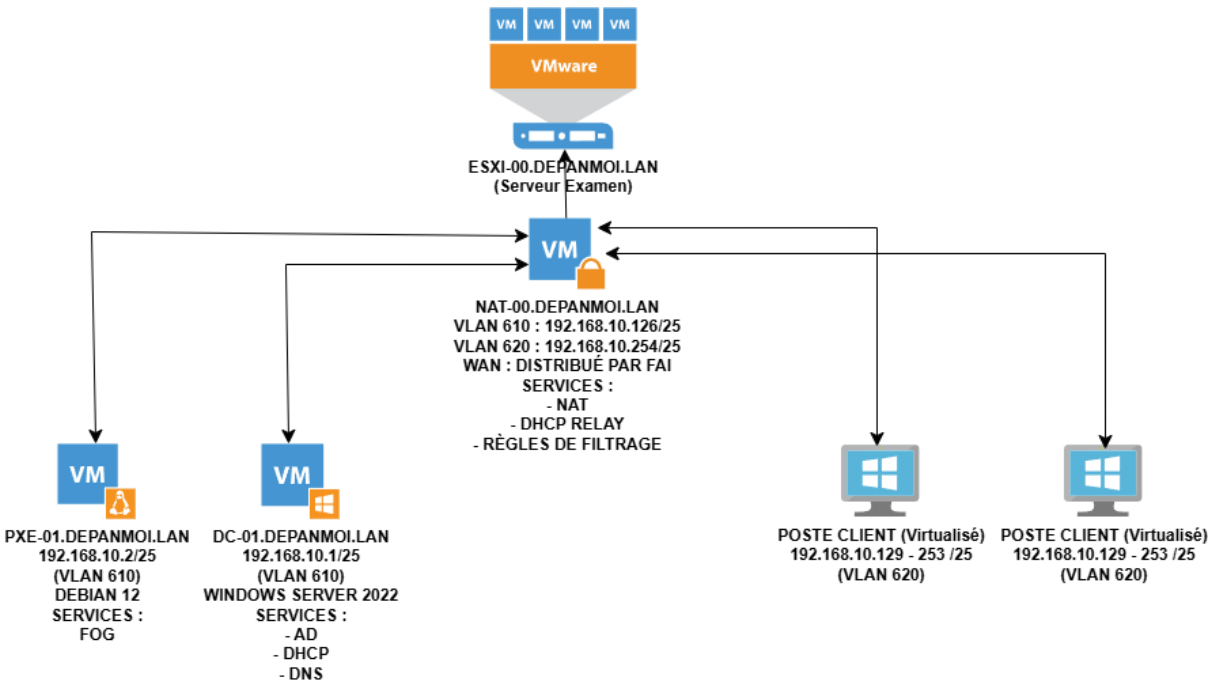
DOCUMENTATION TECHNIQUE

Déploiement d'un environnement d'entreprise

Active Directory · DHCP · DNS · Pare-feu OPNsense · FOG Project

Organisation	DEPANMOI.FR
Projet	Infrastructure système virtualisée sous ESXi
Auteur	LOPES DA SILVA Lucas
Version	1.0
Date	Mars 2026
Public cible	Administrateurs systèmes et réseaux
Classification	Usage interne



Sommaire

1. Introduction

1.1 Contexte et objectifs

DEPANMOI.FR est une TPE spécialisée dans le dépannage informatique, la maintenance de parcs et le conseil technologique, basée au 15 avenue de la République, 69007 Lyon. L'entreprise compte 4 collaborateurs (1 gérant, 2 techniciens systèmes et réseaux, 1 secrétaire comptable) et gère un portefeuille de 20 clients actifs, principalement des PME locales.

Face à l'accroissement de son activité, l'entreprise rencontrait trois problèmes structurels majeurs :

- Absence de segmentation réseau : les machines clientes (souvent infectées) sont connectées au même réseau que les serveurs internes.
- Temps de préparation excessif : l'installation manuelle d'un système d'exploitation via clé USB prenait en moyenne 2 heures par machine.
- Absence de gestion centralisée des accès : aucun annuaire ne permettait de gérer les identités et les droits des utilisateurs.

L'objectif de ce projet est de déployer une infrastructure complète, sécurisée et industrialisée répondant aux trois axes suivants :

- Sécuriser et segmenter le réseau via un pare-feu OPNsense avec isolation par VLANs.
- Centraliser la gestion des identités et des services réseau via Windows Server 2022 (Active Directory, DNS, DHCP).
- Automatiser le déploiement des postes de travail via FOG Project (PXE boot).

1.2 Périmètre de la documentation

Ce document couvre l'intégralité du cycle de déploiement, depuis la préparation de l'environnement virtuel jusqu'à la validation fonctionnelle. Il constitue à la fois un guide d'installation pas à pas et un référentiel de maintenance exploitable en production.

> **NOTE :** Ce document s'adresse à des administrateurs systèmes maîtrisant les bases de la virtualisation, du réseau TCP/IP et de Windows Server.

2. Prérequis

2.1 Ressources matérielles

L'ensemble de l'infrastructure repose sur un unique serveur physique hébergeant un hyperviseur VMware ESXi. Les spécifications minimales recommandées sont les suivantes :

Composant	Spécification recommandée
Processeur	1,5 GHz multi-cœurs ou supérieur
Mémoire RAM	16 Go minimum (32 Go recommandés pour 4 VM)
Stockage	500 Go SSD minimum
Interfaces réseau	1 Carte réseau physique (vSwitchs créés pour les différents VLANS)

Tableau 1 — Spécifications matérielles recommandées pour le serveur ESXi

2.2 Logiciels et versions utilisées

Composant	Version	Rôle
VMware ESXi	8.x	Hyperviseur de type 1
OPNsense	26.1 (amd64)	Pare-feu, routage inter-VLAN, DHCP Relay
Windows Server 2022	Standard (Expérience de bureau)	Contrôleur de domaine AD DS, DNS, DHCP
Debian	12 (Bookworm)	Système hôte du serveur FOG
FOG Project	Dernière stable	Déploiement PXE et clonage de postes
Windows 10	Pro	Postes clients

Tableau 2 — Composants logiciels utilisés dans le projet

2.3 Plan d'adressage réseau

Le plan d'adressage est structuré autour de deux VLANs distincts. La plage 192.168.10.0/24 est découpée en deux sous-réseaux /25 :

Nom VLAN	N° VLAN	Plage IP	Passerelle	Rôle
ADMIN	610	192.168.10.0/25	192.168.10.126	Serveurs internes
ATELIER	620	192.168.10.128/25	192.168.10.254	Machines clientes

Tableau 3 — Plan d'adressage VLAN

2.4 Plan d'adressage des serveurs

Serveur	Nom d'hôte	Adresse(s) IP	VLAN
Pare-feu OPNsense	NAT-00.DEPANMOI.LAN	192.168.10.126 (LAN)(em1) 192.168.10.254 (LAN)(em2) IP WAN DHCP (FAI)(em0)	610 (ADMIN) 620 (ATELIER)
Contrôleur de domaine	DC-01.DEPANMOI.LAN	192.168.10.1	610 (ADMIN)
Serveur FOG (Debian)	PXE-01.DEPANMOI.LAN	192.168.10.2	610 (ADMIN)

Tableau 4 — Adressage statique des serveurs

3. Architecture de l'infrastructure

3.1 Vue d'ensemble

L'infrastructure repose sur un hyperviseur VMware ESXi hébergeant 4 machines virtuelles interconnectées via des VLANs. Le pare-feu OPNsense constitue le point d'entrée et de sortie de tous les flux réseau. Il assure le routage inter-VLAN, le relayage DHCP et le filtrage du trafic.

Chaque VLAN est isolé. Seules les communications explicitement autorisées dans les règles de pare-feu peuvent traverser d'un segment à l'autre. Cette architecture garantit qu'une machine cliente infectée dans le VLAN ATELIER ne peut pas communiquer directement avec les serveurs du VLAN ADMIN.

