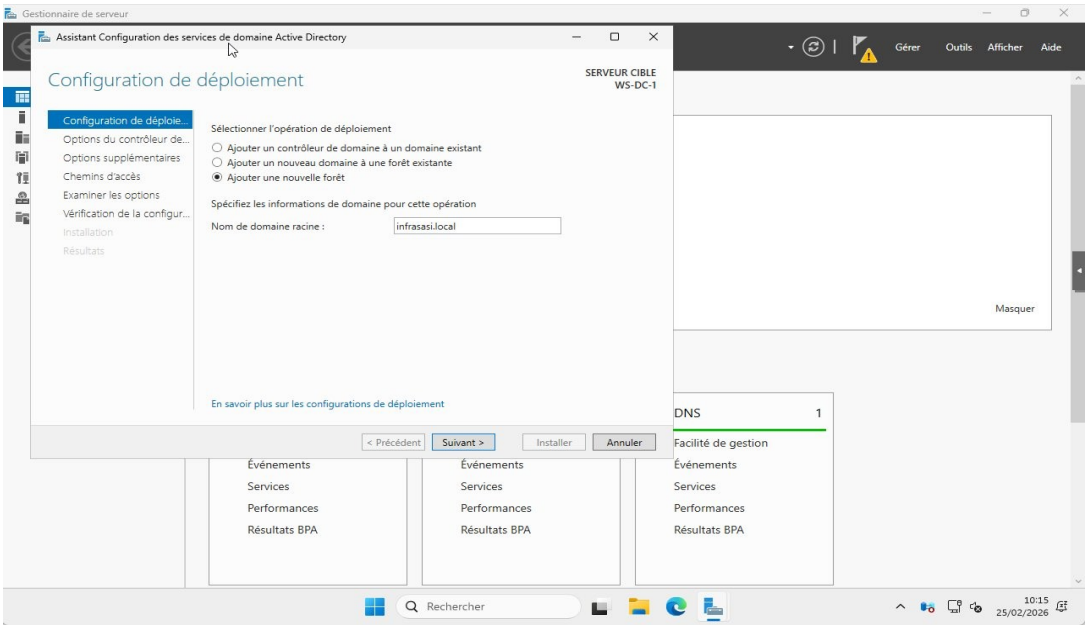
L'assistant propose automatiquement d'ajouter les fonctionnalités requises par chaque rôle (outils de gestion, modules PowerShell). Il suffit d'accepter et de lancer l'installation.

Une fois l'installation terminée, les trois rôles apparaissent dans le tableau de bord du Gestionnaire de serveur, mais ne sont pas encore configurés.

5. PROMOTION EN CONTRÔLEUR DE DOMAINE

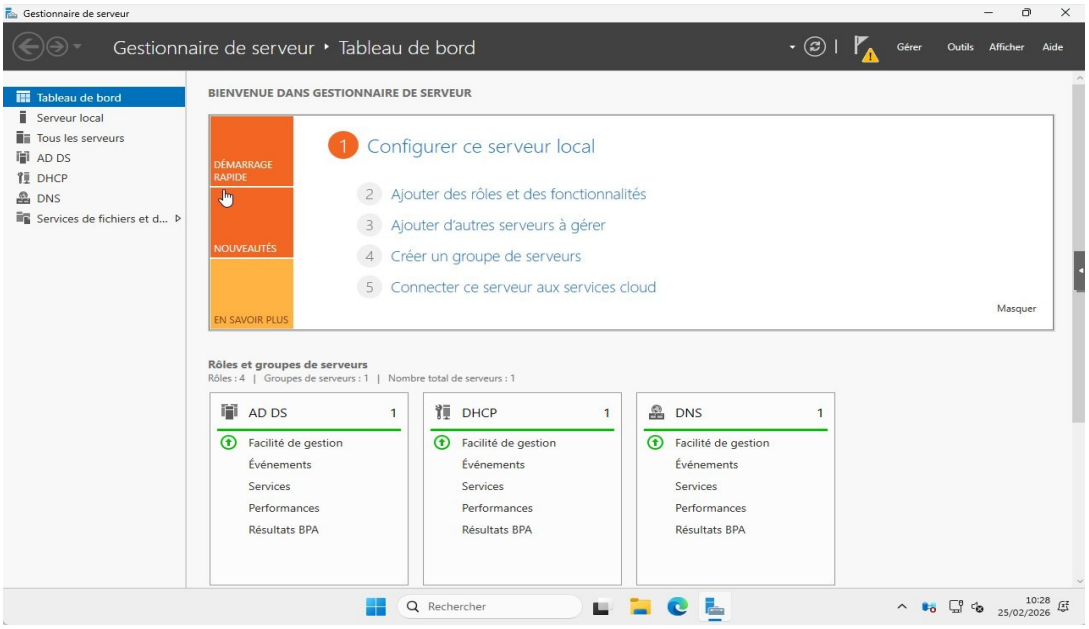
Après l'installation du rôle AD DS, un drapeau jaune d'avertissement apparaît dans le Gestionnaire de serveur. En cliquant dessus, l'option « Promouvoir ce serveur en contrôleur de domaine » est disponible.

