RÉALISATION PROFESSIONNELLE N°2

Domaine Active Directory et déploiement automatisé des postes

Documentation technique de la mission menée pour l'organisation cliente DEPANMOI.FR, mise en place d'un contrôleur de domaine Active Directory (AD DS, DNS, DHCP), d'une passerelle de filtrage OPNsense segmentant le réseau, et d'une chaîne d'industrialisation du déploiement des postes par FOG et amorçage réseau PXE.

VERSION INTÉGRALE

CANDIDAT
LOPES--DA SILVA, Lucas

N° CANDIDAT
02251770429

CENTRE DE FORMATION
SCHOLA NOVA

PÉRIODE DE RÉALISATION
Janvier, Février 2025

MODALITÉ
Réalisation conduite seul

FORME DE L'ÉPREUVE
Épreuve ponctuelle

TABLE DES MATIÈRES

Sommaire

PARTIE 8 Annexes

PARTIE 1

Présentation du contexte client

1.1 · L'organisation DEPANMOI.FR

DEPANMOI.FR est une très petite entreprise (TPE) lyonnaise spécialisée dans le dépannage informatique, la maintenance de parcs et le conseil technologique auprès de professionnels et de particuliers. Une partie significative de son chiffre d'affaires provient de la **préparation et de la livraison de postes** : machines neuves, reconditionnées ou réinstallées après sinistre, qui doivent toutes repartir avec un socle logiciel homogène.

Fiche d'identité

Activité	Dépannage informatique, maintenance de parcs, conseil technologique
Siège et atelier	15 Avenue de la République, 69007 Lyon
Chiffre d'affaires	200 000 € (dernier exercice clos)
Effectif	1 gérant, 2 techniciens systèmes et réseaux, 1 secrétaire comptable
Clientèle	20 clients actifs, PME locales et particuliers

1.2 · Le système d'information existant

Avant la mission, le système d'information de DEPANMOI.FR ne comportait **aucun service centralisé**. Chaque poste était autonome : comptes locaux, adressage IP saisi à la main ou laissé sur la box du fournisseur d'accès, résolution de noms inexistante en interne. Les postes destinés aux clients étaient installés un par un depuis une clé USB, puis chaque logiciel était téléchargé et paramétré manuellement.

Élément	État avant mission
Authentification	Comptes locaux par poste, aucun annuaire
Adressage IP	Box FAI ou saisie manuelle, aucun plan formalisé
Résolution de noms	Aucune zone interne, dépendance au DNS du FAI
Préparation des postes	Installation manuelle, 2 h par machine
Segmentation réseau	Réseau unique à plat, aucune séparation serveurs / postes

1.3 · Problématique

L'installation artisanale des postes coûte du temps non facturable, produit des configurations qui ne sont jamais tout à fait identiques et repose sur la mémoire du technicien plutôt que sur une procédure. L'absence d'annuaire empêche toute administration centralisée des comptes et toute traçabilité. La problématique de la mission est donc double : **doter l'entreprise d'un socle d'annuaire** et **industrialiser la fabrication des postes**.

CONSÉQUENCES DE LA SITUATION INITIALE

- Temps de préparation élevé et non rentable (deux heures par poste).
- Dérive de configuration : deux postes « identiques » ne le sont jamais vraiment.
- Aucune base d'authentification ni de politique commune applicable.
- Aucun inventaire fiable du matériel préparé ni des images livrées.
- Réinstallation après panne repartant systématiquement de zéro.
- **Risque de sécurité** : les machines clientes en réparation, souvent infectées, partageaient le même réseau que les serveurs internes.

CADRE JURIDIQUE

Les postes préparés traitent des données de clients de DEPANMOI.FR. L'annuaire centralise l'authentification et la traçabilité des accès, et l'image de référence garantit une configuration maîtrisée sur chaque machine livrée. Ces deux points soutiennent les obligations de l'entreprise au titre du RGPD (responsabilité du traitement, sécurité et journalisation des accès).

1.4 · Objectifs de la mission

La mission vise à mettre en place un socle système cohérent, articulé autour de quatre briques : un annuaire, des services d'infrastructure (DNS, DHCP), une passerelle segmentant le réseau, et une chaîne de déploiement de masse.

Objectif	Moyen technique retenu
Centraliser l'authentification et l'administration	Domaine **Active Directory** (forêt `DEPANMOI.LAN`) sur DC-01
Fiabiliser la résolution de noms interne	Service **DNS** intégré à l'annuaire, zones directe et inverse
Automatiser l'adressage des postes	Service **DHCP** hébergé sur DC-01, une étendue par périmètre
Segmenter et filtrer les flux	Passerelle **OPNsense** (NAT-00), périmètres ADMIN et ATELIER
Industrialiser l'installation des postes	Déploiement de masse par **FOG** et amorçage réseau PXE

PARTIE 2

Cahier des charges technique

2.1 · Périmètre fonctionnel

La mission porte sur le **socle système et l'industrialisation du déploiement** des postes de DEPANMOI.FR. Elle s'appuie sur une plateforme virtualisée (VMware ESXi) regroupant un contrôleur de domaine Windows Server, une passerelle OPNsense, un serveur de déploiement Debian/FOG et un poste de référence Windows 11. Cinq services composent le périmètre fonctionnel :

1. **Annuaire de domaine** Active Directory (forêt `DEPANMOI.LAN`) pour centraliser l'authentification.
2. **Résolution de noms** par DNS intégré à l'annuaire, zones directe et inverse.
3. **Adressage automatique** par DHCP, une étendue distincte par périmètre réseau.
4. **Segmentation et filtrage** entre le périmètre d'administration (serveurs) et le périmètre atelier (postes).
5. **Déploiement de masse** des postes par amorçage réseau PXE et clonage d'image FOG.

✓ DANS LE PÉRIMÈTRE

- Installation et promotion du contrôleur de domaine (AD DS, DNS, DHCP)
- Configuration de la passerelle OPNsense (interfaces, relais DHCP, filtrage, NAT)
- Installation du serveur FOG sous Debian et préparation du poste master
- Capture et déploiement de l'image de référence
- Plan d'adressage, procédure de mise en œuvre, plan de tests, documentation

✘ HORS PÉRIMÈTRE

- Stratégies de groupe (GPO) avancées et déploiement applicatif par GPO
- Second contrôleur de domaine (haute disponibilité de l'annuaire)
- Sauvegarde applicative et données métier (CRM, comptabilité)
- Messagerie et services collaboratifs
- Supervision centralisée, IDS / IPS, antivirus géré

2.2 · Exigences fonctionnelles

Chaque exigence fonctionnelle est identifiée par un code `EF-XX`, priorisée selon la méthode MoSCoW et associée à un critère de validation testable lors de la recette (partie 5).

MUST
Exigence non négociable
, la solution est rejetée si elle n'est pas remplie.

SHOULD
Exigence importante
, la solution fonctionne sans, mais sa qualité serait dégradée.

COULD
Exigence optionnelle
, réalisée si le temps le permet.

~~WON'T~~
Exclusion explicite
, décision assumée pour ce projet.

EF-01 Annuaire de domaine Active Directory — MUST

Le système d'information doit disposer d'un annuaire de domaine centralisant comptes et authentification. Une nouvelle forêt est créée, de domaine racine `DEPANMOI.LAN`, portée par un contrôleur de domaine dédié (DC-01) au niveau fonctionnel le plus élevé disponible.

CRITÈRE DE VALIDATION

Le domaine `DEPANMOI.LAN` est promu et sain (vérifié par `dcdiag`). Un poste Windows peut être joint au domaine et un compte de domaine peut y ouvrir une session.

EF-02 Résolution de noms interne (DNS) — MUST

Un service DNS intégré à l'annuaire doit résoudre les noms des hôtes du domaine en adresses (zone directe) et les adresses en noms (zone de recherche inversée). Les requêtes externes sont confiées à des redirecteurs publics.

CRITÈRE DE VALIDATION

`nslookup dc-01.depanmoi.lan` renvoie 192.168.10.1 ; `nslookup 192.168.10.2` renvoie `pxe-01.depanmoi.lan` ; un nom public est résolu via les redirecteurs.

EF-03 Adressage automatique par périmètre (DHCP) — MUST

L'adressage IPv4 des postes doit être distribué automatiquement, avec une étendue dédiée par périmètre (ADMIN et ATELIER). Chaque étendue fournit la passerelle et le serveur DNS appropriés.

CRITÈRE DE VALIDATION

Un poste du périmètre ADMIN obtient un bail dans 192.168.10.0/25 (passerelle .126) ; un poste de l'atelier obtient un bail dans 192.168.10.128/25 (passerelle .254). DNS .1 dans les deux cas.

EF-04 Amorçage réseau des postes (PXE) — MUST

Un poste vierge doit pouvoir démarrer entièrement depuis le réseau, sans support physique. Le DHCP distribue les options d'amorçage (066 serveur de démarrage, 067 fichier de démarrage) pointant vers le serveur FOG.

CRITÈRE DE VALIDATION

Un poste configuré pour le démarrage réseau charge `ipxe.efi` depuis 192.168.10.2 et affiche le menu d'amorçage FOG.

EF-05 Image de référence unique et déployable — MUST

Un poste de référence (master) doit être préparé une seule fois, système, pilotes, suite logicielle commune, puis généralisé et capturé en une image que l'on déploie à l'identique sur tout nouveau poste.

CRITÈRE DE VALIDATION

L'image du master est capturée dans FOG, puis déployée sur un poste cible qui démarre opérationnel et conforme au master, sans conflit d'identité (Sysprep appliqué).

EF-06 Segmentation et isolation ADMIN / ATELIER — MUST

Le réseau doit être segmenté en deux périmètres : ADMIN (serveurs : contrôleur de domaine, serveur de déploiement) et ATELIER (postes en cours de préparation). Les postes de l'atelier ne doivent pas pouvoir atteindre librement le périmètre d'administration.

CRITÈRE DE VALIDATION

Un poste de l'atelier ne peut pas joindre 192.168.10.0/25 hors des services explicitement autorisés (DNS du DC, serveur FOG, relais DHCP). Le blocage est porté par une règle de pare-feu vérifiable.

EF-07 Relais DHCP de l'atelier vers le contrôleur

SHOULD

Le serveur DHCP étant hébergé sur DC-01 (périmètre ADMIN), les demandes des postes de l'atelier, situés dans un autre domaine de diffusion, doivent être relayées vers le contrôleur par la passerelle OPNsense.

CRITÈRE DE VALIDATION

Le relais DHCP est actif sur l'interface ATELIER d'OPNsense, destination 192.168.10.1, et un poste de l'atelier obtient bien un bail dans l'étendue ATELIER.

EF-08 Sortie Internet filtrée

MUST

Les deux périmètres doivent accéder à Internet via la passerelle OPNsense, qui assure le NAT vers le lien WAN du FAI. Le trafic sortant est filtré selon le principe du moindre privilège côté atelier.

CRITÈRE DE VALIDATION

Un poste obtient un accès Internet via NAT OPNsense. Les flux atelier suivent les règles définies (services autorisés, blocage ADMIN, Internet en dernier).

2.3 · Exigences non fonctionnelles

Les exigences non fonctionnelles décrivent la qualité attendue : performance, sécurité, maintenabilité, traçabilité.

Identifiant	Catégorie	Exigence	Seuil mesurable
`ENF-01`	Performance	Temps de préparation d'un nouveau poste par déploiement d'image	Inférieur à **30 min** (contre 2 h en manuel)
`ENF-02`	Homogénéité	Conformité des postes déployés au master	Postes **identiques** (même image de référence)
`ENF-03`	Coût	Recours à des solutions libres	Au moins **deux serveurs** sous logiciel libre (Debian, OPNsense)
`ENF-04`	Sécurité	Isolation du périmètre d'administration vis-à-vis de l'atelier	Accès ATELIER → ADMIN **bloqué** par défaut
`ENF-05`	Maintenabilité	Nommage des hôtes	FQDN de la forme `HOTE.DEPANMOI.LAN`
`ENF-06`	Stabilité	Adressage des serveurs	Adresses **fixes** hors plage DHCP (DC-01 .1, PXE-01 .2)
`ENF-07`	Traçabilité	Sauvegarde des configurations et de l'image	Export XML OPNsense + image FOG + machines virtuelles archivées
`ENF-08`	Maintenabilité	Documentation du plan d'adressage et de la topologie	Plan d'adressage + schéma logique livrés (partie 3)

2.4 · Contraintes

Contraintes matérielles et de virtualisation

Élément	Référence	Rôle dans la solution
Hyperviseur	VMware ESXi (machines `.vmx` / `.ovf`)	Plateforme d'hébergement des quatre VM
DC-01	Windows Server 2025 (Expérience de bureau)	Contrôleur de domaine, DNS, DHCP
NAT-00	OPNsense (FreeBSD)	Passerelle, pare-feu, relais DHCP, NAT
PXE-01	Debian 13, FOG 1.5.10	Serveur de déploiement d'images
CLIENT-01	Windows 11 Pro	Poste master puis poste cible

Contraintes logicielles et protocolaires

- Recours privilégié aux **solutions libres** pour les serveurs d'infrastructure périphériques (Debian pour FOG, OPNsense pour la passerelle).
- Amorçage réseau standard **PXE / iPXE** ; protocoles d'image FOG sur TFTP, HTTP et NFS.
- Le serveur DHCP intégré de FOG n'est pas utilisé : l'adressage et les options d'amorçage restent gérés par le DHCP Windows, source unique de vérité.

Contraintes organisationnelles et budgétaires

- **Budget logiciel contraint** : aucune licence supplémentaire au-delà des systèmes déjà détenus.
- **Période de réalisation** : janvier à février 2025, en autonomie (seul), sous supervision pédagogique.
- **Continuité du contrat FAI** : le lien WAN reste géré par le FAI, OPNsense obtient son adresse WAN en DHCP.

2.5 · Justification des choix techniques

Cette section formalise le **dossier de choix** : pour chaque brique, les options envisageables sont mises en regard de critères explicites, et la solution retenue est déclinée jusqu'aux paramètres significatifs mis en œuvre en partie 4.

2.5.1 · Annuaire : Active Directory DS retenu

Le parc est composé de postes Windows. Il faut centraliser l'authentification et fournir les services d'infrastructure (DNS, DHCP) qui accompagnent un domaine.

Option	Intégration Windows	Services fournis	Coût	Décision
Groupe de travail	Aucune centralisation	Aucun	Nul	REJETÉ
Samba AD DC	Bonne mais partielle	LDAP, Kerberos, DNS	Nul (libre)	REJETÉ
Active Directory DS	Native	Annuaire, DNS, DHCP, GPO	Licence Windows Server	RETENU

Justification. Les postes clients étant sous Windows, AD DS offre l'intégration la plus directe : jonction au domaine en quelques clics, gestion par stratégie de groupe, et surtout les rôles *DNS* et *DHCP* hébergés sur le même serveur. Samba AD reproduit une partie de ces fonctions sans licence, mais ajoute une complexité d'administration et des limites de compatibilité avec les outils Windows natifs, sans bénéfice pour une TPE déjà détentrice d'une licence Windows Server. Le groupe de travail est éliminé d'emblée car il ne répond pas à l'objectif de centralisation.

PARAMÈTRES RETENUS

Forêt : nouvelle forêt, domaine racine `DEPANMOI.LAN` . · **Niveau fonctionnel :** Windows Server 2025. · **Rôles co-localisés :** serveur DNS et catalogue global sur DC-01. · **NetBIOS :** `DEPANMOI` .

2.5.2 · Déploiement de masse : FOG retenu

Il faut pouvoir installer un poste complet depuis le réseau et reproduire une image de référence à l'identique sur plusieurs machines.

Option	Coût	Amorçage réseau	Simplicité d'exploitation	Décision
Clonage manuel (clé/disque)	Nul	Non	Pénible, non reproductible	REJETÉ
WDS + MDT (Microsoft)	Licence Windows Server	Oui	Puissant mais lourd à mettre en place	REJETÉ
FOG (sur Debian)	Nul (libre)	Oui (iPXE)	Interface web, capture/déploiement simples	RETENU

Justification. FOG est une solution libre dédiée au clonage par le réseau : un seul serveur capture l'image du master et la redéploie sur tout poste enregistré, via une interface web claire. Le clonage manuel est exclu car ni rapide ni reproductible. WDS+MDT répondrait au besoin mais immobiliserait un second serveur Windows et demanderait une configuration sensiblement plus lourde (séquences de tâches, partages, WinPE) pour un parc modeste. FOG, hébergé sur Debian, satisfait l'exigence de solution libre (`ENF-03`) et tient sur une machine légère.

PARAMÈTRES RETENUS

Hôte : PXE-01, Debian 13. · **Mode d'installation :** `Normal Server` . · **Stockage des images :** `/images` . · **DHCP FOG :** désactivé (le DHCP Windows distribue les options d'amorçage). · **Fichier d'amorçage :** `ipxe.efi` (clients UEFI).

2.5.3 · Adressage des postes de l'atelier : relais DHCP retenu

Le serveur DHCP est sur DC-01, dans le périmètre ADMIN. Les postes de l'atelier sont dans un autre domaine de diffusion : leurs requêtes DHCP (diffusion) n'atteignent pas le contrôleur sans aide.

Option	Source de vérité d'adressage	Complexité	Cohérence options PXE	Décision
DHCP intégré à FOG	Deux serveurs DHCP	Risque de conflit	À synchroniser manuellement	REJETÉ
2e serveur DHCP côté atelier	Dispersée	Élevée	Dédoublée	REJETÉ
Relais DHCP sur OPNsense	DC-01 unique	Faible	Garantie (un seul DHCP)	RETENU

Justification. Conserver un **unique serveur DHCP** (le contrôleur) évite tout conflit de baux et garantit que les options d'amorçage PXE (066/067) sont distribuées de façon homogène aux deux périmètres. Le relais DHCP d'OPNsense transmet simplement les diffusions de l'atelier vers 192.168.10.1, sans dupliquer la configuration. Activer le DHCP de FOG ou poser un second serveur DHCP multiplierait les sources de vérité et les risques d'incohérence pour un bénéfice nul.

PARAMÈTRES RETENUS

Interface relais : ATELIER (OPT1). · **Destination :** `DC-01.DEPANMOI.LAN` = 192.168.10.1. · **Règle de pare-feu associée :** autorisation UDP 67-68 de l'atelier vers le pare-feu.

2.5.4 · Passerelle et filtrage : OPNsense retenu

Il faut une passerelle assurant le NAT vers le FAI, la segmentation des deux périmètres et le relais DHCP, avec un filtrage par interface.

Option	Coût	Filtrage par périmètre	Relais DHCP intégré	Décision
Box / routeur FAI	Nul	Très limité	Non	REJETÉ
pfSense	Nul (libre)	Oui	Oui	REJETÉ
OPNsense	Nul (libre)	Oui (par interface)	Oui	RETENU

Justification. OPNsense et pfSense répondent tous deux au besoin. OPNsense a été retenu pour son interface d'administration récente et lisible, son cycle de mises à jour soutenu et sa gestion claire du relais DHCP et des règles par interface, adaptés à la séparation ADMIN/ATELIER. La box FAI est écartée : elle n'offre pas de filtrage fin par périmètre ni de relais DHCP, et garderait l'entreprise dépendante d'un équipement non maîtrisé.

PARAMÈTRES RETENUS

Interfaces : WAN `em0` (DHCP FAI), LAN `em1` = 192.168.10.126/25 (ADMIN), OPT1 `em2` = 192.168.10.254/25 (ATELIER). · **NAT :** outbound automatique vers le WAN. · **Filtrage :** moindre privilège sur ATELIER, ouverture par défaut sur ADMIN.

2.6 · Hypothèses et exclusions

Hypothèses retenues

HYPOTHÈSES

- La plateforme de virtualisation est opérationnelle et dispose des réseaux virtuels nécessaires aux deux périmètres et au WAN.
- Une licence Windows Server valide est disponible pour DC-01.
- Le lien FAI fournit une adresse WAN en DHCP à OPNsense pendant la mission.
- Les postes cibles supportent l'amorçage réseau UEFI (PXE / iPXE).

Exclusions explicites (Won't have)

Décisions assumées de ne pas traiter dans ce projet, documentées avec leur risque résiduel.

`EF-09` **Haute disponibilité de l'annuaire (second DC)** ~~WON'T~~

Un second contrôleur de domaine fournirait la tolérance de panne de l'annuaire et du DNS, mais immobilise une machine supplémentaire à administrer. Pour une TPE de quatre personnes, le coût l'emporte sur le bénéfice à ce stade.

RISQUE RÉSIDUEL DOCUMENTÉ

DC-01 est un point de défaillance unique pour l'authentification et le DNS interne. Une sauvegarde de l'état système et une procédure de restauration compensent partiellement ce risque.

`EF-10` **Stratégies de groupe (GPO) avancées** ~~WON'T~~

Le déploiement applicatif et le durcissement des postes par GPO dépassent la cible de cette première mise en place du socle. Ils sont renvoyés au plan d'amélioration (partie 7.6).

RISQUE RÉSIDUEL DOCUMENTÉ

Les postes joints au domaine ne reçoivent pas encore de politique commune ; la standardisation repose pour l'instant sur l'image de référence.

EF-11 **Sauvegarde centralisée des données métier** ~~WON'T~~

La sauvegarde des données applicatives (CRM, comptabilité) reste gérée côté DEPANMOI.FR et n'entre pas dans le périmètre de la mission, centré sur le socle système et le déploiement.

