

Préparation du master Windows 11 et capture de l'image sur le serveur FOG

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
Machine master	VM 211 — PC-MASTER-W11
Domaine	lab.julien.local
Contexte	Lab personnel de formation

1. Objet du document

Ce document décrit la construction du poste de référence (le « master ») et la capture de son disque sous forme d'image déployable par FOG. Il s'arrête à l'image disponible sur le serveur ; le déploiement de cette image fait l'objet du document D.

1.1 Ce que couvre ce document

- Configuration de la machine virtuelle destinée à devenir le master
- Préparation du système : paramètres régionaux, client FOG
- Fichier de réponses `unattend.xml`
- Généralisation par sysprep
- Enregistrement du master dans FOG et capture de l'image
- Contrôles de validation

1.2 Principe général

Un déploiement de masse repose sur une image unique, installée une fois puis dupliquée sur l'ensemble du parc. Trois conditions doivent être réunies pour que cette image soit utilisable :

1. **Elle doit être générique.** Un système Windows contient des identifiants uniques, en premier lieu le SID machine. Cloner un disque tel quel produirait des postes partageant ces données. Ce clonage n'est pas pris en charge par Microsoft : c'est le rôle de sysprep.
2. **Elle doit démarrer sans saisie.** Après clonage, Windows relance sa phase de configuration initiale (OOBE), qui pose une dizaine de questions. Le fichier `unattend.xml` y répond par avance.
3. **Elle doit embarquer le client FOG.** C'est lui qui, sur le poste déployé, effectue le renommage, la jonction au domaine et l'exécution des snapins.

1.3 Enchaînement des opérations

Étape	Opération	Résultat attendu
1	Création et installation de la VM master	Windows 11 fonctionnel
2	Paramètres régionaux propagés	fr-FR sur tous les profils
3	Installation du client FOG	Service FOGService actif
4	Dépôt de l' <code>unattend.xml</code>	Fichier présent dans Panther
5	Instantané avant généralisation	Point de retour disponible
6	Sysprep	VM arrêtée, système généralisé
7	Enregistrement dans FOG	Hôte PC-MASTER-W11 créé
8	Capture	Image présente dans /images

2. Configuration de la machine master

La configuration matérielle de la VM 211 est reproduite ci-dessous. Elle a été relevée sur l'hyperviseur par la commande `qm config 211`.

```
root@pve:~# qm config 211
agent: 1
balloon: 2048
bios: ovmf
boot: order=net0;ide2;scsi0;ide0
cores: 2
cpu: host
efidisk0: vmdata:vm-211-disk-0,efitype=4m,size=4M
ide0: none,media=cdrom
ide2: none,media=cdrom
machine: pc-q35-11.0
memory: 4096
meta: creation-qemu=11.0.0,ctime=1787227776
name: PC-Master-Win11
net0: e1000=BC:24:11:35:6A:52,bridge=vbr0
numa: 0
ostype: win11
parent: pret-sysprep
scsi0: vmdata:vm-211-disk-1,discard=on,iothread=1,size=60G,ssd=1
scsihw: virtio-scsi-single
smbios1: uuid=c1f4118f-4b08-4172-bc3f-625376bdf310
sockets: 1
tpmstate0: vmdata:vm-211-disk-2,size=4M,version=v2.0
vmgenid: eb6642ca-7248-44f4-bcc0-c8c4e12af619
root@pve:~#
```

Figure 1 — Configuration complète de la VM 211 (PC-MASTER-W11)

2.1 Paramètres structurants

Paramètre	Valeur	Justification
bios	ovmf	Micrologiciel UEFI, obligatoire pour Windows 11 et pour l'amorçage PXE en mode EFI
net0	e1000	Carte Intel E1000. Modèle reconnu nativement par l'environnement de préamorçage iPXE, contrairement à VirtIO
tpmstate0	version v2.0	Module TPM 2.0, prérequis d'installation de Windows 11
scsi0		

	60 Go, discard=on	Disque système unique. Le paramètre discard permet la restitution de l'espace libéré au pool LVM-thin
memory	4096 Mo	Suffisant pour un poste de référence
ostype	win11	Optimise les horloges et périphériques virtuels pour Windows 11

Point critique : le choix de la carte réseau

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 réseau après la création de la VM ne régénère pas l'entrée de démarrage PXE : la machine ne présente alors plus l'amorçage réseau, même si la carte est fonctionnelle sous Windows. **Toute VM destinée au PXE doit donc être créée avec une carte E1000 dès l'origine**, et avec l'option « clés pré-enregistrées » décochée.

Pourquoi un disque unique

L'image FOG est capturée en mode « Single Disk - Resizable ». Ce mode ne traite qu'un disque physique, mais gère l'ensemble de ses partitions (EFI, réservée, Windows, récupération) et redimensionne la partition Windows à la taille du disque cible lors du déploiement. Un master à disque unique reste donc déployable sur des postes aux capacités différentes.

3. Préparation du système

3.1 Paramètres régionaux

Windows distingue les paramètres du compte en cours d'utilisation de ceux du profil par défaut, qui sert de modèle à tout nouveau compte. Un master configuré uniquement au niveau du compte courant produirait des postes en anglais dès qu'un utilisateur du domaine ouvre une session pour la première fois.

L'opération se fait depuis `intl.cpl`, onglet **Administration**, bouton **Copier les paramètres** :

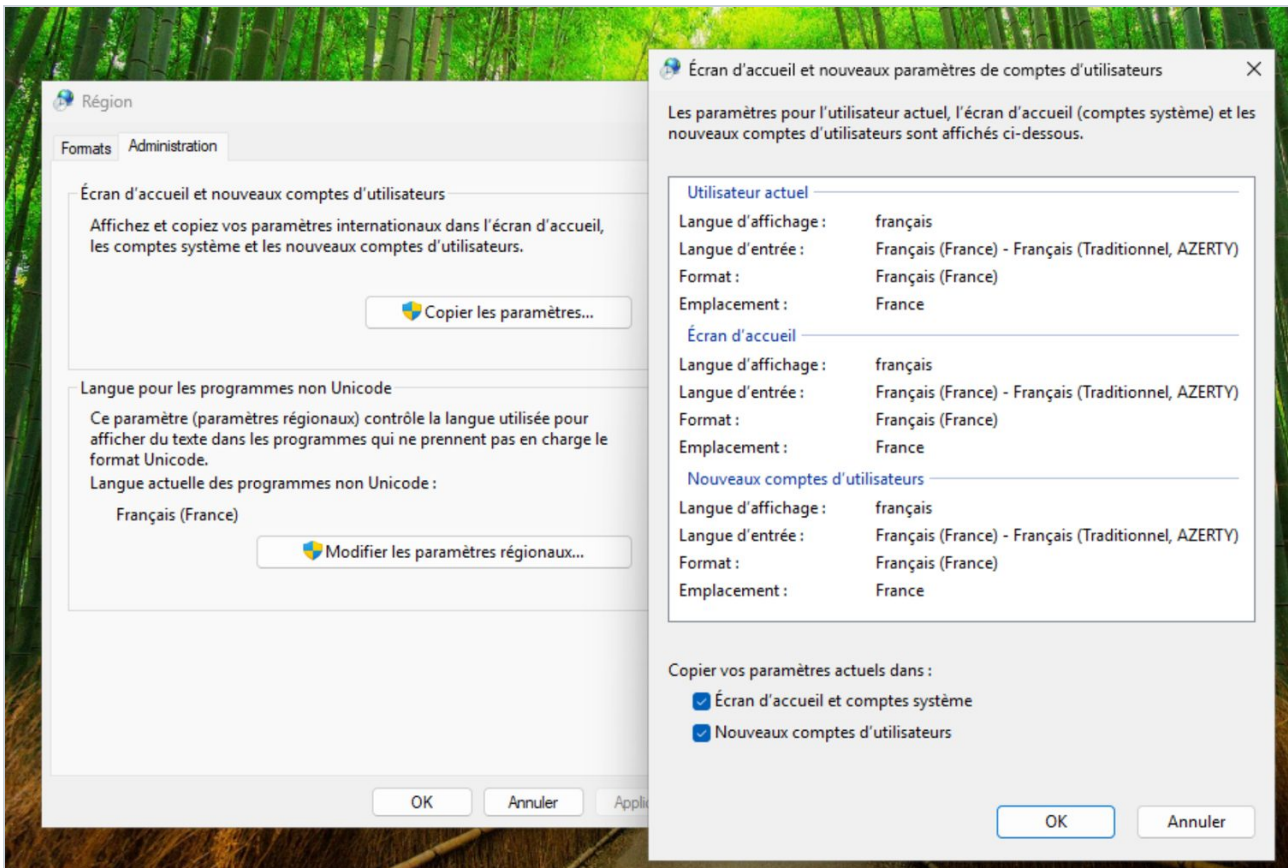


Figure 2 — Propagation des paramètres fr-FR vers l'écran d'accueil et les nouveaux comptes

Les trois blocs affichés — utilisateur actuel, écran d'accueil, nouveaux comptes — doivent tous indiquer **Français (France)** et **Français (Traditionnel, AZERTY)**. Les deux cases du bas doivent être cochées avant validation.