L'assistant de configuration Active Directory demande de choisir le type de déploiement. Puisqu'il s'agit du premier contrôleur de domaine de l'infrastructure, l'option « Ajouter une nouvelle forêt » est sélectionnée :



Paramètre	Valeur
Opération	Ajouter une nouvelle forêt
Nom de domaine racine	infrasasi.local
Niveau fonctionnel	Windows Server 2016 (par défaut)
Mot de passe DSRM	Défini (mode restauration des services d'annuaire)
Nom NetBIOS	INFRASASI

Après validation, le serveur redémarre automatiquement. Au redémarrage, la connexion s'effectue désormais avec le compte INFRASASI\Administrateur, confirmant que le domaine est opérationnel.



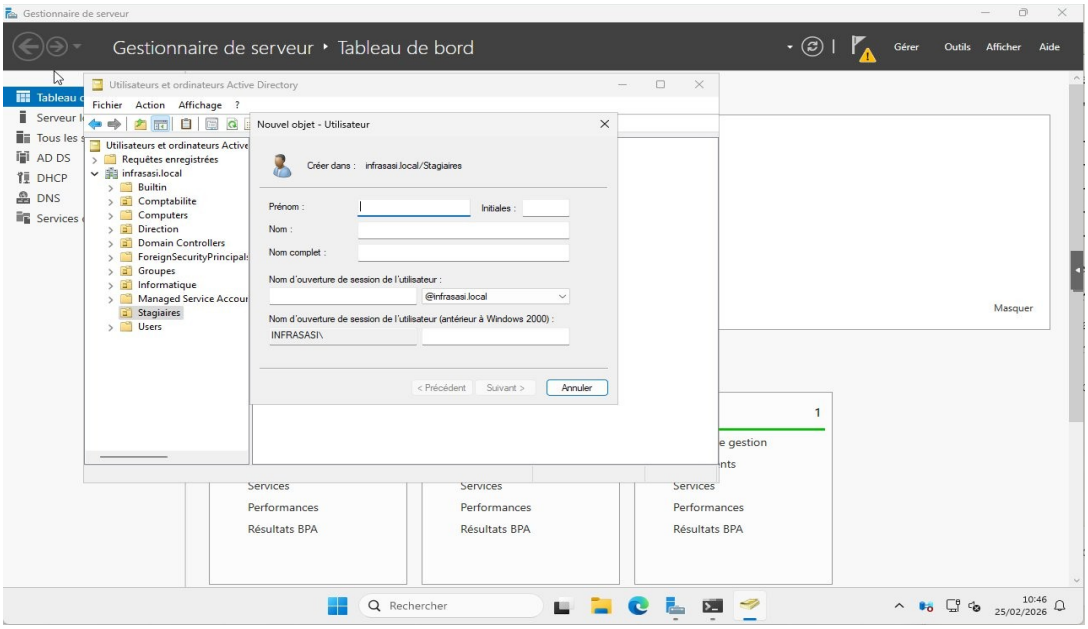
Le tableau de bord du Gestionnaire de serveur affiche désormais les trois rôles actifs : AD DS, DHCP et DNS, tous avec un état de fonctionnement normal.

6. ORGANISATION DE L'ANNUAIRE ACTIVE DIRECTORY

L'annuaire Active Directory a été structuré en unités d'organisation (OU) pour refléter l'organisation d'une entreprise type. Cette structuration facilite l'application de stratégies de groupe (GPO) ciblées et la délégation d'administration.

