PROJET FOG — DOCUMENT D

Déploiement d'images : poste unitaire et flotte de postes

Mode opératoire — Lab TSSR / Infrastructure Proxmox

Auteur	Julien BARBET
Version	1.0
Date	28 août 2026
Serveur	SRV-FOG-01 M192.168.1.207 MFOG 1.5.10.2254
Postes cibles	VM 210, 212 et 213 MPC-TEST-PXE, -2 et -3
Domaine	lab.julien.local
Contexte	Lab personnel de formation

1. Objet du document

Ce document décrit le déploiement d'une image Windows 11 sur des postes vierges, depuis le serveur FOG. Il reprend là où s'arrête le document C : l'image est capturée et disponible sur le serveur. Les captures venant de sessions successives, plusieurs noms d'image apparaissent.

Deux modes sont traités, car ils ne répondent pas au même besoin.

	Déploiement unitaire (unicast)	Déploiement de flotte (multicast)
Déclencheur	Une tâche par poste	Une tâche pour un groupe de postes
Transport	NFS, un flux par poste	UDPCAST, un flux unique diffusé
Bande passante	Se divise entre les postes	Constante quel que soit le nombre de postes
Configuration	Poste par poste	Une fois sur le groupe, héritée par les postes
Cas d'usage	Remplacement d'un poste, réinstallation	Renouvellement de parc, ouverture de salle

1.1 Séquence commune

Quel que soit le mode, un déploiement suit toujours les mêmes étapes :

1. Le poste vierge amorce en réseau et s'enregistre auprès du serveur
2. L'administrateur configure l'hôte : image, jonction au domaine, snapins
3. Une tâche est créée et placée en attente
4. Le poste redémarre en réseau, récupère la tâche et déploie l'image
5. Au premier démarrage Windows, le client FOG renomme la machine, la joint au domaine et exécute les snapins

> **Répartition des rôles entre l'unattend.xml et le client FOG**
>
> Deux mécanismes agissent après le clonage, à des moments différents. Le fichier `unattend.xml`, embarqué dans l'image, traite la phase OOBE : régionalisation, écrans masqués, compte local. Le client FOG, service Windows démarré ensuite, traite ce qui est **propre à chaque poste** : le nom de la machine et la jonction au domaine ne peuvent pas figurer dans une image commune, puisqu'ils diffèrent d'un poste à l'autre. C'est cette répartition qui permet d'utiliser une image unique sur tout le parc.

2. Préparation du poste cible

Les postes cibles sont des machines virtuelles créées en ligne de commande sur l'hyperviseur, afin de garantir une configuration strictement identique :

```
qm stop 210
qm destroy 210
qm create 210 \
  --name PC-TEST-PXE \
  --machine q35 --bios ovmf --ostype win11 \
  --cpu host --cores 2 --sockets 1 --memory 4096 \
  --scsihw virtio-scsi-single \
  --scsi0 vmdata:60,discard=on,iothread=1 \
  --efidisk0 vmdata:1,efitype=4m,pre-enrolled-keys=0 \
  --tpmstate0 vmdata:1,version=v2.0 \
  --net0 e1000=BC:24:11:90:A8:BD,bridge=vmbr0,firewall=1 \
  --boot order=net0\;scsi0 \
  --agent 1
```

Figure 1 — Création d'un poste cible en ligne de commande sur l'hyperviseur

Paramètre	Rôle dans le déploiement
`--bios ovmf`	Micrologiciel UEFI, requis pour l'amorçage PXE en mode EFI
`--net0 e1000`	Carte réseau reconnue par iPXE. L'adresse MAC est fixée explicitement, ce qui permet d'identifier le poste dans FOG
`--efidisk0 pre-enrolled-keys=0`	Disque EFI sans clés Secure Boot pré-enregistrées
`--tpmstate0 version=v2.0`	TPM 2.0, prérequis Windows 11
`--boot order=net0;scsi0`	Amorçage réseau prioritaire sur le disque

> **Le modèle de carte réseau doit être défini à la création**
>
> Le micrologiciel OVMF fige ses entrées d'amorçage lors de la première énumération du matériel et les conserve dans son fichier NVRAM. Changer le modèle de carte après coup ne régénère pas l'entrée PXE : la machine perd la possibilité d'amorcer en réseau. Une VM destinée au déploiement doit être créée directement avec une carte E1000 et l'option de clés pré-enregistrées désactivée.

2.1 Ordre d'amorçage

Sur un poste vierge, le disque est vide : il ne peut pas amorcer. Il est donc décoché dans l'ordre de démarrage, ce qui évite un délai d'attente inutile à chaque cycle :

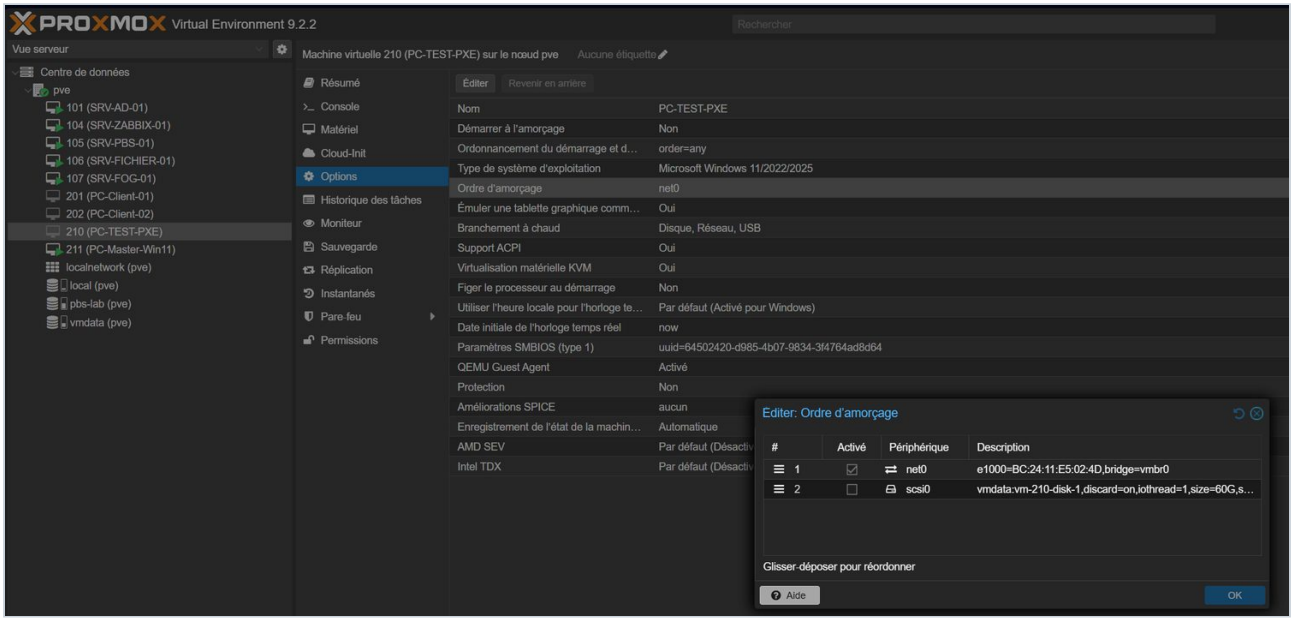

Figure 2 — Ordre d'amorçage du poste cible — net0 activé en position 1, disque décoché

Après le déploiement, le disque doit être réactivé et replacé en première position pour que le poste démarre normalement sur Windows.

3. Enregistrement du poste

FOG n'agit que sur des machines qu'il connaît. Un poste vierge doit donc s'enregistrer avant tout déploiement. L'identifiant utilisé est son **adresse MAC**.

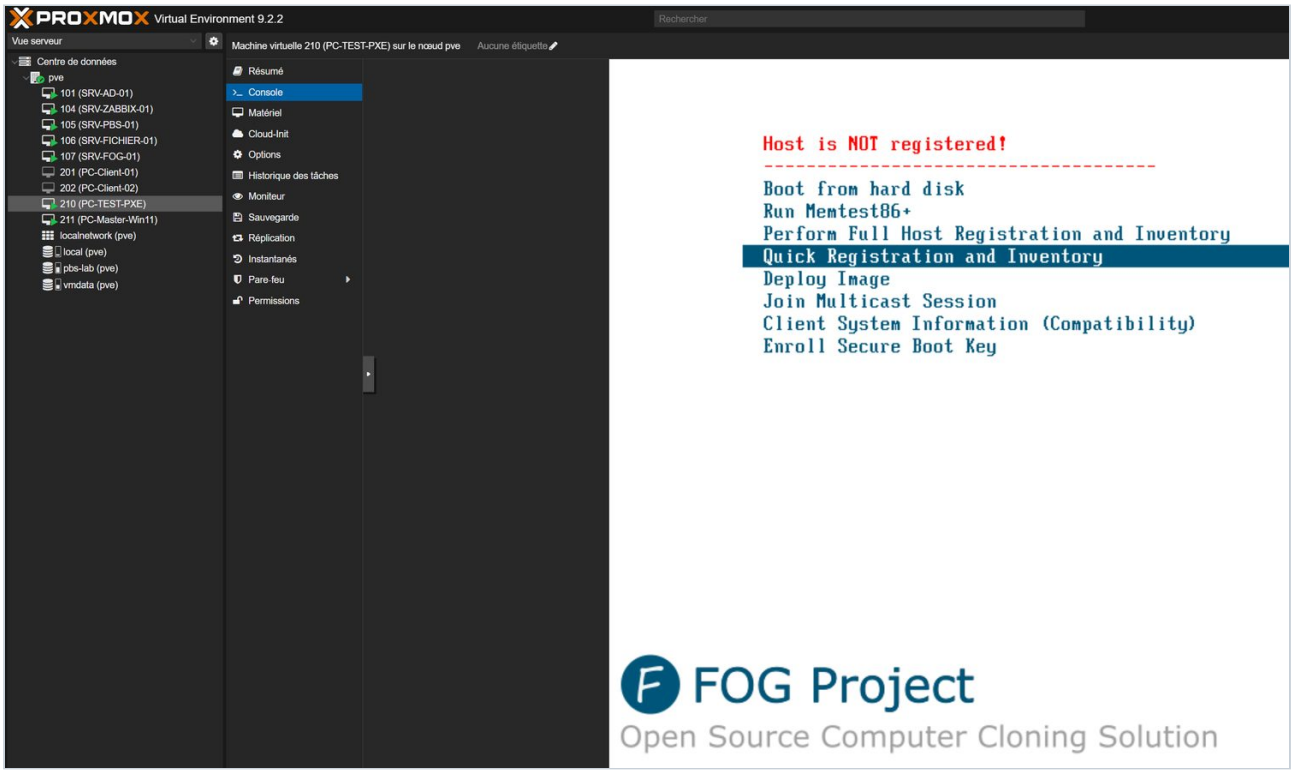

Figure 3 — Menu iPXE sur un poste non enregistré — sélection de Quick Registration and Inventory

3.1 Choix du mode d'enregistrement

Mode	Comportement	Quand l'utiliser
Full Host Registration and Inventory	Pose une série de questions à l'écran : nom de la machine, image associée, groupes, snapins, clé produit, jonction au domaine, utilisateur principal. Réalise également un inventaire matériel.	Poste unique, à configurer immédiatement, quand on est physiquement devant la machine
Quick Registration and Inventory	Enregistre la machine sans aucune question. L'hôte est créé sous un nom dérivé de son adresse MAC.	Enrôlement de plusieurs postes à la chaîne, la configuration étant faite ensuite depuis l'interface web

> **Pourquoi Quick Registration est privilégié**
>
> L'enregistrement rapide sépare deux opérations qui n'ont pas les mêmes contraintes. L'enrôlement se fait devant les machines, il doit être le plus court possible : quelques secondes par poste, sans saisie. La configuration se fait ensuite au bureau, dans l'interface web, où copier une valeur d'un hôte à l'autre est immédiat et où l'on peut travailler par groupe. Sur une flotte, l'enregistrement complet imposerait de saisir sept réponses devant chaque machine.