RISQUE RÉSIDUEL DOCUMENTÉ

La protection des données métier dépend des dispositifs existants de l'entreprise, hors de cette réalisation.

2.7 · Livrables et critères de recette

Livrable	Description	Format
Documentation technique	Présent dossier en huit parties (contexte, cahier des charges, architecture, configurations, tests, incidents, retour d'expérience, annexes)	HTML / PDF
Machines virtuelles	VM archivées de DC-01, NAT-00, PXE-01 et CLIENT-01	VMware (.vmx / .ovf / .vmdk)
Sauvegarde OPNsense	Export XML de la configuration (interfaces, relais DHCP, règles)	XML
Image de référence	Image FOG du poste master (PC-MASTER)	Image FOG (stockage `/images`)
Plan d'adressage et schémas	Plan IPv4, schéma logique des périmètres et services	Tableaux + SVG (partie 3)
Procédure de mise en œuvre	Pas-à-pas reproductible permettant de redéployer le socle depuis zéro	Partie 4 du document

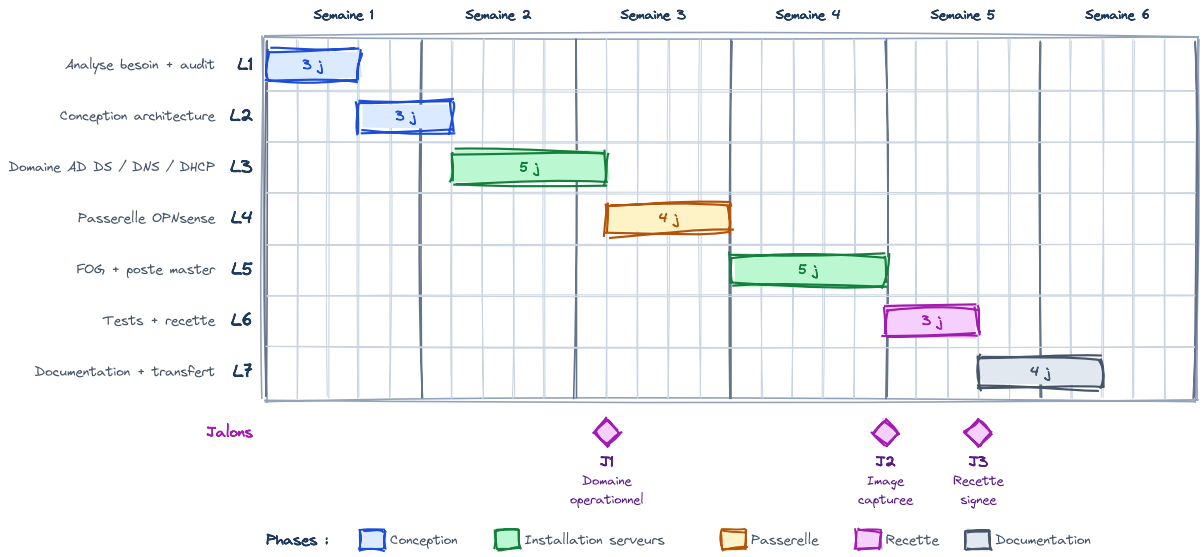
Critères de recette

LA SOLUTION EST RECETTE SI ET SEULEMENT SI

- Tous les livrables ci-dessus sont fournis et conformes.
- Les exigences `EF-01` à `EF-08` sont validées par leur critère respectif.
- Les exigences `ENF-01` à `ENF-08` respectent leur seuil mesurable (plan de tests partie 5).
- Les exclusions `EF-09` à `EF-11` sont documentées et leurs risques résiduels acceptés.
- Une démonstration de déploiement d'un poste depuis l'image est réalisée en présence du commanditaire.

2.8 · Planification du projet

Le projet s'étend sur six semaines (30 jours ouvrés), organisé en sept lots avec quelques recouvrements pour absorber les aléas de plateau.



Macroplanning du projet · sept lots, trois jalons, six semaines.

Lot	Objet	Durée	Jalon de sortie
L1	Analyse du besoin et audit du parc existant	3 jours	Cahier des charges figé
L2	Conception de l'architecture cible et du plan d'adressage	3 jours	Schémas validés
L3	Contrôleur de domaine (AD DS, DNS, DHCP)	5 jours	J1, Domaine opérationnel
L4	Passerelle OPNsense, segmentation et filtrage	4 jours	Segmentation validée
L5	Serveur FOG et préparation du poste master	5 jours	J2, Image de référence capturée
L6	Tests d'intégration, déploiement d'un poste et recette	3 jours	J3, Recette signée
L7	Documentation et transfert de connaissances	4 jours	Dossier remis

PARTIE 3

Architecture cible

3.1 · Vue d'ensemble

Le réseau interne est découpé en deux périmètres portés par la passerelle OPNsense (NAT-00). Le périmètre **ADMIN** héberge les serveurs : le contrôleur de domaine DC-01 (annuaire, DNS, DHCP) et le serveur de déploiement PXE-01 (FOG). Le périmètre **ATELIER** accueille les postes en cours de préparation. La passerelle assure le NAT vers le FAI, relaie les requêtes DHCP de l'atelier vers le contrôleur, et filtre les flux pour empêcher l'atelier d'atteindre librement les serveurs.

3.2 · Schéma logique annoté

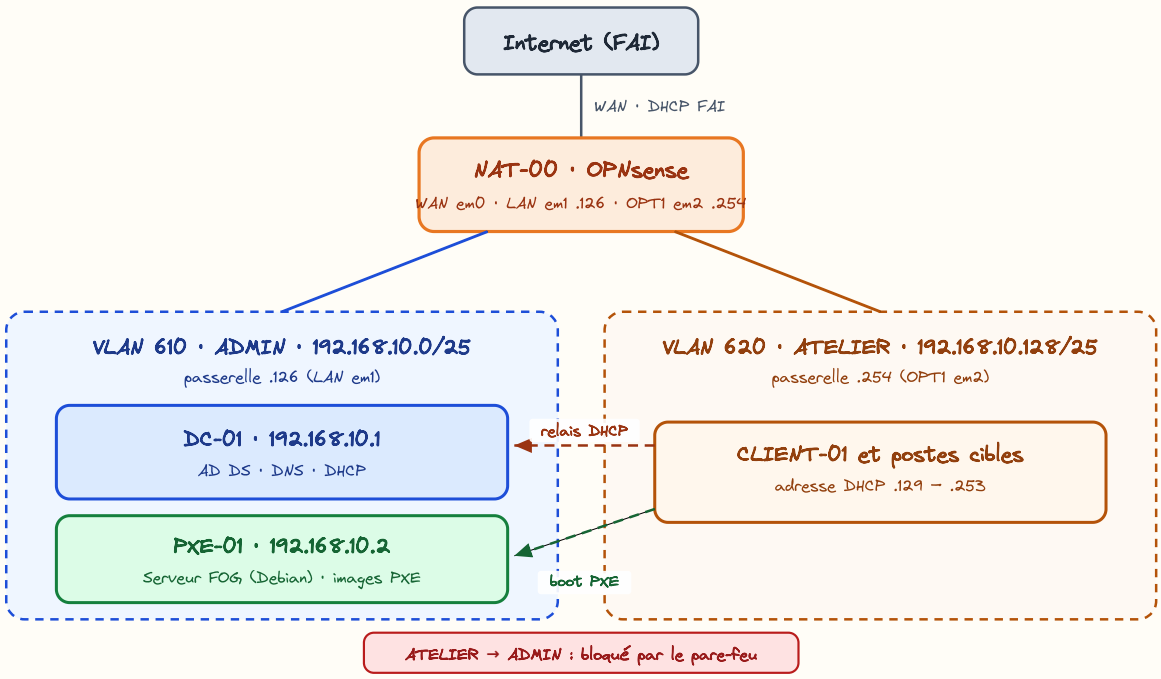


Schéma logique : deux périmètres séparés par OPNsense ; les postes de l'atelier sont adressés par relais DHCP vers DC-01 et déployés par PXE depuis FOG, sans pouvoir atteindre librement les serveurs.

3.3 · Plan d'adressage IPv4

Le réseau interne occupe `192.168.10.0/24`, découpé en deux `/25` : moitié basse pour ADMIN, moitié haute pour ATELIER. Le contrôleur porte la première adresse, le serveur FOG la deuxième ; les passerelles sont les dernières adresses utilisables de chaque `/25`.

Sous-réseaux

Périmètre	Sous-réseau	Passerelle	Plage DHCP	Serveurs fixes
ADMIN (VLAN 610)	192.168.10.0/25	192.168.10.126 (OPNsense LAN)	192.168.10.3 → .125	DC-01 .1 · PXE-01 .2
ATELIER (VLAN 620)	192.168.10.128/25	192.168.10.254 (OPNsense OPT1)	192.168.10.129 → .253	—

Paramètres distribués par DHCP

Étendue	Routeur (003)	DNS (006)	Domaine (015)	Bail	Options PXE
ADMIN	192.168.10.126	192.168.10.1	ADMIN.DEPANMOI.LAN	8 jours	066 = 192.168.10.2 067 = `ipxe.efi`
ATELIER	192.168.10.254	192.168.10.1	DEPANMOI.LAN	2 jours	

Les redirecteurs DNS du contrôleur sont `1.1.1.1` et `8.8.8.8` pour la résolution externe. La zone de recherche inversée est `10.168.192.in-addr.arpa`.

3.4 · Architecture de virtualisation

La maquette est entièrement virtualisée sous **VMware ESXi**, hébergée sur un unique serveur physique. Trois machines virtuelles portent les serveurs (pare-feu OPNsense, contrôleur AD/DNS/DHCP, serveur FOG) et une quatrième sert de poste client de validation. Chaque machine est raccordée à un ou plusieurs réseaux virtuels correspondant aux périmètres et au lien WAN. OPNsense, à cheval sur les trois réseaux, joue le rôle de point de passage entre eux.

Réseau virtuel	Rôle	Machines raccordées
WAN	Lien vers le FAI (NAT sortant)	NAT-00 (em0)
ADMIN	Périmètre serveurs (192.168.10.0/25)	NAT-00 (em1), DC-01, PXE-01
ATELIER	Périmètre postes (192.168.10.128/25)	NAT-00 (em2), CLIENT-01 et postes cibles

ENVIRONNEMENT TECHNOLOGIQUE RÉEL

Les systèmes, services et protocoles sont effectivement installés et configurés sur ces machines : il s'agit d'un environnement technologique opérationnel, et non d'une simple simulation logicielle.

ÉVOLUTION DEPUIS LA FICHE DESCRIPTIVE

La fiche descriptive mentionnait Windows Server 2022 et Debian 12. Le socle a depuis été **mis à niveau** vers Windows Server 2025, Windows 11 côté poste et Debian 13 pour le serveur FOG, sans changement d'architecture ni de plan d'adressage.

3.5 · Inventaire des machines

Hôte	Rôle	Système	Adresse
DC-01	Contrôleur de domaine · AD DS, DNS, DHCP	Windows Server 2025	192.168.10.1/25
PXE-01	Serveur de déploiement FOG	Debian 13	192.168.10.2/25
NAT-00	Passerelle, pare-feu, relais DHCP, NAT	OPNsense	.126 (LAN) · .254 (OPT1) · WAN DHCP
CLIENT-01	Poste master puis poste cible	Windows 11 Pro	DHCP (ATELIER)

3.6 · Conventions de nommage

- **Hôtes** : `RÔLE-NN` (DC-01, PXE-01, NAT-00, CLIENT-01), complété en FQDN `RÔLE-NN.DEPANMOI.LAN`.
- **Domaine** : forêt et domaine racine `DEPANMOI.LAN`, NetBIOS `DEPANMOI`.
- **Périmètres** : `ADMIN` (serveurs) et `ATELIER` (postes), repris dans les noms d'interfaces OPNsense et les étendues DHCP.
- **Image** : `PC-MASTER` pour l'image de référence dans FOG.

PARTIE 4

Configurations et procédure de mise en œuvre

Cette partie tient lieu de **procédure de mise en œuvre reproductible** : chaque sous-section présente, dans l'ordre, les paramètres à appliquer, accompagnés des captures de vérification réelles. Un tiers technicien peut redéployer le socle depuis zéro en suivant cet ordre.

4.1 · Vue d'ensemble et ordre de mise en œuvre

Machine	Système	Rôle synthétique	Section
DC-01	Windows Server 2025	Contrôleur de domaine, DNS (zones directe/inverse, redirecteurs), DHCP (2 étendues, options PXE)	4.2
NAT-00	OPNsense	Interfaces WAN/LAN/OPT1, relais DHCP, alias, règles de filtrage, NAT	4.3
PXE-01	Debian 13	Installation de FOG (Normal Server), stockage des images, interface web	4.4
CLIENT-01	Windows 11 Pro	Poste master, suite Ninite, Sysprep, enregistrement et capture FOG, déploiement	4.5

4.1.1 · Ordre recommandé

1. **DC-01** d'abord : sans annuaire ni DNS, rien d'autre ne peut se nommer ni s'authentifier.
2. **NAT-00** ensuite : segmentation, relais DHCP vers le DC, filtrage et sortie Internet.
3. **PXE-01** : installation de FOG, qui consomme les options 066/067 du DHCP.
4. **CLIENT-01** : préparation du master, généralisation, capture puis déploiement.

> **POINT D'ATTENTION**
>
> Le serveur DHCP est unique (DC-01). Avant de tester le déploiement d'un poste de l'atelier, vérifier que le relais DHCP d'OPNsense est actif et que les options 066/067 sont bien distribuées : c'est la condition de l'amorçage réseau.

4.2 · DC-01 · Contrôleur de domaine (AD DS, DNS, DHCP)

4.2.1 · Adressage fixe

Un contrôleur de domaine ne doit jamais dépendre du DHCP. DC-01 reçoit une adresse fixe `192.168.10.1/25`, passerelle `192.168.10.126`. Le serveur DNS préféré pointera vers lui-même une fois le rôle DNS installé.

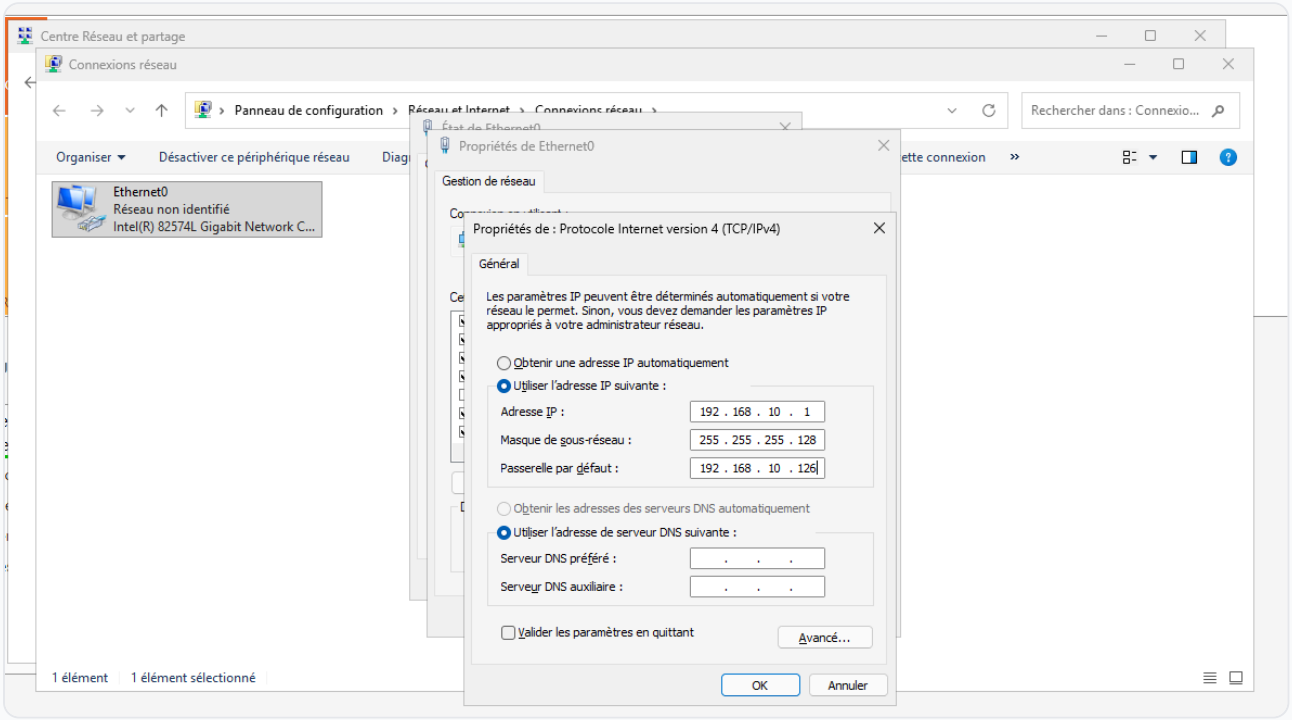


Figure 4.1 · Adressage fixe de DC-01 : `192.168.10.1 / 255.255.255.128`, passerelle `192.168.10.126`.

4.2.2 · Installation du rôle AD DS et promotion de la forêt

Le rôle **Services de domaine Active Directory** est ajouté via le Gestionnaire de serveur, avec les fonctionnalités de gestion associées. Le serveur est ensuite promu contrôleur d'une **nouvelle forêt**, de domaine racine `DEPANMOI.LAN`, au niveau fonctionnel Windows Server 2025, avec les rôles DNS et catalogue global. Une fois le domaine en place, les **comptes utilisateurs** et les **groupes de sécurité** (Direction, Techniciens) sont créés dans l'annuaire pour structurer les droits d'accès.

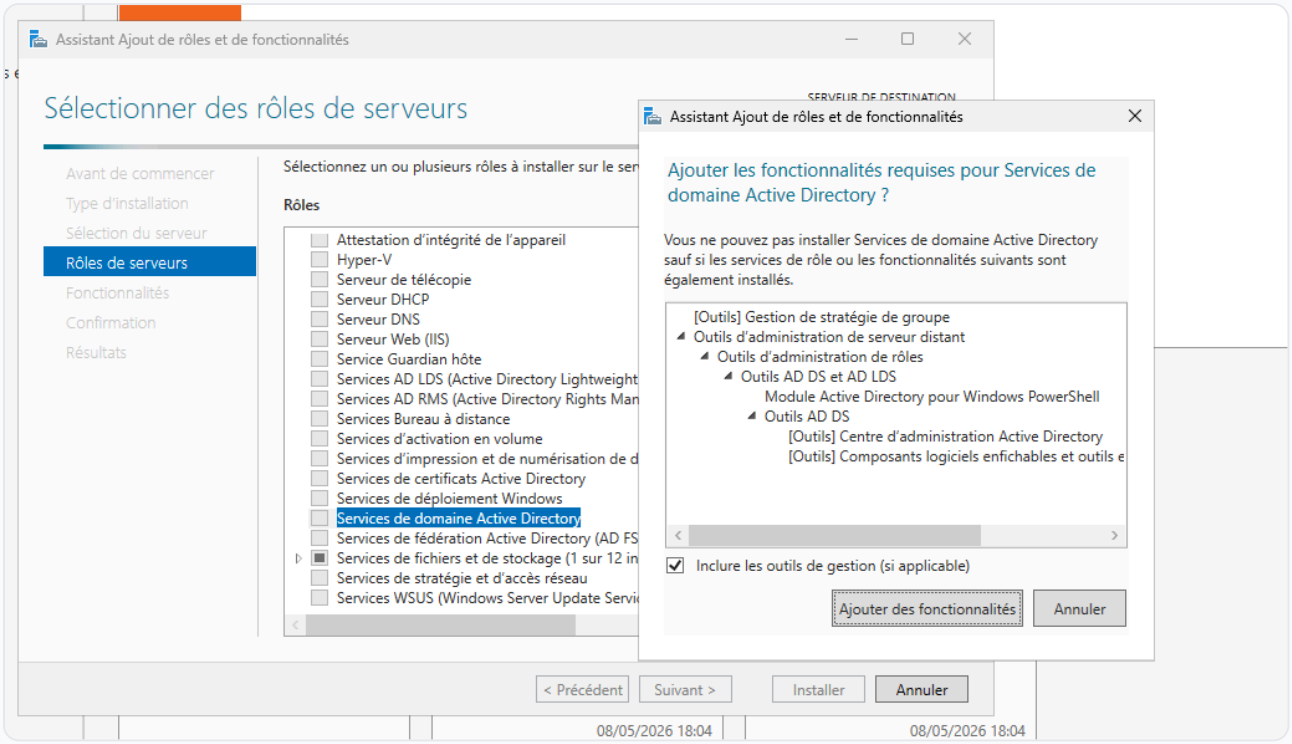


*Figure 4.2 · Ajout du rôle **Services de domaine Active Directory** et de ses outils de gestion.*