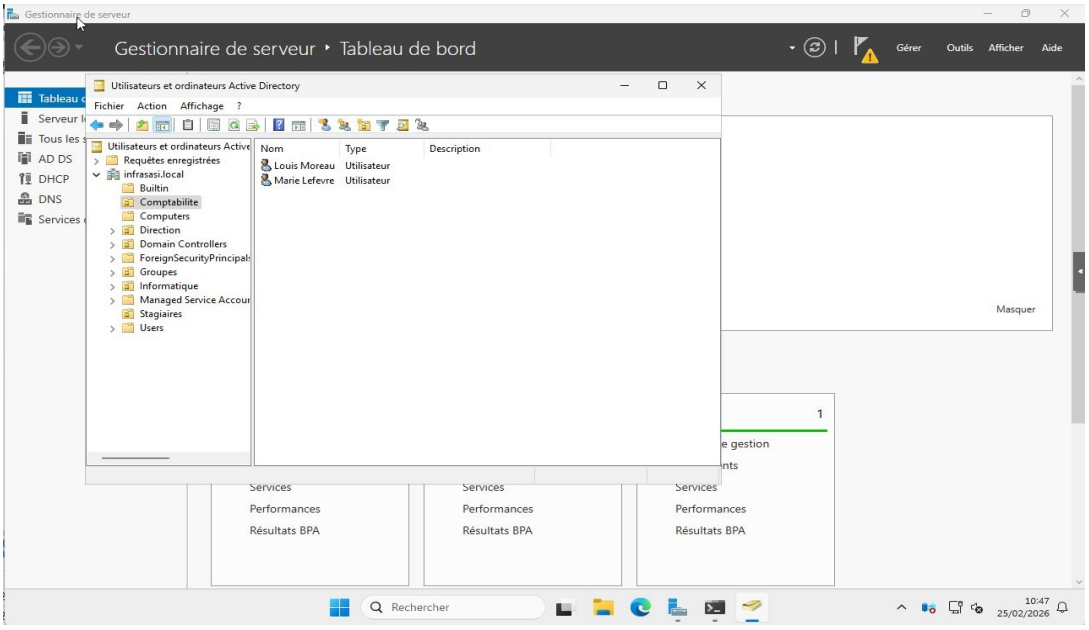
▸ Unités d'organisation créées

OU	Description
Direction	Comptes des membres de la direction générale
Informatique	Comptes du service informatique (administrateurs, techniciens)
Comptabilité	Comptes du service comptable et financier
Stagiaires	Comptes temporaires pour les stagiaires avec droits limités
Groupes	Groupes de sécurité pour la gestion des permissions



▸ Comptes utilisateurs

Nom complet	Identifiant	OU	Groupe
Jean Dupont	jdupont	Direction	G_Direction
Sophie Lamour	slamour	Direction	G_Direction
Antoine Girard	agirard	Informatique	G_Informatique
Julien Martin	jmartin	Informatique	G_Informatique
Marie Lefevre	mlefevre	Comptabilité	G_Comptabilite
Louis Moreau	lmoreau	Comptabilité	G_Comptabilite
Emilie Laurent	elaurent	Stagiaires	G_Stagiaires



▸ Groupes de sécurité

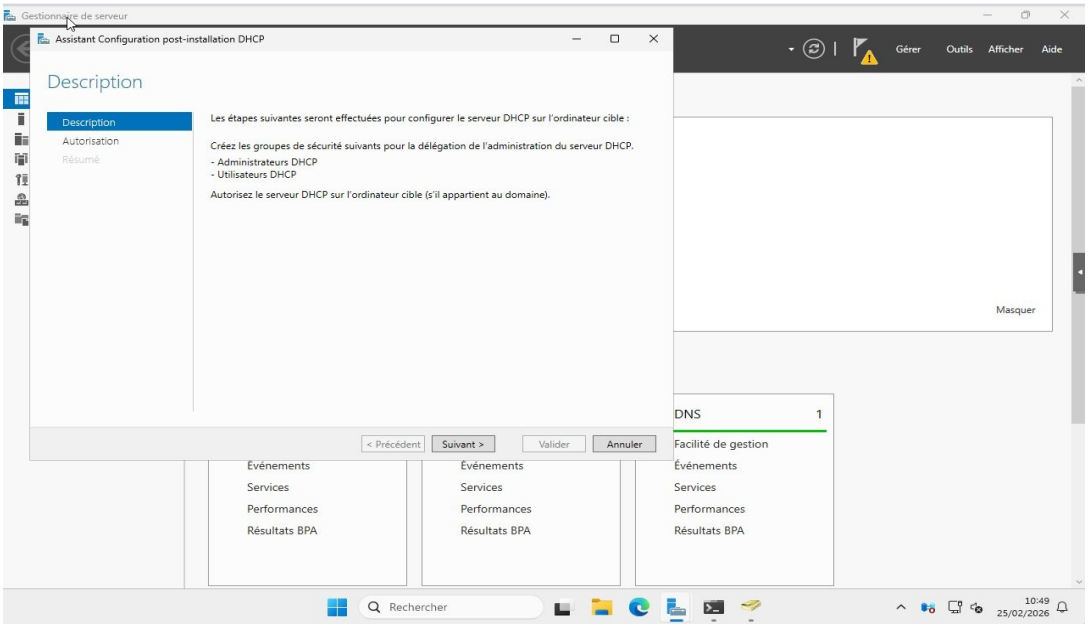
Cinq groupes de sécurité globaux ont été créés dans l'OU Groupes : G_Direction, G_Informatique, G_Comptabilite, G_Stagiaires et G_Tous_Employes. Chaque utilisateur est membre de son groupe de service ainsi que du groupe G_Tous_Employes. Cette organisation permet d'attribuer des permissions par groupe plutôt que par utilisateur individuel.