3.2 Résultat côté serveur

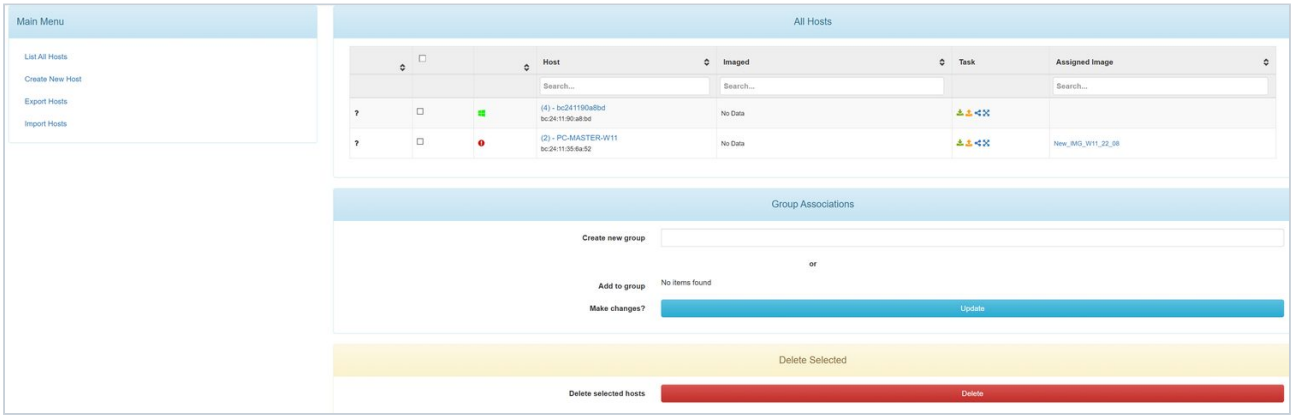

Figure 4 — L'hôte apparaît dans All Hosts, nommé d'après son adresse MAC

Le nom généré reprend l'adresse MAC sans séparateurs. Le poste n'a encore ni image associée, ni configuration : il est simplement connu du serveur. La colonne **Imaged** indique *No Data*, aucun déploiement n'ayant encore eu lieu.

> **L'enregistrement n'a lieu qu'une fois dans la vie du poste**
>
> FOG identifie une machine par son **adresse MAC**, et non par son nom ou par le contenu de son disque. Une fois l'hôte créé, le serveur le reconnaît à chaque amorçage réseau : le menu affiche alors directement les actions disponibles au lieu du message *Host is NOT registered!*. Un poste peut donc être redéployé autant de fois que nécessaire sans jamais être réenregistré, et il conserve entre deux déploiements son nom, son unité d'organisation, ses snapins et son historique.

> **Deux conséquences pratiques**
>
> **Le remplacement d'une carte réseau rend le poste inconnu du serveur.** L'adresse MAC étant la clé d'identification, une carte changée à la suite d'une panne fait perdre la correspondance : le poste redevient non enregistré. Il faut alors mettre à jour le champ *Primary MAC* sur la fiche existante plutôt que de créer un nouvel hôte, sous peine de perdre toute la configuration associée.
>
> **Un réenregistrement crée un doublon.** Relancer une inscription sur une machine déjà connue n'actualise pas sa fiche : il en résulte deux hôtes pour une seule machine, ce qui provoque des conflits de tâches. Avant tout enregistrement, il convient donc de vérifier que l'adresse MAC n'est pas déjà présente dans la liste des hôtes.

4. Configuration de l'hôte

La configuration se fait depuis la fiche de l'hôte, dans l'interface web. Trois onglets sont renseignés.

4.1 Identité et image

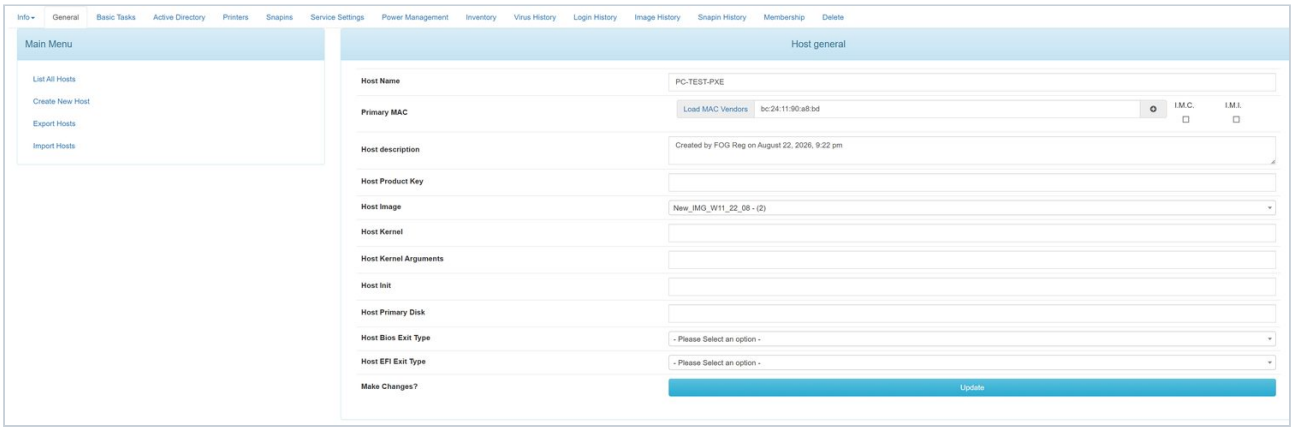

Figure 5 — Onglet General — renommage de l'hôte et association de l'image

Champ	Contenu
Host Name	Nom définitif du poste. C'est ce nom que le client FOG appliquera à Windows après le déploiement.
Primary MAC	Adresse MAC relevée à l'enregistrement. C'est la clé d'identification du poste : elle ne doit pas être modifiée.
Host Image	Image qui sera déployée sur ce poste.
Host EFI Exit Type	Méthode par laquelle iPXE rend la main au disque à la fin du déploiement.

> **Le nom de l'hôte devient le nom de la machine Windows**
>
> Le champ **Host Name** n'est pas une simple étiquette dans la base FOG. Après le déploiement, le module HostnameChanger du client compare ce nom à celui de la machine Windows et, s'ils diffèrent, renomme le poste puis le redémarre. Une convention de nommage doit donc être définie avant l'enrôlement, car la corriger après coup impose un redémarrage supplémentaire sur chaque poste concerné.

4.2 Jonction au domaine

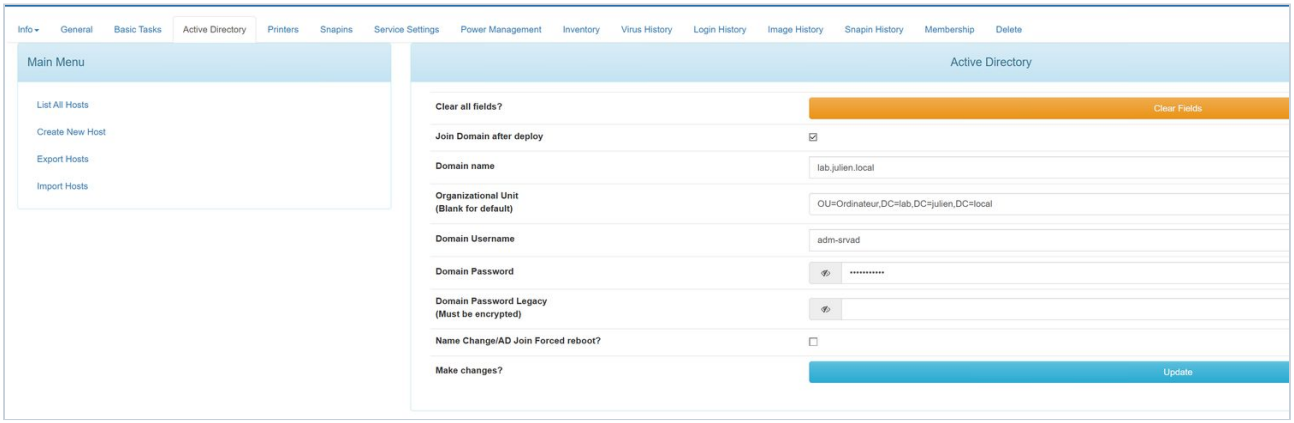

Figure 6 — Onglet Active Directory — paramètres de jonction au domaine

Champ	Valeur	Rôle
Join Domain after deploy	Coché	Active la jonction automatique après le déploiement
Domain name	lab.julien.local	Nom DNS complet du domaine
Organizational Unit	OU=Ordinateur,DC=lab,DC=julien,DC=local	Unité d'organisation de destination, en notation *distinguished name*. Sans cette valeur, l'objet est créé dans le conteneur Computers par défaut.
Domain Username	Compte disposant du droit de jonction	Identifiant utilisé pour créer l'objet ordinateur
Domain Password	Masqué	Mot de passe du compte, stocké chiffré dans la base FOG

> **Pourquoi préciser l'unité d'organisation**
>
> Les stratégies de groupe s'appliquent à des unités d'organisation. Un poste créé dans le conteneur `Computers` par défaut ne recevrait aucune des GPO liées à l'OU `Ordinateur` — notamment celles qui gèrent l'accès distant et le déploiement de l'agent de supervision. Renseigner ce champ garantit que le poste est correctement rattaché dès sa création, sans déplacement manuel ultérieur.

> **Point de sécurité : le compte utilisé pour la jonction**
>
> Le compte renseigné ici est stocké dans la base FOG et transmis au client sur le poste déployé. Utiliser un compte d'administration du domaine revient à exposer des privilèges élevés sur chaque machine déployée. La pratique recommandée est un **compte de service dédié**, sans autre privilège que la création d'objets ordinateur dans l'OU visée, droit accordé par délégation depuis la console Utilisateurs et ordinateurs Active Directory. Le lab utilise un compte d'administration par simplicité ; cet écart est identifié et la correction est connue.