Ce réglage ne fait pas double emploi avec l'unattend.xml

Les deux mécanismes agissent à des moments différents. `intl.cpl` agit **sur le master** : le réglage est figé dans l'image capturée. Le bloc International-Core de l'unattend agit **sur le poste déployé**, pendant l'OOBE. Le premier couvre les profils créés après déploiement, le second couvre la phase d'installation. Il s'agit d'une double sécurité volontaire.

3.2 Installation du client FOG

Le client FOG est le composant qui exécute, sur le poste déployé, les actions post-clonage : renommage, jonction au domaine, exécution des snapins. Il doit impérativement être présent dans l'image.

L'installateur est récupéré depuis l'interface web du serveur puis exécuté sur le master :

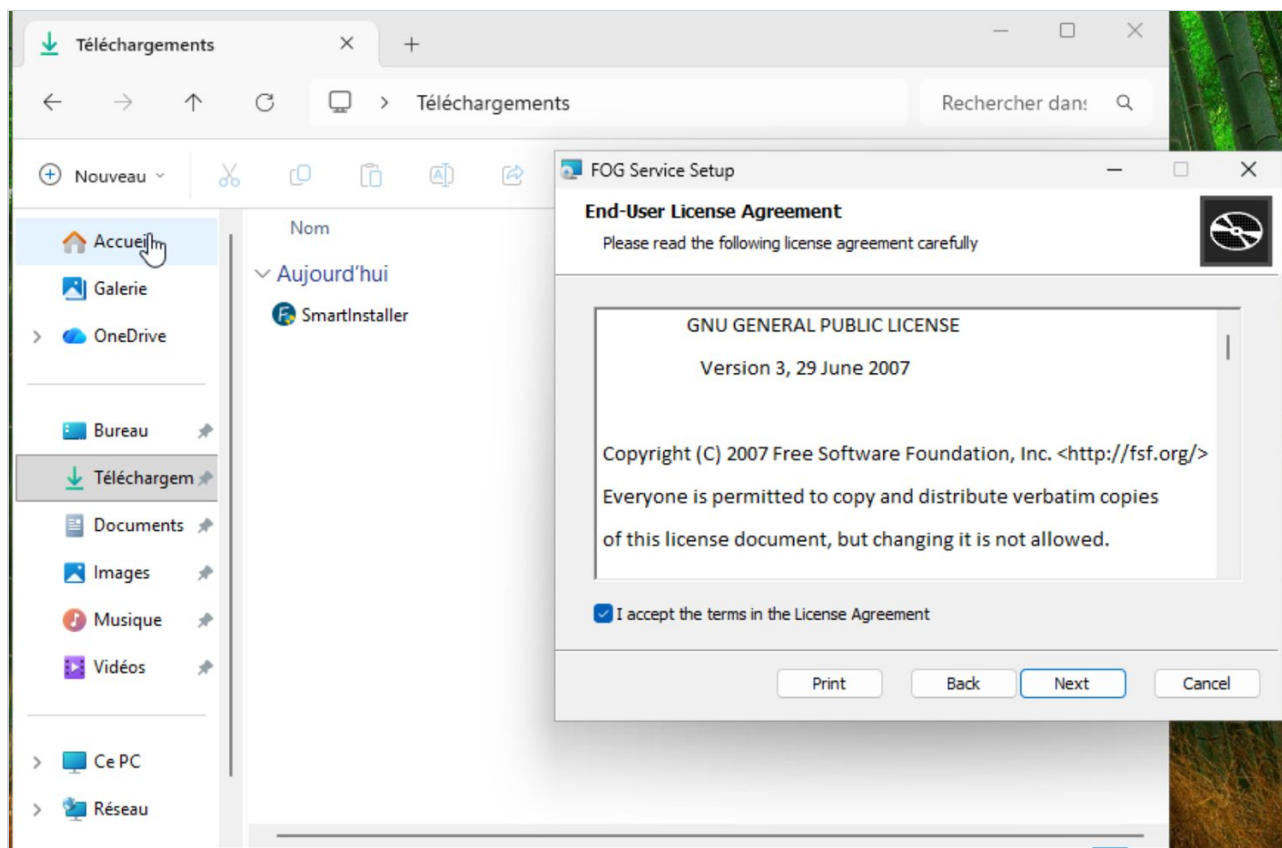


Figure 3 — Lancement de l'installateur FOG Service — licence GNU GPL v3

L'écran de configuration est le seul qui demande une intervention :

Figure 4 — Configuration du client : adresse du serveur et protocole

Champ	Valeur
Server Address	192.168.1.207
Web Root	/fog
Enable FOG Tray	Coché
Put Log File in filesystem root	Coché
Use HTTPS to connect to FOG server	Décoché

Pourquoi HTTPS est décoché

Le serveur FOG est configuré en HTTP. Ce choix découle d'une contrainte technique : sur cette infrastructure, l'amorçage PXE utilise le fichier `snponly-shimx64.efi`, compatible Secure Boot. Or le chargeur shim signé par Microsoft ne valide pas les chaînes HTTPS auto-signées : **Secure Boot et HTTPS sont mutuellement exclusifs** dans cette configuration. Le lab étant sur un réseau privé et fermé, la compatibilité Secure Boot a été privilégiée. Avec FOG 1.5.10, seule la levée par un certificat d'une autorité reconnue du parc s'applique. À réévaluer en version 1.6.

Le chemin d'installation et l'écran de confirmation restent aux valeurs par défaut. À l'issue de l'installation, le service doit être vérifié dans `services.msc` :

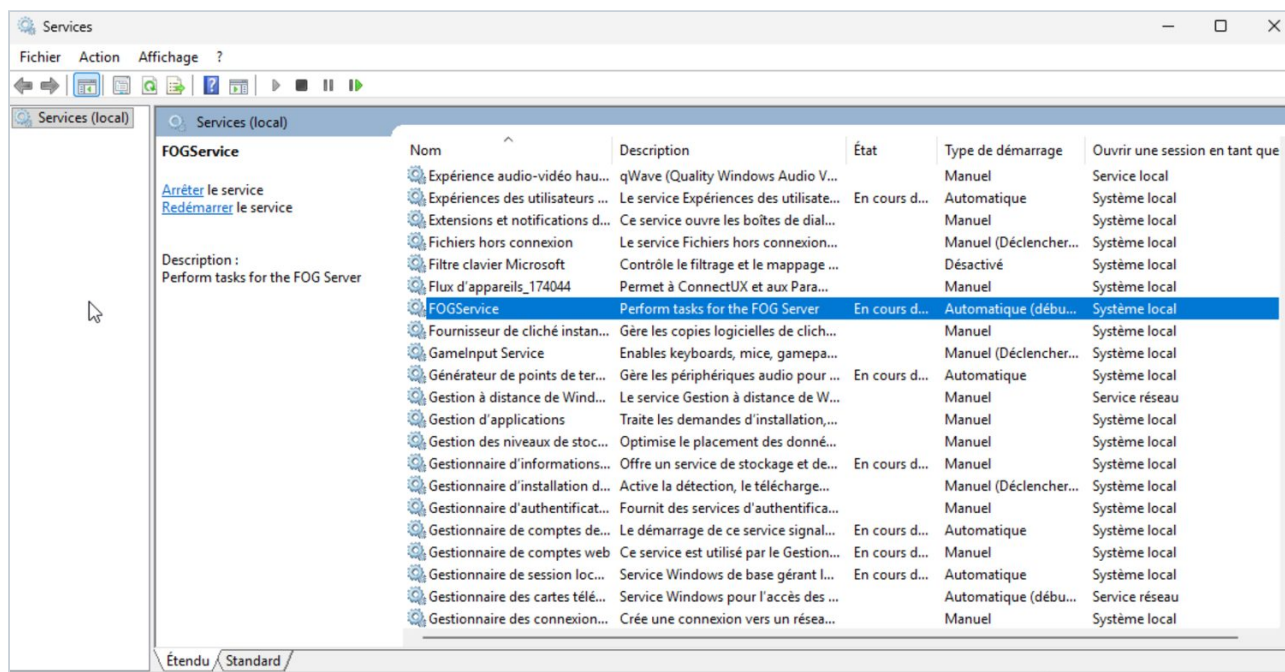


Figure 5 — Le service FOGService est en cours d'exécution, démarrage automatique différé, sous le compte Système local

Trois éléments sont à contrôler sur cet écran : l'état **En cours d'exécution**, le type de démarrage **Automatique (début différé)** et le compte d'exécution **Système local**. Ce dernier point signifie que le client FOG fonctionne **sans qu'aucune session utilisateur soit ouverte**.