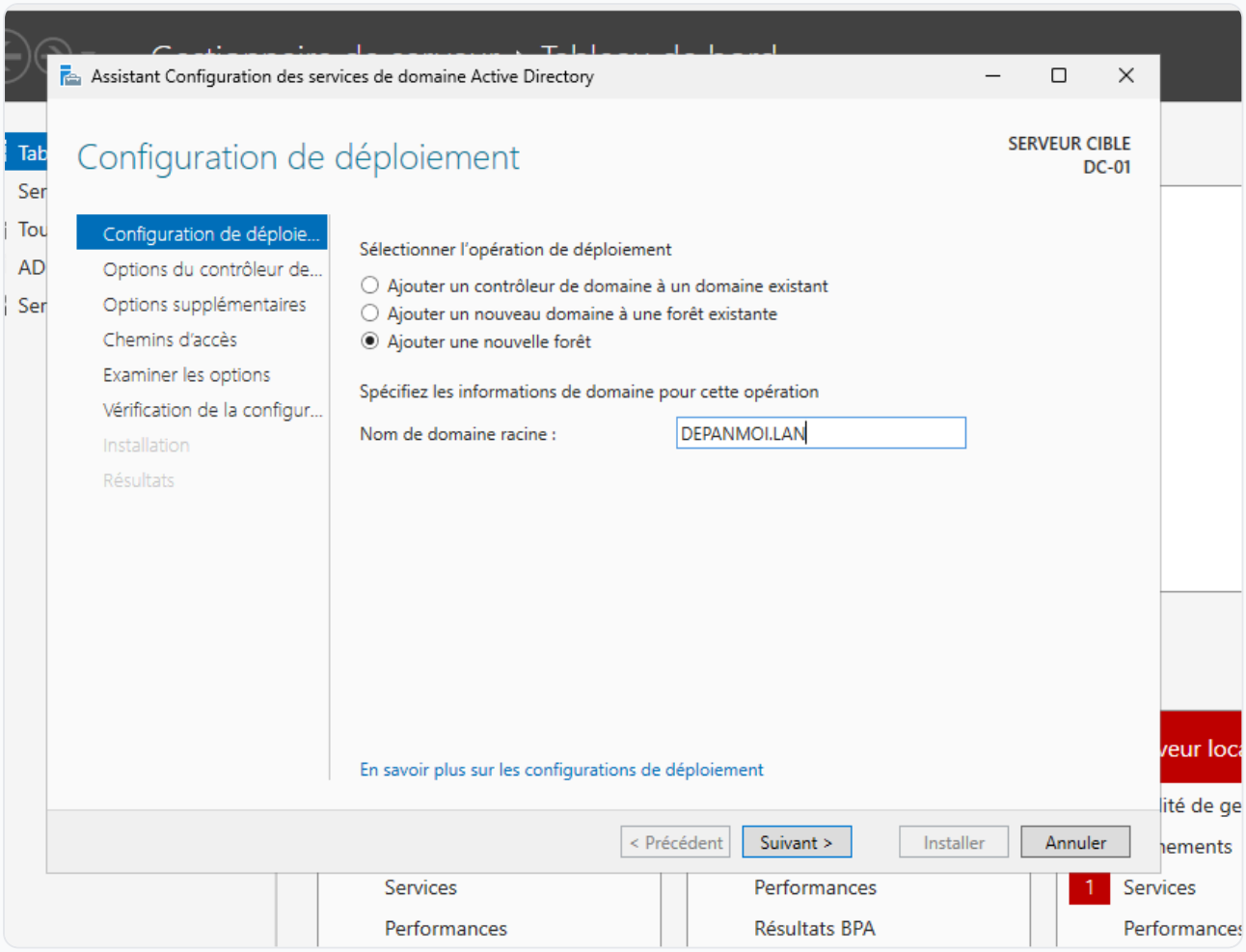


*Figure 4.3 · Promotion : création d'une **nouvelle forêt**, domaine racine `DEPANMOI.LAN` .*

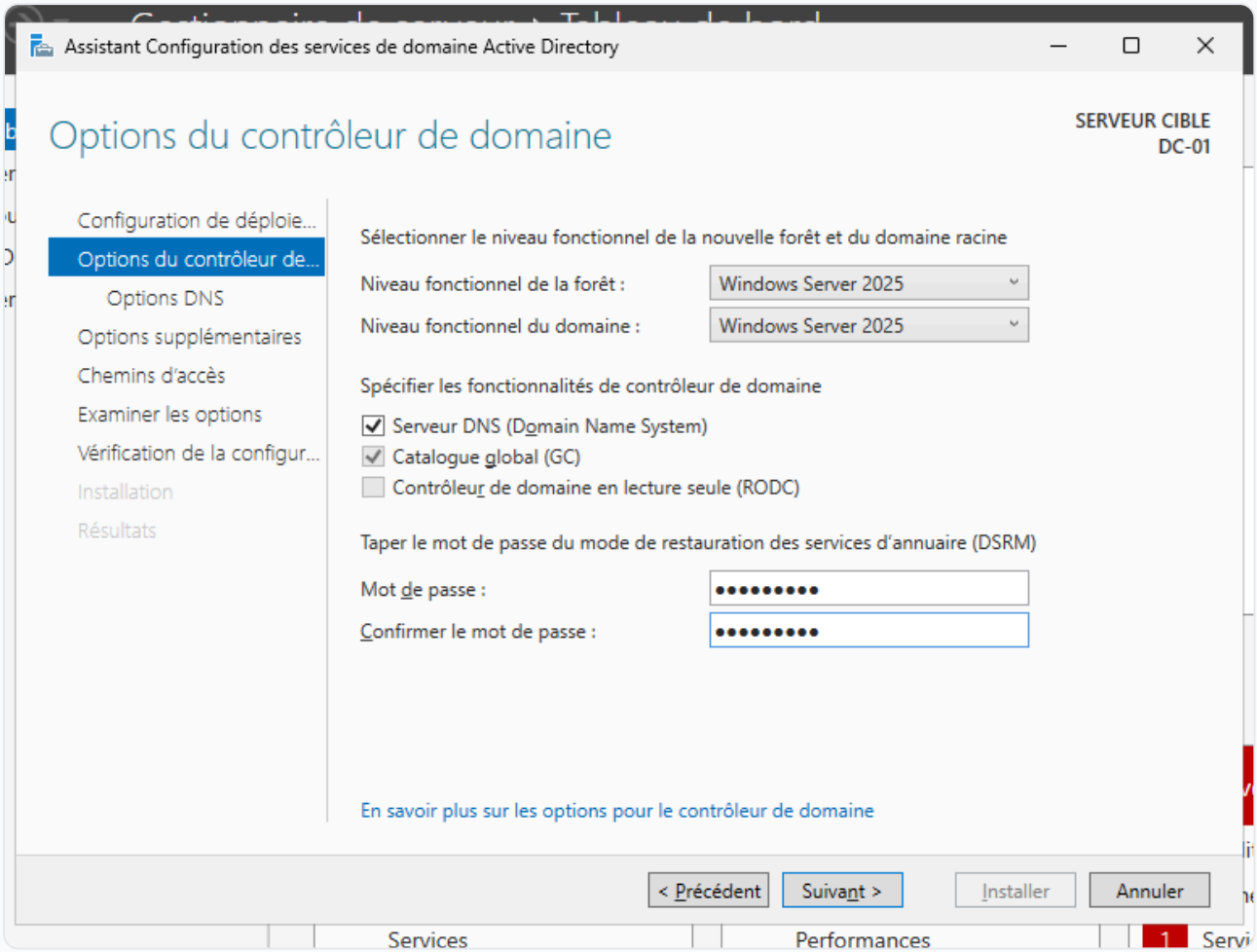


*Figure 4.4 · Niveau fonctionnel **Windows Server 2025** ; rôles Serveur DNS et Catalogue global activés.*

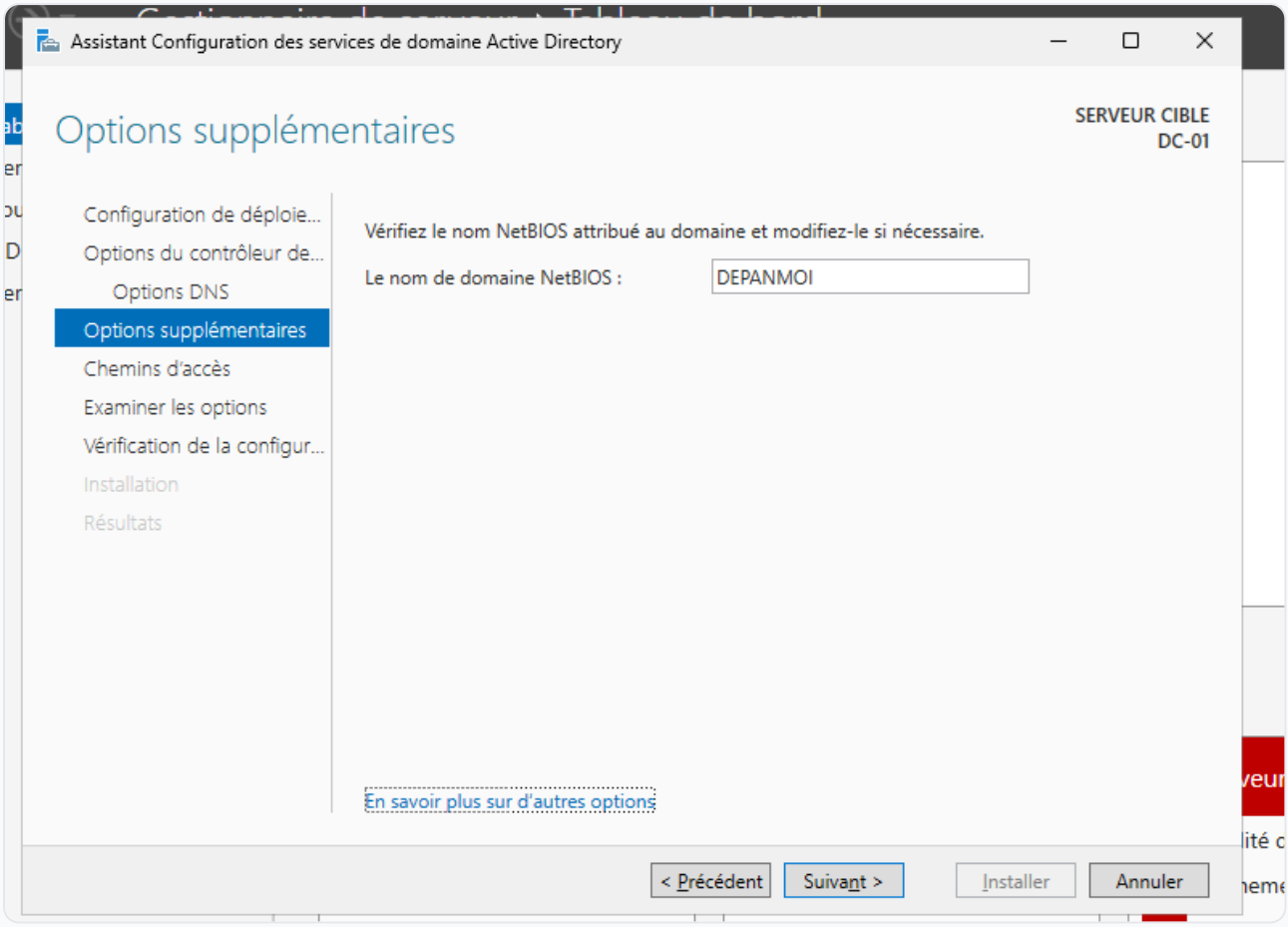


Figure 4.5 · Nom NetBIOS du domaine : `DEPANMOI` .

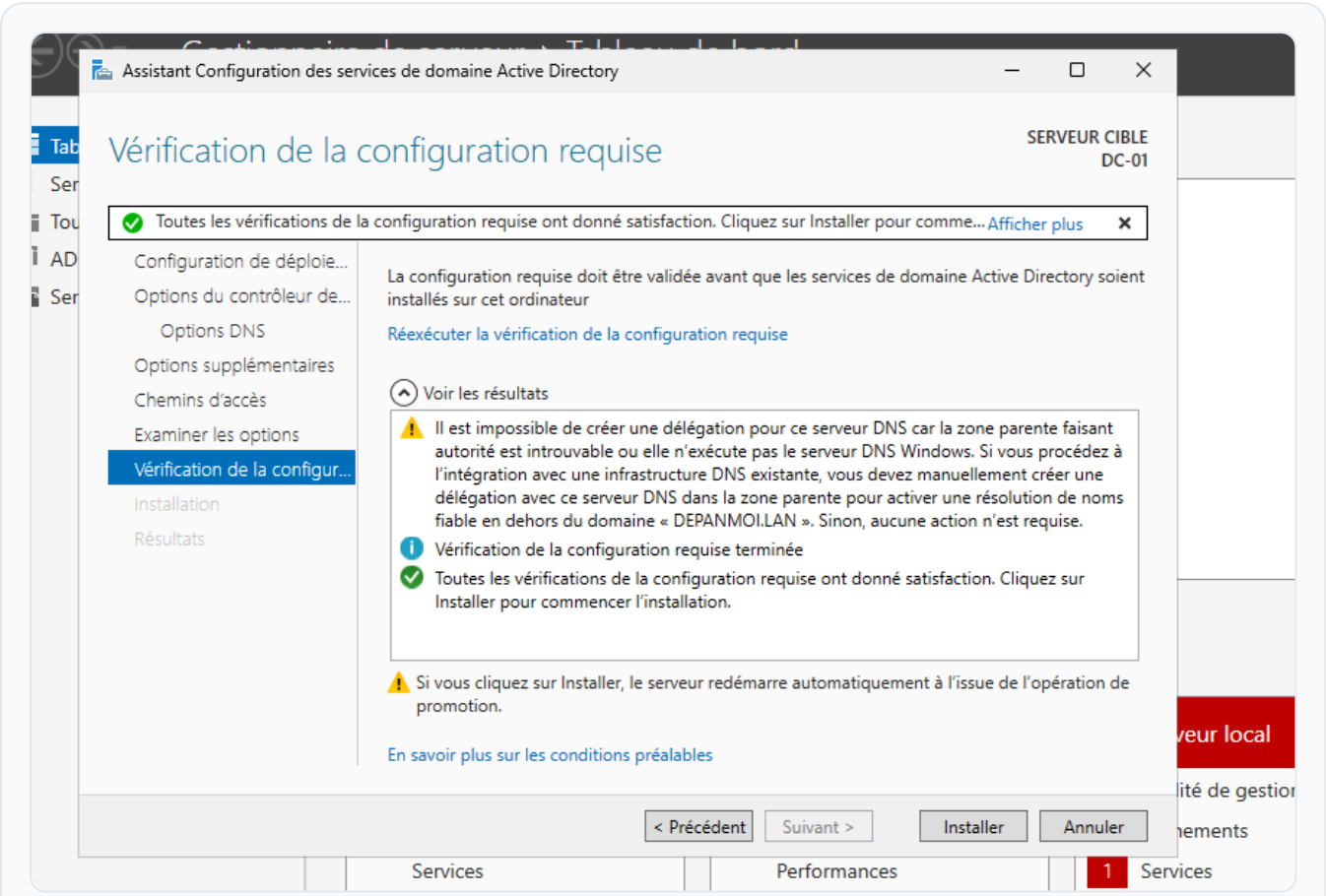


Figure 4.6 · Vérification des prérequis validée avant promotion. L'avertissement sur la délégation DNS est attendu pour une nouvelle forêt.

4.2.3 · Service DNS : zones et redirecteurs

La zone directe `DEPANMOI.LAN` est créée par la promotion. On ajoute une **zone de recherche inversée** pour `192.168.10.x` afin de résoudre les adresses en noms, et on déclare les **redirecteurs** publics pour la résolution externe. Le serveur de déploiement est enregistré comme hôte `pxe-01`.

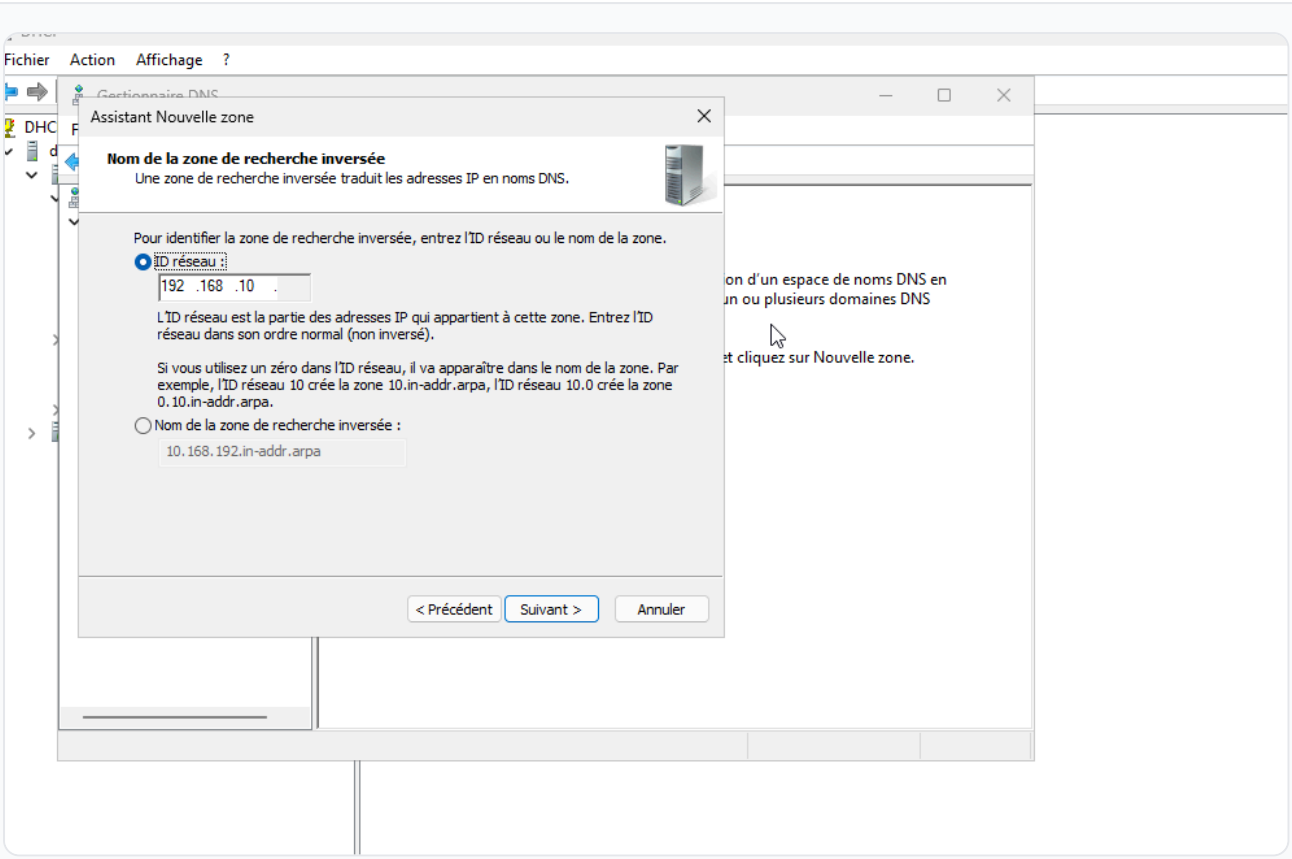


Figure 4.7 · Création de la zone inverse, ID réseau `192.168.10` (zone `10.168.192.in-addr.arpa`).

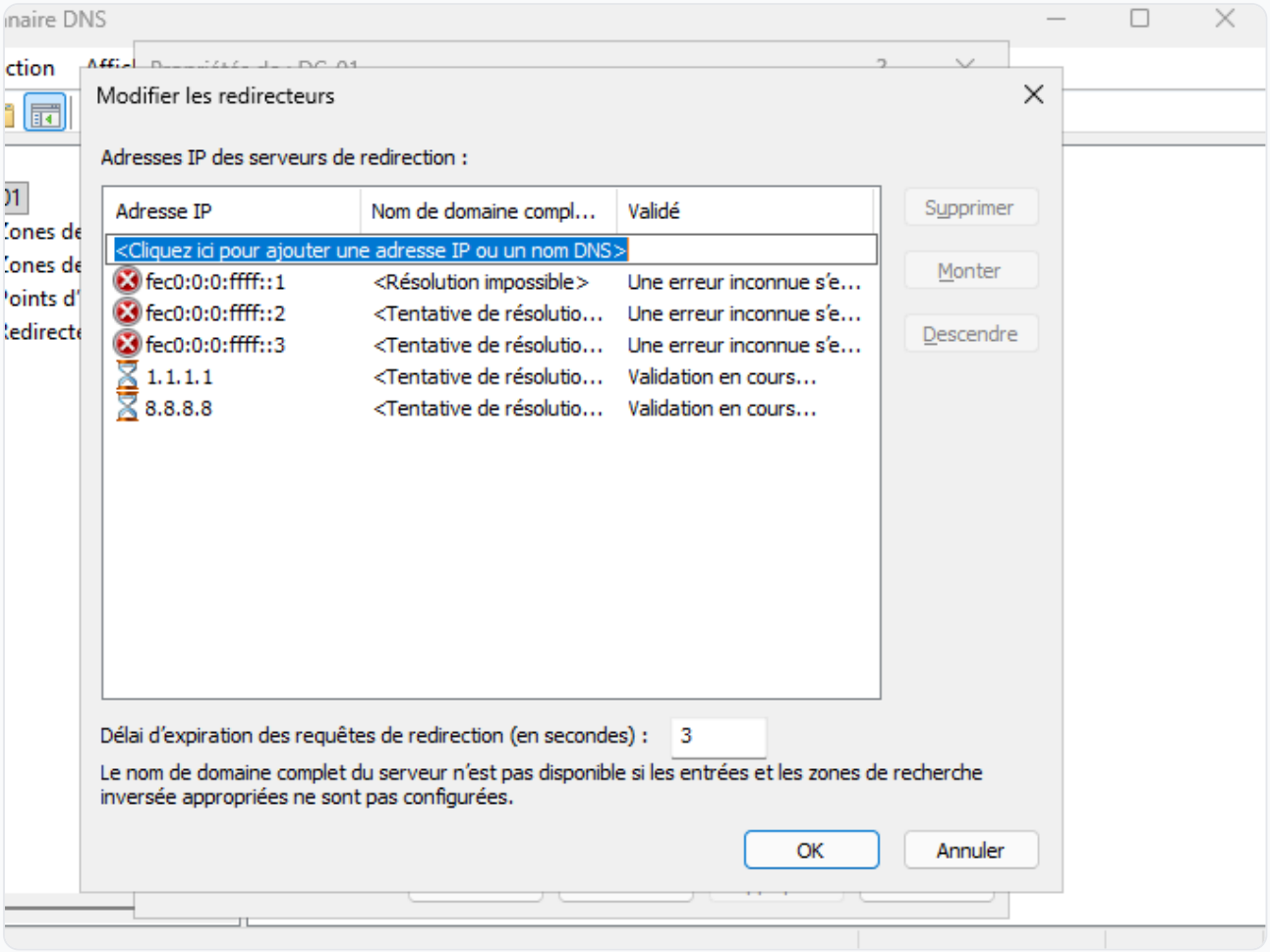


Figure 4.8 · Redirecteurs DNS publics : `1.1.1.1` et `8.8.8.8` pour la résolution externe.