4.3 Snapins

L'onglet **Snapins** associe au poste les paquets logiciels et le script de post-déploiement à exécuter après la jonction au domaine :

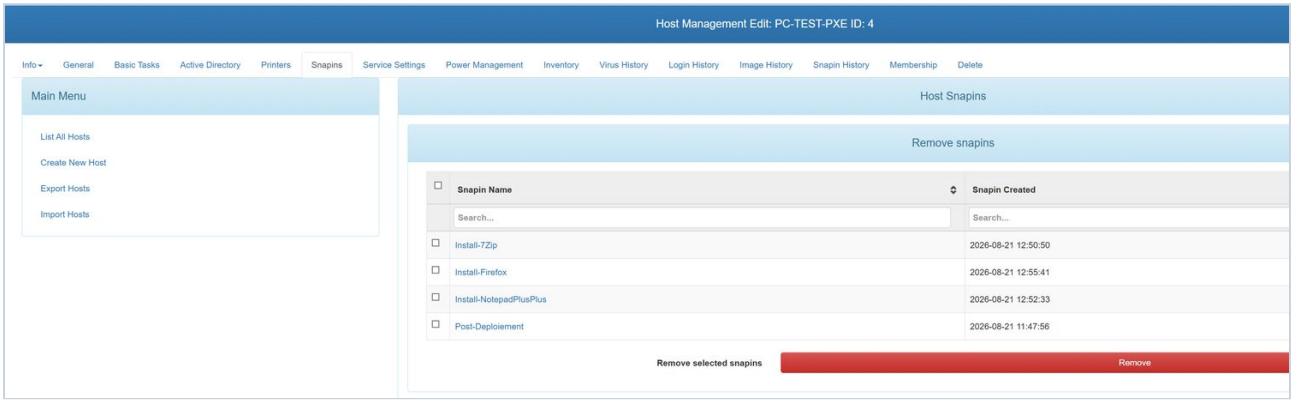

Figure 7 — Onglet Snapins — les quatre snapins associés à l'hôte

Le contenu et la construction de ces snapins font l'objet du document E.

5. Déploiement unitaire

5.1 Création de la tâche

Depuis la fiche de l'hôte, onglet **Basic Tasks** :

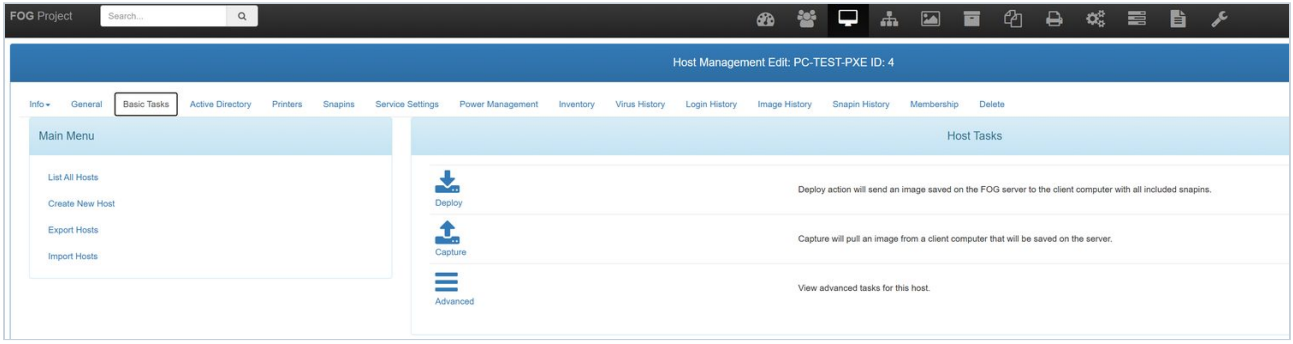

Figure 8 — Onglet Basic Tasks — l'action Deploy envoie l'image vers le poste

L'action **Deploy** envoie l'image du serveur vers le poste, avec les snapins associés. C'est l'opération inverse de **Capture**, décrite dans le document C.

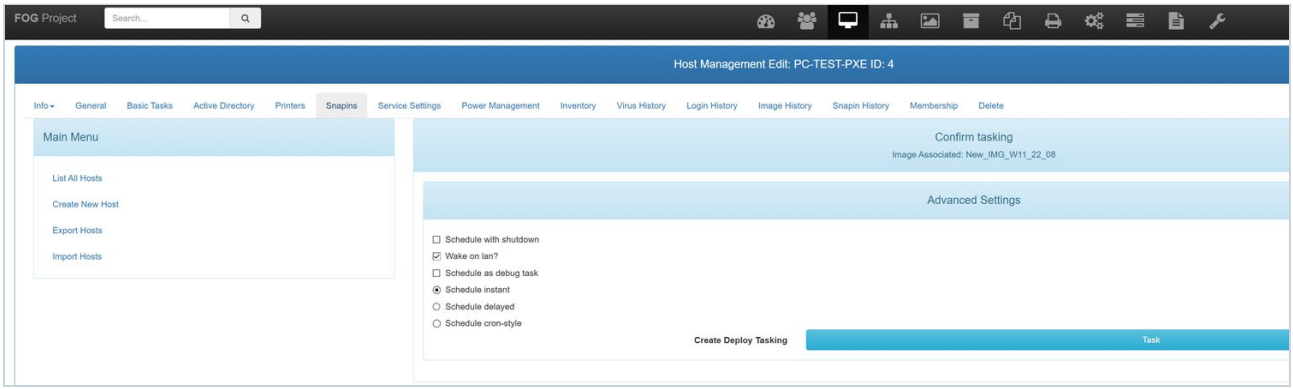

Figure 9 — Écran de confirmation — planification immédiate, création par le bouton Task

Option	Effet
Schedule instant	La tâche est créée immédiatement et attend que le poste amorce en réseau. Option retenue ici.
Schedule delayed	La tâche ne devient active qu'à une date et une heure données.
Schedule cron-style	Déclenchement récurrent, par exemple pour réinitialiser une salle de formation chaque semaine.
Wake on lan	Envoie une trame de réveil au poste, ce qui permet de déclencher un déploiement sur une machine éteinte.
Schedule with shutdown	Éteint le poste à la fin du déploiement au lieu de le redémarrer.

> **L'intérêt de la planification différée**
>
> Un déploiement sature le lien réseau et immobilise les postes. Combinée au réveil par le réseau, la planification différée permet de lancer un renouvellement de parc en dehors des heures de travail : les postes s'allument seuls, se déploient, et sont opérationnels le lendemain matin sans aucune intervention. C'est le principal gain d'exploitation de l'outil.

5.2 Contrôle de la tâche

La tâche est visible dans l'onglet **Task Management**, où elle reste en attente jusqu'à l'amorçage réseau du poste :

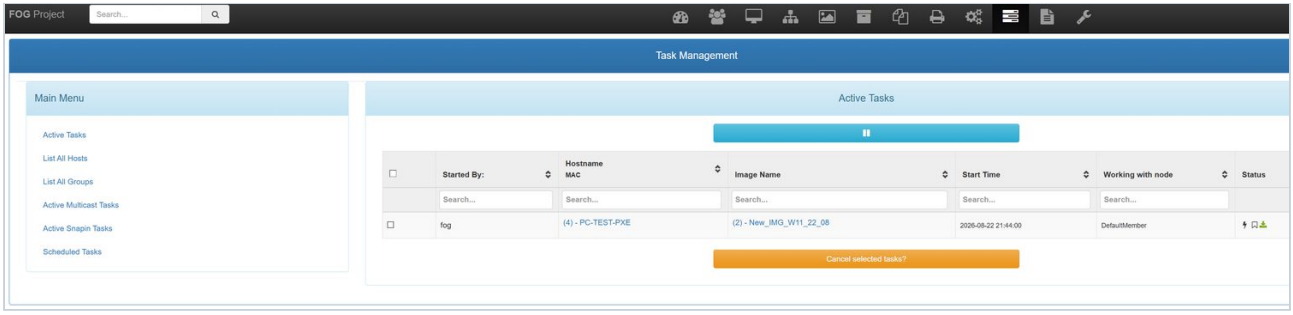

Figure 10 — Task Management — la tâche de déploiement est en attente

Les colonnes indiquent le poste concerné, l'image à déployer, l'heure de création et le nœud de stockage qui servira le flux.

5.3 Chaîne d'amorçage réseau

Le poste est démarré. La console montre l'enchaînement complet du préamorçage :

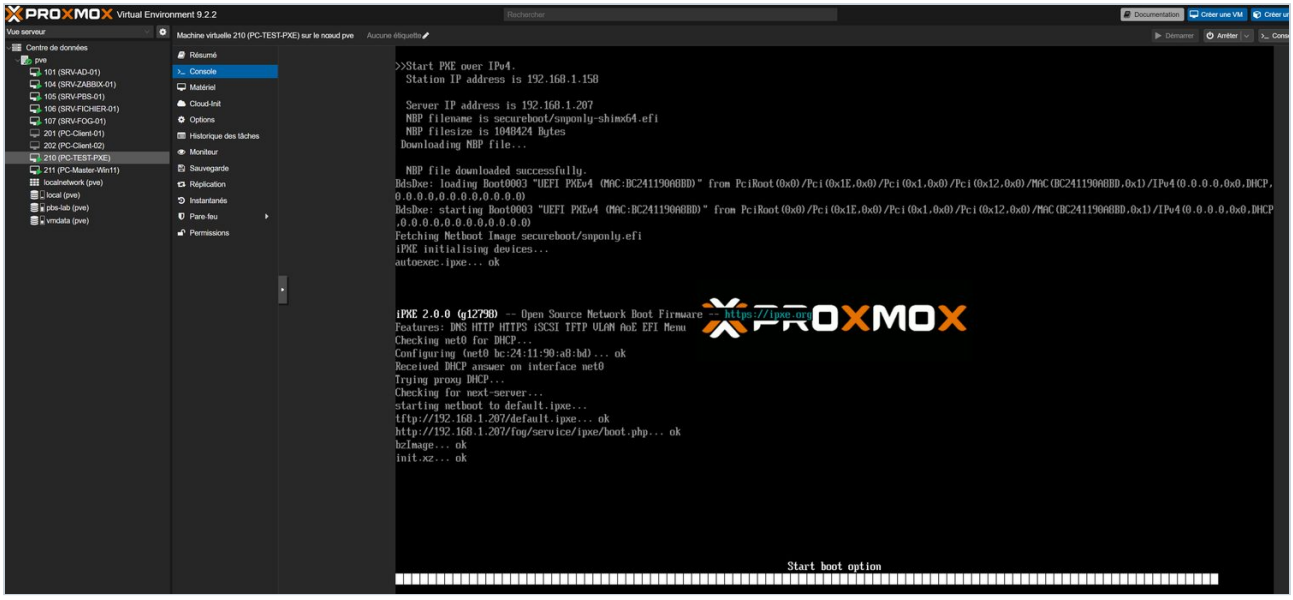

Figure 11 — Chaîne d'amorçage PXE, du micrologiciel UEFI jusqu'au noyau FOG

Ligne	Signification
	Le poste obtient une adresse du serveur DHCP du réseau

`Station IP address is 192.168.1.158`	
`Server IP address is 192.168.1.207`	Le serveur FOG est désigné comme source du fichier d'amorçage
`NBP filename is secureboot/snponly-shimx64.efi`	Fichier d'amorçage réseau retenu, compatible Secure Boot
`Trying proxy DHCP...`	Le poste interroge le service ProxyDHCP, qui complète la réponse du serveur DHCP existant
`tftp://192.168.1.207/default.ipxe`	Second passage : iPXE récupère son script de configuration
`http://192.168.1.207/fog/service/ipxe/boot.php`	Le script interroge le serveur, qui répond en fonction des tâches en attente pour cette adresse MAC
`bzImage / init.xz`	Chargement du noyau Linux et du système de fichiers initial de FOG

Pourquoi un ProxyDHCP

L'amorçage PXE suppose que le serveur DHCP transmette au poste l'adresse du serveur de démarrage et le nom du fichier à charger. Sur ce réseau, le DHCP est assuré par la box de l'opérateur, qui ne permet pas de configurer ces options. Le ProxyDHCP résout le problème : il écoute les requêtes d'amorçage et y répond **en complément** du serveur DHCP existant, qui continue d'attribuer les adresses. Aucune modification du réseau existant n'est nécessaire — un point qui compte autant en entreprise, où l'on souhaite rarement toucher au DHCP de production, que dans ce lab.