3.2 Matrice des flux

La politique de filtrage implémentée dans OPNsense définit les règles suivantes :

Source	Destination	Service	Action
VLAN 620 (ATELIER)	DC-01 192.168.10.1	UDP/TCP 67/68 (DHCP)	AUTORISER
VLAN 620 (ATELIER)	DC-01 192.168.10.1	UDP/TCP 53 (DNS)	AUTORISER
VLAN 620 (ATELIER)	PXE-01 192.168.10.2	UDP 69 (TFTP/PXE)	AUTORISER
VLAN 620 (ATELIER)	Internet / WAN	*	AUTORISER
VLAN 620 (ATELIER)	VLAN 610 (ADMIN)	Tout	BLOQUER
VLAN 610 (ADMIN)	Internet / WAN	*	AUTORISER

Tableau 5 — Matrice des flux réseau inter-VLANs

4. Installation et configuration d'OPNsense

4.1 Installation du pare-feu

OPNsense est déployé en tant que machine virtuelle sur ESXi. L'ISO est téléchargée depuis le site officiel opnsense.org. La VM est configurée avec 3 interfaces réseau : WAN, LAN (VLAN 610 ADMIN) et OPT1 (VLAN 620 ATELIER).

Procédure d'installation initiale :

1. Démarrer la VM depuis l'ISO OPNsense 26.1.
2. Se connecter avec le compte "installer" (mot de passe : opnsense).
3. Sélectionner "Install (ZFS)" puis valider le disque cible.
4. Une fois l'installation terminée, retirer l'ISO et redémarrer.
5. À la console, vérifier l'assignation automatique des interfaces.

Console OPNsense au premier démarrage : interface WAN assignée sur 192.168.1.1/24

4.2 Configuration initiale via l'assistant web

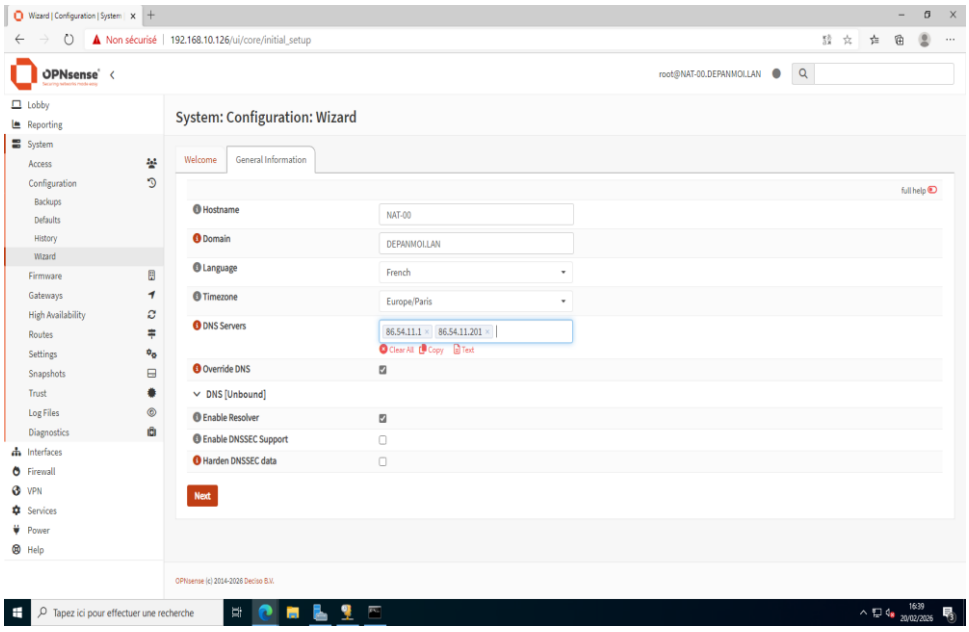
Depuis un poste branché sur le LAN, accéder à l'interface web via https://192.168.10.126. L'assistant de configuration (Wizard) guide les étapes initiales.

4.2.1 Informations générales du système

6. Accéder à System > Configuration > Wizard.
7. Renseigner les paramètres suivants :

- Hostname : NAT-00
- Domain : DEPANMOI.LAN
- Language : French
- Timezone : Europe/Paris
- DNS Servers : 86.54.11.1 et 86.54.11.201 (serveurs DNS4EU avec filtrage malveillant activé)

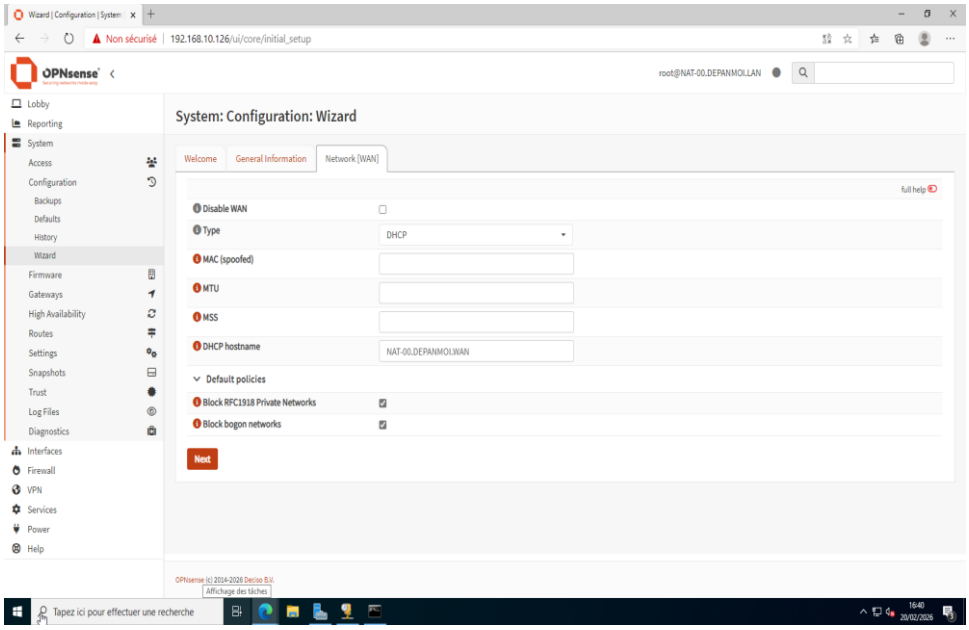
8. Cocher "Override DNS" et activer le resolver DNS (Unbound).
9. Cliquer sur "Next".



Assistant OPNsense : configuration générale avec hostname NAT-00.DEPANMOI.LAN et DNS4EU

4.2.2 Configuration de l'interface WAN

10. Dans l'onglet "Network [WAN]", définir le type de connexion sur "DHCP".
11. Activer "Block RFC1918 Private Networks" et "Block bogon networks".
12. Définir le DHCP hostname : NAT-00.DEPANMOI.WAN.
13. Cliquer sur "Next" pour valider.



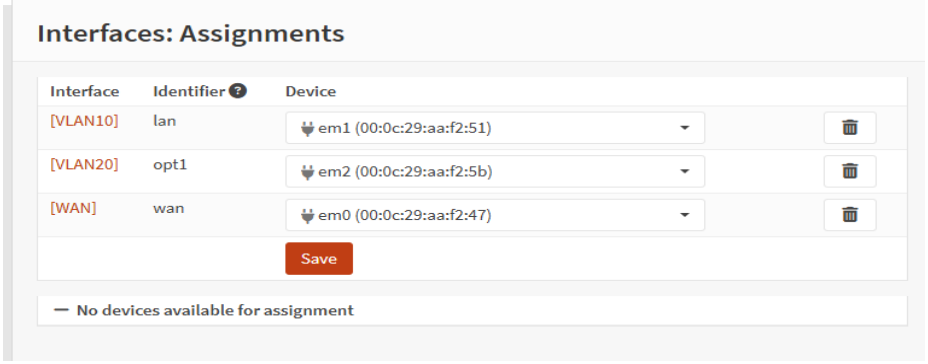
Configuration de l'interface WAN en DHCP avec protection anti-bogon activée

ATTENTION : Les options "Block RFC1918" et "Block bogon networks" sont essentielles en production. Elles empêchent l'usurpation d'adresses privées depuis Internet.

4.3 Configuration des interfaces VLAN

Après l'assistant, les interfaces doivent être assignées aux bons VLANs. Accéder à Interfaces > Assignments.

14. Vérifier que VLAN 610 est associé à l'interface "lan" (em1).
15. Vérifier que VLAN 620 est associé à l'interface "opt1" (em2).
16. Cliquer sur "Save" pour enregistrer les affectations.