4. Fichier de réponses unattend.xml

Le fichier de réponses automatise la phase OOBE du poste déployé. Il est déposé dans `C:\Windows\Panther\unattend.xml`, l'un des emplacements que sysprep interroge automatiquement : aucun paramètre `/unattend:` n'est nécessaire sur la ligne de commande.

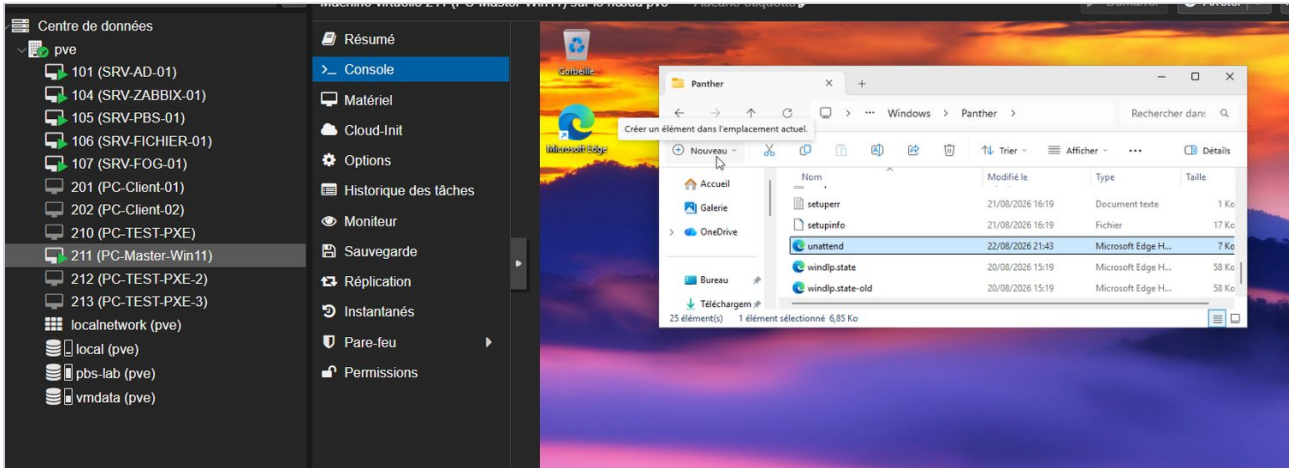


Figure 6 — Le fichier unattend.xml en place dans C:\Windows\Panther

4.1 Contenu fonctionnel

Passe	Composant	Rôle
specialize	Deployment	Contournement de l'obligation de connexion réseau (BypassNRO)
oobeSystem	International-Core	Langue, formats et clavier AZERTY
oobeSystem	Shell-Setup / OOBE	Masquage des écrans de la configuration initiale
oobeSystem	Shell-Setup / UserAccounts	Création du compte administrateur local de secours

Contournement de l'obligation de connexion réseau

```
<RunSynchronousCommand wcm:action="add">
  <Order>1</Order>
  <Description>Contournement de l'obligation de connexion reseau</Description>
  <Path>reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\OOBE"
    /v BypassNRO /t REG_DWORD /d 1 /f</Path>
</RunSynchronousCommand>
```

Les versions récentes de Windows 11 exigent une connexion Internet et un compte Microsoft pendant l'OOBE. Cette clé de registre rétablit la possibilité de créer un compte local, indispensable en environnement d'entreprise.

Écrans masqués

```
<OOBE>
  <HideEULAPage>true</HideEULAPage>
  <HideOEMRegistrationScreen>true</HideOEMRegistrationScreen>
  <HideOnlineAccountScreens>true</HideOnlineAccountScreens>
```

```
<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
<NetworkLocation>Work</NetworkLocation>
<ProtectYourPC>3</ProtectYourPC>
</OOBE>
```

Chaque balise supprime un écran qui exigerait un clic. C'est ce bloc qui rend le déploiement de masse possible : sans lui, chaque poste demanderait l'intervention d'un technicien pendant plusieurs minutes.

`ProtectYourPC` à 3 désactive les paramètres Express. Il ne s'agit que d'un réglage initial : sur un poste joint au domaine, la stratégie de groupe *Allow Telemetry* prend ensuite le dessus et fixe la valeur définitive.

Compte administrateur local

```
<LocalAccount wcm:action="add">
  <Name>adm-local</Name>
  <DisplayName>Administrateur local</DisplayName>
  <Group>Administrators</Group>
  <Password>
    <Value>***</Value>
    <PlainText>true</PlainText>
  </Password>
</LocalAccount>
```

Ce compte est le recours du technicien lorsque le contrôleur de domaine est injoignable : sans lui, un poste dont le canal sécurisé est rompu devient inaccessible.

Limite assumée : le mot de passe est stocké en clair

Trois points doivent être connus. **Premièrement**, `PlainText` à `true` stocke la valeur telle quelle ; à `false`, Windows attend une chaîne encodée en base64, ce qui n'est pas du chiffrement mais évite la lecture directe. **Deuxièmement**, sysprep supprime le fichier après traitement et masque les mots de passe dans la copie mise en cache, mais ne nettoie pas les journaux d'installation du dossier Panther : la vérification post-déploiement doit porter sur les deux. **Troisièmement**, ce mot de passe est identique sur tous les postes déployés ; sa compromission sur un poste vaut compromission du parc. En production, la réponse est Windows LAPS, qui génère un mot de passe unique par machine et le stocke chiffré dans l'annuaire.

4.2 Ouverture de session automatique : volontairement absente

Une version antérieure du fichier comportait un bloc `AutoLogon` sur le compte `adm-local`. Il a été retiré après analyse du comportement observé en déploiement. Le raisonnement est détaillé au document E, section 5.3.

Contrainte de syntaxe XML

Un commentaire XML ne peut pas contenir deux tirets consécutifs. Cette règle a provoqué l'échec de la première version du fichier, avec le code d'erreur `0x800705b9` lors du sysprep. Un contrôle systématique doit être effectué avant chaque généralisation :

```
[xml](Get-Content C:\Windows\Panther\unattend.xml) | Out-Null
```

L'absence d'erreur confirme que le fichier est analysable.

5. Nettoyage et généralisation

5.1 Nettoyage préalable

Tout ce qui est présent sur le master sera dupliqué sur l'ensemble du parc. Le nettoyage précède donc la généralisation :

Opération	Objet
Windows Update complet	Éviter que chaque poste déployé télécharge les mêmes correctifs
Suppression des comptes et profils de travail	Ne pas propager de profils inutiles
DISM /StartComponentCleanup / ResetBase	Purger les versions antérieures des composants, réduire la taille de l'image
Vidage des journaux d'événements	Repartir d'un historique vierge sur chaque poste
Suppression des fichiers temporaires	Réduire le volume capturé

5.2 Instantané avant généralisation

Un instantané de la VM est pris avant le sysprep :

```
qm snapshot 211 pret-sysprep -description "Master nettoye, pret pour generalisation"
```

Pourquoi cet instantané est indispensable

Deux raisons. La première est pratique : une machine généralisée ne revient pas dans son état de travail, et la moindre correction sur le master imposerait de tout reconstruire. La seconde est réglementaire : Windows n'autorise qu'un **nombre limité de généralisations** sur une même installation (jusqu'à 1001 depuis Windows 8.1). Repartir d'un instantané pré-sysprep ne consomme pas ce compteur, contrairement à un nouveau sysprep sur une machine déjà généralisée.