Pourquoi ce fichier d'amorçage précis

`snponly-shimx64.efi` est un chargeur signé par Microsoft, accepté par les micrologiciels dont le Secure Boot est actif. Il est retenu pour **tous les clients UEFI 64 bits**, que le Secure Boot soit activé ou non : le serveur DHCP n'a aucun moyen de détecter l'état du Secure Boot d'un poste au moment où il lui répond. Le chargeur passe la validation, mais le noyau FOS chargé ensuite est refusé si Secure Boot est actif : les déploiements sont menés Secure Boot inactif.

5.4 Déroulement du déploiement

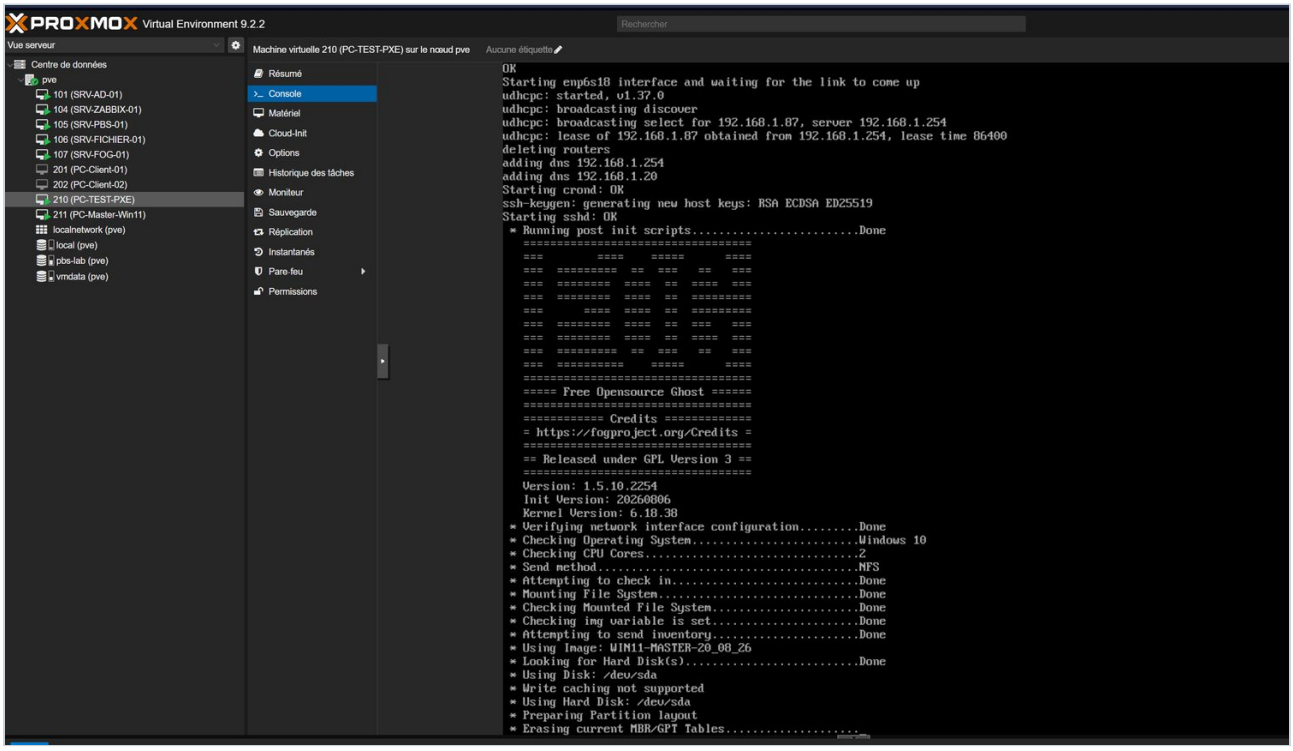

Figure 12 — Séquence de déploiement : vérifications, préparation du disque, restauration

La console détaille les opérations successives :

Étape	Opération
Checking Operating System	Identification du système contenu dans l'image
Send method: NFS	Mode de transport retenu : flux dédié à ce poste
Mounting File System	Montage du partage `/images` du serveur
Erasing current MBR/GPT Tables	Effacement de la table de partitions existante
Restoring Partition Tables (GPT)	Écriture de la table de partitions issue de l'image
Attempting to expand/fill partitions	Redimensionnement de la partition Windows à la taille du disque cible

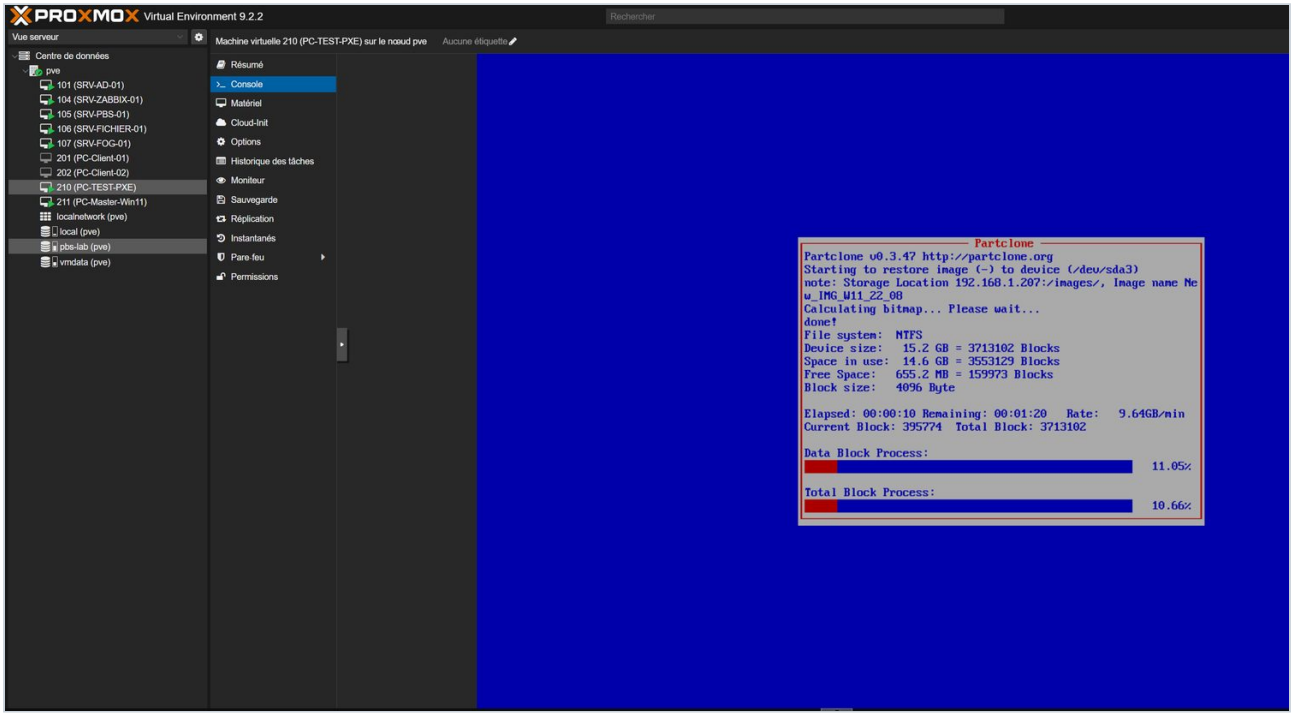

Figure 13 — Restauration de la partition Windows par Partclone

L'étape de redimensionnement mérite attention : c'est elle qui permet de déployer une image capturée sur un disque de 60 Go vers un poste équipé d'un disque de capacité différente. C'est la conséquence du type d'image **Single Disk - Resizable** retenu à la capture.

6. Validation du déploiement unitaire

Le poste redémarre, exécute l'OOBE automatisée par le fichier de réponses, puis le client FOG prend le relais. Trois contrôles indépendants confirment le résultat.

6.1 Présence dans l'annuaire

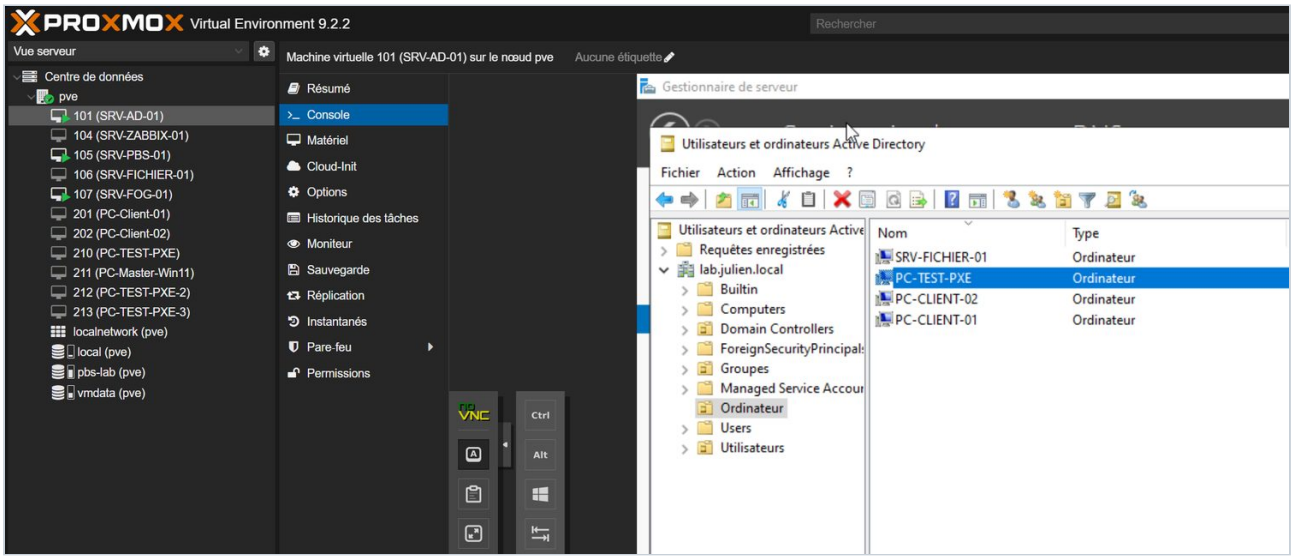

Figure 14 — Utilisateurs et ordinateurs Active Directory — le poste apparaît dans l'OU Ordinateur

L'objet ordinateur a été créé au bon emplacement, celui renseigné dans l'onglet Active Directory de l'hôte. Il recevra donc les stratégies de groupe liées à cette unité d'organisation.