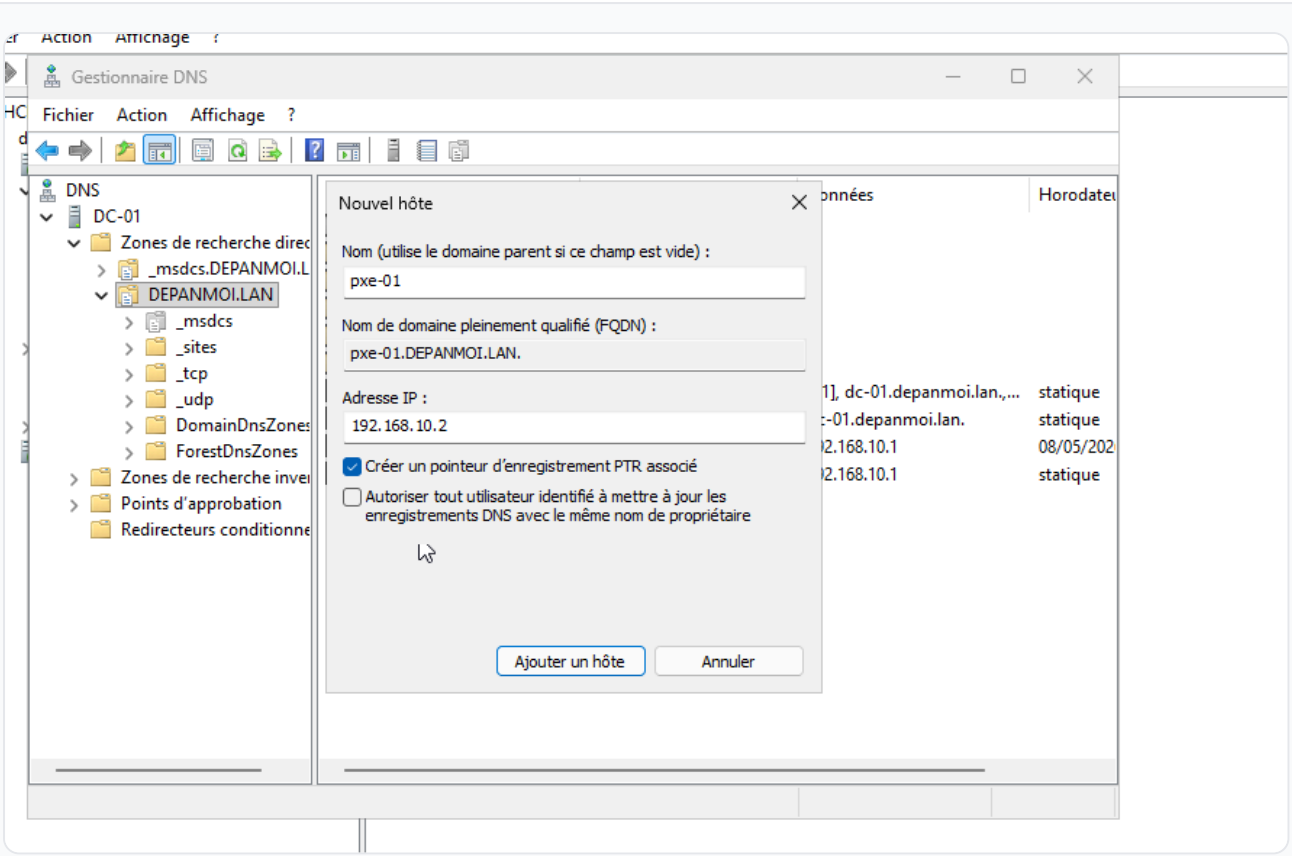


Figure 4.9 · Enregistrement de l'hôte `pxe-01.DEPANMOI.LAN` en `192.168.10.2`, avec pointeur PTR associé.

4.2.4 · Service DHCP : étendues et options d'amorçage

Le rôle DHCP est installé sur DC-01. Deux étendues couvrent les périmètres. L'étendue ADMIN distribue `192.168.10.3 → .125` (passerelle .126), l'étendue ATELIER `192.168.10.129 → .253` (passerelle .254). Les bornes des plages laissent hors distribution les adresses fixes (.1, .2) et les passerelles. Au niveau des **options serveur**, les options 066 et 067 orientent les clients PXE vers FOG.

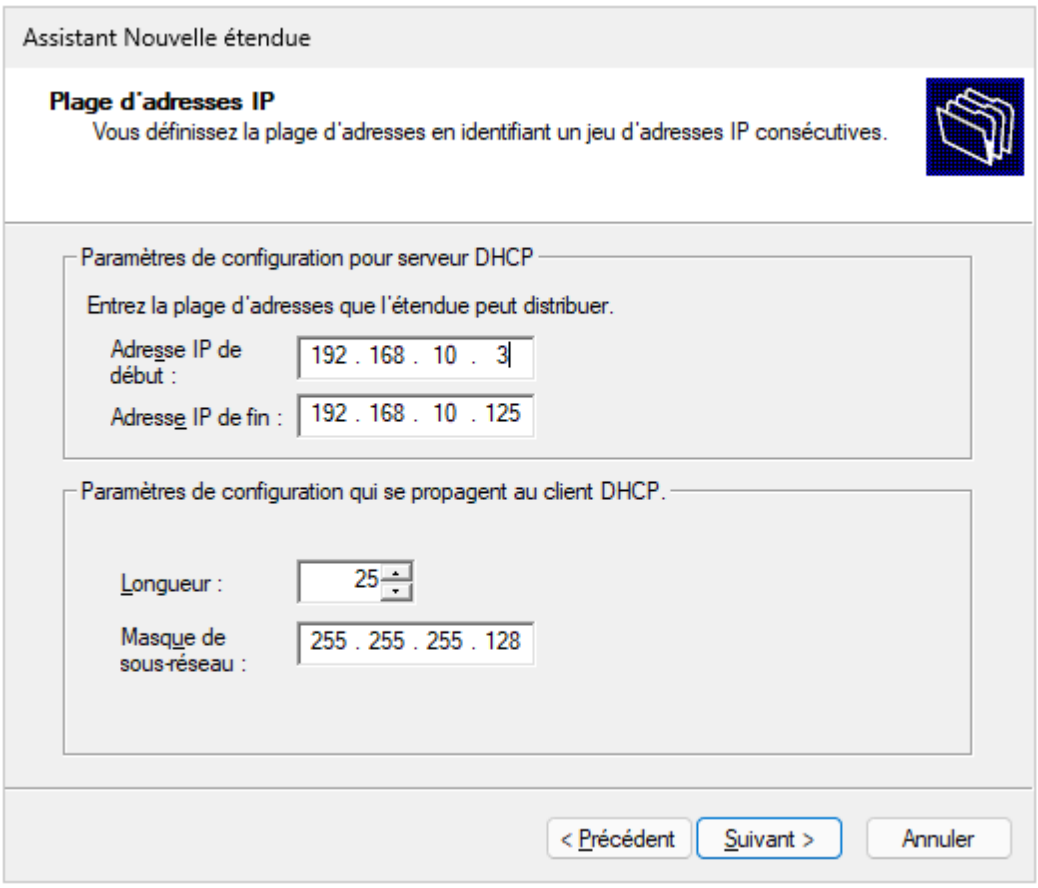


Figure 4.10 · Étendue ADMIN : plage `192.168.10.3 → .125`, masque `/25`.

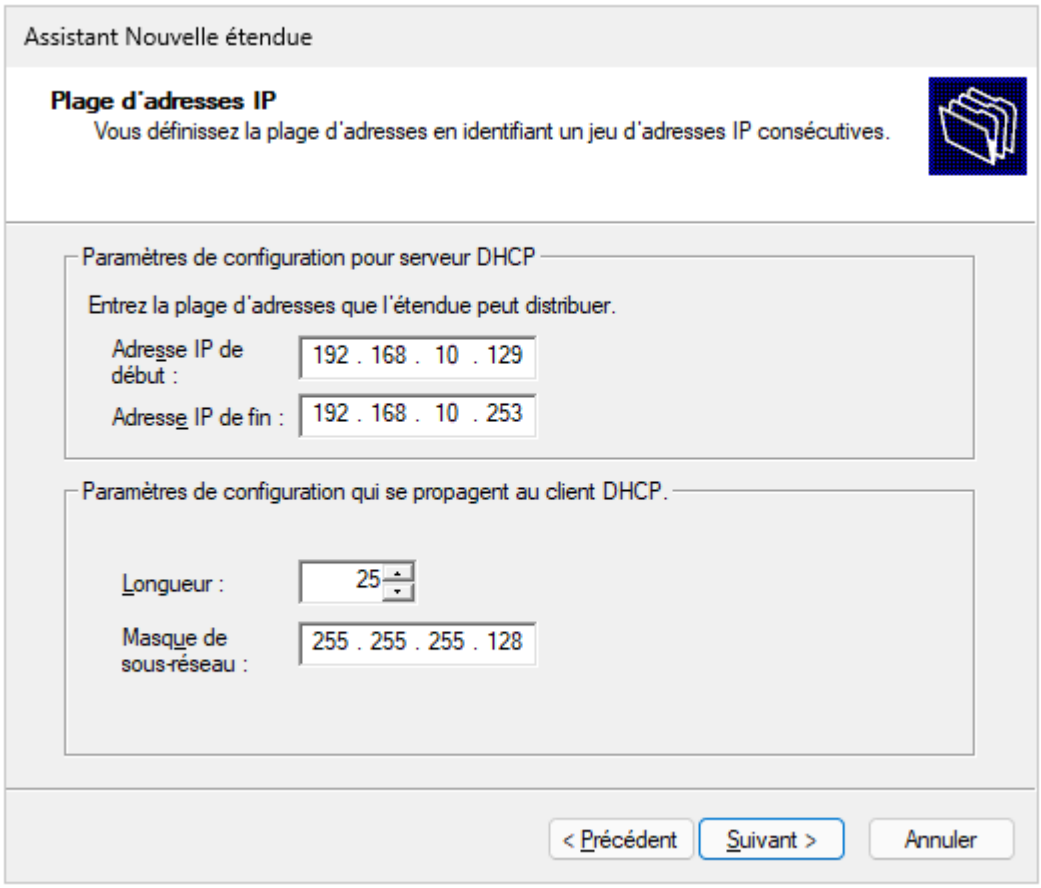


Figure 4.11 · Étendue ATELIER : plage `192.168.10.129 → .253`, masque `/25`.

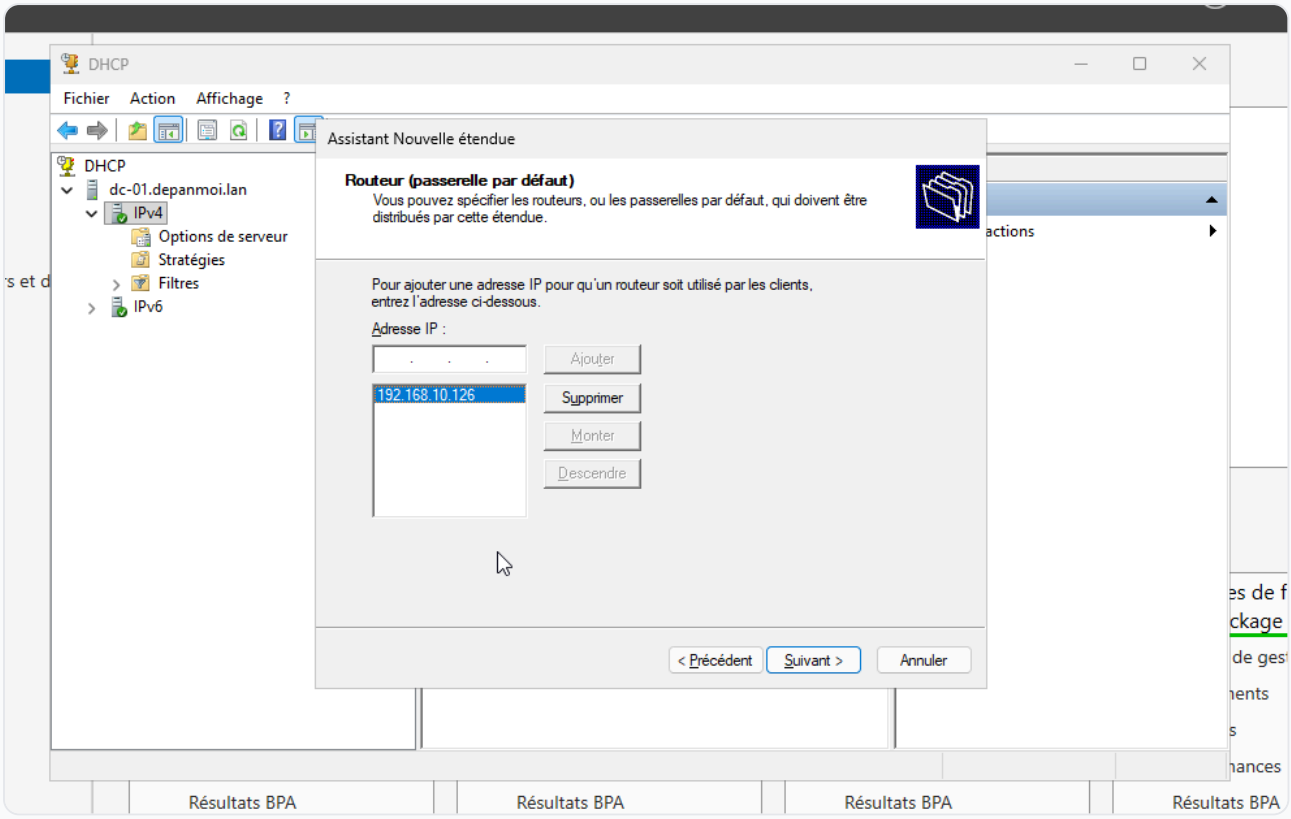


Figure 4.12 · Passerelle distribuée à l'étendue ADMIN : `192.168.10.126` (l'étendue ATELIER reçoit `.254`).

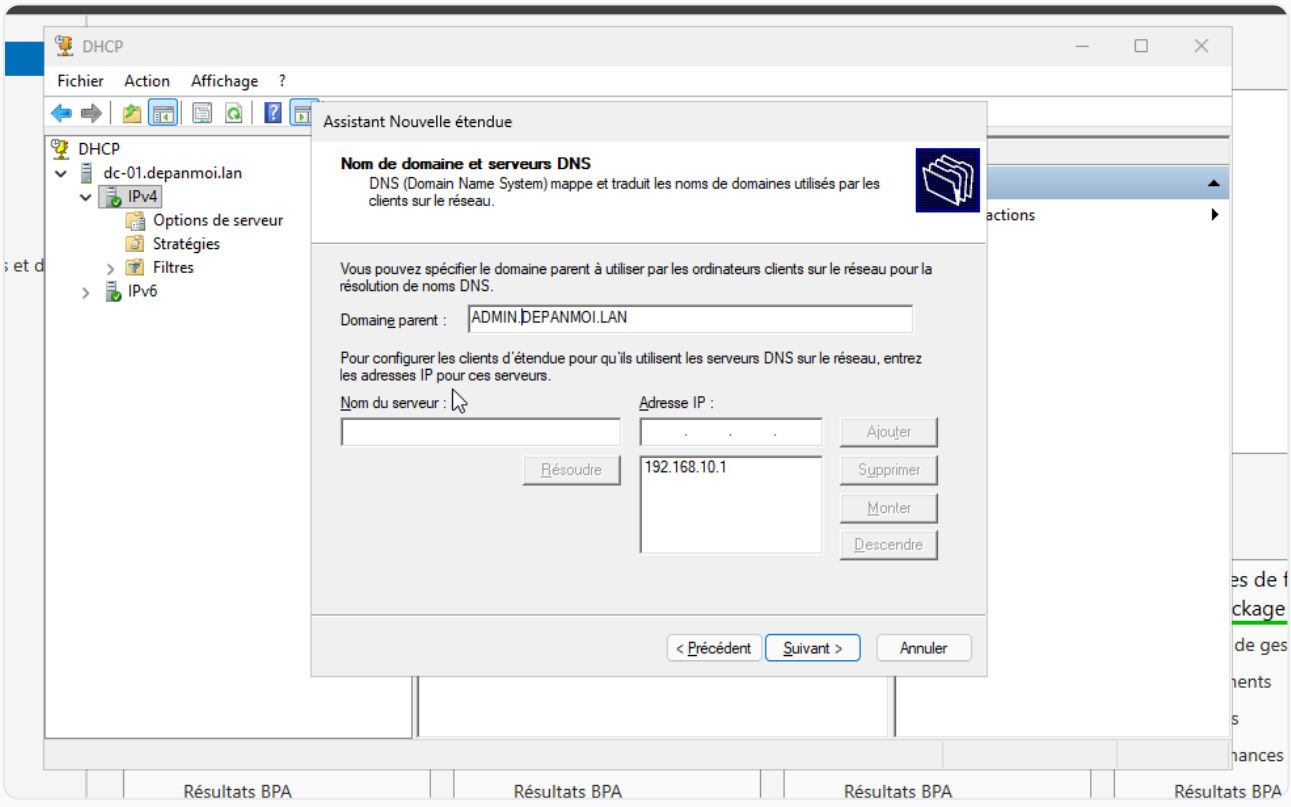


Figure 4.13 · Serveur DNS distribué : `192.168.10.1` (le contrôleur lui-même).