7. CONFIGURATION DU SERVICE DHCP

Le rôle DHCP est installé sur le serveur WS-DC-1 afin de centraliser la gestion de l'adressage IP. Cependant, le serveur se trouve sur le réseau LAN-SRV (172.16.1.0/24) alors que les postes clients à adresser sont sur le réseau LAN-PDT (172.31.1.0/24). Un relais DHCP est donc nécessaire sur pfSense.

▸ Autorisation du serveur DHCP

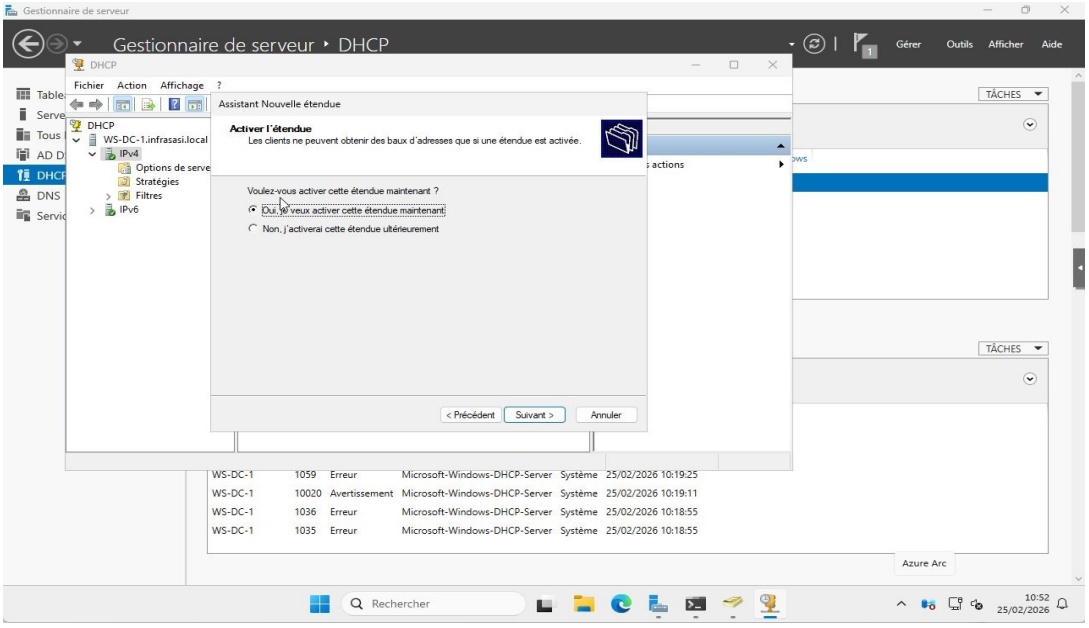
Après l'installation du rôle, un assistant de configuration post-installation demande d'autoriser le serveur DHCP dans Active Directory. Cette étape est obligatoire pour que le serveur puisse distribuer des adresses IP dans un domaine AD.



▸ Création de l'étendue LAN-PDT

Une étendue DHCP a été créée pour le réseau des postes de travail :