6.2 Authentification sur le domaine

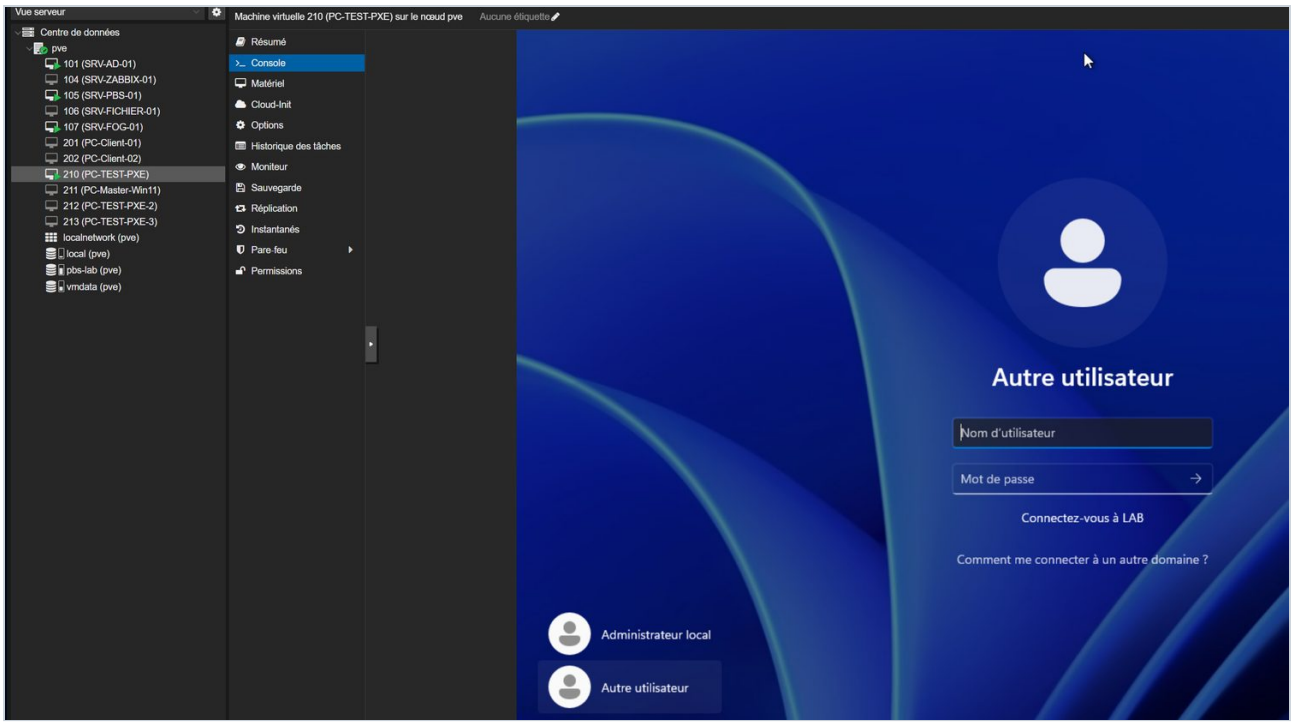

Figure 15 — Écran de connexion du poste — la mention « Connectez-vous à LAB » confirme l'appartenance au domaine

La mention du domaine sur l'écran de connexion prouve que le poste n'est pas seulement inscrit dans l'annuaire. Le canal sécurisé se vérifie, lui, par Test-ComputerSecureChannel.

6.3 Contrôle système

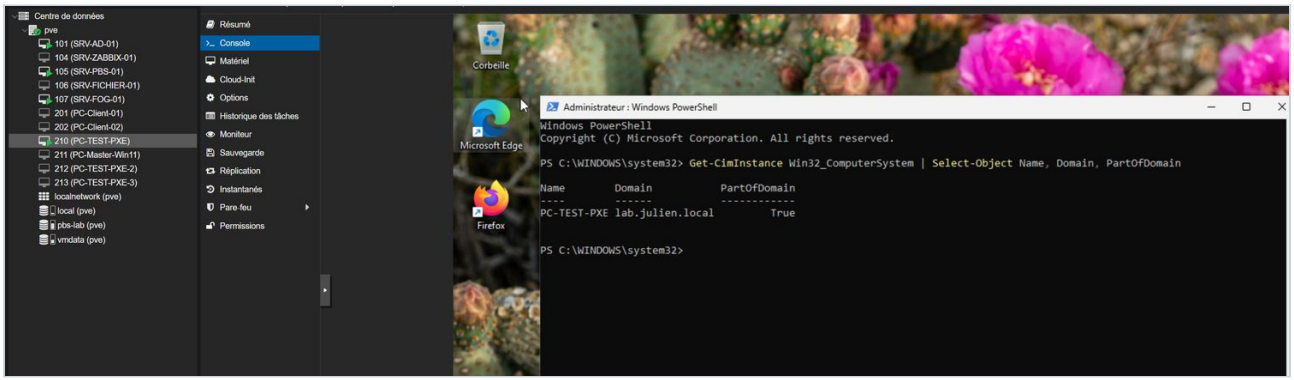

Figure 16 — Vérification en PowerShell — nom de la machine, domaine et appartenance

```
Get-CimInstance Win32_ComputerSystem | Select-Object Name, Domain, PartOfDomain
```

Trois informations sont validées d'un coup : le nom appliqué par le client FOG, le domaine rejoint, et la valeur `PartOfDomain: True`.

> **Pourquoi trois contrôles plutôt qu'un**
>
> Ils ne prouvent pas la même chose. La présence dans l'annuaire montre que l'objet a été créé, mais un objet peut exister sans que le poste soit réellement opérationnel. L'écran de connexion montre que le poste voit le domaine. La commande système confirme le nom appliqué et l'appartenance effective. Aucun des trois ne prouve que le canal sécurisé fonctionne à l'instant présent : Test-ComputerSecureChannel le confirme.

7. Déploiement de flotte

Le déploiement unitaire convient au remplacement d'un poste. Pour un renouvellement de parc, il présente deux limites : la configuration doit être répétée sur chaque hôte, et le débit du serveur se divise entre les postes. Le déploiement de flotte répond aux deux.

7.1 Enrôlement des postes

Chaque poste est enregistré par **Quick Registration**, sans saisie :

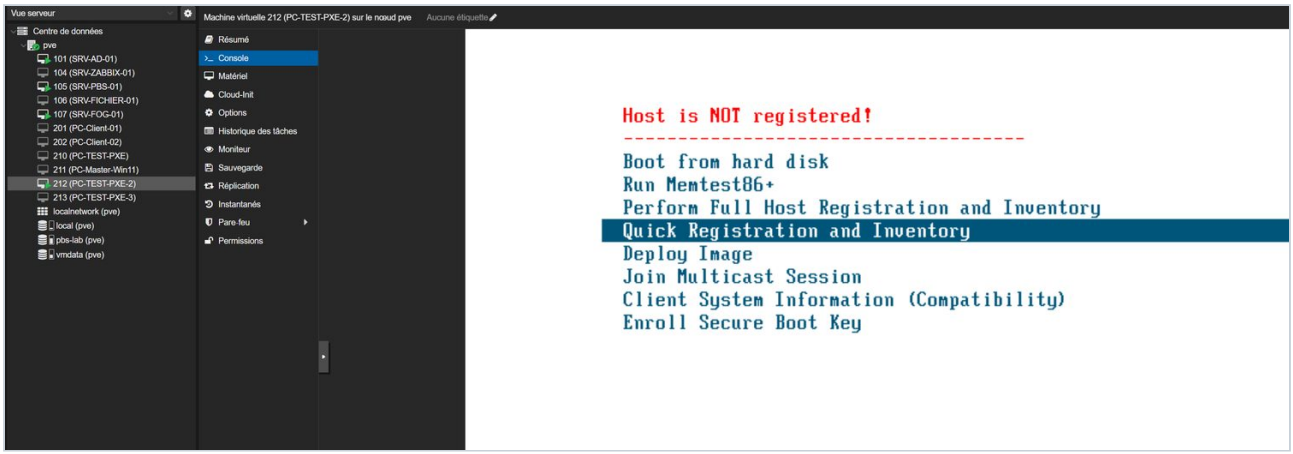

Figure 17 — Enregistrement rapide d'un poste supplémentaire

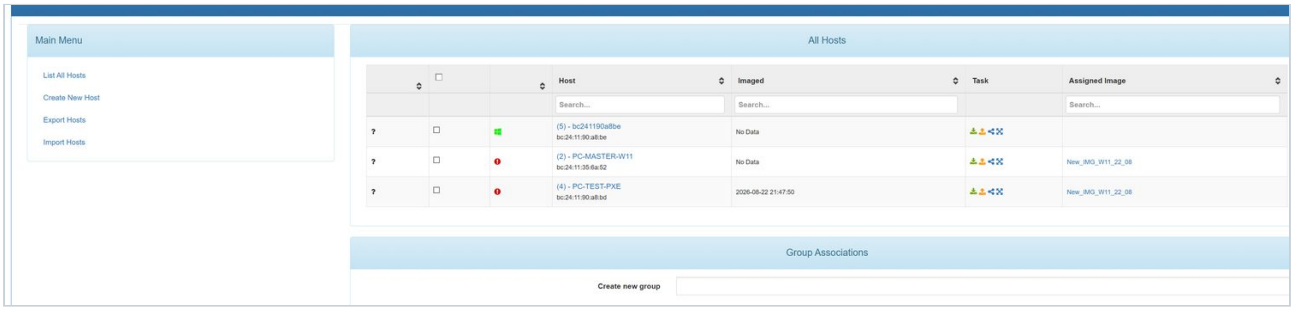

Figure 18 — Le nouvel hôte apparaît dans All Hosts, nommé d'après son adresse MAC

Les hôtes sont ensuite renommés depuis l'interface. La liste complète sert de point de contrôle avant de constituer le groupe :

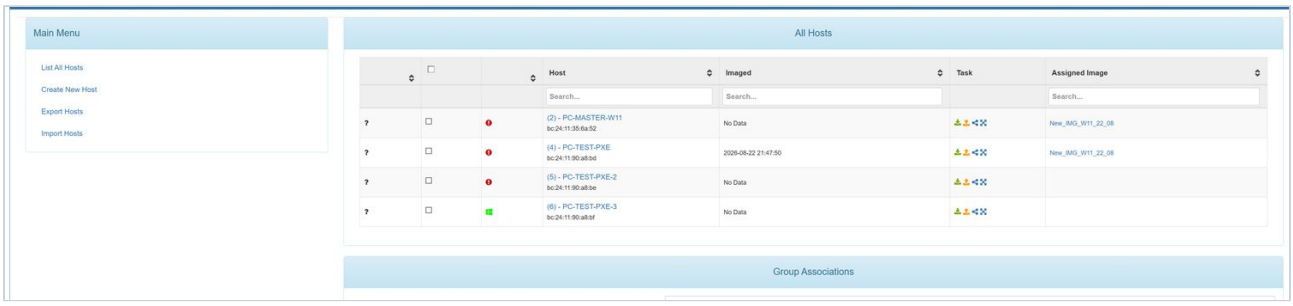

Figure 19 — Liste des hôtes enregistrés, chacun avec son adresse MAC

7.2 Création du groupe

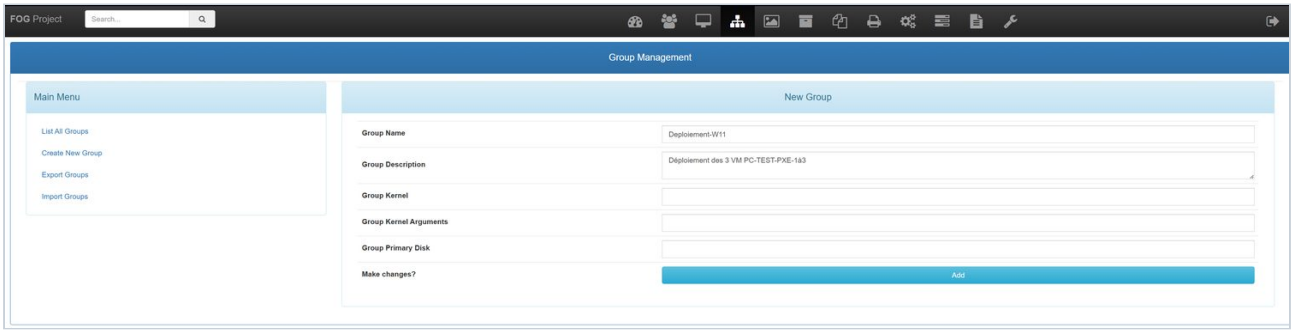

Figure 20 — Création du groupe de déploiement

Le groupe est un conteneur logique. Il ne contient aucun poste à sa création : les hôtes lui sont rattachés dans un second temps.