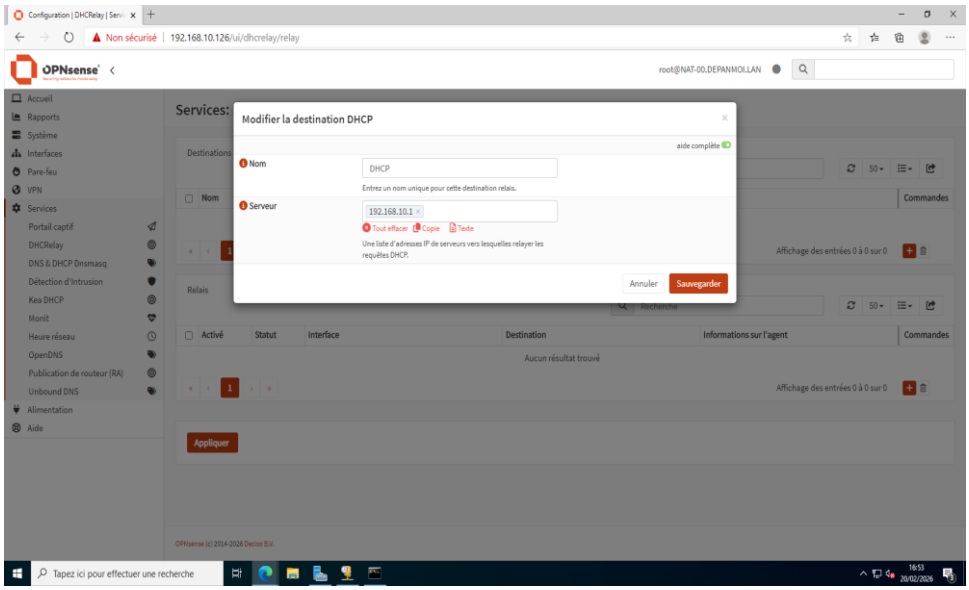


Attribution des interfaces VLANs : LAN → em1 (ADMIN), OPT1 → em2 (ATELIER), WAN → em0

4.4 Configuration du DHCP Relay

Le serveur DHCP est centralisé sur Windows Server 2022. OPNsense joue le rôle de relais DHCP pour rediriger les demandes du VLAN ATELIER vers le serveur Windows.

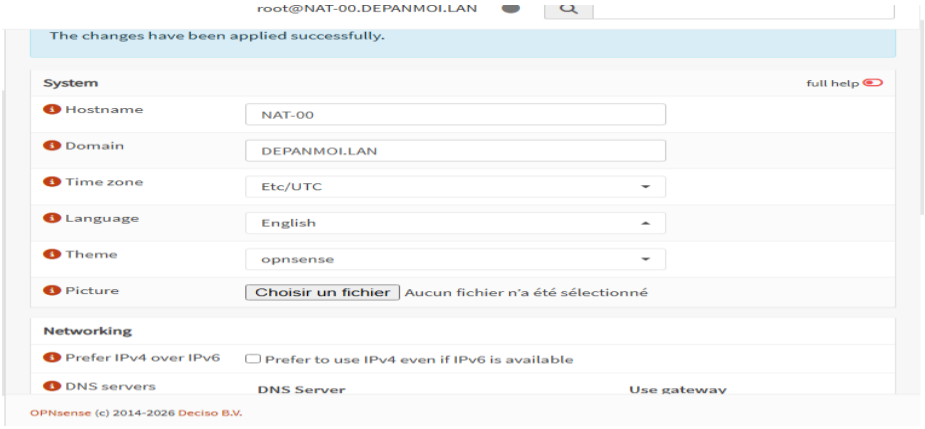
17. Accéder à Services > DHCPRelay.
18. Cliquer sur "Modifier la destination DHCP".
19. Saisir le nom "DHCP" et l'adresse IP du serveur : 192.168.10.1.
20. Cliquer sur "Sauvegarder" puis "Appliquer".



Configuration du DHCP Relay pointant vers le serveur Windows Server (192.168.10.1)

4.5 Règles de pare-feu

Les règles de filtrage sont configurées dans Firewall > Rules. La règle principale bloque toute communication du VLAN ATELIER (620) vers le VLAN ADMIN (610), tout en autorisant les services nécessaires.



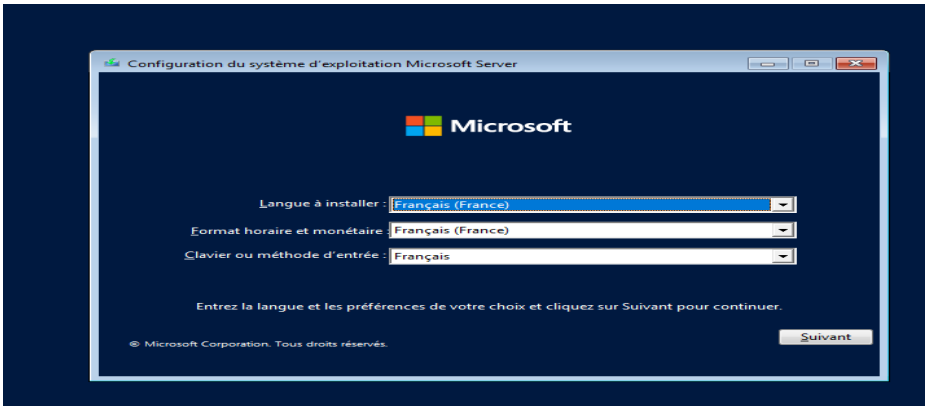
Interface de gestion OPNsense avec confirmation d'application des changements (root@NAT-00.DEPANMOI.LAN)

CONSEIL : Après chaque modification de règle de pare-feu, OPNsense affiche le message "The changes have been applied successfully". Vérifier toujours ce retour avant de continuer.

5. Installation de Windows Server 2022 et des rôles

5.1 Installation du système d'exploitation

Windows Server 2022 Standard est installé sur une VM dédiée hébergée sur ESXi. La VM est configurée avec une adresse IP statique 192.168.10.1/25 dans le VLAN ADMIN.

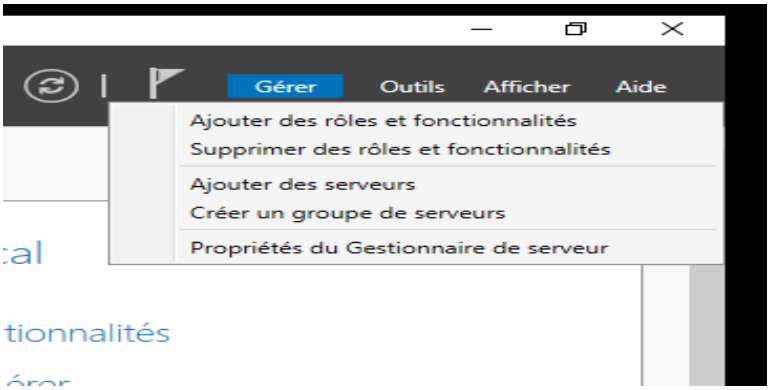


Étapes initiales de l'installation Windows Server 2022

5.2 Ajout des rôles AD DS, DNS et DHCP

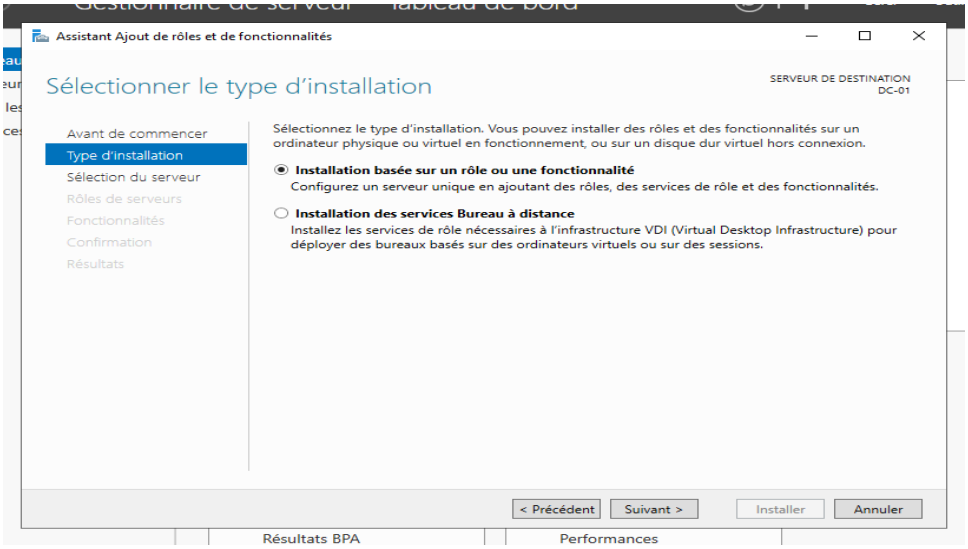
L'ajout des rôles se fait depuis le Gestionnaire de serveur. L'ensemble des trois rôles (Active Directory, DNS, DHCP) est installé en une seule opération pour simplifier la configuration.