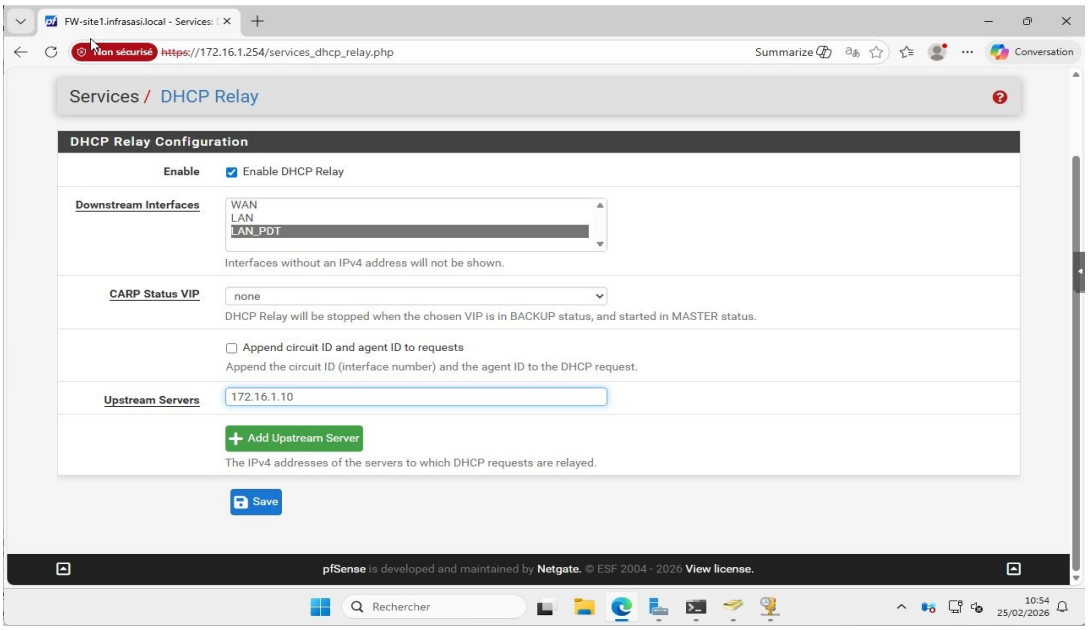
Paramètre	Valeur
Nom de l'étendue	LAN-PDT
Plage d'adresses	172.31.1.50 à 172.31.1.200
Masque	255.255.255.0 (/24)
Passerelle par défaut	172.31.1.254 (pfSense OPT1)
Serveur DNS	172.16.1.10 (WS-DC-1)
Durée du bail	8 jours (par défaut)



▸ Relais DHCP sur pfSense

Comme le serveur DHCP et les postes clients sont sur des sous-réseaux différents, les requêtes DHCP (broadcast) ne traversent pas le routeur par défaut. Il faut configurer un relais DHCP (DHCP Relay) sur pfSense pour transmettre les requêtes des postes du LAN-PDT vers le serveur DHCP sur le LAN-SRV.

La configuration s'effectue dans pfSense via Services → DHCP Relay :



Paramètre	Valeur
Enable	DHCP Relay activé
Downstream Interface	LAN_PDT (réseau où se trouvent les clients)
Upstream Server	172.16.1.10 (serveur DHCP sur LAN-SRV)

> *Le relais DHCP fonctionne en convertissant les broadcasts DHCP du LAN-PDT en paquets unicast dirigés vers le serveur 172.16.1.10. Le serveur répond ensuite via pfSense qui retransmet au client.*

8. VÉRIFICATIONS

Afin de s'assurer du bon fonctionnement de l'ensemble, plusieurs vérifications sont effectuées.

▸ Domaine Active Directory

- Connexion avec le compte INFRASASI\Administrateur : fonctionnelle
- Les rôles AD DS, DNS et DHCP sont visibles et actifs dans le Gestionnaire de serveur
- Les OU, utilisateurs et groupes sont correctement créés dans l'annuaire

▸ Service DNS

- La zone de recherche directe infrasasi.local est créée automatiquement
- Les enregistrements SRV et A du contrôleur de domaine sont présents
- La résolution externe fonctionne via les redirecteurs (8.8.8.8 et 1.1.1.1)

▸ Service DHCP

- L'étendue LAN-PDT est active avec la plage 172.31.1.50 à 172.31.1.200
- Le relais DHCP est configuré sur pfSense pour l'interface LAN_PDT
- Un poste client connecté au LAN-PDT recevra automatiquement une adresse IP dans cette plage

9. CONCLUSION

Le serveur Windows Server 2022 est désormais pleinement opérationnel en tant que contrôleur de domaine de l'infrastructure. Les services Active Directory, DNS et DHCP sont configurés et prêts à accueillir les postes clients et les autres serveurs du domaine.

L'annuaire Active Directory est structuré de manière professionnelle avec des unités d'organisation par service, des comptes utilisateurs nominatifs et des groupes de sécurité permettant une gestion fine des permissions.

Les prochaines étapes du projet impliqueront ce serveur de manière transversale :

- GLPI : import automatique des utilisateurs via une connexion LDAP
- Zabbix : supervision du contrôleur de domaine via l'agent
- TrueNAS : intégration au domaine pour les partages authentifiés
- Windows 11 : jonction au domaine, application des GPO et test d'authentification