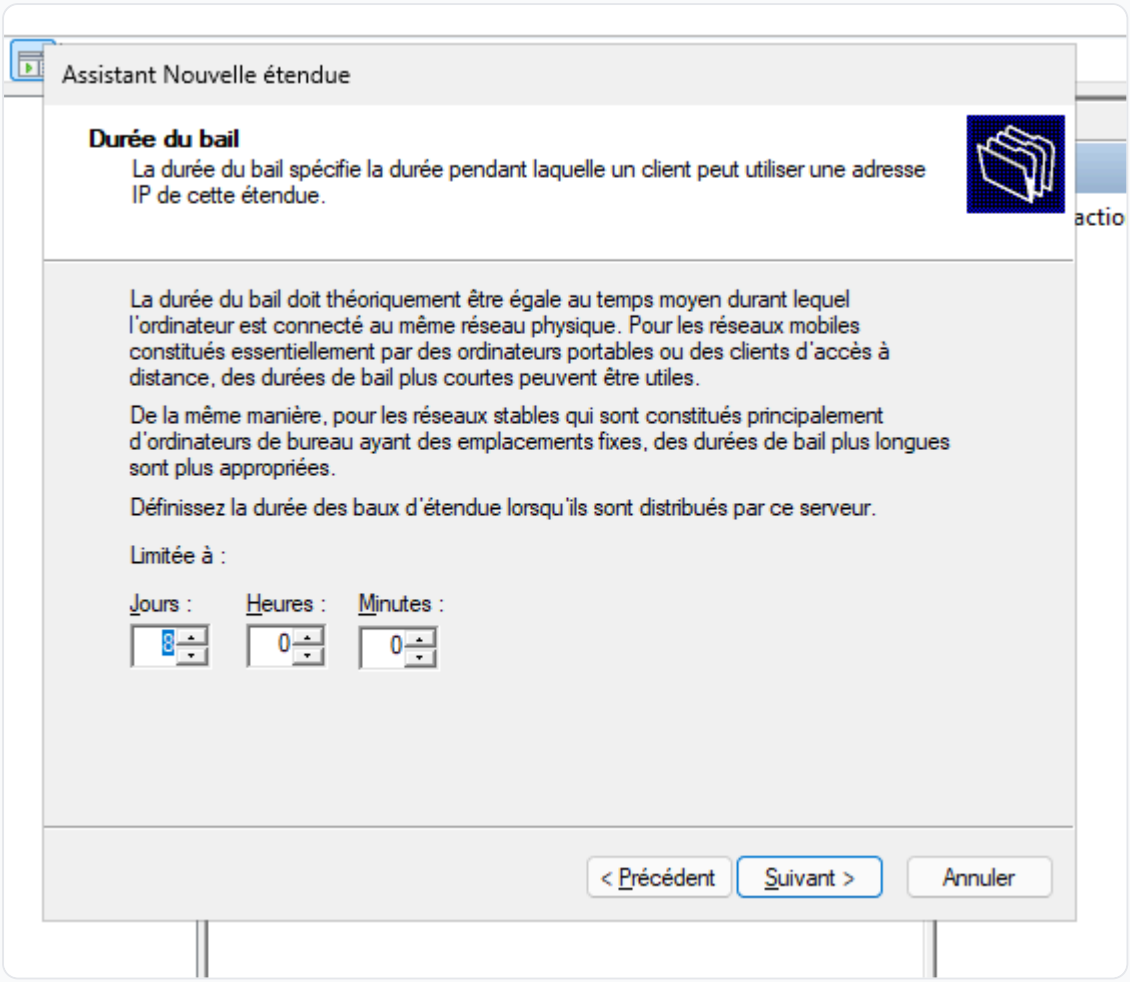


*Figure 4.14 · Durée de bail de l'étendue ADMIN : **8 jours** (postes fixes du périmètre serveurs).*

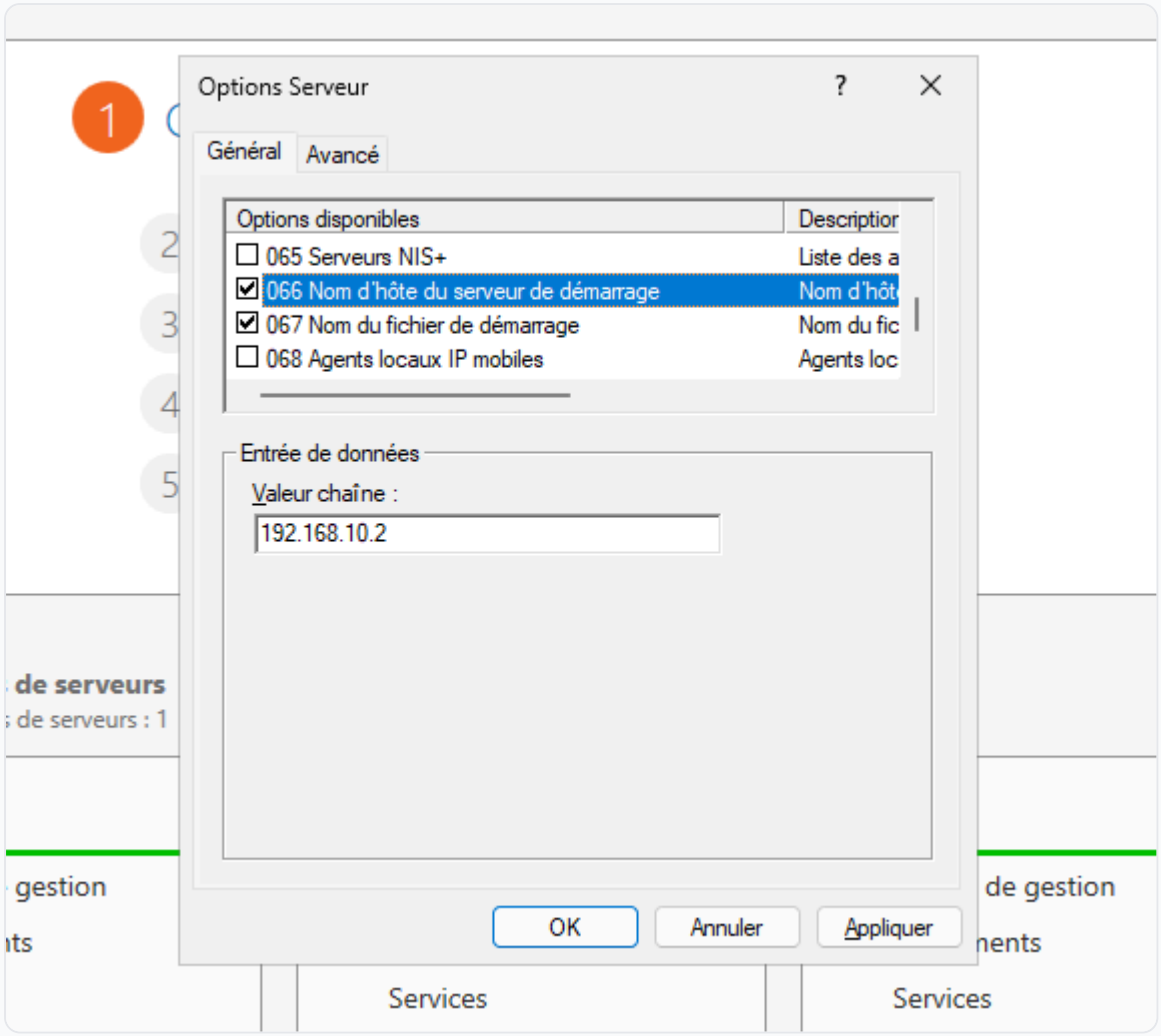


*Figure 4.15 · Option **066** (serveur de démarrage) : `192.168.10.2` .*

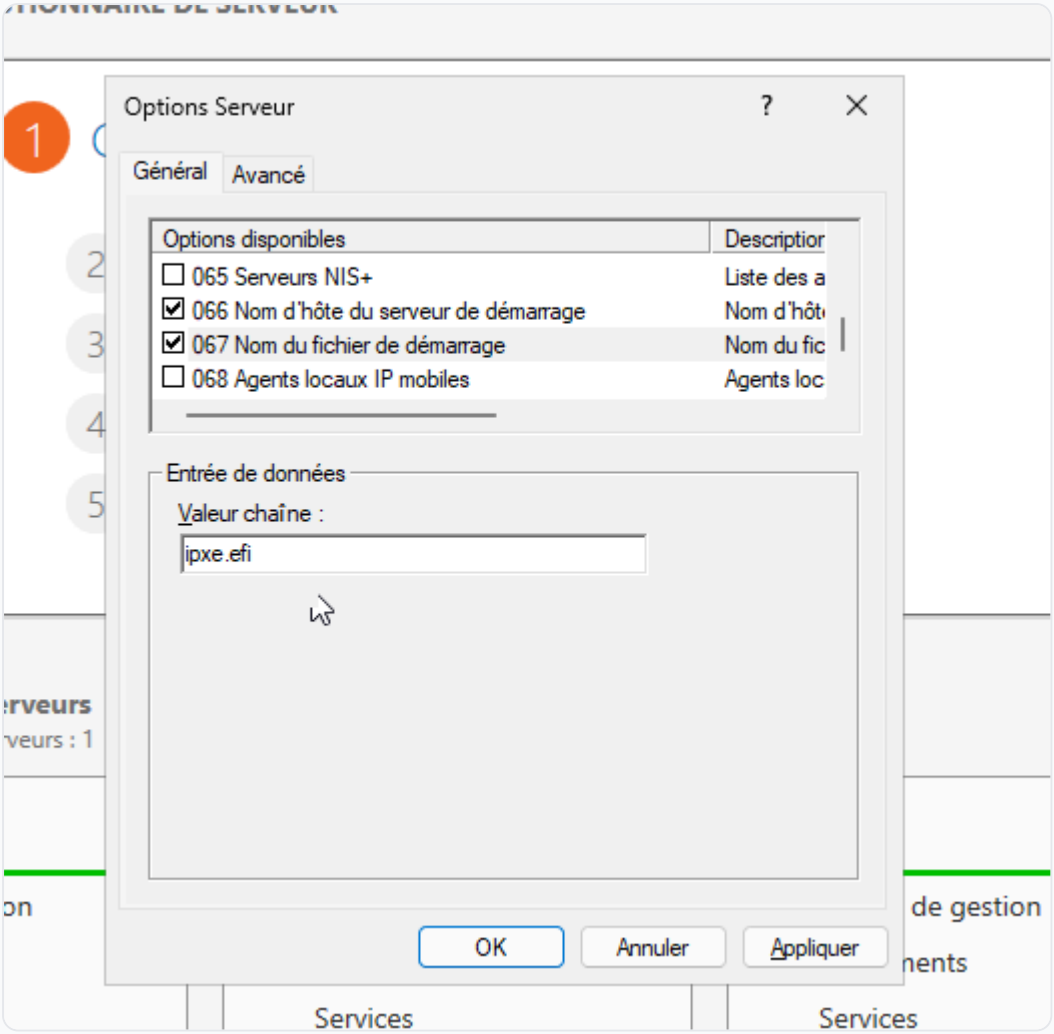


*Figure 4.16 · Option **067** (fichier de démarrage) : `ipxe.efi` . C'est ce couple 066/067 qui permet l'amorçage réseau PXE.*

4.3 · NAT-00 · Passerelle et filtrage (OPNsense)

4.3.1 · Affectation des interfaces

OPNsense répartit trois cartes : **WAN** (`em0` , vers le FAI), **LAN** (`em1` , périmètre ADMIN) et **OPT1** (`em2` , périmètre ATELIER). Le WAN obtient son adresse en DHCP du FAI ; LAN est fixée à `192.168.10.126/25` et OPT1 à `192.168.10.254/25` . Le serveur DHCP d'OPNsense reste désactivé sur LAN et OPT1, l'adressage étant assuré par le contrôleur.

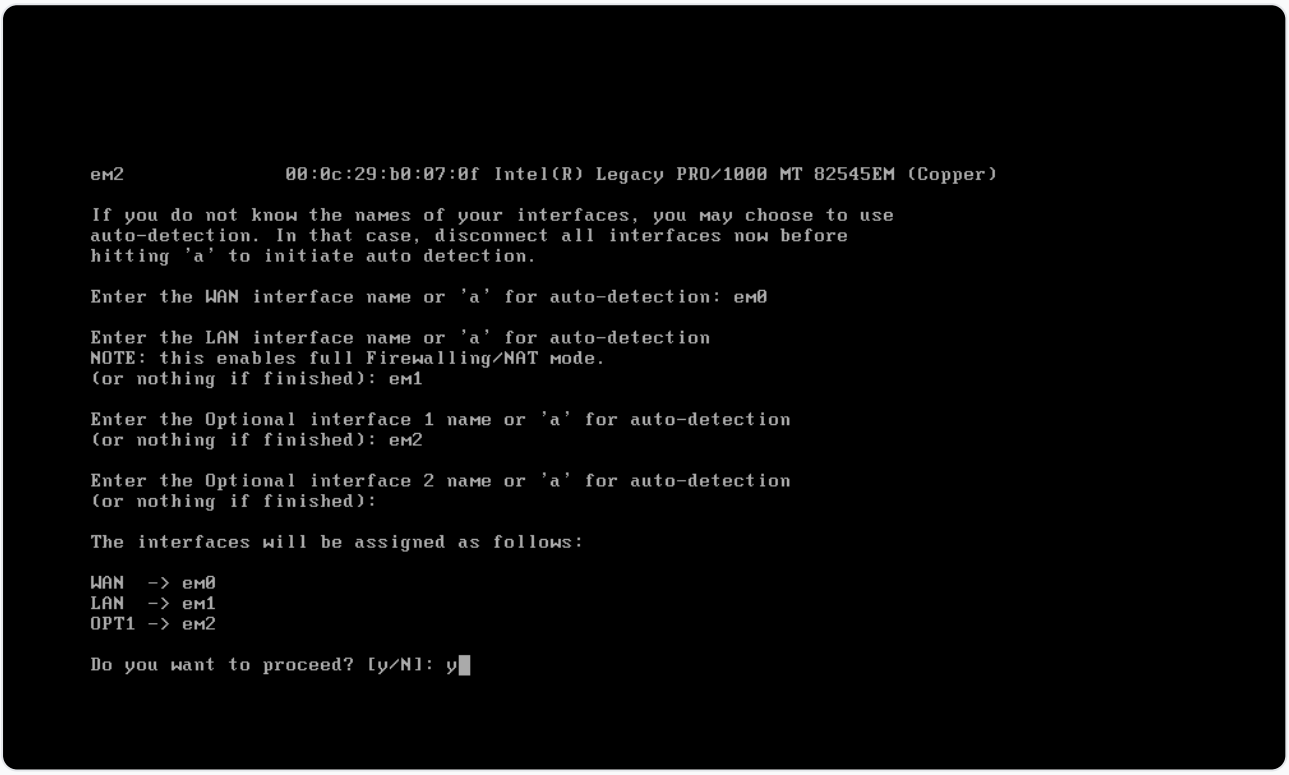


Figure 4.17 · Affectation : `WAN → em0` , `LAN → em1` , `OPT1 → em2` .

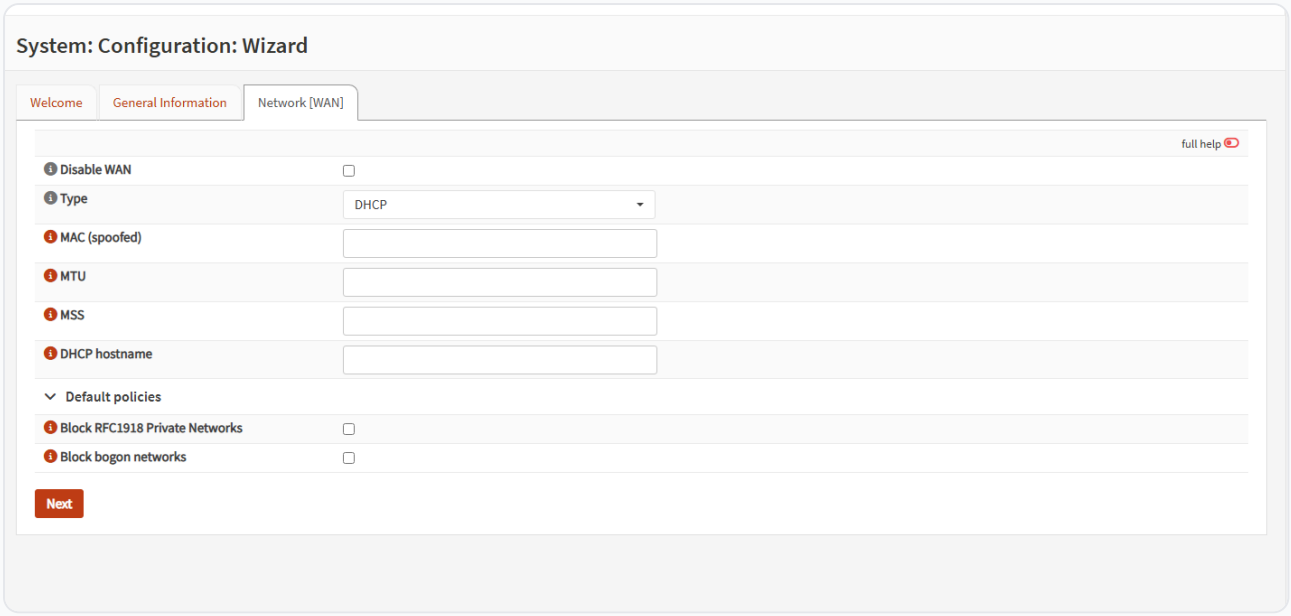


*Figure 4.18 · Interface WAN configurée en **DHCP** (adresse fournie par le FAI).*

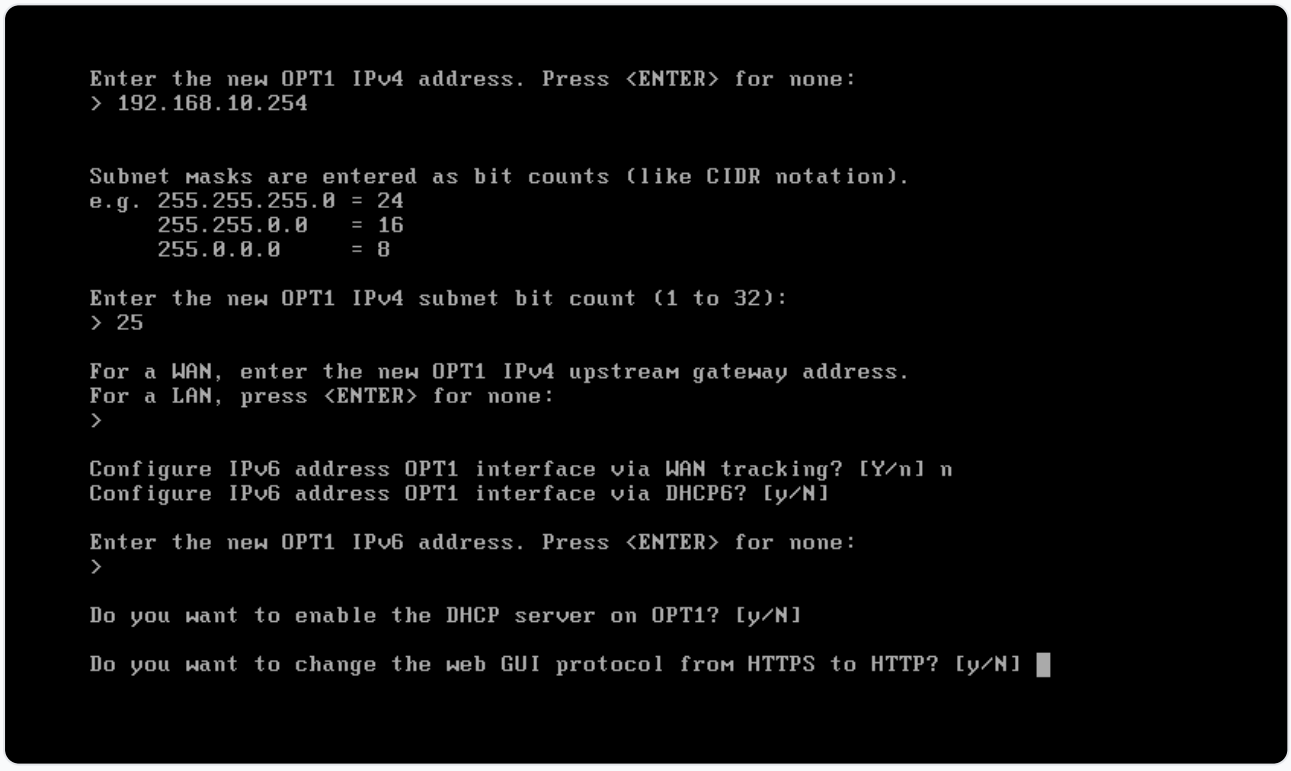


Figure 4.19 · Interface OPT1 (ATELIER) : `192.168.10.254/25` , sans serveur DHCP local.

4.3.2 · Relais DHCP vers le contrôleur

Les postes de l'atelier étant hors du domaine de diffusion du DC, OPNsense relaie leurs requêtes DHCP vers `192.168.10.1` . La destination est déclarée, puis le relais est activé sur l'interface ATELIER.

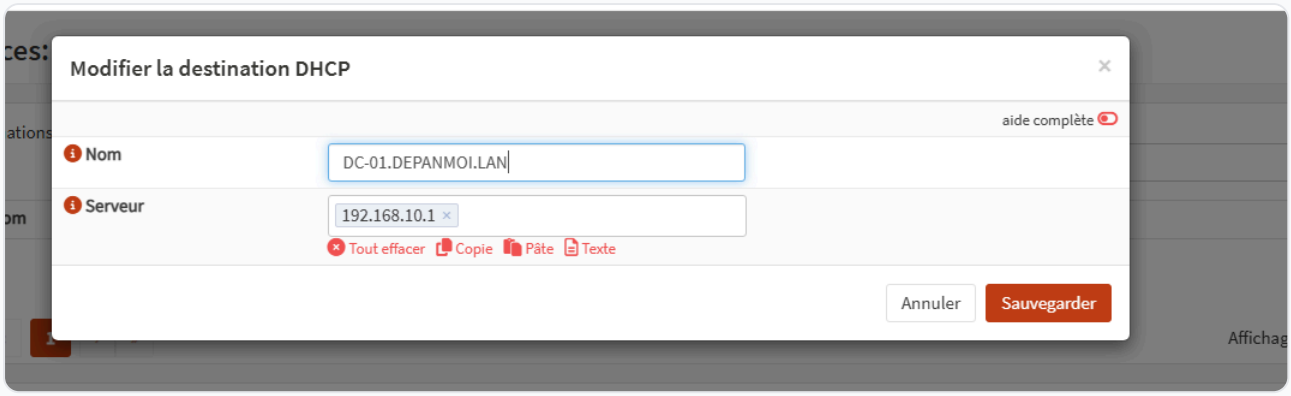


Figure 4.20 · Destination du relais : `DC-01.DEPANMOI.LAN` = `192.168.10.1`.