5.3 Sysprep

La généralisation est lancée depuis une console PowerShell administrateur :

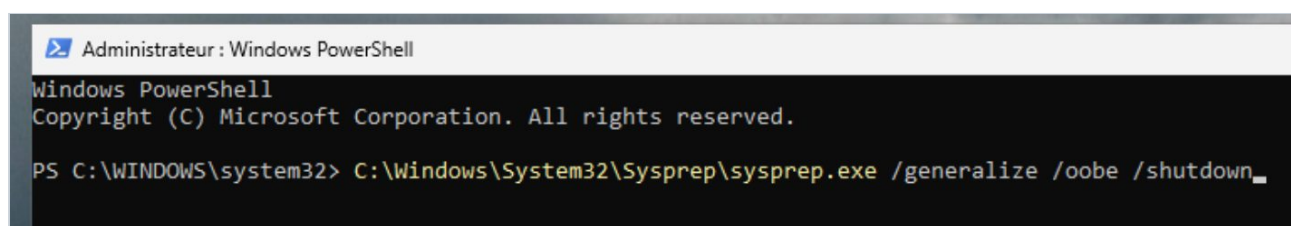


Figure 7 — Commande de généralisation

```
C:\Windows\System32\Sysprep\sysprep.exe /generalize /oobe /shutdown
```

Paramètre	Effet
/generalize	Désinstalle les périphériques configurés, supprime le SID et les identifiants uniques. C'est ce paramètre qui rend l'image déployable.
/oobe	Programme le démarrage suivant sur la phase de configuration initiale, celle que l'unattend.xml automatise.
/shutdown	Arrête la machine à la fin du traitement. Indispensable : un redémarrage relancerait l'Oobe sur le master lui-même et invaliderait le travail.

La même opération est accessible par interface graphique, avec le mode **Oobe**, la case **Généraliser** cochée et l'option **Arrêter le système**. La ligne de commande est privilégiée ici car elle est scriptable et reproductible à l'identique.

5.4 Contrôle de réussite

Le succès de la généralisation se vérifie par la présence du fichier témoin `Sysprep_succeeded.tag` :

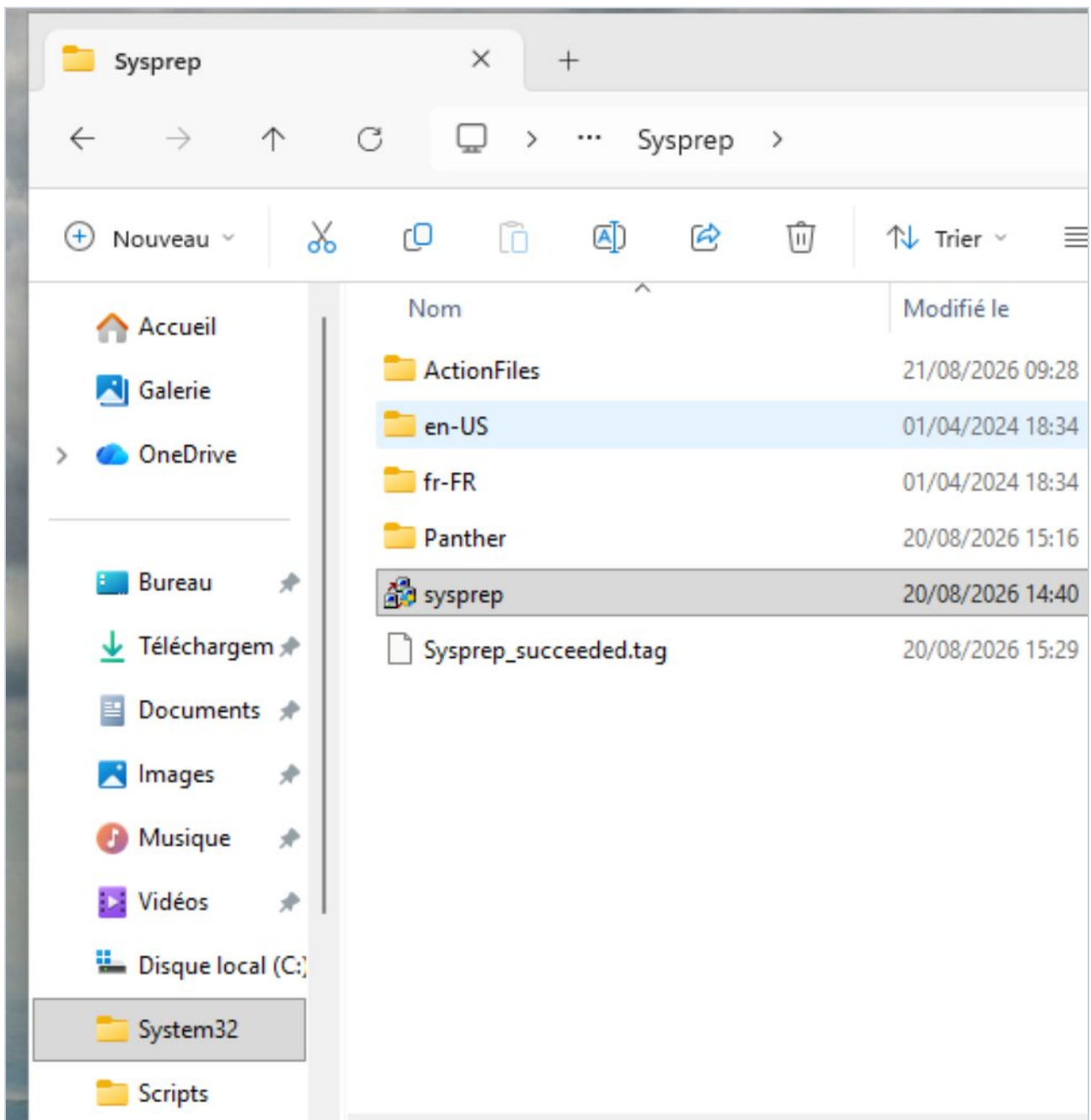


Figure 8 — Présence du fichier témoin Sysprep_succeeded.tag dans le dossier Sysprep

En cas d'échec, le journal `C:\Windows\System32\Sysprep\Panther\setuperr.log` indique la cause. La plus fréquente sur Windows 11 est une erreur de syntaxe dans l'unattend.xml (voir 4.2).

6. Enregistrement du master dans FOG

FOG ne peut agir que sur des machines qu'il connaît. Le master doit donc être enregistré comme hôte avant toute capture.

6.1 Amorçage réseau

La VM est démarrée en PXE. Le micrologiciel étant configuré avec `net0` en première position, le menu FOG apparaît automatiquement :

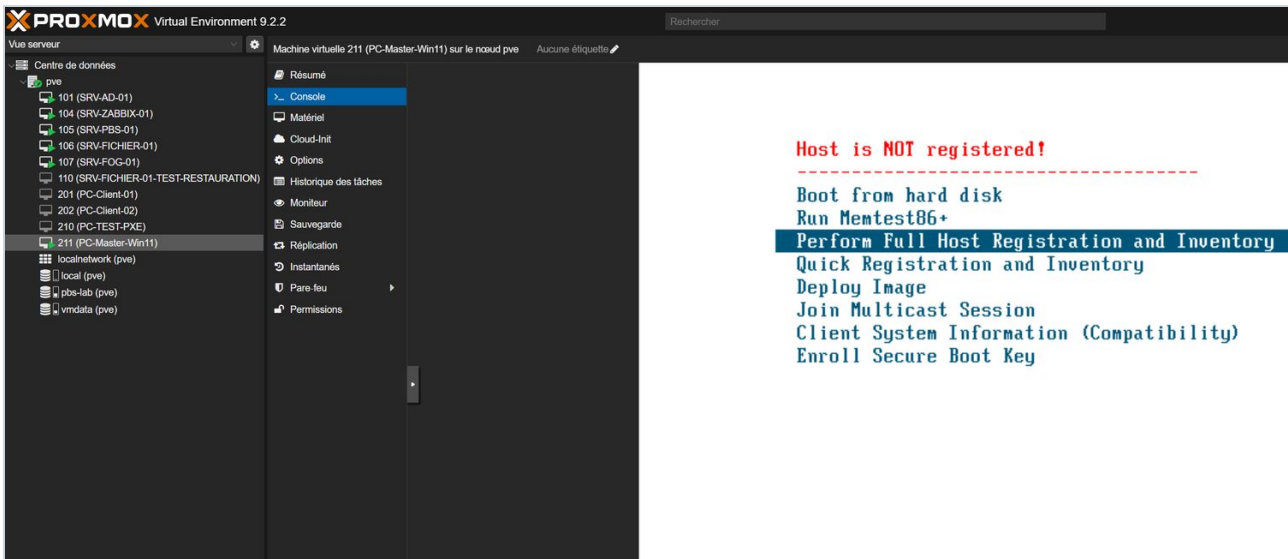


Figure 9 — Menu iPXE — la machine n'est pas encore enregistrée

La mention **Host is NOT registered!** confirme que la machine est inconnue du serveur. Deux modes d'enregistrement sont proposés :

Mode	Comportement	Usage
Full Host Registration	Pose une série de questions : nom, image associée, groupes, snapins, clé produit, jonction au domaine, utilisateur principal	Machine unique à configurer immédiatement
Quick Registration	Enregistre la machine sans aucune question, sous un nom dérivé de son adresse MAC	Enrôlement de flotte, configuration ultérieure par groupe

Pour le master, l'enregistrement complet est retenu : la machine est unique et sa configuration doit être posée dans la foulée.