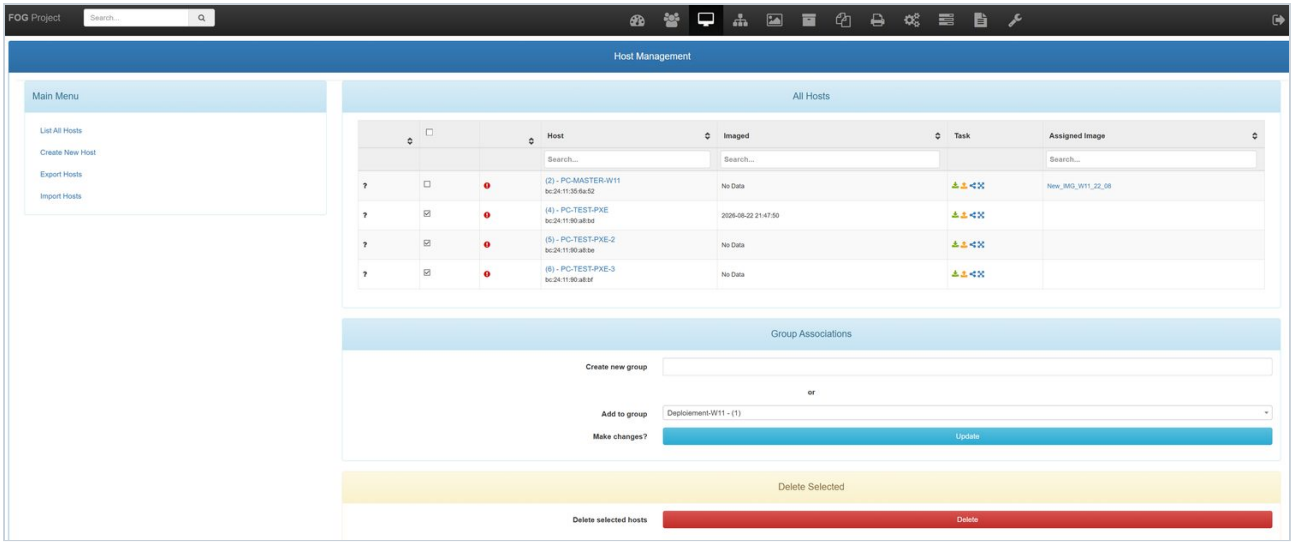

Figure 21 — Rattachement des hôtes au groupe depuis la liste des hôtes

Les postes concernés sont cochés, le groupe est sélectionné dans la liste **Add to group**, puis la modification est validée.

7.3 Configuration au niveau du groupe

La configuration se fait une seule fois, sur le groupe, et se propage à tous ses membres. Trois onglets sont renseignés, les mêmes que pour un hôte isolé.

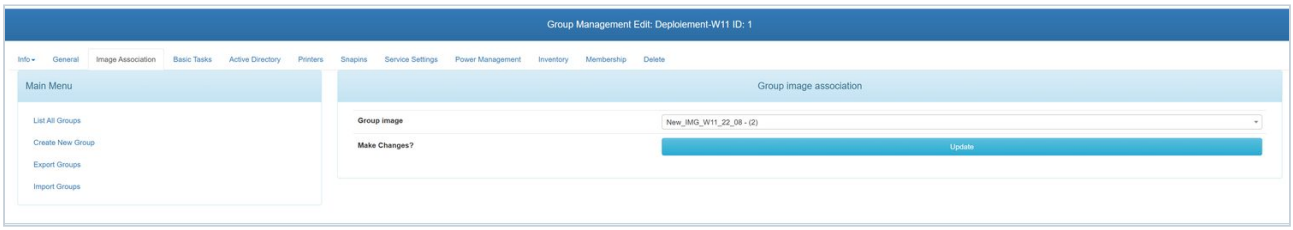

Figure 22 — Onglet Image Association — image commune à tous les membres

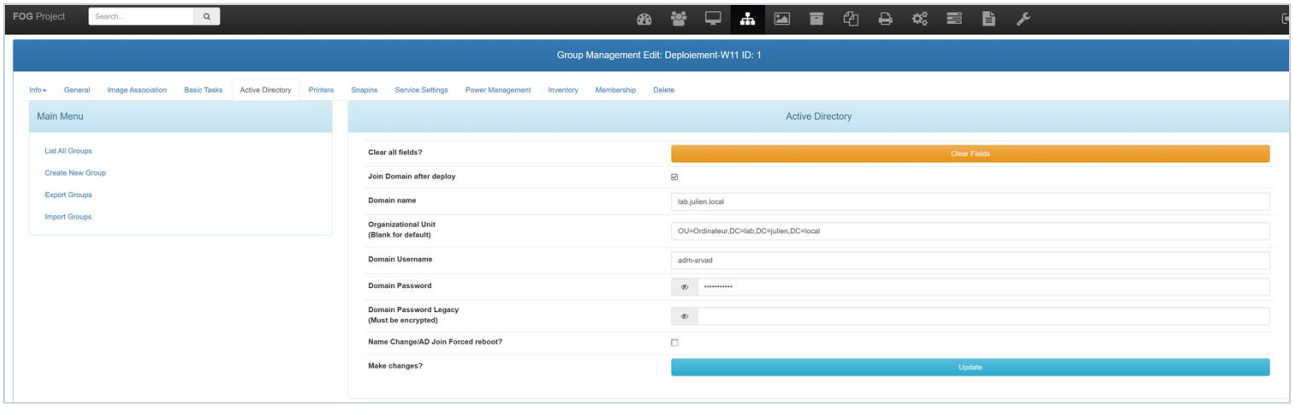

Figure 23 — Onglet Active Directory du groupe — paramètres de jonction communs

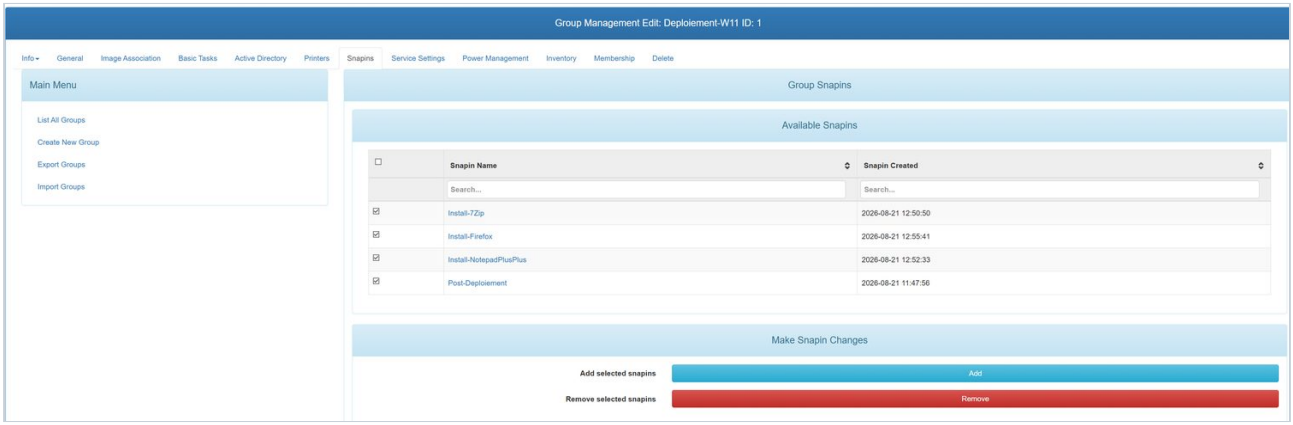

Figure 24 — Onglet Snapins du groupe — les quatre snapins sont sélectionnés puis ajoutés

7.4 Vérification de la propagation

La configuration appliquée au groupe est écrite sur chaque hôte membre. Elle se vérifie à deux niveaux.

Sur la liste des hôtes, la colonne **Assigned Image** est désormais renseignée pour les trois postes :

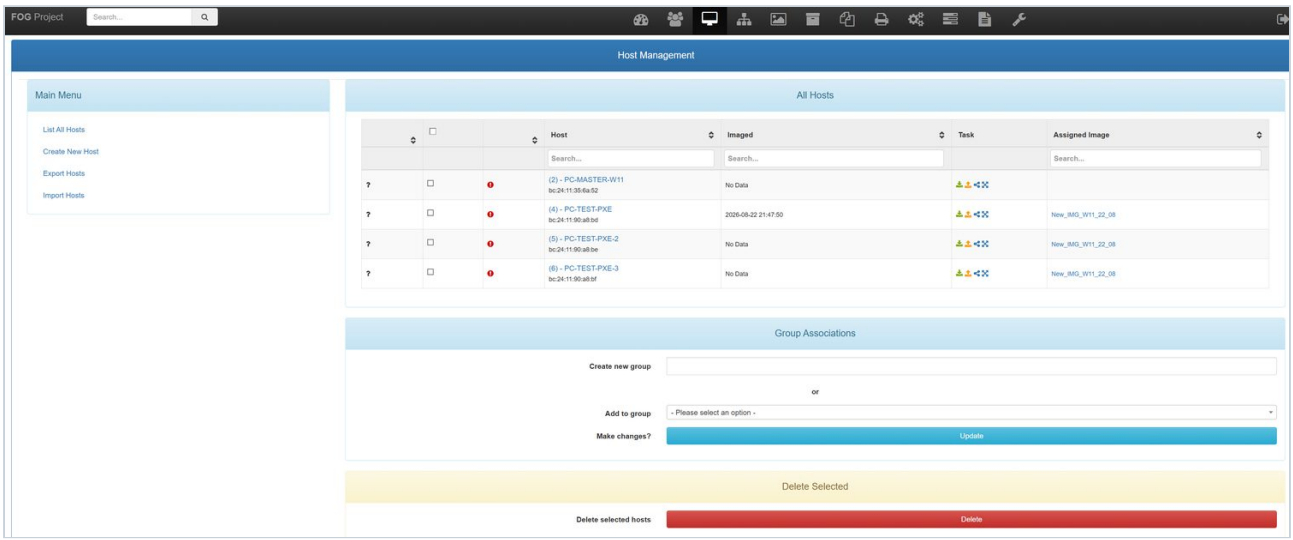

Figure 25 — L'image a été propagée du groupe vers les trois hôtes membres

Sur la fiche d'un hôte pris individuellement, les paramètres de jonction au domaine et les snapins sont présents alors qu'ils n'ont jamais été saisis sur cet hôte :