21. Ouvrir le Gestionnaire de serveur.
22. Cliquer sur Gérer > Ajouter des rôles et fonctionnalités.



Menu Gestionnaire de serveur : accès à l'assistant d'ajout de rôles

23. Sélectionner "Installation basée sur un rôle ou une fonctionnalité".

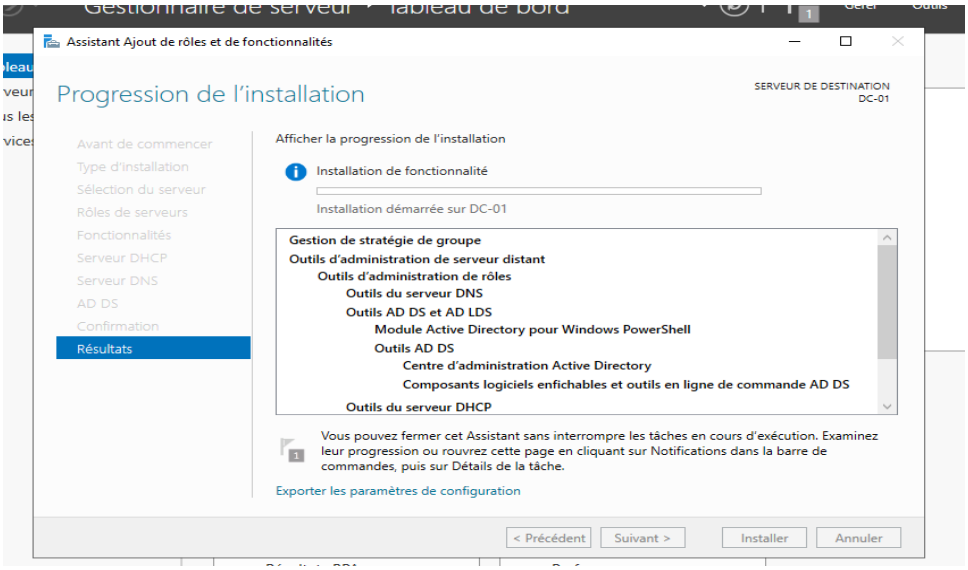


Sélection du type d'installation : basée sur un rôle, serveur de destination DC-01

24. Sélectionner le serveur de destination "DC-01".
25. Dans la liste des rôles, cocher :

- Services AD DS (Active Directory Domain Services)
- Serveur DNS
- Serveur DHCP

26. Cliquer sur "Installer". L'assistant installe automatiquement les dépendances.

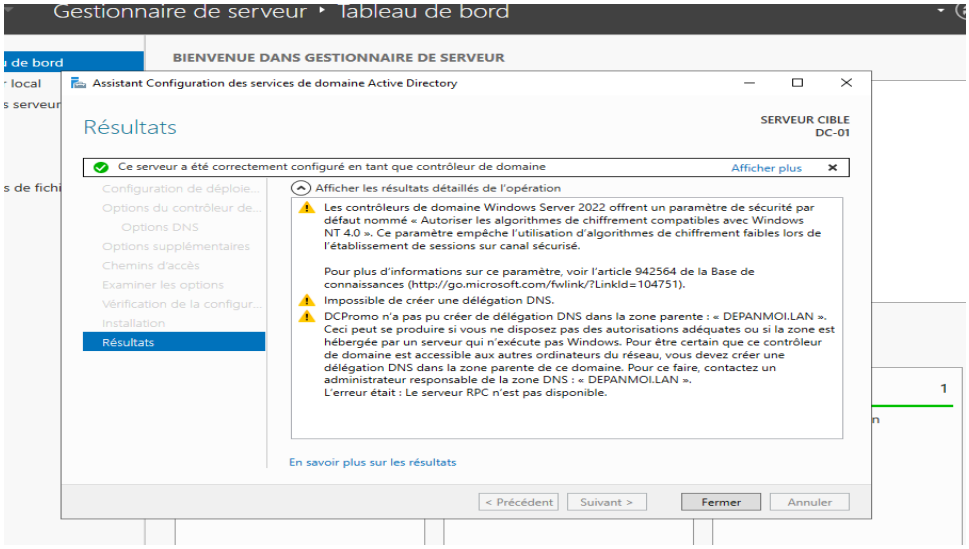


Progression de l'installation : les outils AD DS, DNS, DHCP et PowerShell pour AD sont installés simultanément

5.3 Promotion en contrôleur de domaine

Après l'installation des rôles, une alerte apparaît dans le Gestionnaire de serveur invitant à promouvoir le serveur en contrôleur de domaine.

27. Cliquer sur la notification "Promouvoir ce serveur en contrôleur de domaine".
28. Sélectionner "Ajouter une nouvelle forêt".
29. Saisir le nom de domaine racine : DEPANMOI.LAN.
30. Définir un mot de passe DSRM sécurisé (Mode de restauration des services d'annuaire).
31. Laisser le niveau fonctionnel sur Windows Server 2016 ou supérieur.
32. Valider et lancer la promotion. Le serveur redémarre automatiquement.



Résultats de la promotion : le serveur DC-01 est configuré comme contrôleur de domaine DEPANMOI.LAN avec succès

ATTENTION : Les avertissements relatifs à la délégation DNS ("Impossible de créer une délégation DNS") sont normaux lors de la création d'une première forêt. Ils n'impactent pas le fonctionnement.

6. Configuration de l'Active Directory

6.1 Structure organisationnelle (OUs)

L'annuaire Active Directory est structuré selon les besoins opérationnels de DEPANMOI.FR. Les unités organisationnelles (OU) reflètent la hiérarchie métier :

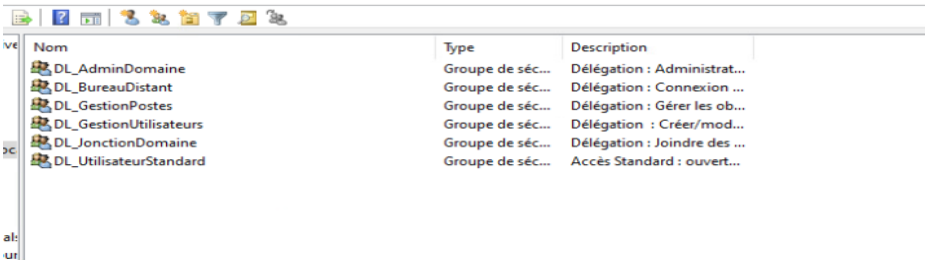
- OU Direction : contient les comptes des responsables avec droits étendus.
- OU Techniciens : contient les comptes des techniciens systèmes et réseaux.
- OU Postes : contient les objets ordinateurs joints au domaine.

6.2 Création des groupes de sécurité

Six groupes de délégation (préfixe DL_) sont créés pour structurer les permissions sans affecter directement les comptes utilisateurs :

Groupe	Rôle et description
DL_AdminDomaine	Délégation : administration complète du domaine
DL_BureauDistant	Délégation : connexion Bureau à distance autorisée
DL_GestionPostes	Délégation : gestion des objets ordinateurs
DL_GestionUtilisateurs	Délégation : création/modification des comptes utilisateurs
DL_JonctionDomaine	Délégation : jonction de postes au domaine
DL_UtilisateurStandard	Accès standard : ouverture de session de base

Tableau 6 — Groupes de délégation Active Directory créés dans DEPANMOI.LAN

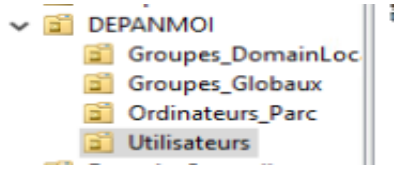


Groupes de sécurité DL_ visibles dans la console Utilisateurs et ordinateurs Active Directory

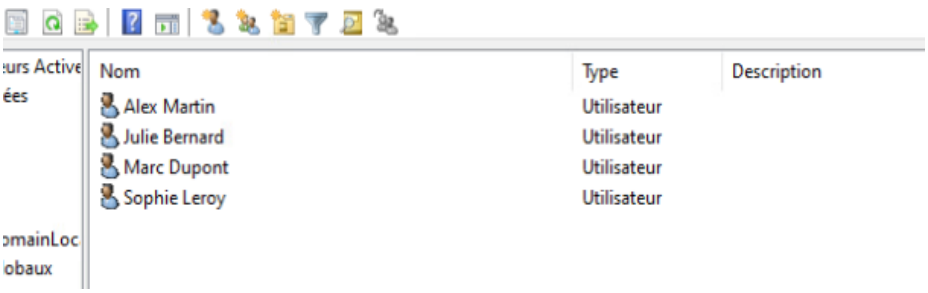
6.3 Création des comptes utilisateurs

Les comptes utilisateurs sont créés dans les OUs correspondantes. La convention de nommage retenue est : première lettre du prénom + nom de famille (ex. : ltechnicien1).