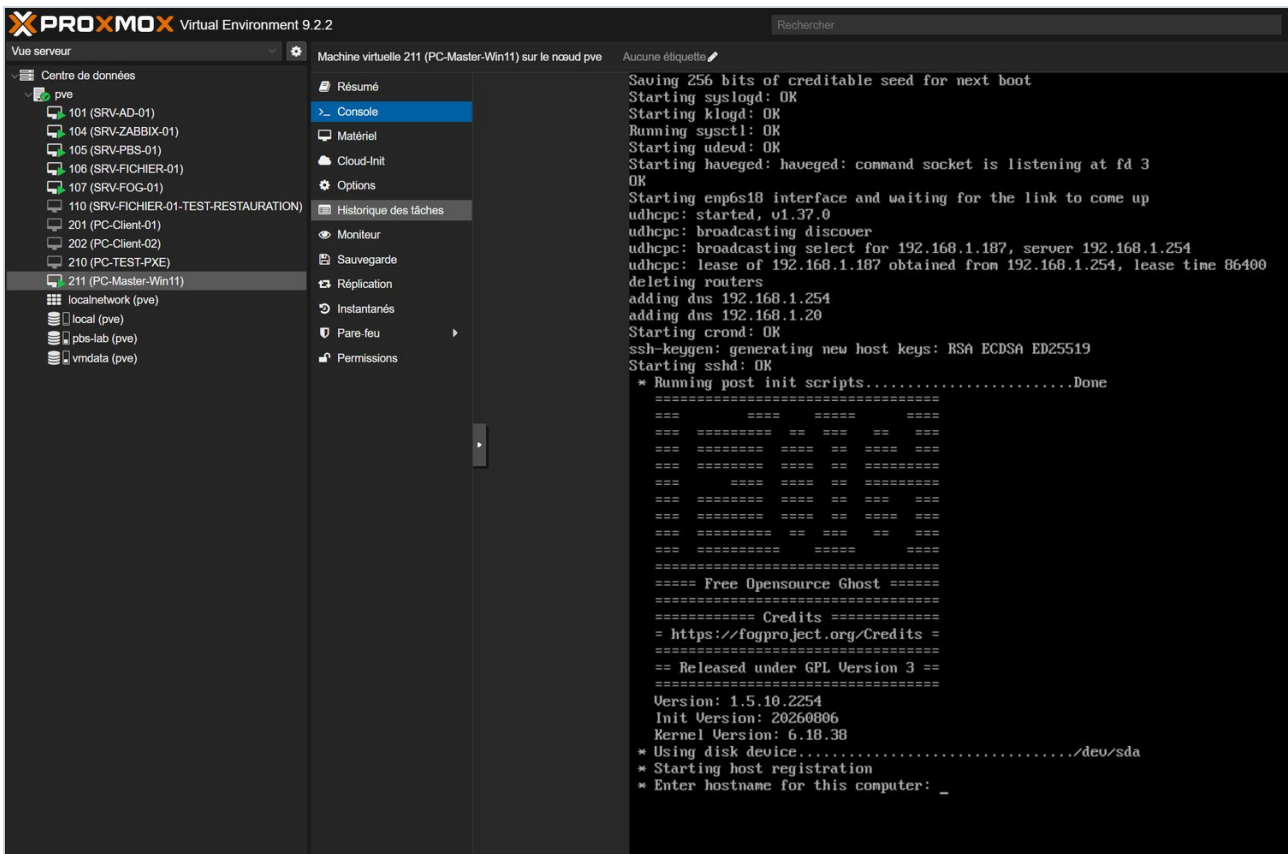


Figure 10 — Début de l'enregistrement — saisie du nom de la machine

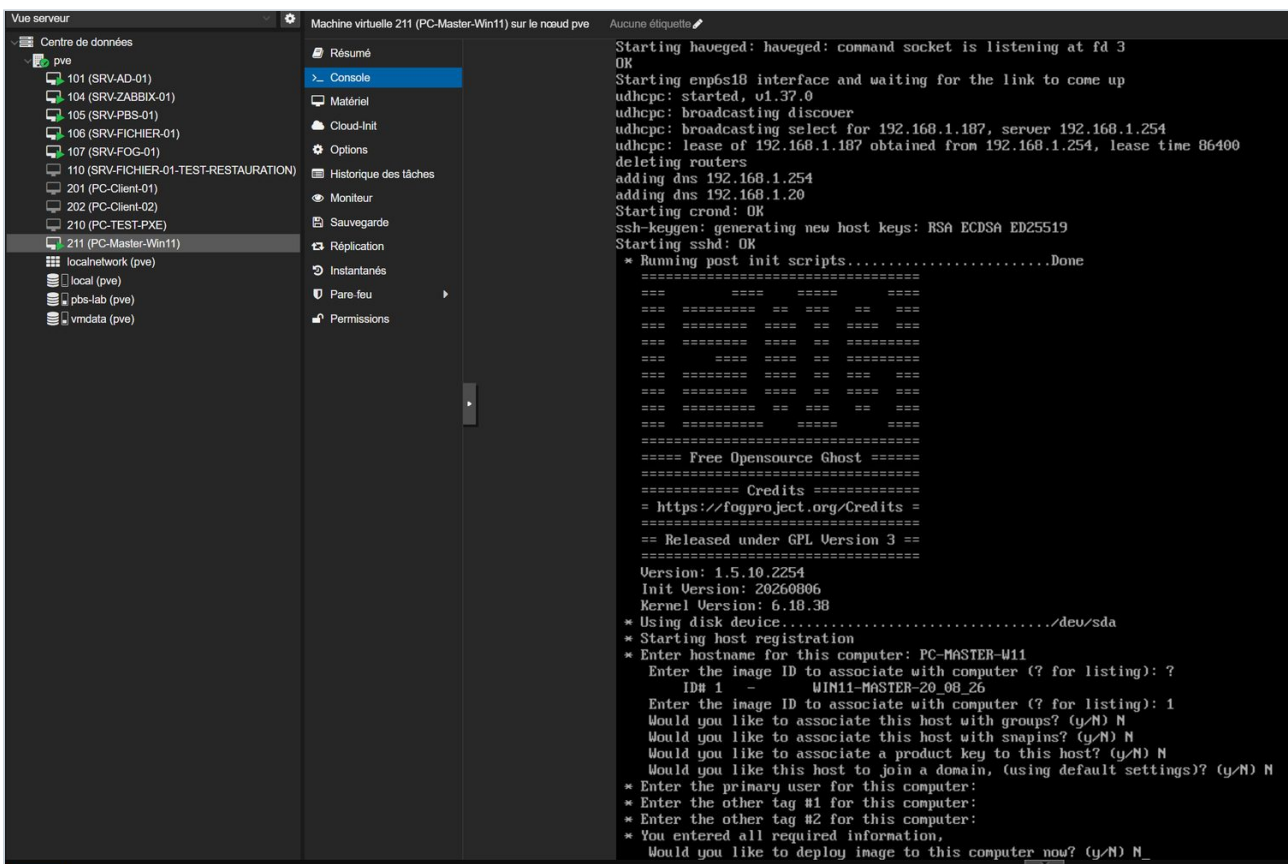
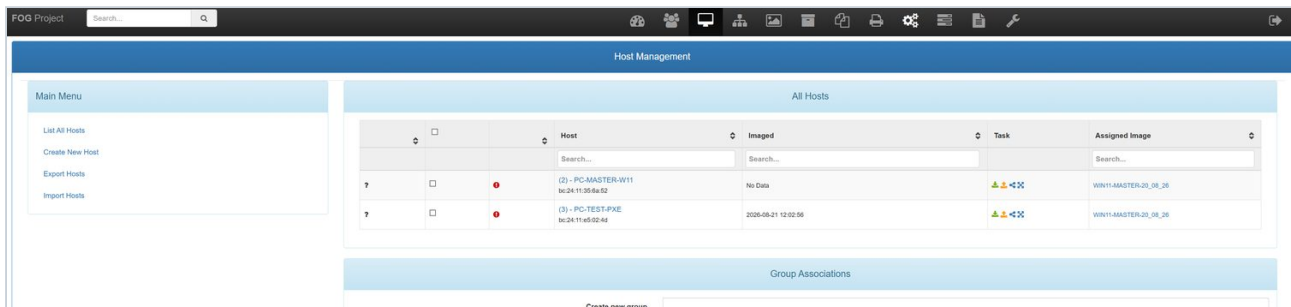