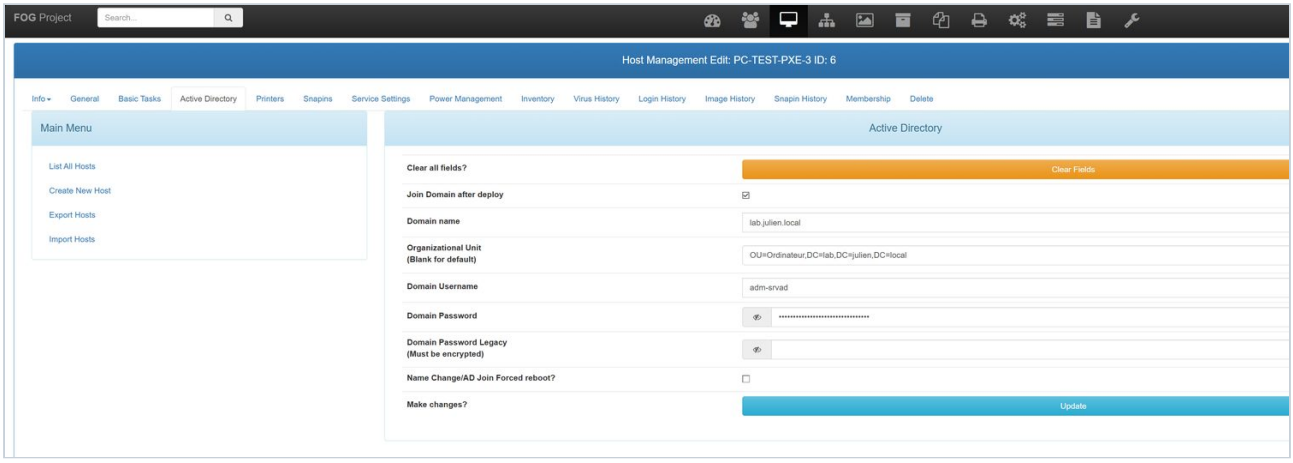

Figure 26 — Onglet Active Directory d'un hôte membre — configuration héritée du groupe

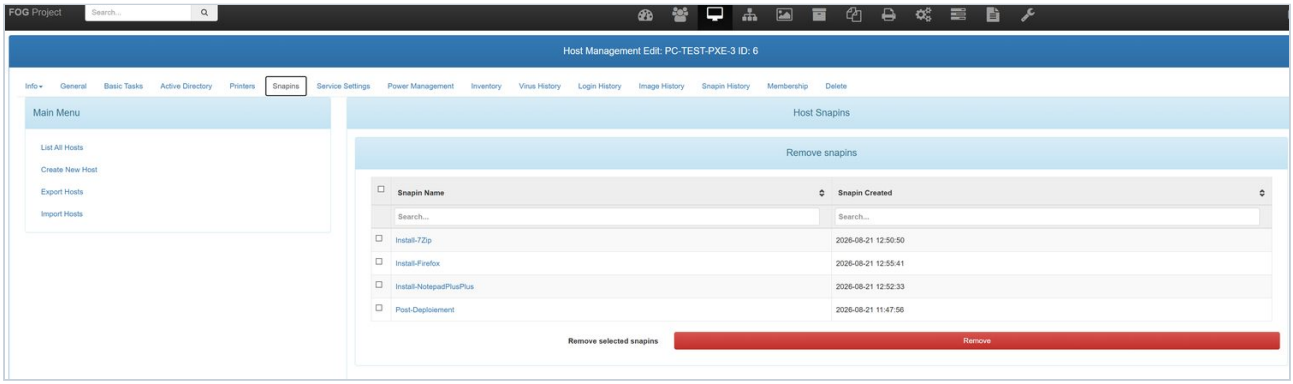

Figure 27 — Onglet Snapins du même hôte — les quatre snapins sont hérités

Une propagation, pas un lien permanent

FOG écrit la configuration du groupe dans la fiche de chaque membre au moment de la validation. Il ne maintient pas de lien dynamique : modifier le groupe plus tard n'actualise pas rétroactivement les hôtes déjà configurés, et modifier un hôte ne le désolidarise pas du groupe. En pratique, toute modification doit être réappliquée depuis le groupe pour être répercutée sur l'ensemble des membres.

8. Lancement du multicast

8.1 Deux actions distinctes

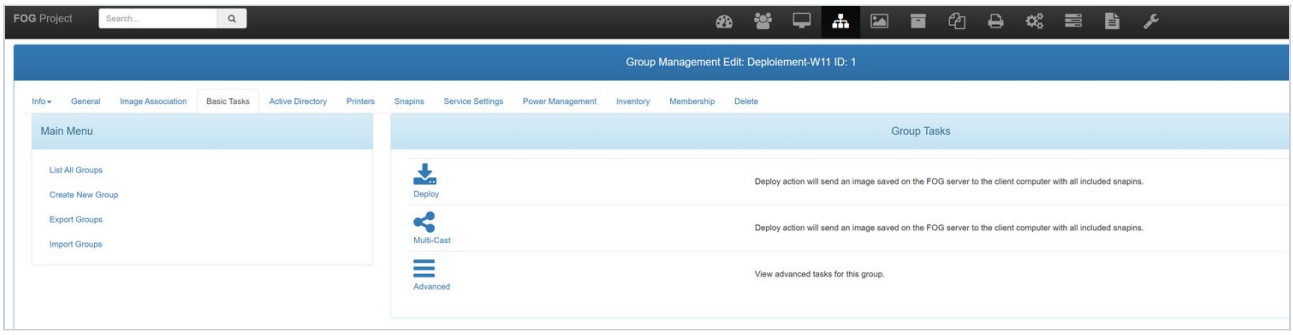

Figure 28 — Onglet Basic Tasks du groupe — Deploy et Multi-Cast

L'onglet Basic Tasks d'un groupe propose deux actions dont la description affichée est identique, mais dont le fonctionnement diffère fondamentalement :

Action	Fonctionnement
Deploy	Crée une tâche unicast **par membre** du groupe. Chaque poste reçoit son propre flux. Le débit disponible se divise entre eux.
Multi-Cast	Crée une **session unique** à laquelle les postes se raccordent. Le serveur émet un seul flux, reçu simultanément par tous.

8.2 Création de la session

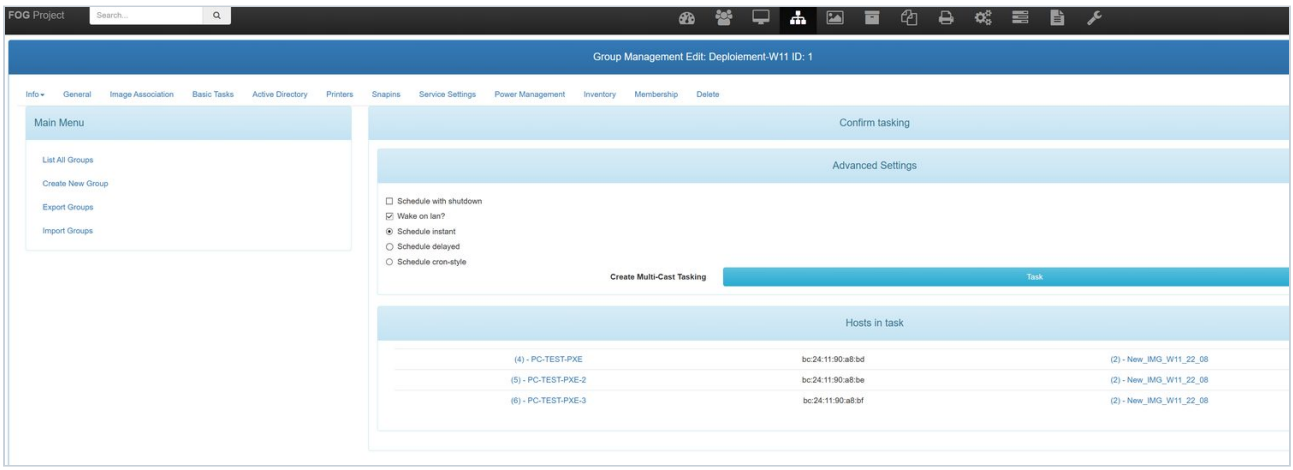

Figure 29 — Confirmation de la tâche multicast — les trois postes participants sont listés

Le bloc **Hosts in task** énumère les postes qui participeront à la session, avec leur adresse MAC et l'image associée. C'est le dernier point de contrôle avant lancement : un poste absent de cette liste ne recevra rien.

8.3 Déroulement

Les trois postes sont démarrés. Le mode de transport diffère de celui du déploiement unitaire :

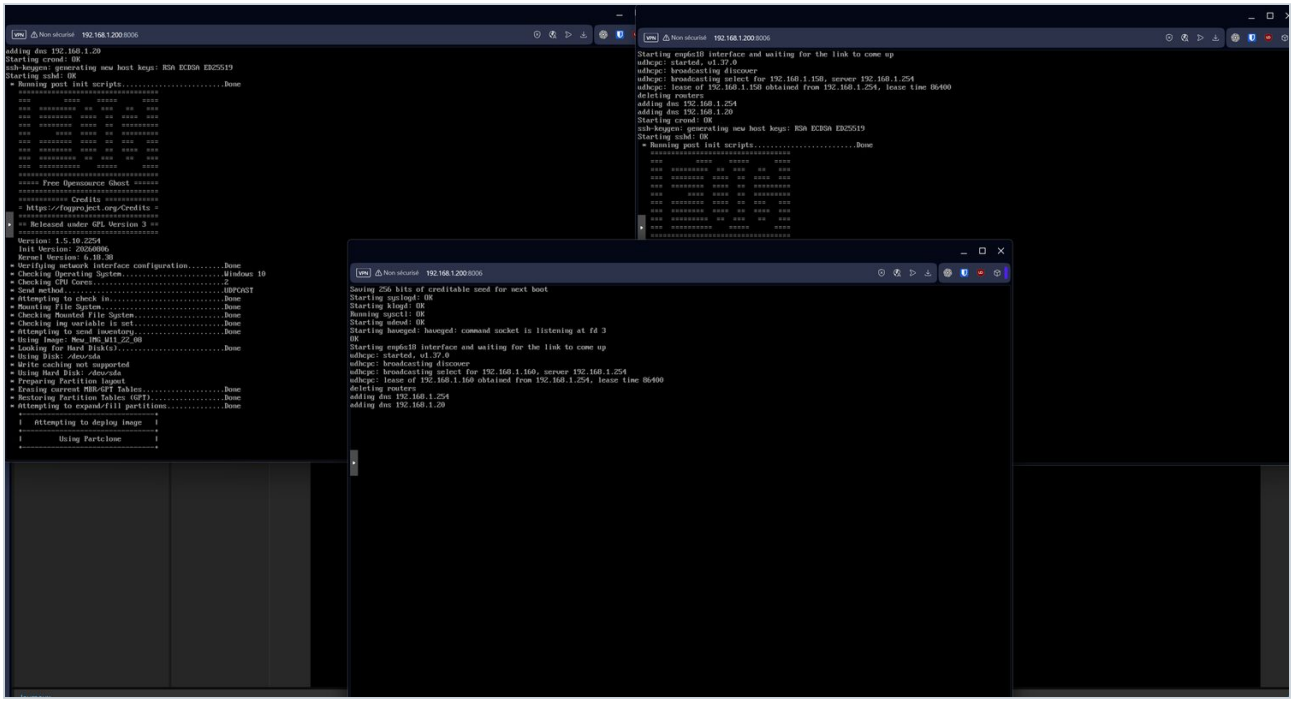

Figure 30 — Consoles des trois postes — le mode d'envoi est UDPCAST

La ligne `Send method: UDPCAST` remplace le `NFS` observé en unicast. Le serveur n'envoie plus un fichier à chaque poste : il diffuse un flux que tous écoutent en parallèle.