33. Ouvrir Outils > Utilisateurs et ordinateurs Active Directory.
34. Naviguer vers l'OU cible.
35. Clic droit > Nouveau > Utilisateur.
36. Renseigner le nom d'affichage, le nom de connexion et le mot de passe initial.
37. Cocher "L'utilisateur doit changer de mot de passe à la prochaine ouverture de session".
38. Ajouter l'utilisateur dans les groupes DL_ appropriés.



Arborescence AD : UO et comptes utilisateurs dans la console MMC



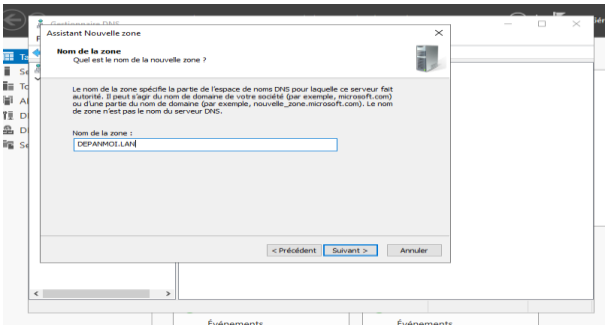
Liste des utilisateurs et groupes dans l'OU DEPANMOI.LAN

7. Configuration du service DNS

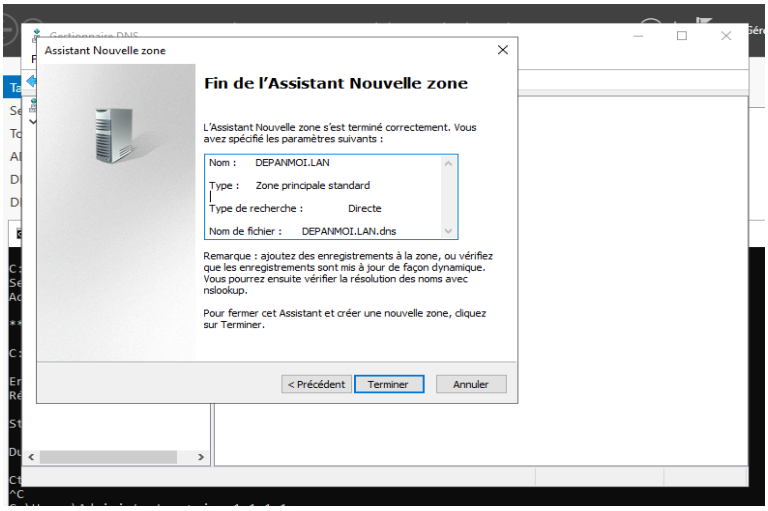
7.1 Zone de recherche directe

Le serveur DNS de Windows Server 2022 gère la résolution des noms internes au domaine DEPANMOI.LAN. Une zone principale standard est configurée pour les enregistrements internes.

39. Ouvrir Outils > Gestionnaire DNS.
40. Dans le volet gauche, faire un clic droit sur "Zones de recherche directe" > Nouvelle zone.
41. Sélectionner "Zone principale" et cocher "Stocker la zone dans Active Directory".
42. Saisir le nom de zone : DEPANMOI.LAN.
43. Terminer l'assistant.



Gestionnaire DNS : affichage des zones disponibles dans le domaine DEPANMOI.LAN

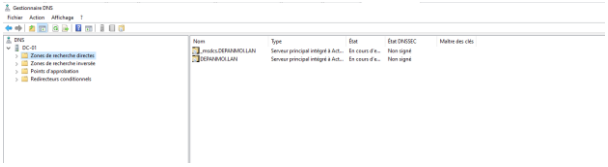


Fin de l'assistant de création de zone : zone DEPANMOI.LAN créée en zone principale standard

7.2 Transfert conditionnel (Forwarders)

Les requêtes DNS externes (Internet) sont transmises aux serveurs DNS4EU qui filtrent les sites malveillants. Ce choix est cohérent avec le contexte professionnel d'une TPE ne disposant pas d'un filtrage web dédié.

44. Dans le Gestionnaire DNS, clic droit sur le serveur > Propriétés.
45. Onglet "Redirecteurs" > Modifier.
46. Ajouter les IP : 86.54.11.1 et 86.54.11.201 (DNS4EU, filtrage malveillant).
47. Valider et fermer.



Confirmation de la résolution DNS interne opérationnelle depuis le gestionnaire DNS

NOTE : Les serveurs DNS4EU (86.54.11.1 / 86.54.11.201) sont des serveurs publics européens incluant un blocage automatique des domaines malveillants. Ils constituent un premier niveau de protection sans coût supplémentaire.

8. Configuration du service DHCP

8.1 Autorisation du serveur DHCP dans Active Directory

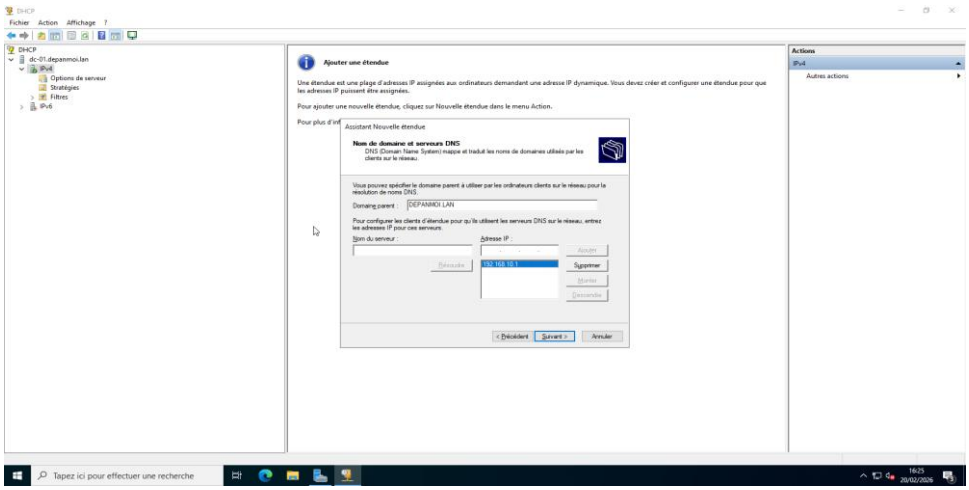
Un serveur DHCP Windows doit être autorisé dans Active Directory avant de pouvoir distribuer des adresses. Cette mesure de sécurité empêche les serveurs DHCP non autorisés de fonctionner sur le réseau.

48. Dans le Gestionnaire DHCP, clic droit sur le nom du serveur.
49. Sélectionner "Autoriser".
50. Attendre quelques secondes, l'icône du serveur passe au vert.

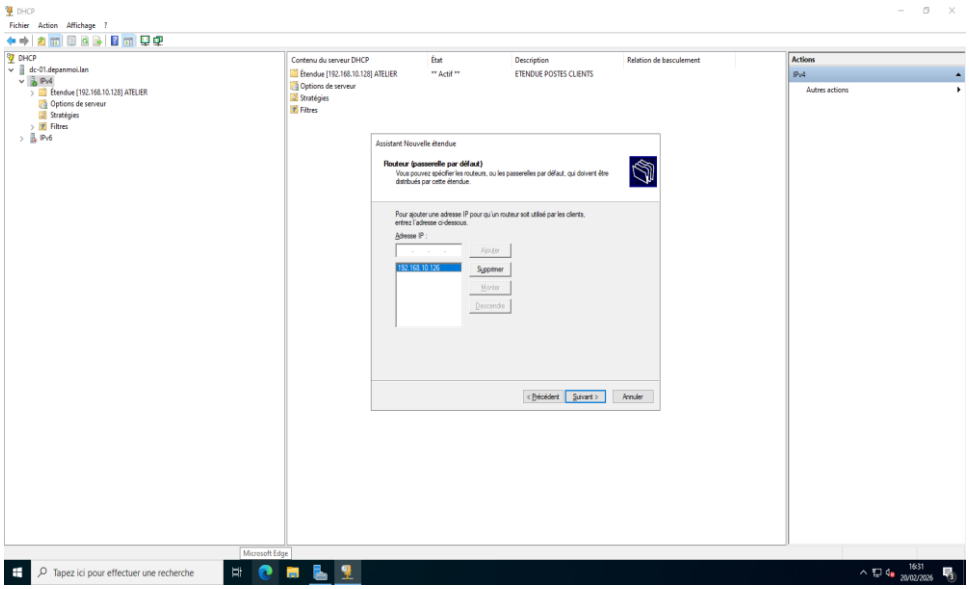
8.2 Création de l'étendue VLAN ADMIN (610)

L'étendue ADMIN distribue des adresses IP aux postes et serveurs du VLAN interne. Les options DHCP 066 et 067 sont configurées pour le boot PXE via FOG.