Figure 11 — Séquence complète de l'enregistrement complet, avec association de l'image au master

Pourquoi refuser groupes, snapins et domaine sur le master

Les réponses aux questions « associer à des groupes », « associer des snapins » et « joindre un domaine » sont toutes négatives. Le master n'est pas un poste de production : il ne doit ni recevoir de logiciels par snapin, ni être joint au domaine. Un master joint au domaine transporterait dans l'image un compte machine et un canal sécurisé qui deviendraient invalides sur chaque poste déployé.

6.2 Vérification côté serveur

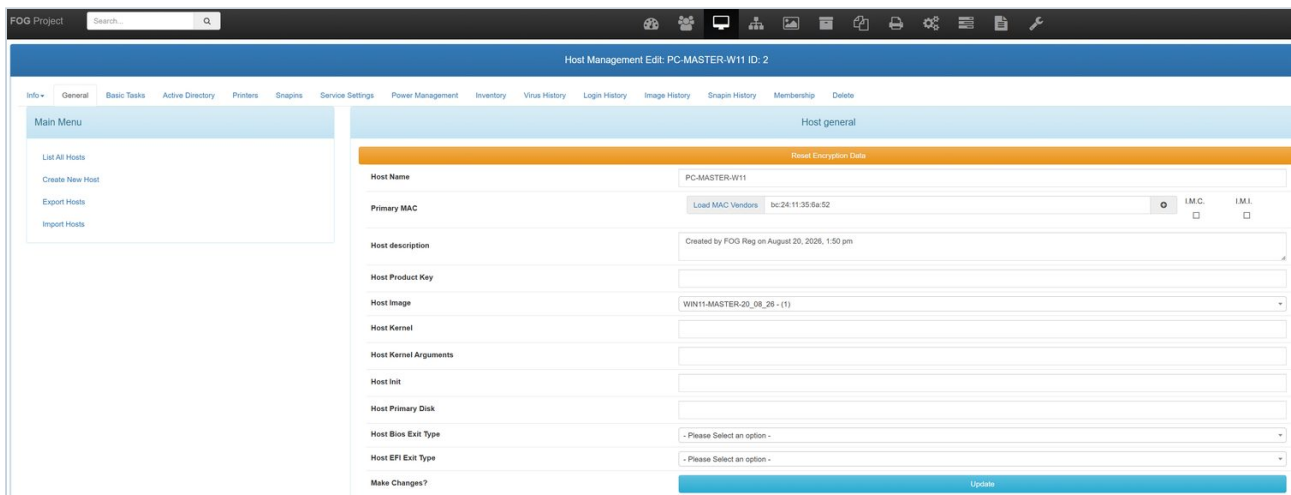


The screenshot shows the 'Host Management' section of the FOG Project web interface. On the left is a 'Main Menu' with links: 'List All Hosts', 'Create New Host', 'Export Hosts', and 'Import Hosts'. The main area is titled 'All Hosts' and contains a table with columns: 'Host', 'Imaged', 'Task', and 'Assigned Image'. There are two rows of host data:

Host	Imaged	Task	Assigned Image
(2) - PC-MASTER-W11 bc:24:11:35:6a:52	No Data		WIN11-MASTER-20_08_26
(3) - PC-TEST-PXE bc:24:11:35:6a:52	2020-08-21 12:02:56		WIN11-MASTER-20_08_26

Below the table is a 'Group Associations' section with a 'Create new group' button.

Figure 12 — L'hôte PC-MASTER-W11 apparaît dans la liste des hôtes



The screenshot shows the 'Host Management Edit: PC-MASTER-W11 ID: 2' page. It has a top navigation bar with tabs: 'Info', 'General', 'Basic Tasks', 'Active Directory', 'Printers', 'Snapins', 'Service Settings', 'Power Management', 'Inventory', 'Virus History', 'Login History', 'Image History', 'Snapin History', 'Membership', and 'Delete'. The 'General' tab is selected, showing 'Host general' settings. The form includes fields for:

- Host Name:** PC-MASTER-W11
- Primary MAC:** bc:24:11:35:6a:52 (with a 'Load MAC Vendors' button and checkboxes for 'I.M.C.' and 'I.M.I.')
- Host description:** Created by FOG Reg on August 20, 2020, 1:50 pm
- Host Product Key:** (empty)
- Host Image:** WIN11-MASTER-20_08_26 - (1)
- Host Kernel:** (empty)
- Host Kernel Arguments:** (empty)
- Host Init:** (empty)
- Host Primary Disk:** (empty)
- Host Bios Exit Type:** - Please Select an option -
- Host EFI Exit Type:** - Please Select an option -
- Make Changes?:** (checkbox)

An 'Update' button is at the bottom right.

Figure 13 — Fiche de l'hôte : adresse MAC et image de destination associée

Deux points sont à contrôler avant de lancer la capture : l'adresse MAC doit correspondre à celle de la carte `net0` de la VM 211 (`bc:24:11:35:6a:52`), et le champ **Host Image** doit désigner l'image dans laquelle le contenu du disque sera écrit.

7. Capture de l'image

7.1 Création de la tâche

Depuis la fiche de l'hôte, onglet **Basic Tasks**, l'action **Capture** lit le disque du poste et l'écrit sur le serveur. C'est l'opération inverse de **Deploy**.

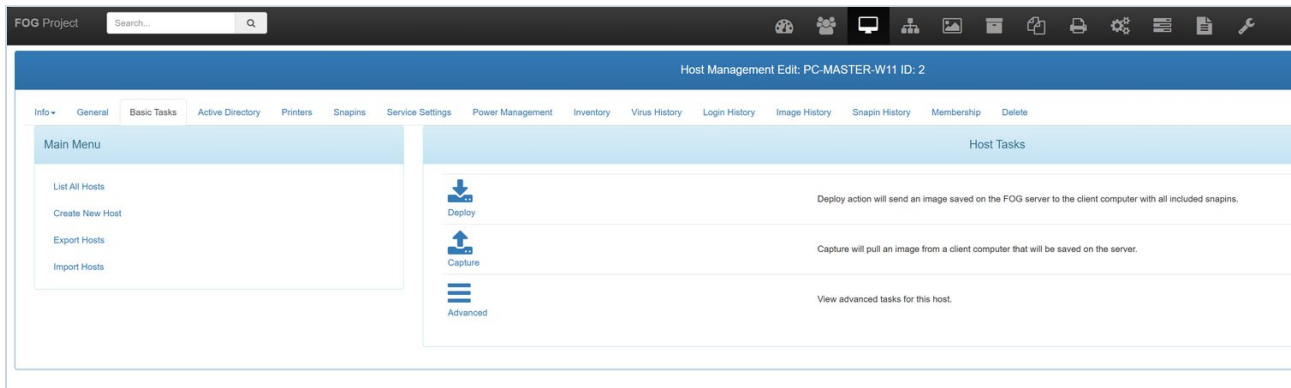


Figure 14 — Onglet Basic Tasks — Deploy envoie une image vers le poste, Capture la récupère depuis le poste

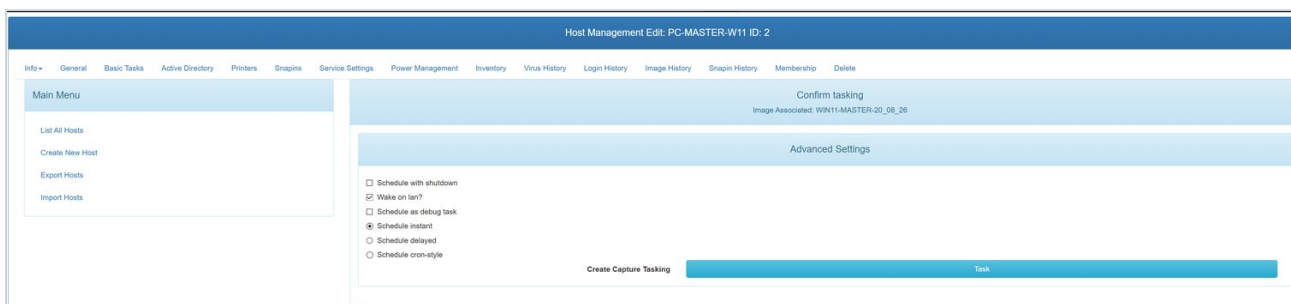


Figure 15 — Confirmation de la tâche de capture — planification immédiate

Cet écran rappelle l'image de destination et propose les modalités de planification. L'option **Schedule instant** est retenue : la tâche est créée dès la validation. La création se fait par le bouton **Task**, en bas de l'écran.