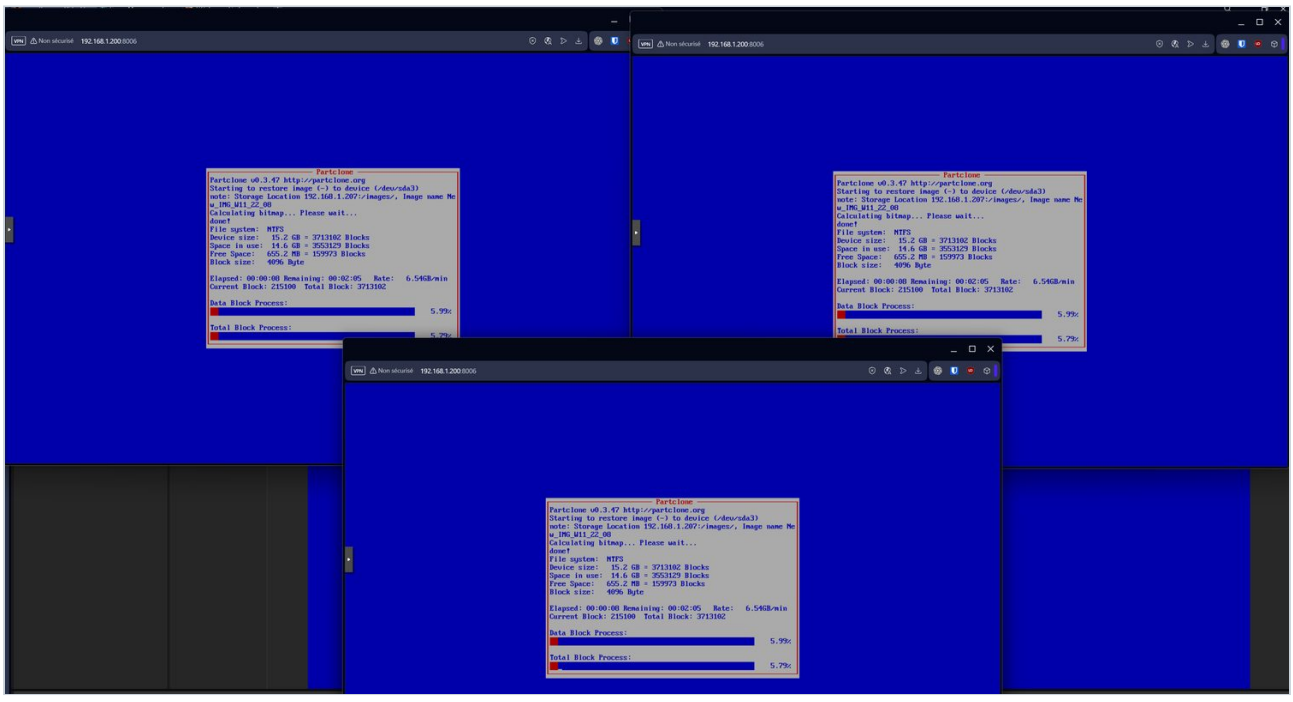

Figure 31 — Les trois postes progressent avec des valeurs strictement identiques

> **La preuve que le flux est bien mutualisé**
>
> Les trois fenêtres affichent exactement les mêmes valeurs au même instant : même nombre de blocs traités, même pourcentage, même débit. Cette synchronisation parfaite ne peut pas résulter de trois transferts indépendants, qui dériveraient inévitablement les uns par rapport aux autres. Elle démontre que les trois postes reçoivent le **même flux**, émis une seule fois par le serveur.

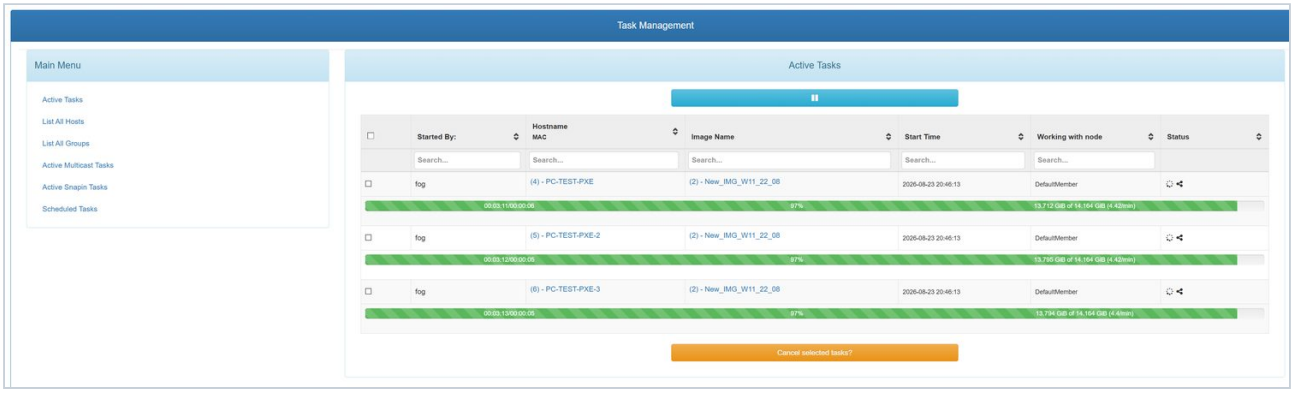

Figure 32 — Task Management — les trois tâches progressent ensemble, à débit identique

Le suivi centralisé confirme la mesure : chaque poste reçoit environ 4,4 Go par minute, soit 13 Go par minute cumulés côté clients. Le serveur, lui, n'émet qu'un seul flux de 4,4 Go par minute. Le débit par poste ne s'effondre pas quand le nombre de machines augmente.

8.4 Fin de session

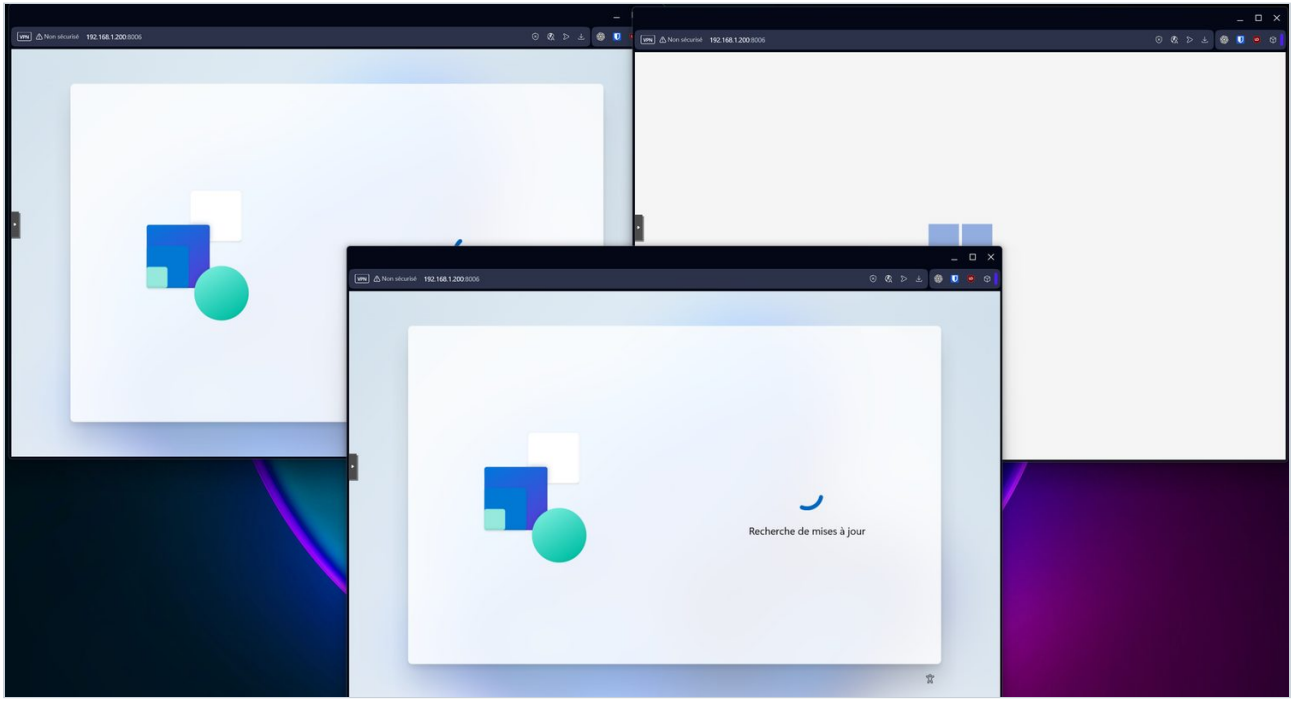

Figure 33 — Les trois postes exécutent leur phase de configuration initiale simultanément

> **Seule la copie de l'image est mutualisée**
>
> Le gain du multicast porte exclusivement sur le transfert de l'image. Tout ce qui suit — phase OOBE, renommage, jonction au domaine, installation des logiciels par snapin — reste propre à chaque poste et s'exécute en parallèle sans mutualisation possible, puisque ces opérations diffèrent d'une machine à l'autre. Sur un déploiement de trois postes, le gain est mesurable mais modeste ; il devient déterminant à partir d'une dizaine de machines, où l'unicast saturerait le lien du serveur.

9. Liste de contrôle

Points à vérifier lors d'un déploiement, quel que soit le mode retenu.

Point	Contrôle
Amorçage	net0 en première position avant déploiement, disque remis en tête après
Enregistrement	L'hôte apparaît dans All Hosts avec la bonne adresse MAC
Configuration	Image, OU de destination et snapins renseignés
Tâche	Visible et en attente dans Task Management
Chaîne PXE	ProxyDHCP répond, default.ipxe puis boot.php sont récupérés
Transport	NFS en unitaire, UDPCAST en flotte
Jonction	Bonne OU, PartOfDomain à True, canal sécurisé testé
Nommage	Le nom Windows correspond au Host Name de FOG