51. Dans le Gestionnaire DHCP, clic droit sur IPv4 > Nouvelle étendue.
52. Nom de l'étendue : ETENDUE ADMIN.
53. Plage de distribution : 192.168.10.10 à 192.168.10.120.
54. Masque de sous-réseau : 255.255.255.128 (/25).
55. Passerelle par défaut (option 3) : 192.168.10.126.
56. Serveur DNS (option 6) : 192.168.10.1.
57. Configurer l'option 066 (serveur de boot TFTP) : 192.168.10.2.
58. Configurer l'option 067 (fichier de boot PXE) : ipxe.efi
59. Activer l'étendue.



Console DHCP : étendue ADMIN configurée avec plage 192.168.10.0/25

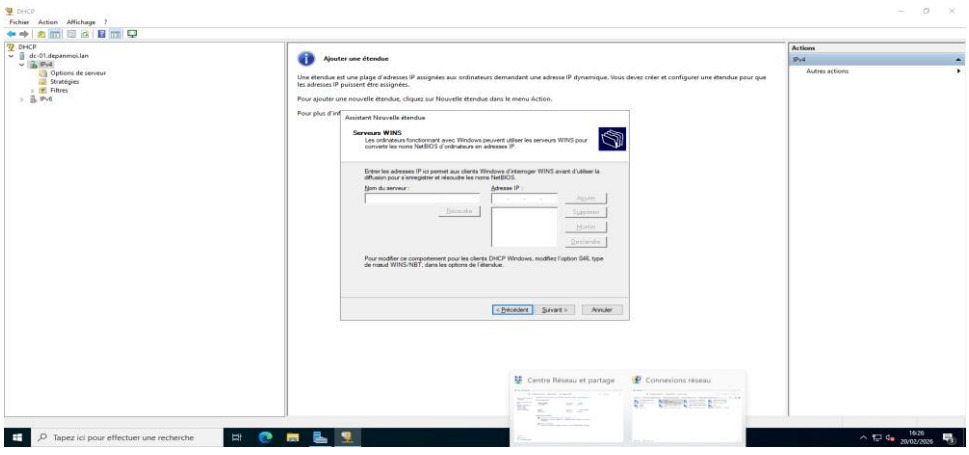


Configuration du routeur (passerelle) dans l'étendue ADMIN : 192.168.10.126

8.3 Création de l'étendue VLAN ATELIER (620)

L'étendue ATELIER distribue des adresses aux machines clientes déposées pour réparation. Les mêmes options PXE sont définies pour permettre le redéploiement automatique des postes.

60. Créer une nouvelle étendue nommée "ETENDUE POSTES CLIENTS".
61. Plage de distribution : 192.168.10.130 à 192.168.10.250.
62. Masque de sous-réseau : 255.255.255.128 (/25).
63. Passerelle par défaut : 192.168.10.254.
64. Serveur DNS : 192.168.10.1.
65. Options 066 et 067 identiques à l'étendue ADMIN.
66. Activer l'étendue.



Étendue ATELIER active dans la console DHCP avec plage 192.168.10.128/25

CONSEIL : Réserver les adresses des serveurs (192.168.10.1 pour DC-01, 192.168.10.2 pour PXE-01, 192.168.10.126 pour NAT-00) en tant qu'exclusions dans les étendues pour éviter tout conflit.

9. Installation du serveur FOG Project

9.1 Installation de Debian 12 (système hôte)

FOG Project nécessite un système Linux. Debian 12 (Bookworm) est utilisé pour sa stabilité et sa compatibilité avec les packages FOG. La VM est configurée avec une adresse IP statique 192.168.10.2/25 dans le VLAN ADMIN.

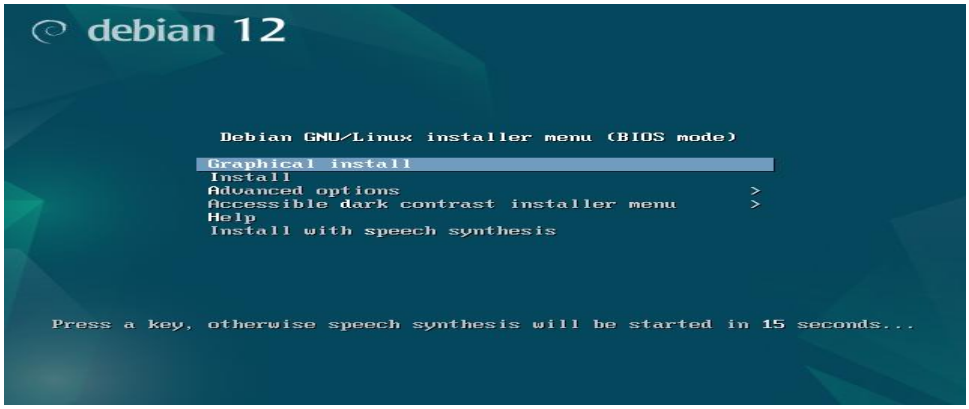
9.1.1 Configuration réseau post-installation

Éditer le fichier de configuration réseau :

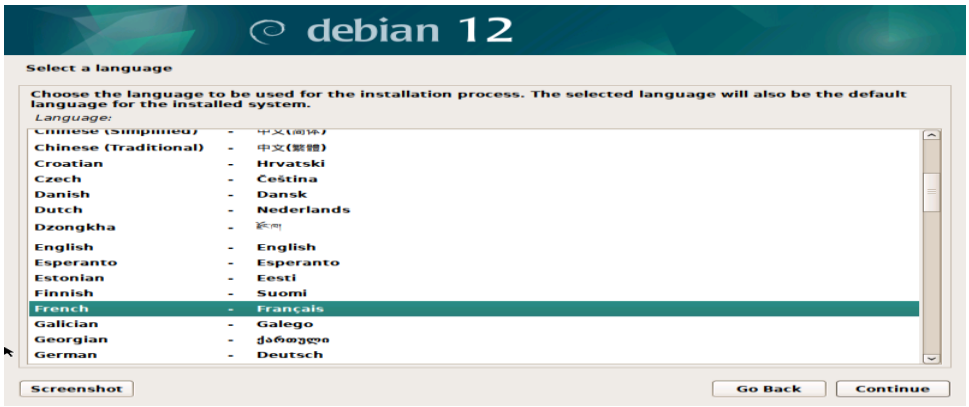
```
nano /etc/network/interfaces
```

Ajouter la configuration statique :

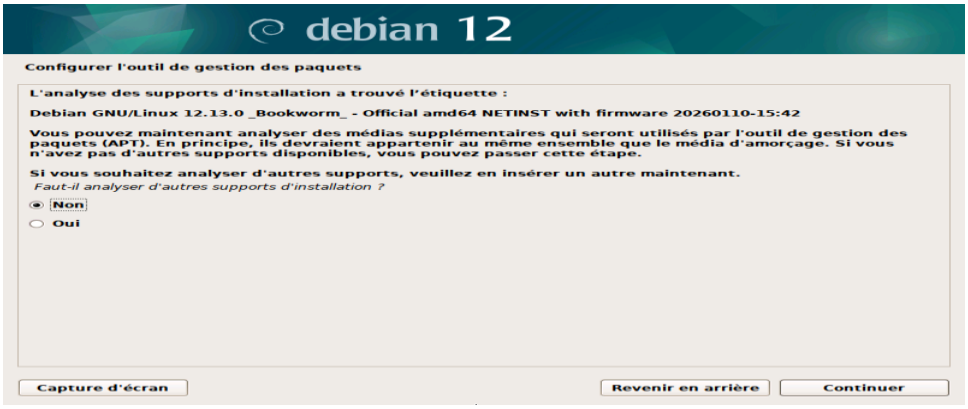
```
auto ens192
iface ens192 inet static
    address 192.168.10.2
    netmask 255.255.255.128
    gateway 192.168.10.126
    dns-nameservers 192.168.10.1
```



Écran de démarrage de l'installation Debian 12 sur la VM PXE-01



Partitionnement et configuration du système Debian 12



Finalisation de l'installation Debian et configuration du compte root

9.2 Installation de FOG Project

FOG Project est installé via son script d'installation officiel. La procédure nécessite une connexion Internet active pour télécharger les dépendances.