La tâche est ensuite visible dans l'onglet **Task Management**, où elle reste en attente jusqu'à ce que la machine amorce en réseau :

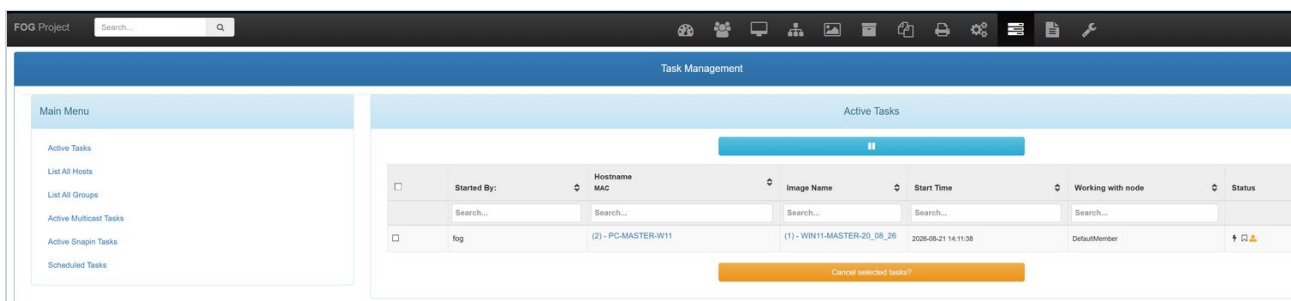


Figure 16 — La tâche de capture apparaît dans Task Management

7.2 Contrôle de l'ordre d'amorçage

La tâche est en attente : elle ne se déclenchera que lorsque la machine amorcera en réseau. L'ordre de démarrage doit donc placer `net0` en première position :

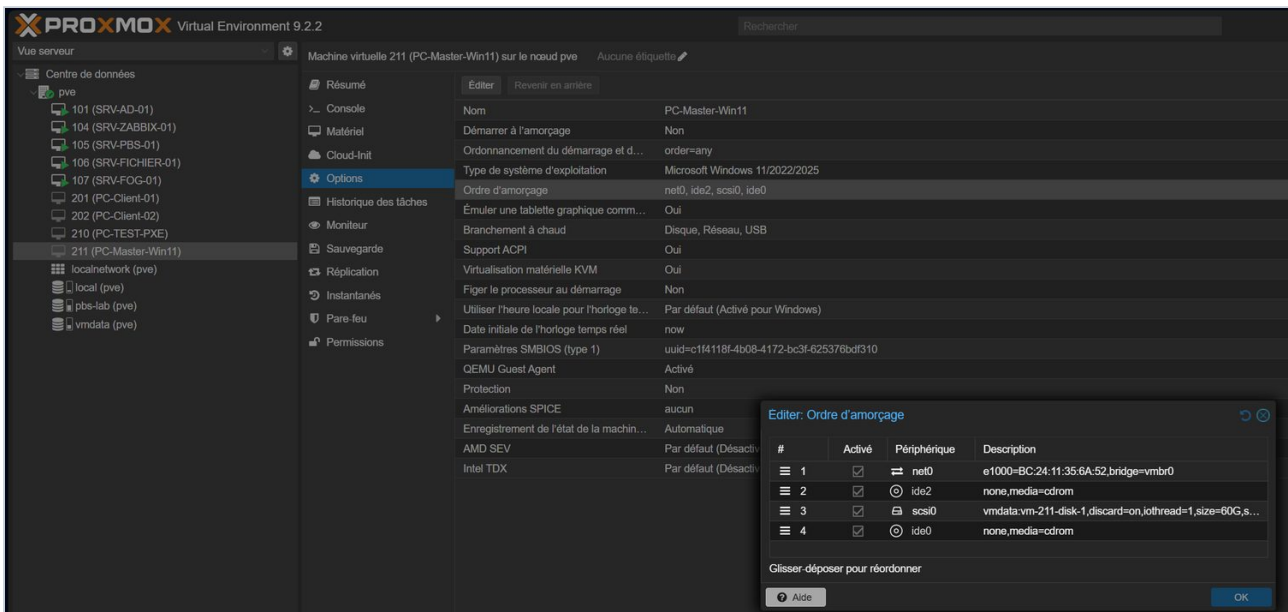


Figure 17 — Ordre d'amorçage de la VM 211 — `net0` en position 1

Le master ne doit pas rester en amorçage PXE permanent

Tant que `net0` précède le disque, le master interroge le serveur FOG à chaque démarrage. Si une tâche de déploiement traîne sur cet hôte, elle s'exécutera et **écrasera le master**. La règle d'exploitation est de remettre le disque en tête après chaque capture. Sur ce lab, `net0` reste en tête pour les tests en cours : aucune tâche ne doit alors rester assignée au master.

7.3 Déroulement

Au démarrage de la VM, FOG prend la main et lance Partclone, qui lit les partitions les unes après les autres. La partition Windows constitue l'essentiel du volume :

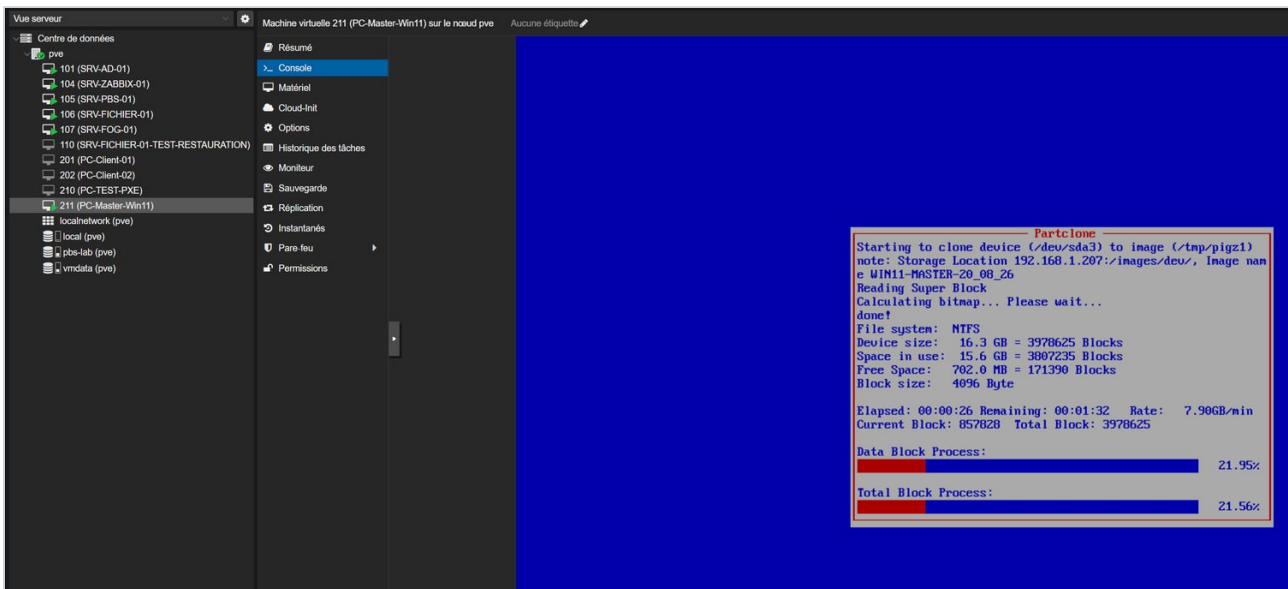


Figure 18 — Capture de la partition Windows : 16,3 Go NTFS, débit 7,90 Go/min

Les autres partitions du disque GPT sont traitées de la même manière. La partition système EFI, très petite, est copiée en une seconde :