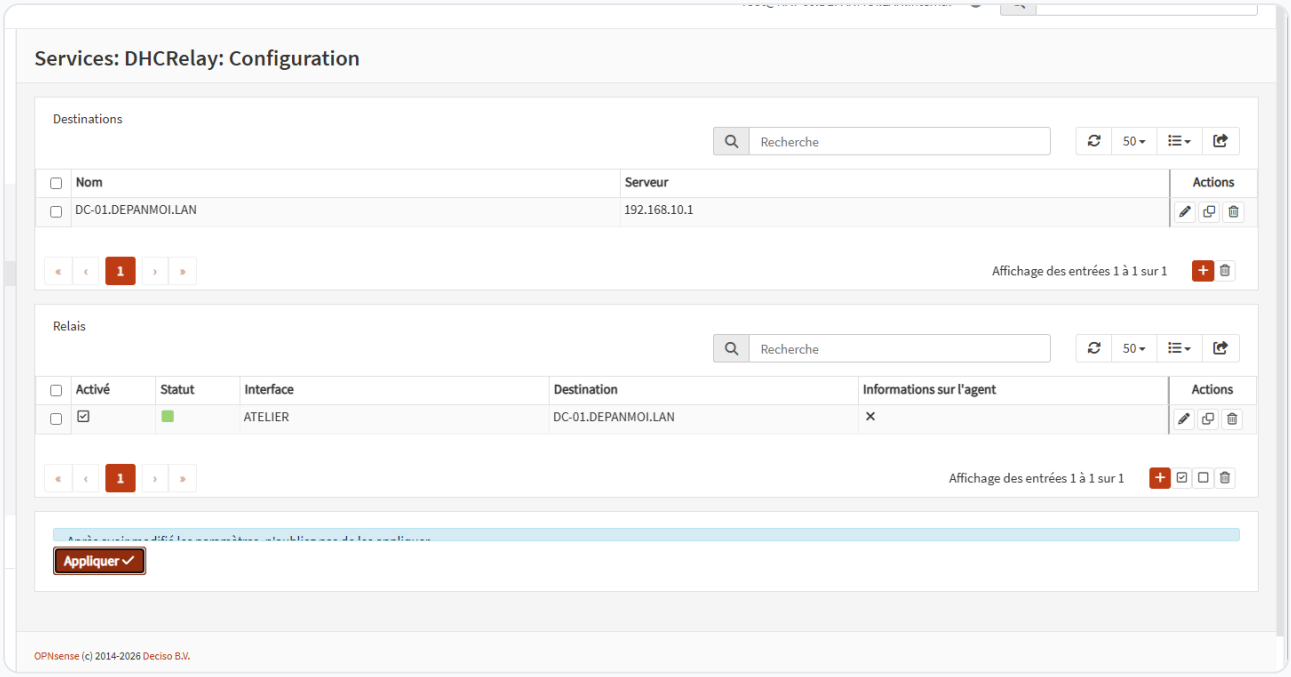


*Figure 4.21 · Relais DHCP **activé** sur l'interface ATELIER, destination DC-01, statut opérationnel.*

4.3.3 · Alias de services et règles de filtrage

Un alias `PORTS_FOG` regroupe les ports utilisés par FOG (21 FTP, 69 TFTP, 80 HTTP, 443 HTTPS). Les règles du périmètre ATELIER appliquent le moindre privilège : autoriser le relais DHCP, le DNS du contrôleur et le serveur FOG, **bloquer** l'accès au périmètre ADMIN, puis autoriser Internet. Le périmètre ADMIN conserve une autorisation par défaut.

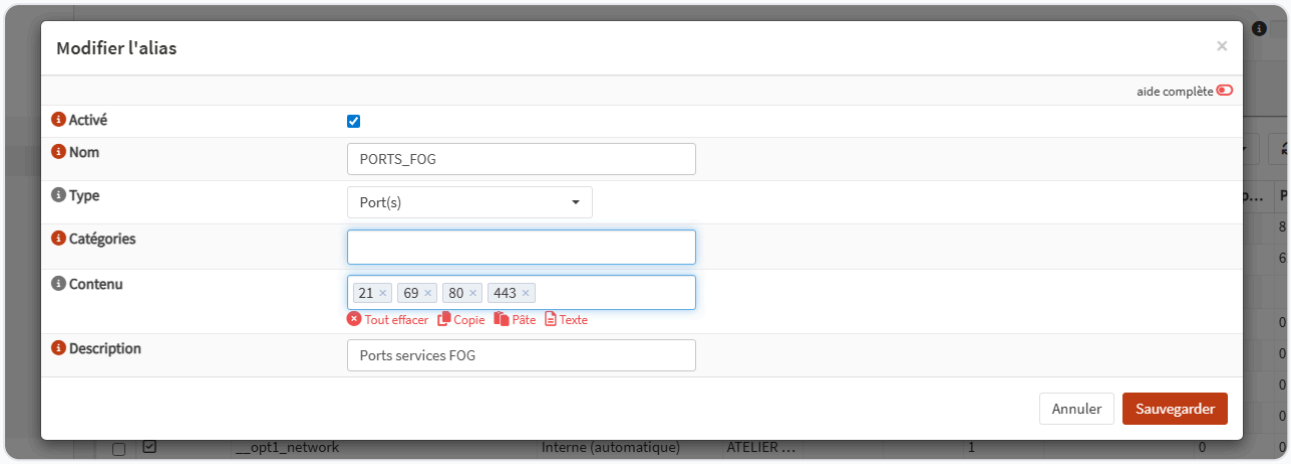


Figure 4.22 · Alias `PORTS_FOG` = ports `21, 69, 80, 443`.

#	Action	Source	Destination	Port	Objet
1	Autoriser	ATELIER	Ce pare-feu	UDP 67-68	Relais DHCP
2	Autoriser	ATELIER	192.168.10.1	53	DNS vers le DC
3	Autoriser	ATELIER	192.168.10.2	`PORTS_FOG`	Accès serveur FOG
4	Bloquer	ATELIER	192.168.10.0/25	tout	Isolation du périmètre ADMIN
5	Autoriser	ATELIER	tout	tout	Accès Internet

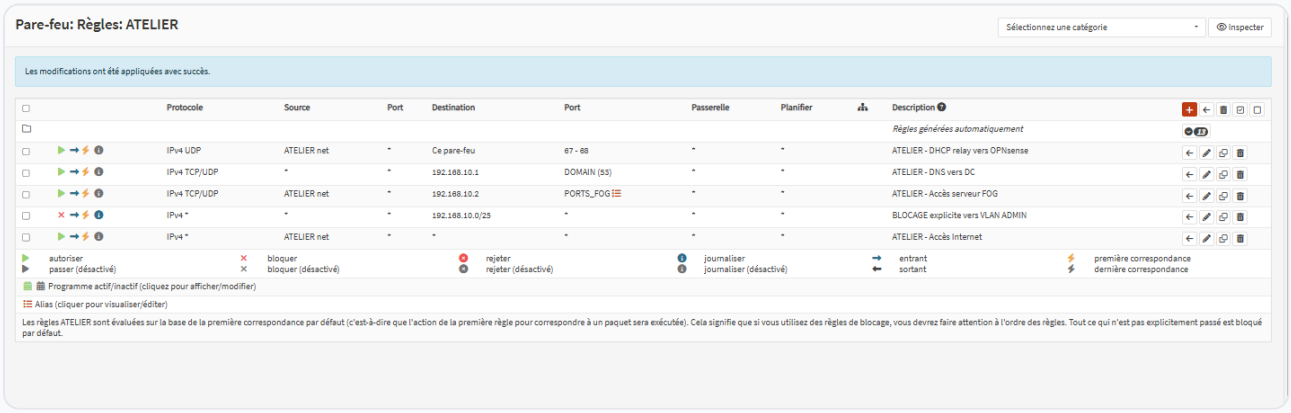


Figure 4.23 · Règles du périmètre ATELIER, dans l'ordre d'évaluation : services autorisés, puis blocage explicite vers ADMIN, puis Internet.

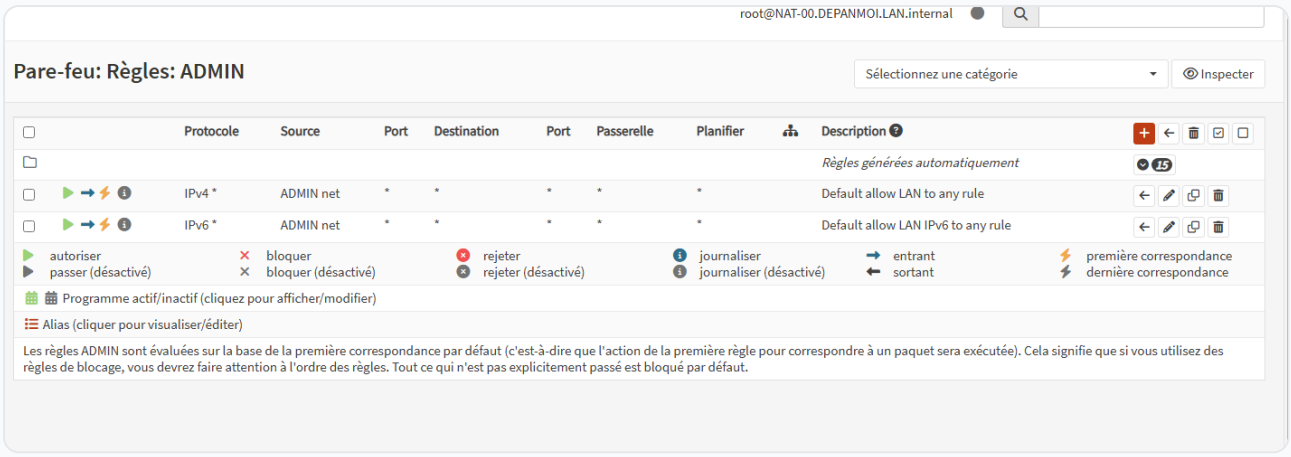


Figure 4.24 · Périmètre ADMIN : autorisation par défaut (les serveurs accèdent aux ressources et à Internet).

ANNOTATIONS

- L'**ordre** des règles est déterminant : les autorisations de service précèdent le blocage vers ADMIN, lui-même placé avant l'autorisation Internet.
- Le NAT sortant (outbound) est laissé en mode automatique : OPNsense traduit les deux `/25` vers l'adresse WAN.
- Le serveur DHCP local d'OPNsense reste désactivé ; seul le relais est utilisé sur ATELIER.

4.4 · PXE-01 · Serveur de déploiement FOG

4.4.1 · Installation de Debian 13

PXE-01 est installé sous Debian 13, nom de machine `PXE-01`, avec une adresse fixe `192.168.10.2` dans le périmètre ADMIN.

Figure 4.25 · Installation de Debian 13, nom de machine `PXE-01`.

4.4.2 · Installation de FOG

FOG est récupéré depuis son dépôt Git puis installé par son script en mode **Normal Server** : déploiement du serveur web, du service TFTP, de la base de données et du partage d'images `/images`. Le DHCP intégré de FOG est laissé désactivé, conformément au choix 2.5.3.

```
FOG Server installation modes:
    * Normal Server: (Choice N)
        This is the typical installation type and
        will install all FOG components for you on this
        machine.  Pick this option if you are unsure what to pick.

    * Storage Node: (Choice S)
        This install mode will only install the software required
        to make this server act as a node in a storage group

More information:
   http://www.fogproject.org/wiki/index.php?title=InstallationModes

What type of installation would you like to do? [N/s (Normal/Storage)] N_
```

*Figure 4.26 · Mode d'installation FOG : **Normal Server**.*

```
    We would like to simply track the common types of OS
    being used, along with the OS Version, and the various
    versions of FOG being used.

 Are you ok with sending this information? [Y/n] n

  ###########################################################################
  #     FOG now has everything it needs for this setup, but please          #
  #   understand that this script will overwrite any setting you may        #
  #   have setup for services like DHCP, apache, pxe, tftp, and NFS.        #
  ###########################################################################
  # It is not recommended that you install this on a production system #
  #        as this script modifies many of your system settings.        #
  ###########################################################################
  #            This script should be run by the root user.              #
  #      It will prepend the running with sudo if root is not set       #
  ###########################################################################
  #              Please see our wiki for more information at:           #
  ###########################################################################
  #                https://wiki.fogproject.org/wiki/index.php             #
  ###########################################################################
  #                          or our new documentation at:                 #
  ###########################################################################
  #                    https://docs.fogproject.org/en/latest/             #
  ###########################################################################

* Here are the settings FOG will use:
* Base Linux: Debian
* Detected Linux Distribution: Debian GNU/Linux
* Interface: ens33
* Server IP Address: 192.168.10.4
* Server Subnet Mask: 255.255.255.128
* Hostname: PXE-01.DEPANMOI.LAN
* Installation Type: Normal Server
* Internationalization: Yes
* Image Storage Location: /images
* Using FOG DHCP: No
* DHCP will NOT be setup but you must setup your
| current DHCP server to use FOG for PXE services.

* On a Linux DHCP server you must set: next-server and filename

* On a Windows DHCP server you must set options 066 and 067

* Option 066/next-server is the IP of the FOG Server: (e.g. 192.168.10.4)
* Option 067/filename is the bootfile: (e.g. undionly.kkpxe or snponly.efi)
* Send OS Name, OS Version, and FOG Version: No


* Are you sure you wish to continue (Y/N)
```

Figure 4.27 · Récapitulatif d'installation : stockage `/images`, Using FOG DHCP: No ; FOG rappelle d'utiliser les options 066/067 du DHCP existant.

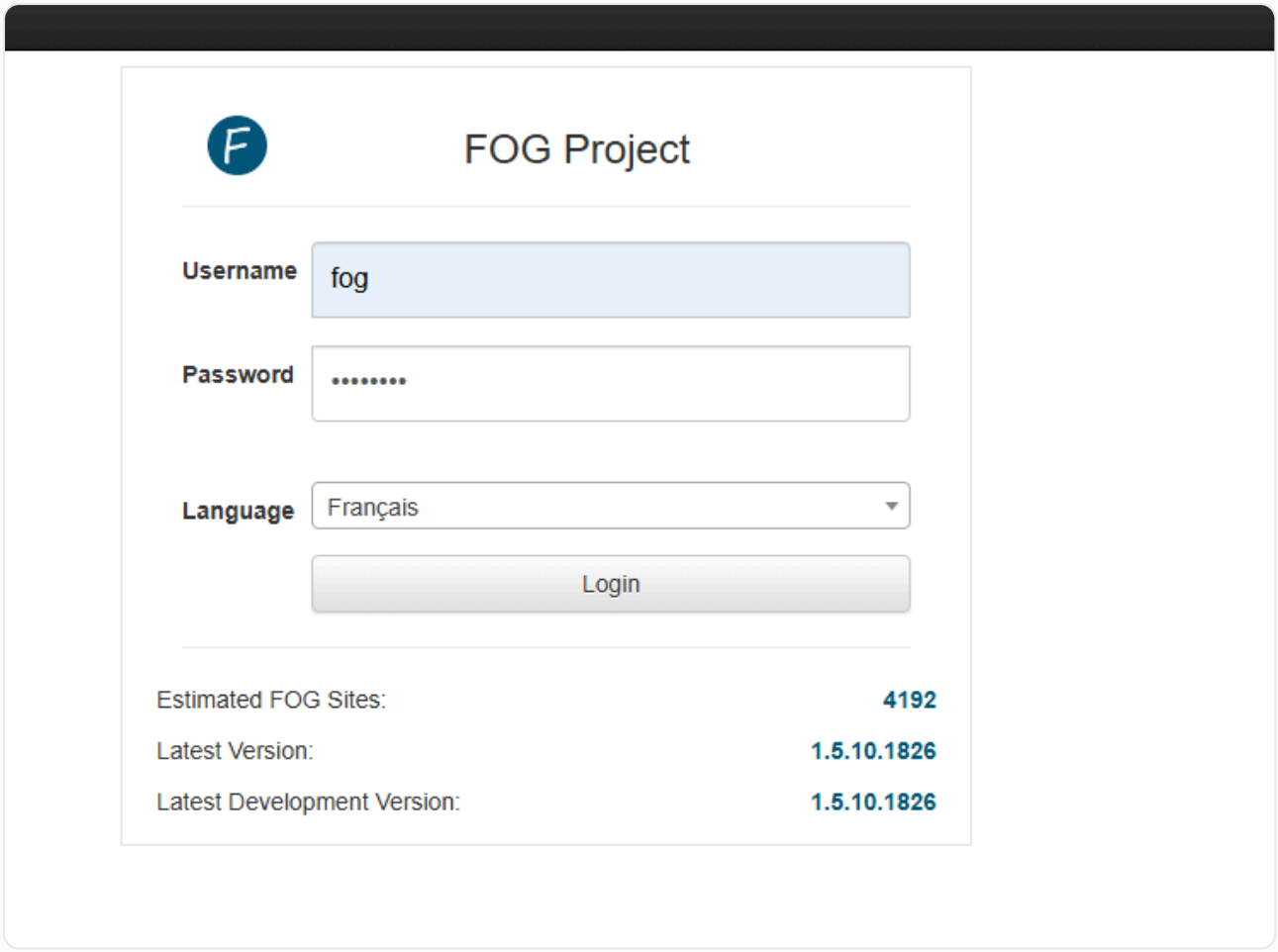


Figure 4.28 · Interface web FOG opérationnelle (version 1.5.10) : connexion administrateur.

4.5 · CLIENT-01 · Poste master et déploiement

4.5.1 · Préparation du master

Un poste de référence est installé une seule fois sous Windows 11 Pro : pilotes (VMware Tools), mises à jour, puis la **suite logicielle commune** déployée d'un bloc avec Ninite (navigateurs, bureautique, utilitaires, lecteurs multimédia et environnements d'exécution). Centraliser l'installation des logiciels en un seul lot garantit l'homogénéité du master.

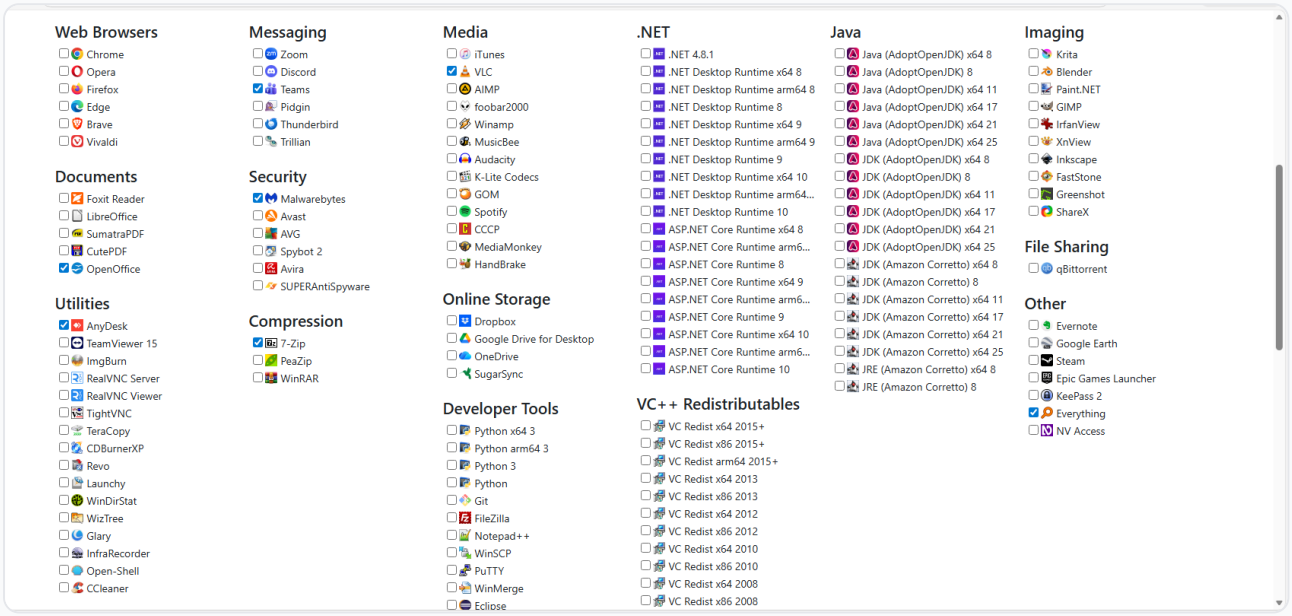


Figure 4.29 · Suite logicielle commune sélectionnée dans Ninite (installation groupée et silencieuse).

4.5.2 · Généralisation par Sysprep

Avant capture, le master est **généralisé** avec Sysprep en mode OOBE et option *Généraliser* : cela efface l'identité de la machine (SID, nom) pour éviter les conflits lorsque l'image sera déployée sur plusieurs postes.

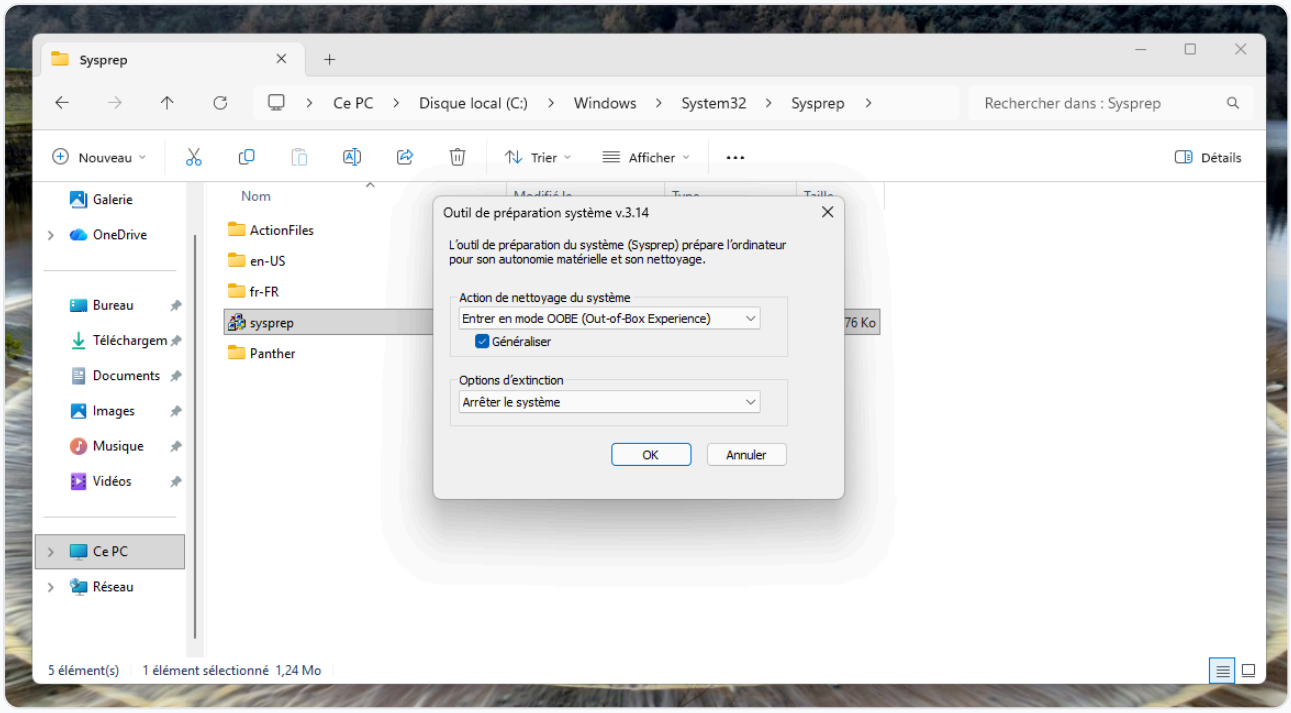


*Figure 4.30 · Sysprep : mode OOBE, case **Généraliser** cochée, action Arrêter le système.*

4.5.3 · Enregistrement et capture de l'image

Le poste démarre ensuite sur le réseau (PXE). Le menu FOG signale que l'hôte n'est pas enregistré ; on procède à un enregistrement rapide (*Quick Registration and Inventory*), ce qui inventorie la machine dans FOG. L'image du master est alors capturée et stockée.