67. Mettre à jour le système Debian :

```
apt update && apt upgrade -y
```

68. Installer git :

```
apt install git -y
```

69. Cloner le dépôt FOG Project :

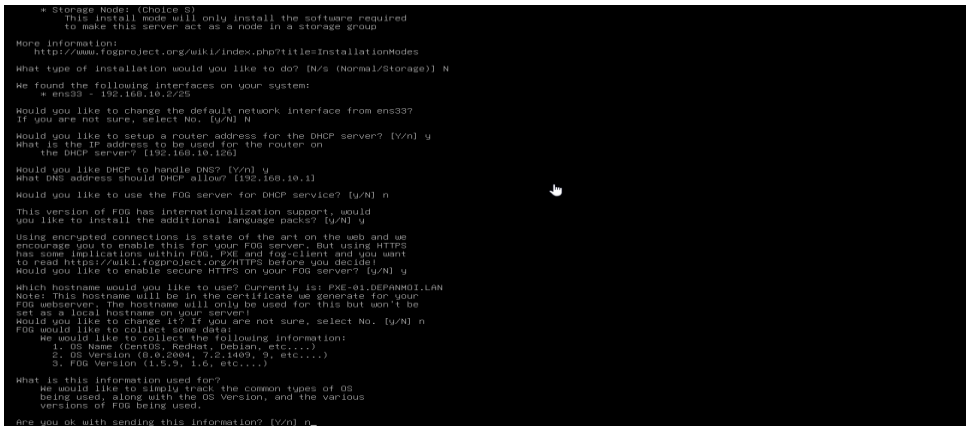
```
cd /root && git clone https://github.com/FOGProject/fogproject.git fogproject
```

70. Lancer le script d'installation :

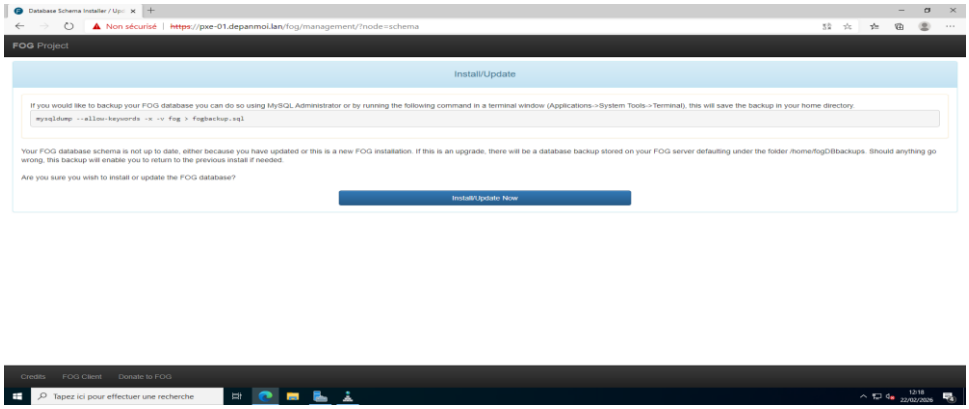
```
cd fogproject/bin && ./installfog.sh
```

71. Répondre aux questions de l'assistant :

- Linux OS : Debian
- Utiliser les paramètres par défaut pour la majorité des options.
- Désactiver l'option "DHCP" intégrée à FOG (le DHCP est géré par Windows Server).
- Activer HTTPS si souhaité.



Interface web FOG accessible via https://pxe-01.depanmoi.lan/fog/management après installation

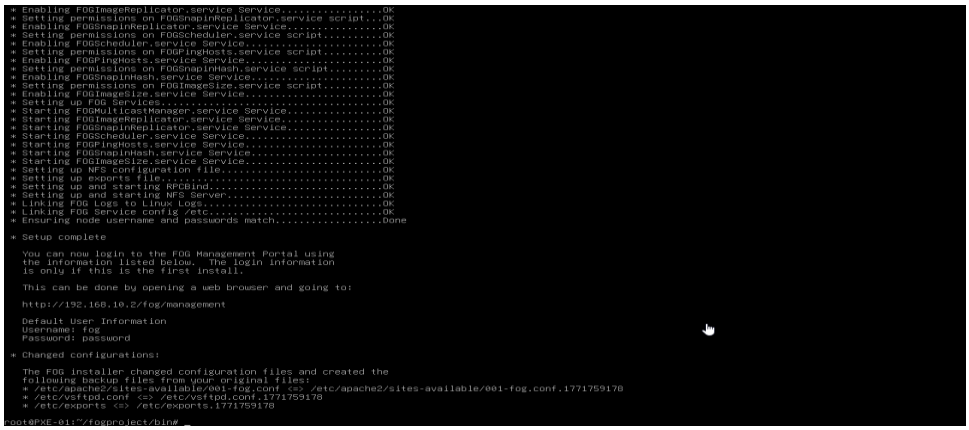


Page de mise à jour du schéma de base de données FOG : cliquer sur "Install/Update Now" pour finaliser

72. Une fois l'installation terminée, accéder à l'interface web :

```
https://pxe-01.depanmoi.lan/fog/management
```

73. Cliquer sur "Install/Update Now" pour initialiser la base de données FOG.
74. Se connecter avec les identifiants par défaut : fog / password.
75. Changer immédiatement le mot de passe administrateur.

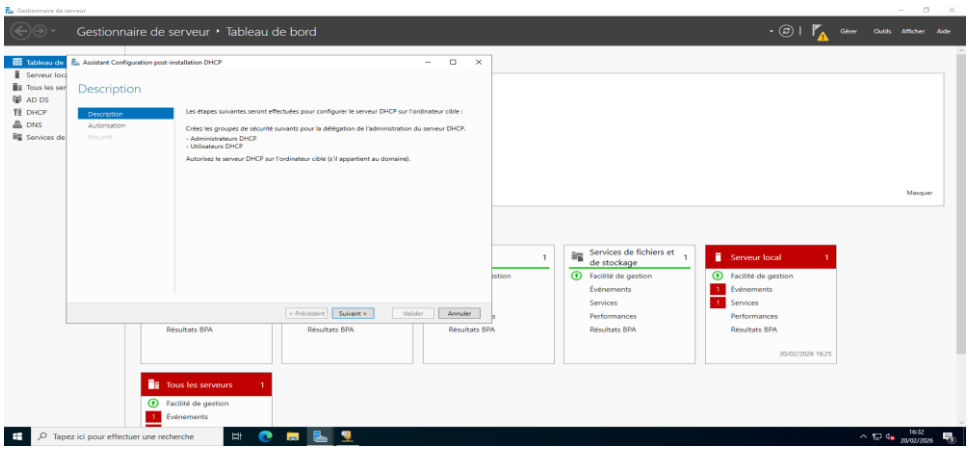


Fin de l'installation FOG en console : tous les services démarrés avec succès (Setup complete)

NOTE : L'URL de gestion FOG finale est : http://192.168.10.2/fog/management. Les identifiants par défaut sont fog/password. Ce mot de passe doit être changé immédiatement après la première connexion.

9.3 Vérification DNS et DHCP pour FOG

Une fois FOG installé, vérifier que l'enregistrement DNS du serveur est correctement résolu et que le DHCP distribue bien les options PXE.



Console DHCP : configuration des options serveur (066 et 067) pour le boot PXE via FOG

10. Intégration des postes clients Windows 10

10.1 Capture d'une image master via FOG

Avant de déployer des postes, il est nécessaire de capturer une image "maître" Windows 10 proprement configurée. Cette image sera ensuite déployée en masse via PXE.

76. Préparer un poste Windows 10 avec les configurations souhaitées (logiciels, paramètres).
77. Inscrire ce poste dans FOG (hôte FOG avec MAC address).
78. Dans l'interface FOG, créer une nouvelle image et l'associer à l'hôte.
79. Planifier une tâche "Capture" pour cet hôte.
80. Démarrer le poste en PXE (F12 ou boot réseau dans le BIOS).
81. FOG démarre automatiquement la capture. La durée est d'environ 15 à 30 minutes selon la taille du disque.

10.2 Déploiement PXE d'un poste client

Le déploiement automatisé d'un poste via PXE réduit le temps d'installation de 2 heures à moins de 30 minutes, sans intervention physique.

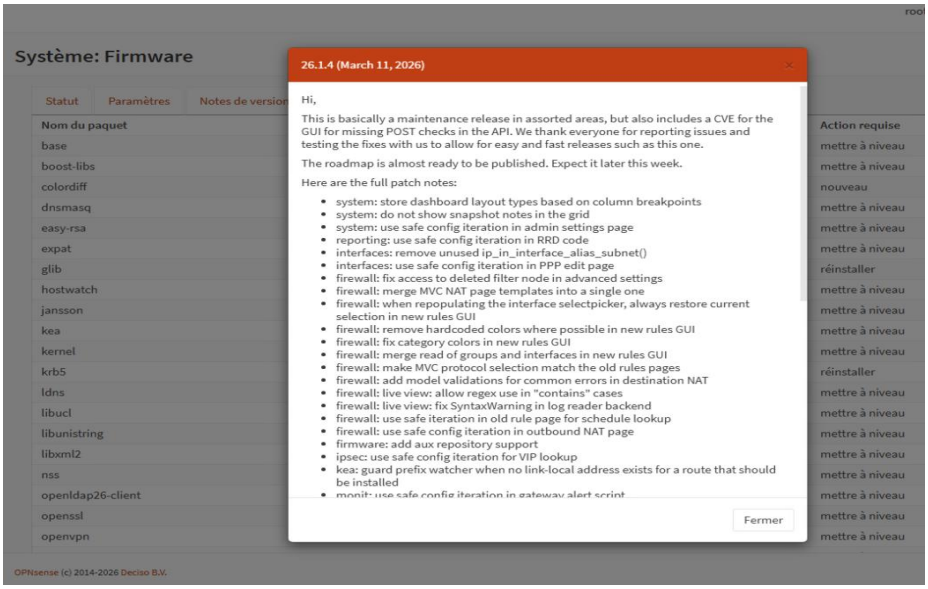
82. Brancher la machine cliente sur le réseau VLAN ATELIER (620).
83. Configurer le BIOS/UEFI du poste pour booter en réseau (PXE) en première priorité.
84. Au démarrage, le poste obtient une adresse DHCP et reçoit les options 066/067.
85. Le menu FOG apparaît, choisir "Deploy" pour déployer l'image.
86. Le déploiement s'effectue automatiquement. Le poste redémarre sur Windows 10 une fois terminé

11. Guide de maintenance

11.1 Mises à jour OPNsense

OPNsense publie régulièrement des mises à jour de sécurité et des correctifs. Il est recommandé d'appliquer les mises à jour au minimum une fois par mois.

87. Accéder à System > Firmware > Status.
88. Cliquer sur "Vérifier les mises à jour".
89. Si des mises à jour sont disponibles, cliquer sur "Mettre à niveau".
90. Planifier la mise à jour en dehors des heures de bureau.



Interface de gestion des mises à jour firmware OPNsense : version 26.1.4 disponible avec notes de version détaillées

ATTENTION : Effectuer une sauvegarde de la configuration OPNsense (System > Configuration > Backups) avant toute mise à jour majeure. Un snapshot ESXi de la VM est également recommandé.

11.2 Sauvegarde de l'Active Directory

La sauvegarde de l'état système de Windows Server inclut l'Active Directory, le DNS et le DHCP. Utiliser Windows Server Backup ou un outil tiers compatible VSS.

91. Installer la fonctionnalité "Sauvegarde Windows Server" depuis le Gestionnaire de serveur.
92. Configurer une sauvegarde quotidienne vers un partage réseau ou un disque externe.
93. Vérifier régulièrement les journaux de sauvegarde.

```
wbadmin start systemstatebackup -backupTarget:D: -quiet
```

11.3 Vérification des services

Une procédure de vérification hebdomadaire est recommandée pour s'assurer du bon fonctionnement de l'infrastructure. La commande suivante vérifie les services clés sur Windows Server :

```
Get-Service ADWS,DNS,DHCPServer | Select Name,Status
```

Pour tester la résolution DNS depuis un client :

```
nslookup dc-01.depanmoi.lan 192.168.10.1
```

Pour tester la connectivité DHCP depuis un client :

```
ipconfig /release
```

```
ipconfig /renew
```

11.4 Surveillance des logs FOG

FOG génère des journaux accessibles via l'interface web et sur le serveur Debian.

```
tail -f /var/log/apache2/error.log
journalctl -u FOGMulticastManager -f
```

12. FAQ et guide de dépannage

Un poste ATELIER ne reçoit pas d'adresse IP via DHCP

ATTENTION : Vérifier que le DHCP Relay est actif sur OPNsense (Services > DHCPRelay) et que la destination pointe vers 192.168.10.1. Vérifier également que l'étendue ATELIER est active dans la console DHCP Windows Server.

Un poste ne démarre pas en PXE

ATTENTION : Vérifier les options DHCP 066 et 067 dans les deux étendues. S'assurer que le poste est correctement configuré pour booter en réseau (UEFI vs Legacy BIOS peut nécessiter des fichiers de boot différents : ipxe.efi pour UEFI, undionly.kpxe pour BIOS).

Un poste ne parvient pas à rejoindre le domaine

ATTENTION : Contrôler que le DNS du poste pointe sur 192.168.10.1. Tester avec nslookup depanmoi.lan. Si la résolution échoue, vérifier la configuration DNS sur Windows Server. Vérifier aussi que le compte utilisé appartient bien au groupe DL_JonctionDomaine.

L'interface web d'OPNsense affiche une erreur de certificat

NOTE : C'est un comportement normal avec le certificat auto-signé par défaut. Cliquer sur "Continuer (non sécurisé)" ou installer un certificat signé par une PKI interne. Ne pas supprimer l'avertissement en désactivant HTTPS.

Un poste ATELIER peut communiquer avec un serveur ADMIN

ATTENTION : Vérifier les règles de pare-feu OPNsense sur l'interface OPT1 (VLAN 620). La règle de blocage du trafic vers le VLAN ADMIN doit être la première règle active. Relancer un test avec ping ou tracert pour confirmer le blocage.

FOG affiche "No hosts found" lors d'une tâche de déploiement

NOTE : Vérifier que l'adresse MAC du poste est bien enregistrée dans FOG. L'enregistrement peut se faire automatiquement si l'option "Auto registration" est activée dans FOG, ou manuellement via l'interface web.

Le service DHCP Windows Server ne démarre pas

ATTENTION : Vérifier que le serveur est autorisé dans Active Directory (clic droit > Autoriser dans la console DHCP). Si l'autorisation est présente mais que le service ne démarre pas, vérifier le journal des événements Windows (Observateur d'événements > Journaux Windows > Système).

Les mises à jour OPNsense échouent

NOTE : S'assurer que l'interface WAN dispose d'un accès Internet. Tester depuis la console OPNsense avec : ping 8.8.8.8. Vérifier également que la passerelle WAN est bien configurée dans System > Gateways.

13. Conclusion

L'infrastructure déployée pour DEPANMOI.FR répond à l'ensemble des problématiques identifiées en phase de diagnostic. Les trois axes du projet ont été pleinement réalisés :

- Sécurisation réseau : la segmentation par VLANs avec OPNsense garantit l'isolation stricte des machines clientes vis-à-vis des serveurs internes. Le risque de propagation d'une infection depuis un poste client est fortement limité.
- Centralisation des accès : l'Active Directory sur Windows Server 2022 offre une gestion unifiée des utilisateurs, des groupes et des politiques de sécurité. Les droits sont attribués via des groupes de délégation, facilitant l'évolution future de l'organisation.
- Industrialisation du déploiement : FOG Project permet de déployer un poste de travail complet en moins de 30 minutes contre 2 heures auparavant, sans aucune intervention physique sur le poste. Le gain de productivité est immédiat et mesurable.

Cette architecture, bien que déployée sur un environnement virtualisé de taille modeste, est directement applicable en production et évolutive. Elle constitue une base solide pour intégrer de futures améliorations :

- Mise en place de GPO (Group Policy Objects) pour standardiser les postes de travail qui intègreront le domaine.
- Déploiement d'un serveur WSUS pour centraliser les mises à jour Windows interne.

Documentation rédigée par LOPES DA SILVA Lucas — BTS SIO SISR — Session 2026

Portfolio : https://portfolio.kairrin.net/fr/epreuves/e6/#situation-2-systeme