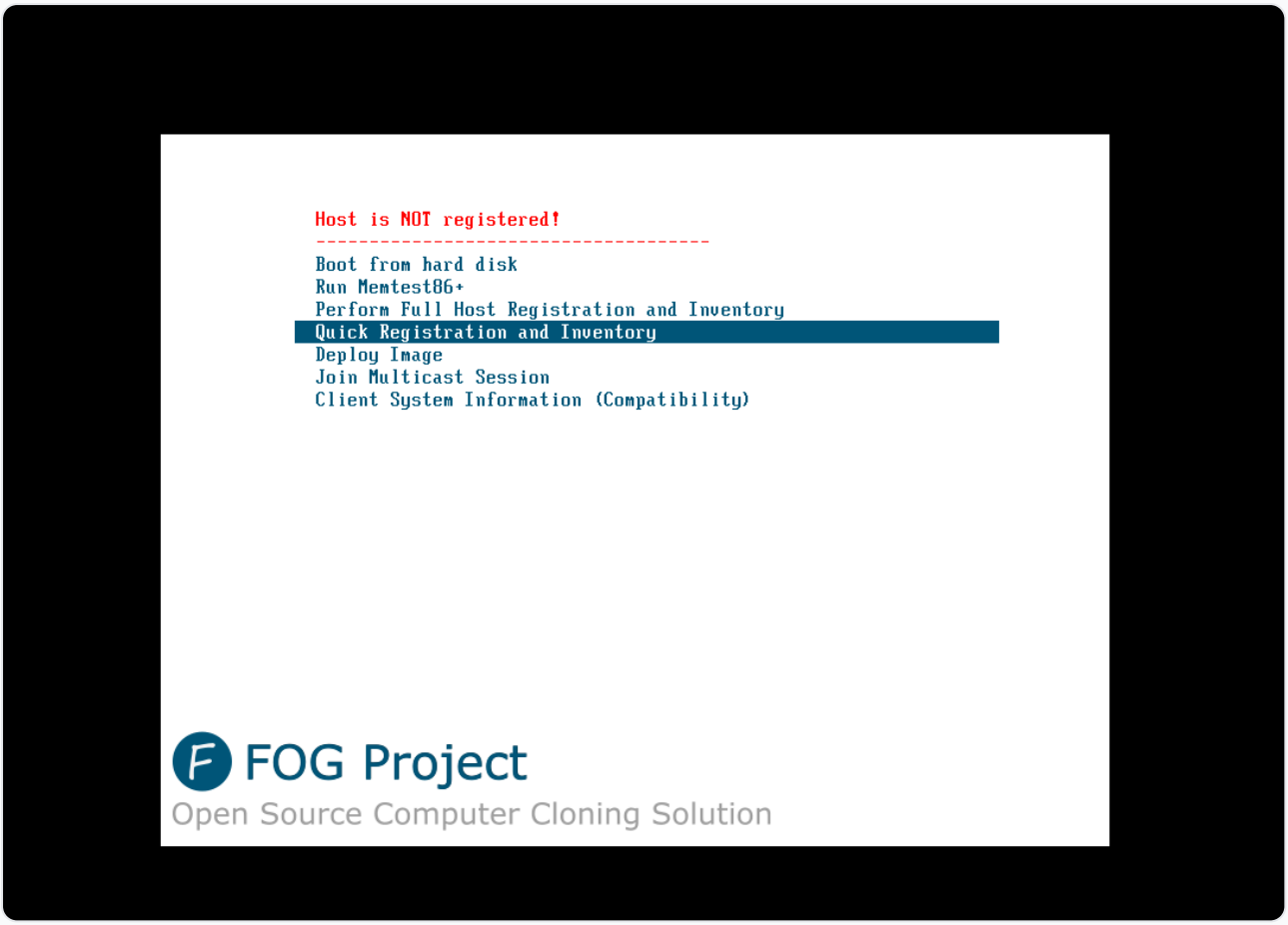


Figure 4.31 · Menu d'amorçage FOG : `Host is NOT registered` → Quick Registration and Inventory.

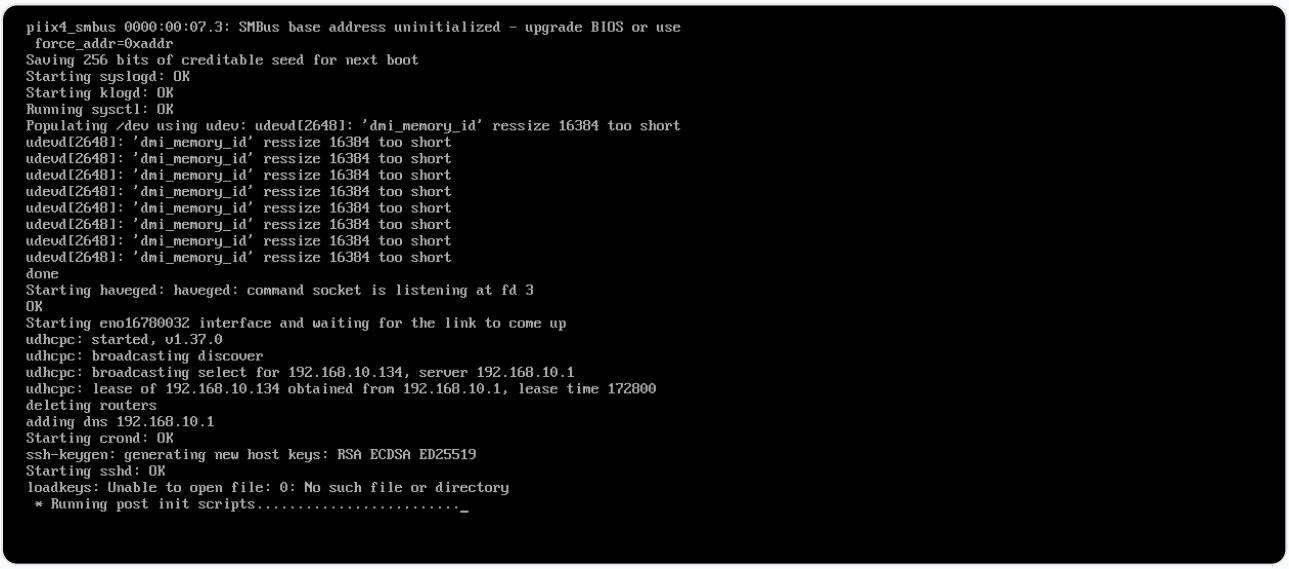


Figure 4.32 · Au démarrage réseau, le poste de l'atelier obtient un bail `192.168.10.134` de `192.168.10.1` via le relais : le relais DHCP et l'amorçage fonctionnent.

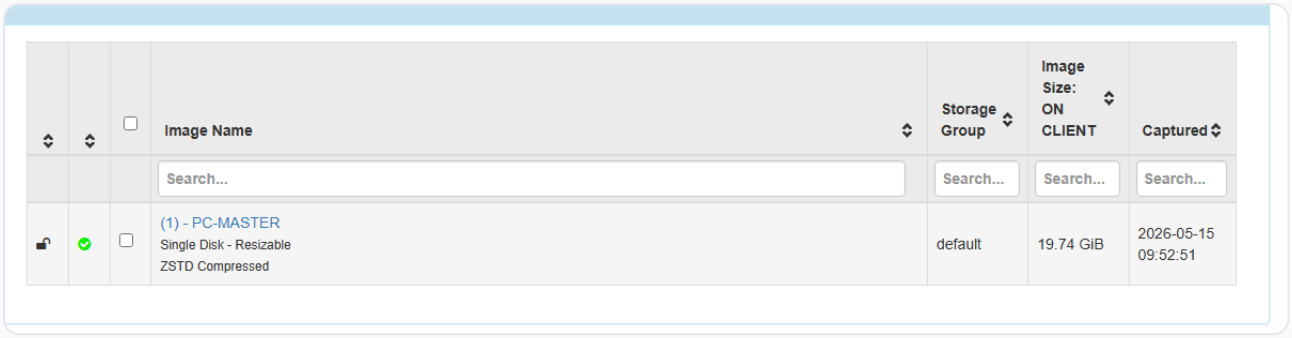


Figure 4.33 · Image de référence `PC-MASTER` capturée dans FOG (disque unique redimensionnable, compression ZSTD, 19,74 Gio).

DÉPLOIEMENT D'UN NOUVEAU POSTE

Pour fabriquer un poste : le brancher dans l'atelier, démarrer sur le réseau, l'enregistrer dans FOG, puis lancer *Deploy Image* avec `PC-MASTER`. Le poste redémarre opérationnel, conforme au master, en quelques minutes.

PARTIE 5

Plan de tests et validation

5.1 · Méthodologie

Chaque test couvre une ou plusieurs exigences du cahier des charges. La fiche précise l'identifiant, la procédure, le résultat attendu et le résultat observé. Les preuves sont apportées par captures (terminal, console DC, interface OPNsense, menu FOG). La synthèse 5.4 récapitule la couverture.

Catégorie	Tests	Outils mobilisés
Fonctionnels	T-01 à T-08 : domaine, DNS, DHCP, relais, isolation, Internet, PXE, déploiement	`dcdiag`, `nslookup`, `ipconfig`, `ping`, console OPNsense, menu FOG
Transverses	T-09, T-10 : nommage FQDN, documentation et sauvegardes	Gestionnaire DNS, export XML, archivage des VM et de l'image

5.2 · Tests fonctionnels

Test T-01 : Promotion et santé du domaine

Exigence couverte : `EF-01` . **Statut :** VALIDÉ

Procédure :

1. Sur DC-01 : `dcdiag /v` .
2. Joindre un poste Windows au domaine `DEPANMOI.LAN` .
3. Ouvrir une session avec un compte de domaine.

Résultat attendu : `dcdiag` sans erreur bloquante, jonction réussie, ouverture de session de domaine effective.

Résultat observé : conforme. Domaine sain, poste joint, session de domaine ouverte.

Test T-02 : Résolution DNS directe et inverse

Exigence couverte : `EF-02` . **Statut :** VALIDÉ

Procédure :

1. `nslookup dc-01.depanmoi.lan` puis `nslookup pxe-01.depanmoi.lan` .
2. `nslookup 192.168.10.2` (résolution inverse).
3. `nslookup www.exemple.fr` (résolution externe via redirecteurs).

Résultat attendu : .1 et .2 résolus en direct, .2 résolu en `pxe-01.depanmoi.lan` en inverse, nom public résolu par les redirecteurs.

Résultat observé : conforme, zones directe et inverse opérationnelles.

Test T-03 : Adressage DHCP du périmètre ADMIN

Exigence couverte : `EF-03` . **Statut :** VALIDÉ

Procédure :

1. Brancher un poste dans le périmètre ADMIN, `ipconfig /release` puis `/renew` .
2. Vérifier l'adresse, la passerelle et le DNS obtenus.

Résultat attendu : adresse dans `192.168.10.3 → .125` , passerelle `.126` , DNS `.1` .

Résultat observé : conforme.

Test T-04 : Relais DHCP du périmètre ATELIER

Exigences couvertes : `EF-03`, `EF-07`. **Statut :** VALIDÉ

Procédure :

1. Démarrer un poste dans l'atelier et observer l'obtention du bail.
2. Vérifier que l'adresse provient de l'étendue ATELIER via le relais OPNsense.

Résultat attendu : bail dans `192.168.10.129 → .253`, serveur `192.168.10.1` (relayé), passerelle `.254`.

Résultat observé : conforme. Le poste obtient `192.168.10.134` de `192.168.10.1`.

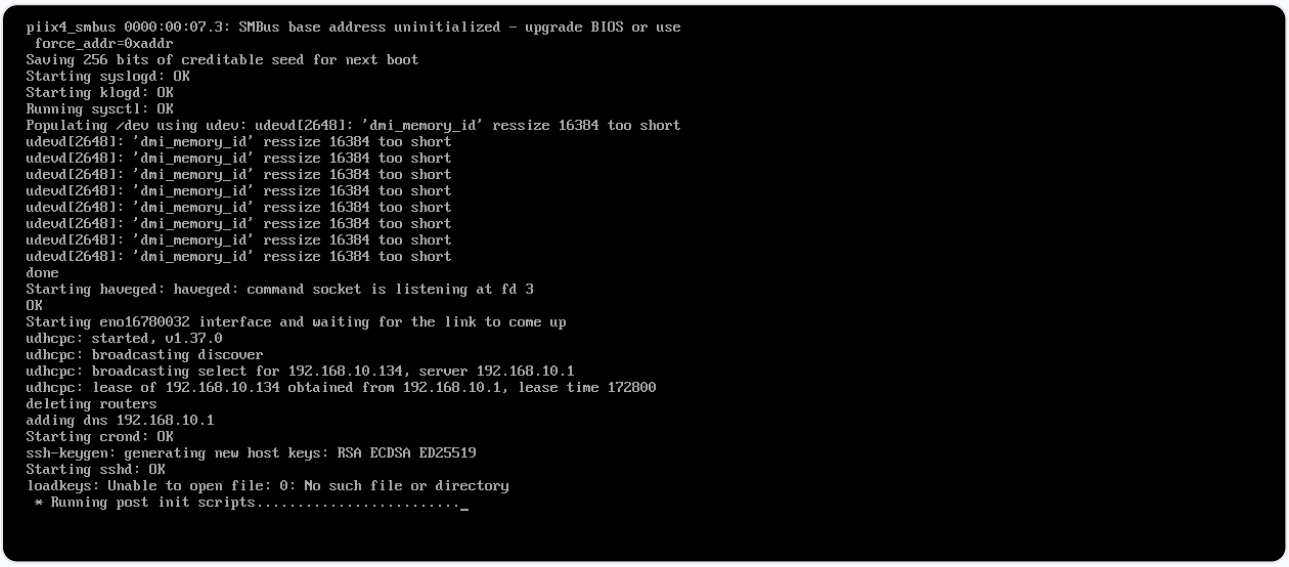


Figure 5.1 · Test T-04 : au démarrage réseau, `lease of 192.168.10.134 obtained from 192.168.10.1`, DNS `192.168.10.1`. Le relais DHCP achemine bien les requêtes de l'atelier vers le contrôleur.

Test T-05 : Isolation ATELIER → ADMIN

Exigences couvertes : `EF-06`, `ENF-04`. **Statut :** VALIDÉ

Procédure :

1. Depuis un poste de l'atelier : `ping 192.168.10.1` (DC) hors des services autorisés.
2. Vérifier le rejet dans les journaux du pare-feu OPNsense.

Résultat attendu : trafic vers `192.168.10.0/25` bloqué (hors DNS/FOG/relais explicitement autorisés).

Résultat observé : conforme. La règle de blocage rejette l'accès au périmètre ADMIN.

Test T-06 : Accès Internet et NAT

Exigence couverte : `EF-08` . **Statut :** VALIDÉ

Procédure :

1. Depuis un poste : `ping 1.1.1.1` puis navigation web.
2. Vérifier la traduction NAT sur OPNsense.

Résultat attendu : sortie Internet fonctionnelle via NAT OPNsense.

Résultat observé : conforme.

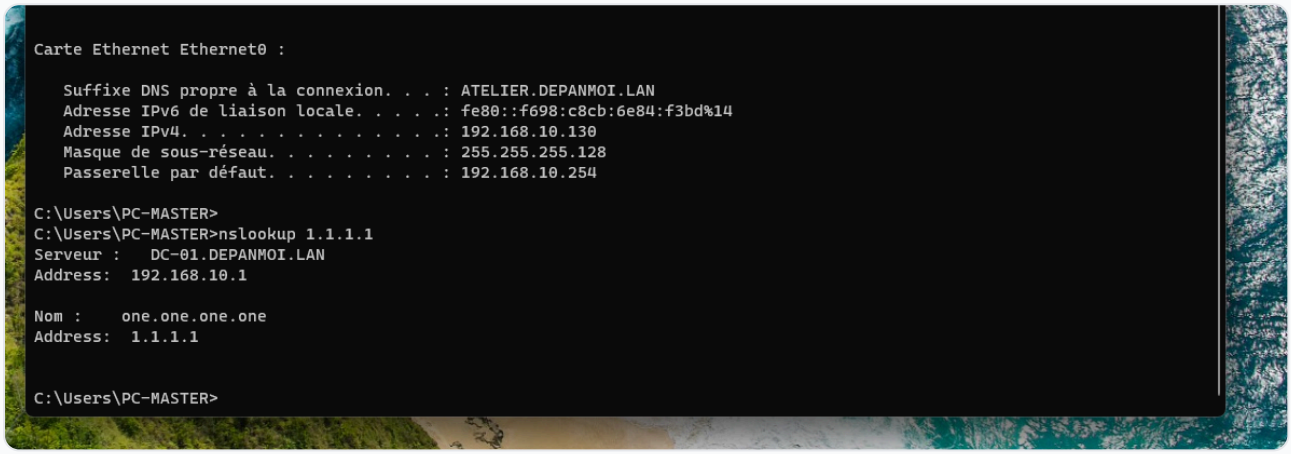


Figure 5.2 · Tests T-03/T-06 : vérification de l'adressage, de la passerelle et de la connectivité depuis le poste.

Test T-07 : Amorçage réseau PXE

Exigence couverte : `EF-04` . **Statut :** VALIDÉ

Procédure :

1. Configurer un poste pour le démarrage réseau (UEFI/PXE).
2. Observer le chargement de `ipxe.efi` depuis `192.168.10.2` .

Résultat attendu : chargement du fichier d'amorçage et affichage du menu FOG.

Résultat observé : conforme. Menu FOG affiché.

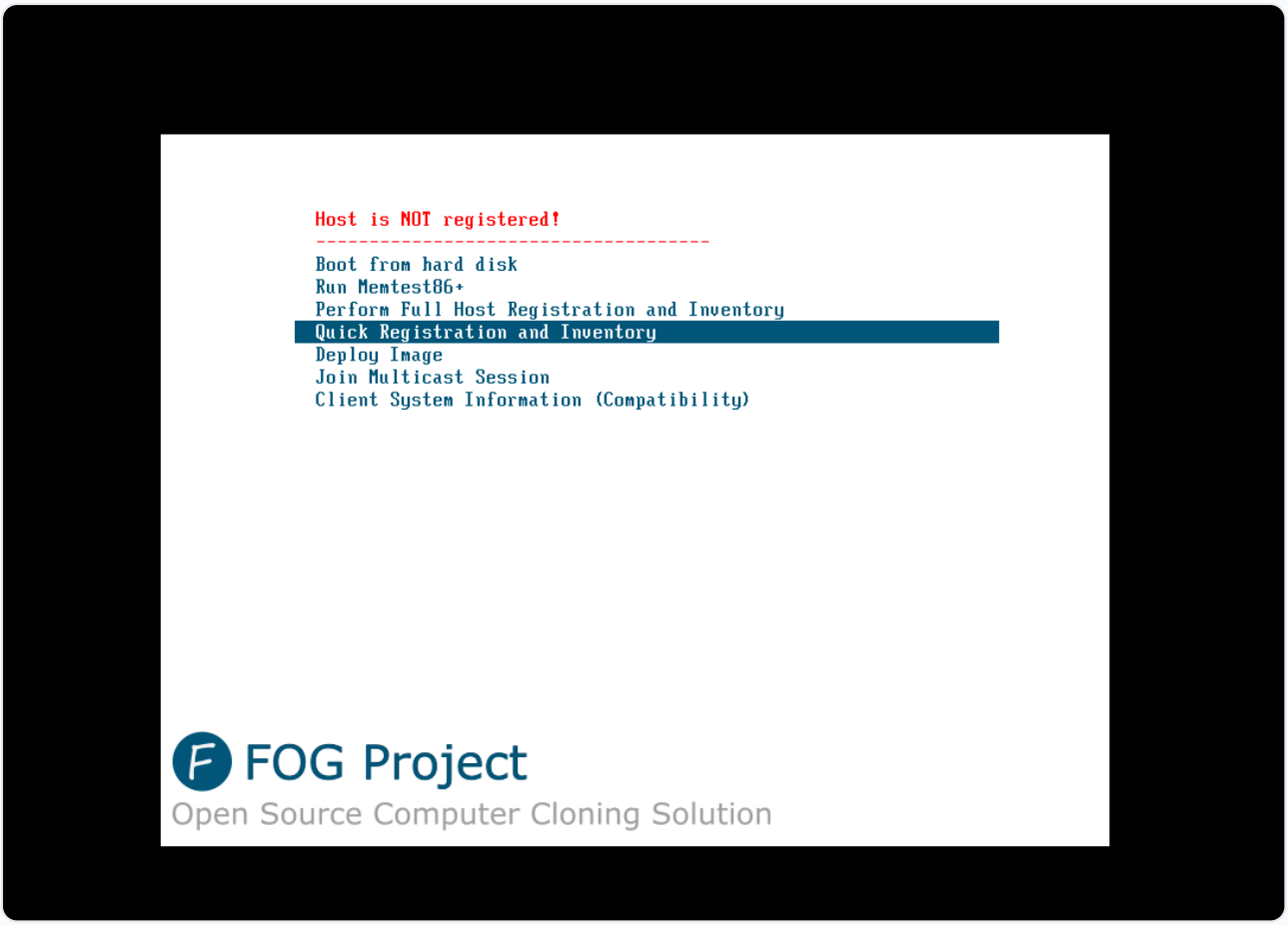


Figure 5.3 · Test T-07 : menu d'amorçage FOG chargé par le réseau (options 066/067 distribuées par le DHCP).

Test T-08 : Capture et déploiement de l'image

Exigences couvertes : `EF-05`, `ENF-01`, `ENF-02`. **Statut :** VALIDÉ

Procédure :

1. Capturer le master généralisé dans FOG (image `PC-MASTER`).
2. Lancer *Deploy Image* sur un poste cible enregistré.
3. Démarrer le poste cible et vérifier sa conformité au master.

Résultat attendu : image capturée, déploiement réussi, poste opérationnel conforme, durée < 30 min.

Résultat observé : conforme. Image `PC-MASTER` (19,74 Gio, ZSTD) capturée puis déployée à l'identique.

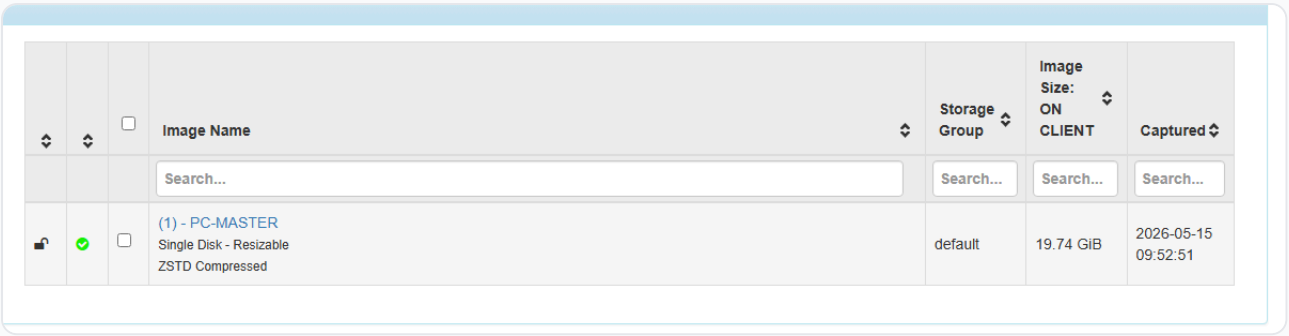


Figure 5.4 · Test T-08 : image `PC-MASTER` disponible dans FOG, prête au déploiement.

5.3 · Tests non fonctionnels transverses

Test T-09 : Nommage FQDN cohérent

Exigence couverte : `ENF-05` . **Statut :** VALIDÉ

Les hôtes sont nommés `DC-01`, `PXE-01`, `NAT-00`, `CLIENT-01` et résolus en `*.DEPANMOI.LAN` par le DNS interne. Vérifié dans le Gestionnaire DNS et par `nslookup`.

Test T-10 : Documentation et sauvegardes

Exigences couvertes : `ENF-07`, `ENF-08` . **Statut :** VALIDÉ

Présent dossier livré ; export XML d'OPNsense, image FOG et machines virtuelles archivés (annexe 8.3). Plan d'adressage et schéma logique fournis en partie 3.

5.4 · Synthèse de recette

Test	Exigences	Objet	Statut
T-01	EF-01	Promotion et santé du domaine	VALIDÉ
T-02	EF-02	DNS direct / inverse / externe	VALIDÉ
T-03	EF-03	DHCP ADMIN	VALIDÉ
T-04	EF-03, EF-07	Relais DHCP ATELIER	VALIDÉ
T-05	EF-06, ENF-04	Isolation ATELIER → ADMIN	VALIDÉ
T-06	EF-08	Accès Internet et NAT	VALIDÉ
T-07	EF-04	Amorçage PXE	VALIDÉ
T-08	EF-05, ENF-01, ENF-02	Capture / déploiement d'image	VALIDÉ
T-09	ENF-05	Nommage FQDN	VALIDÉ
T-10	ENF-07, ENF-08	Documentation et sauvegardes	VALIDÉ

RECETTE PRONONCÉE

Les dix tests sont conformes, l'ensemble des exigences `EF` et `ENF` du périmètre est couvert. La solution est recevable.

PARTIE 6

Gestion des incidents

6.1 · Méthodologie et échelle de criticité

Chaque incident est qualifié selon une échelle de quatre niveaux, déterminée par l'impact métier et l'urgence d'intervention.

Niveau	Définition	Délai d'intervention
CRITIQUE	Service entier interrompu, ou faille de sécurité active.	Immédiat, ≤ 30 min
HAUTE	Fonction métier dégradée, plusieurs utilisateurs gênés.	Heures ouvrées, ≤ 4 h
MOYENNE	Performance ou redondance partielle perdue, aucun blocage.	Jour ouvré, ≤ 1 j
BASSE	Anomalie sans impact direct, correction planifiée.	Hebdomadaire, ≤ 1 sem

ID	Incident	Criticité
I-01	Panne du contrôleur de domaine (DC-01)	CRITIQUE
I-02	Échec d'amorçage PXE d'un poste	MOYENNE
I-03	Postes de l'atelier sans adresse IP	HAUTE
I-04	Panne du serveur FOG (PXE-01)	MOYENNE
I-05	Résolution de noms en échec	HAUTE
I-06	Fuite ATELIER → ADMIN	CRITIQUE
I-07	Coupure du lien WAN (FAI)	MOYENNE
I-08	Conflit d'identité après déploiement	BASSE

6.2 · Catalogue des incidents

Incident I-01 : Panne du contrôleur de domaine (DC-01)

Criticité : CRITIQUE · **Bascule automatique :** non (pas de second DC)

Symptômes observables :

- Échec des ouvertures de session de domaine.
- Résolution DNS interne KO, accès aux ressources nommées impossible.
- Plus de distribution de nouveaux baux DHCP.

Cause probable : panne matérielle de la VM, corruption système ou arrêt inopiné de l'hôte de virtualisation.

Impact métier : authentification, DNS et DHCP indisponibles. DC-01 étant unique (cf. EF-09 Won't), l'impact est majeur.

Action immédiate :

1. Vérifier l'état de la VM et de l'hôte ; redémarrer la VM si elle est figée.
2. Si le système ne démarre plus : restaurer DC-01 depuis la sauvegarde de l'état système (annexe 8.4).
3. Contrôler la santé du domaine après reprise (`dcdiag`).

Action de fond : mettre en place un **second contrôleur de domaine** (perspective 7.6) pour supprimer ce point de défaillance unique, et planifier des sauvegardes régulières de l'état système.

Commandes de diagnostic :

```
! Sur DC-01 (PowerShell) :
dcdiag /v
Get-Service NTDS,DNS,DHCPServer
Get-DnsServerZone
Get-DhcpServerv4Scope
```

Incident I-02 : Échec d'amorçage PXE d'un poste

Criticité : MOYENNE · **Bascule automatique :** sans objet

Symptômes observables :

- Le poste démarre sur le disque local au lieu du réseau, ou affiche `PXE-E…` .
- Pas de chargement de `ipxe.efi` , menu FOG absent.

Cause probable : options DHCP 066/067 absentes ou erronées, mode d'amorçage (UEFI/Legacy) incohérent, ou serveur FOG injoignable.

Impact métier : impossible de déployer un nouveau poste ; les postes existants ne sont pas affectés.

Action immédiate :

1. Vérifier les options serveur DHCP : 066 = `192.168.10.2`, 067 = `ipxe.efi`.
2. Contrôler que le poste est bien en démarrage réseau UEFI.
3. Vérifier l'accès au serveur FOG (ports TFTP/HTTP) depuis l'atelier.

Action de fond : documenter le mode d'amorçage attendu sur l'affiche technicien (annexe 8.5).

Commandes de diagnostic :

```
! Depuis l'atelier :
ping 192.168.10.2          ! serveur FOG joignable ?
! Sur DC-01 :
Get-DhcpServerv4OptionValue -OptionId 66
Get-DhcpServerv4OptionValue -OptionId 67
```

Incident I-03 : Postes de l'atelier sans adresse IP

Criticité : HAUTE · **Bascule automatique :** non

Symptômes observables :

- Les postes de l'atelier obtiennent une adresse APIPA (`169.254.x.x`) ou aucune adresse.
- Les postes du périmètre ADMIN, eux, sont correctement adressés.

Cause probable : relais DHCP d'OPNsense désactivé sur l'interface ATELIER, ou règle de pare-feu UDP 67-68 manquante, ou DC-01 injoignable.

Impact métier : aucun poste ne peut être préparé dans l'atelier.

Action immédiate :

1. Vérifier que le relais DHCP est actif sur l'interface ATELIER, destination `192.168.10.1`.
2. Vérifier la règle autorisant UDP 67-68 de l'atelier vers le pare-feu.
3. Vérifier que le service DHCP de DC-01 fonctionne.

Action de fond : intégrer la vérification du relais à la check-list de mise en service.

Incident I-04 : Panne du serveur FOG (PXE-01)

Criticité : MOYENNE · **Bascule automatique :** sans objet

Symptômes observables :

- Le menu FOG ne s'affiche plus au démarrage réseau ; déploiements impossibles.
- L'interface web FOG est inaccessible.

Cause probable : panne de la VM PXE-01, service web/TFTP arrêté, ou disque `/images` plein.

Impact métier : arrêt de la chaîne de déploiement ; les postes déjà installés et le domaine ne sont pas affectés.

Action immédiate :

1. Redémarrer PXE-01 et les services FOG ; vérifier l'espace disque de `/images`.
2. Si la VM est perdue : reconstruire FOG (annexe 8.4) et restaurer les images sauvegardées.

Action de fond : sauvegarder régulièrement le dossier `/images` et exporter la configuration FOG.

Incident I-05 : Résolution de noms en échec

Criticité : HAUTE · **Bascule automatique :** non

Symptômes observables :

- Accès aux ressources internes par nom impossible ; navigation externe KO depuis les postes.
- `nslookup` échoue ou renvoie des réponses incohérentes.

Cause probable : zone DNS corrompue, redirecteurs injoignables, ou service DNS arrêté sur DC-01.

Impact métier : dégradation générale de l'accès aux ressources nommées et à Internet.

Action immédiate :

1. Vérifier le service DNS de DC-01 et l'état des zones (directe et inverse).
2. Tester les redirecteurs : `nslookup www.exemple.fr 1.1.1.1`.
3. Vider le cache DNS du serveur si nécessaire.

Action de fond : surveiller la disponibilité des redirecteurs ; envisager un second serveur DNS avec le futur DC.

Incident I-06 : Fuite ATELIER → ADMIN

Criticité : CRITIQUE · **Bascule automatique :** non

Symptômes observables :

- Un poste de l'atelier parvient à joindre un serveur du périmètre ADMIN hors des services prévus.

Cause probable : mauvais ordre des règles de pare-feu (Internet placé avant le blocage), règle de blocage désactivée ou supprimée.

Impact métier : faille de cloisonnement, exposition des serveurs aux postes en préparation.

Action immédiate :

1. Vérifier l'ordre des règles ATELIER : le blocage vers `192.168.10.0/25` doit précéder l'autorisation Internet.

2. Réactiver ou réordonner la règle, puis appliquer.
3. Contrôler les journaux pour mesurer l'exposition.

Action de fond : documenter l'ordre attendu des règles et le contrôler après toute modification.

Incident I-07 : Coupure du lien WAN (FAI)

Criticité : MOYENNE · **Bascule automatique :** non

Symptômes observables :

- Plus d'accès Internet ; les services internes (domaine, déploiement) restent opérationnels.
- Interface WAN d'OPNsense sans adresse ou sans passerelle.

Cause probable : incident chez le FAI ou lien WAN coupé.

Impact métier : perte de la navigation et des services externes ; la préparation des postes en local continue.

Action immédiate : vérifier le lien WAN, redemander un bail DHCP côté WAN, ouvrir un ticket FAI.

Action de fond : le SLA du FAI s'applique ; un secours 4G pourrait être étudié si l'activité l'exige.

Incident I-08 : Conflit d'identité après déploiement

Criticité : BASSE · **Bascule automatique :** sans objet

Symptômes observables :

- Deux postes déployés portent le même nom ou le même SID ; problèmes de jonction au domaine.

Cause probable : image capturée **sans généralisation Sysprep**.

Impact métier : doublons dans l'annuaire, comportements erratiques sur les postes concernés.

Action immédiate : renommer / rejoindre proprement les postes concernés.

Action de fond : re-généraliser le master avec Sysprep (*Généraliser*) puis recapturer l'image avant tout nouveau déploiement.

6.3 · Tableau d'escalade

Niveau	Prise en charge	Escalade si non résolu
BASSE / MOYENNE	Technicien DEPANMOI.FR	Gérant (sous 1 jour ouvré)
HAUTE	Technicien + gérant informés	Support éditeur / FAI selon le service
CRITIQUE	Intervention immédiate, gérant prévenu	Restauration depuis sauvegarde (annexe 8.4)

PARTIE 7

Retour d'expérience et perspectives d'évolution

7.1 · Bilan personnel du projet

Ce projet m'a fait dérouler une chaîne système complète, du contrôleur de domaine jusqu'au poste déployé. Le fil conducteur a été la cohérence entre les briques : le DHCP du contrôleur distribue les options qui amorcent le PXE, le relais d'OPNsense permet à l'atelier d'atteindre ce DHCP, et le pare-feu garde les deux périmètres séparés. Comprendre comment ces services se passent le relais a été plus formateur que chaque service pris isolément.

7.2 · Ce qui a fonctionné dès la première mise en œuvre

- La promotion de la forêt `DEPANMOI.LAN` et l'installation conjointe du DNS.
- La création des deux étendues DHCP et la résolution directe des hôtes du domaine.
- La capture de l'image du master après Sysprep, puis son déploiement à l'identique.

7.3 · Difficultés rencontrées et résolution

Difficulté	Diagnostic	Résolution
Postes de l'atelier sans adresse IP	Le DHCP est sur DC-01, hors du domaine de diffusion de l'atelier	Activation du relais DHCP sur l'interface OPT1 (ATELIER) d'OPNsense vers 192.168.10.1, plus règle UDP 67-68
Démarrage réseau qui n'aboutit pas	Options 066/067 non distribuées	Déclaration des options serveur (066 = 192.168.10.2, 067 = `ipxe.efi`)
Crainte de conflits après déploiement	Image risquant d'être capturée sans généralisation	Passage systématique de Sysprep en mode *Généraliser* avant capture
Atelier capable d'atteindre les serveurs	Règle Internet trop large évaluée avant le blocage	Réordonnancement : blocage vers ADMIN avant l'autorisation Internet

7.4 · Choix techniques que je referais autrement

- Prévoir dès le départ un **second contrôleur de domaine** pour ne pas laisser DC-01 en point de défaillance unique.
- Mettre en place une **réservation DHCP** pour les postes durables plutôt que de longs baux, afin de garder un inventaire plus lisible.
- Documenter le mode d'amorçage (UEFI vs Legacy) des postes cibles avant la phase de déploiement.

7.5 · Compétences acquises

Compétence (référentiel SISR)	Mise en œuvre dans la réalisation
Concevoir une solution d'infrastructure réseau	Analyse du besoin d'industrialisation, dossier de choix (AD DS, FOG, OPNsense, relais DHCP), plan d'adressage, préparation des tests
Installer, tester et déployer	Installation du contrôleur (AD DS, DNS, DHCP), de la passerelle et du serveur FOG, capture et déploiement de l'image, recette des dix tests
Exploiter, dépanner et superviser	Administration du domaine, diagnostic des incidents (relais, PXE, Sysprep, filtrage), catalogue d'incidents et procédures

7.6 · Plan d'amélioration de l'infrastructure

Horizon	Amélioration
COURT TERME (≤ 3 mois)	Stratégies de groupe (GPO) pour standardiser les postes joints au domaine ; sauvegarde planifiée de l'état système de DC-01
MOYEN TERME (3 à 12 mois)	Second contrôleur de domaine (HA annuaire + DNS) ; sauvegarde régulière du dossier `/images` de FOG
LONG TERME (> 1 an)	Supervision centralisée (SNMP / Syslog), serveur de fichiers, déploiement applicatif par GPO

7.7 · Bilan global

L'objectif est atteint : DEPANMOI.FR dispose désormais d'un domaine qui centralise authentification, résolution de noms et adressage, d'une passerelle qui sépare proprement serveurs et postes, et d'une chaîne qui pose une image complète en quelques minutes. Le temps de préparation d'un poste passe de deux heures à moins de trente minutes, pour un résultat homogène et reproductible.

PARTIE 8

Annexes

8.1 · Glossaire des acronymes

AD DS	Active Directory Domain Services · annuaire et service de domaine Windows
Forêt	Niveau le plus haut de l'organisation Active Directory, contenant un ou plusieurs domaines
Catalogue global	Index partiel de tous les objets de la forêt, porté par un contrôleur de domaine
DNS	Domain Name System · résolution des noms en adresses, et inversement
Zone inverse	Zone DNS traduisant une adresse IP en nom (`in-addr.arpa`)
Redirecteur	Serveur DNS externe vers lequel les requêtes non locales sont transmises
DHCP	Dynamic Host Configuration Protocol · attribution automatique d'adresses
Relais DHCP	Service transmettant les requêtes DHCP d'un sous-réseau vers un serveur distant
Option 066 / 067	Serveur et fichier de démarrage réseau distribués par le DHCP (amorçage PXE)
PXE / iPXE	Preboot eXecution Environment · démarrage d'un poste depuis le réseau
FOG	Free Open-source Ghost · serveur libre de capture et de déploiement d'images
Sysprep	Outil Windows de généralisation d'une image avant clonage (efface SID et nom)
NAT	Network Address Translation · traduction d'adresses vers Internet
FQDN	Fully Qualified Domain Name · nom pleinement qualifié (`hote.depanmoi.lan`)

8.2 · Références aux RFC et standards

RFC 2131	Dynamic Host Configuration Protocol (DHCP)
RFC 1034 / 1035	DNS · concepts, spécifications et implémentation
RFC 4578	Options DHCP pour le client PXE (architecture système, identifiant)
Documentation FOG	docs.fogproject.org
Documentation OPNsense	docs.opnsense.org
Microsoft Learn	Active Directory Domain Services, DNS et DHCP sous Windows Server

8.3 · Configurations et images archivées

EMPLACEMENT DES ÉLÉMENTS ARCHIVÉS

Les machines virtuelles complètes (`DC-01.DEPANMOI.LAN`, `NAT-00.DEPANMOI.LAN`, `PXE-01.DEPANMOI.LAN`, `CLIENT-01.DEPANMOI.LAN`) sont archivées au format VMware. L'export XML de la configuration OPNsense et l'image FOG `PC-MASTER` (stockage `/images`) complètent la sauvegarde. Les captures d'écran justificatives sont rangées par machine dans le dossier `CAPTURES/`.

8.4 · Procédure de reconstruction du serveur FOG

En cas de perte de PXE-01, la chaîne de déploiement se reconstruit ainsi :

1. Réinstaller Debian 13 sur une nouvelle VM, nom `PXE-01`, adresse fixe `192.168.10.2/25`.
2. Récupérer FOG depuis son dépôt Git et lancer l'installation en mode **Normal Server** (DHCP FOG désactivé).
3. Restaurer le dossier `/images` depuis la sauvegarde (image `PC-MASTER`).
4. Vérifier l'enregistrement DNS `pxe-01 → 192.168.10.2` et les options DHCP 066/067 sur DC-01.
5. Tester un amorçage PXE et un déploiement depuis l'atelier.

8.5 · Affiche technicien · Déployer un nouveau poste

PROCÉDURE RAPIDE

1. Brancher le poste dans le réseau **ATELIER** et l'allumer.
2. Forcer le **démarrage réseau** (UEFI / PXE) dans le BIOS.
3. Au menu FOG : *Quick Registration and Inventory* si le poste est nouveau.
4. Lancer *Deploy Image* et choisir `PC-MASTER`.
5. Attendre la fin du clonage, puis laisser le poste redémarrer et finir l'OOBE.

En cas d'échec : vérifier que le poste obtient bien une adresse en `192.168.10.129-.253` et que le serveur FOG (`192.168.10.2`) répond.