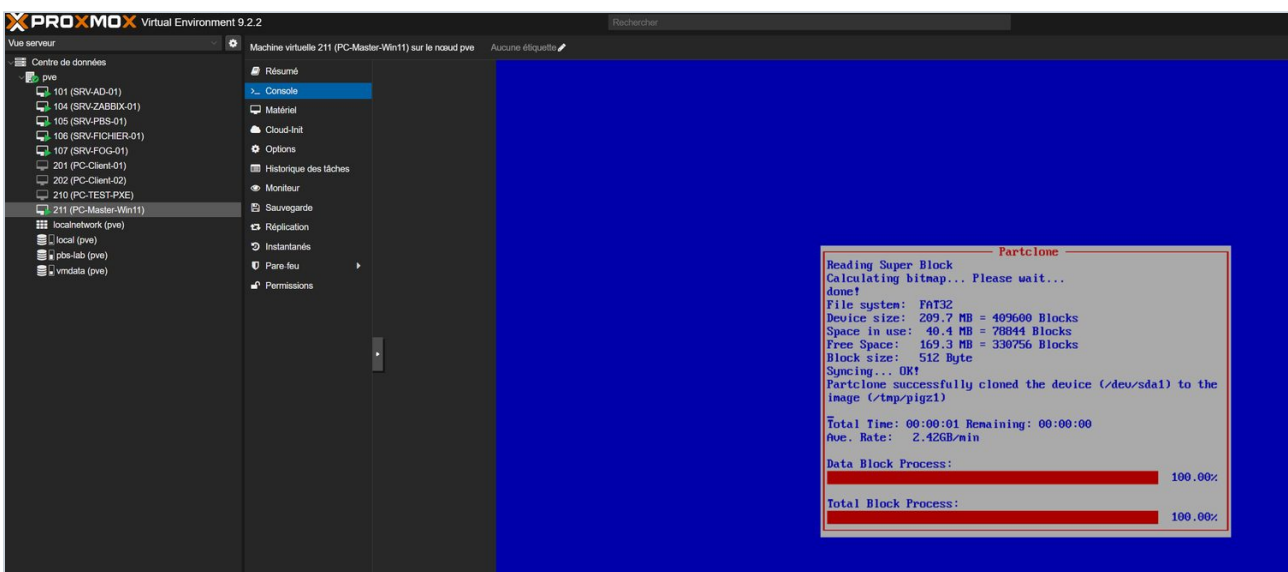


Figure 19 — Capture de la partition système EFI : 209,7 Mo en FAT32

Pourquoi Partclone et pas une copie brute

Partclone lit la table d'allocation du système de fichiers et ne copie que les blocs réellement occupés. Sur la partition Windows, 15,6 Go sont utilisés sur 16,3 Go de partition — mais sur un disque de 60 Go, une copie brute aurait transféré les 60 Go. Ce mécanisme, combiné à la compression ZSTD, explique qu'une image d'un poste de 60 Go n'occupe que 16 Go sur le serveur.

8. Validation

8.1 Présence de l'image sur le serveur

Premier contrôle, sur le système de fichiers du serveur :

```
ls -lh /images/
```

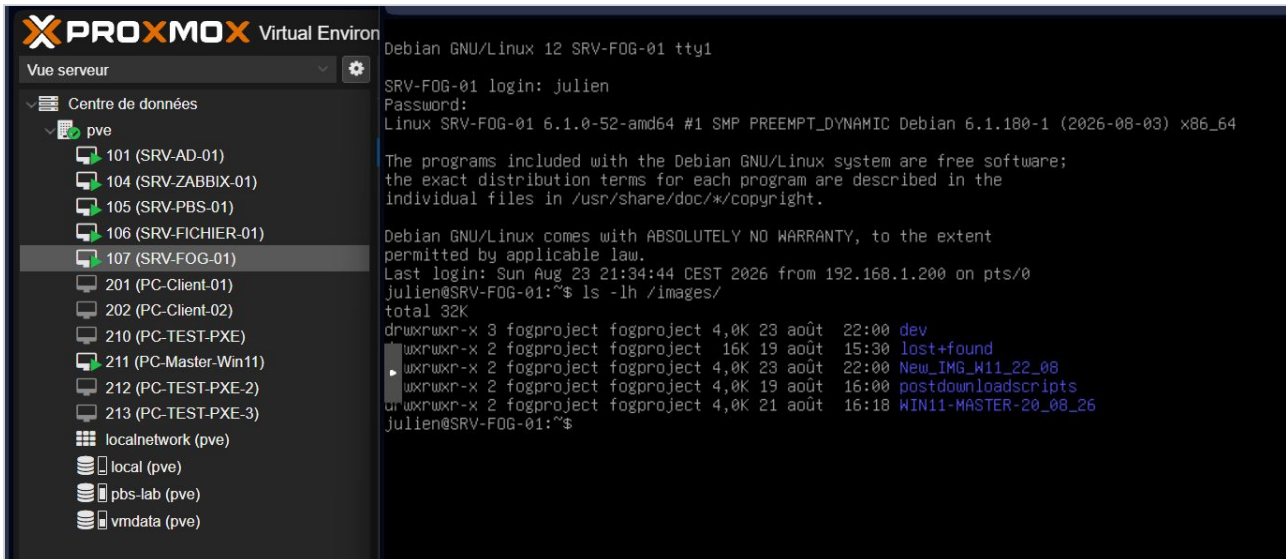


Figure 20 — Contenu du répertoire /images sur SRV-FOG-01

Le répertoire portant le nom de l'image doit être présent, appartenir à l'utilisateur `fogproject` et porter une date de modification cohérente avec la fin de la capture.

8.2 Déclaration dans l'interface

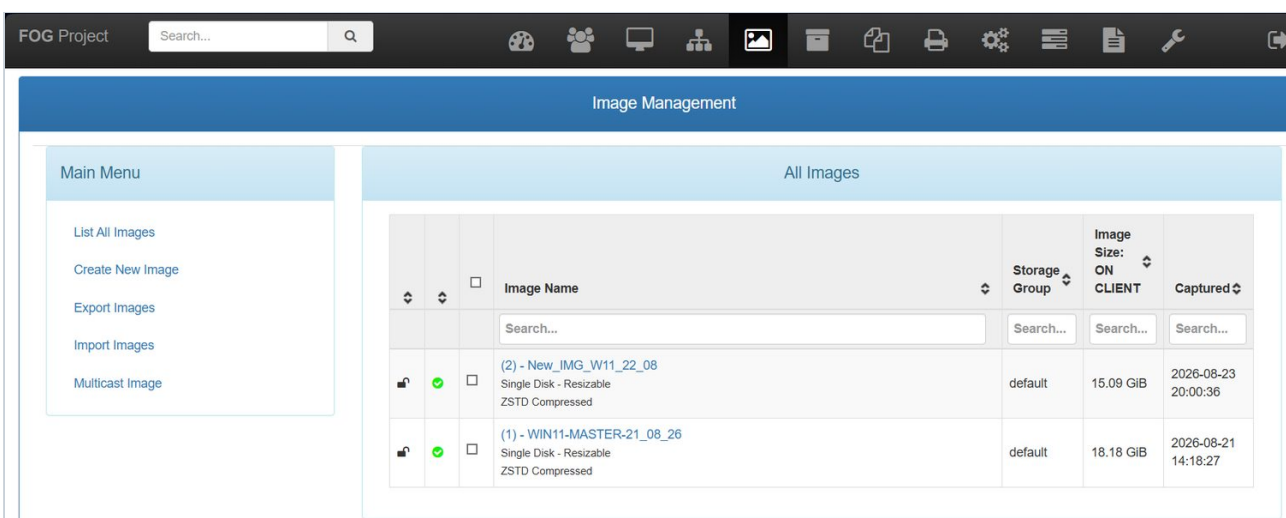


Figure 21 — Image Management — les images disponibles sur le serveur

Champ

Signification

Single Disk - Resizable	Type d'image : un disque, partition Windows redimensionnable au déploiement
ZSTD Compressed	Algorithme de compression retenu, bon compromis entre taux et vitesse
Image Size: ON CLIENT	Taille des données telles qu'elles seront écrites sur le poste cible
Captured	Horodatage de fin de capture

8.3 Contrôle fonctionnel du fichier de réponses

La validation définitive du master n'intervient qu'au premier déploiement : c'est là que l'on constate si l'Oobe se déroule sans saisie. Une validation reste demandée : l'écran suivant montre la sélection du pays déjà positionnée sur **France** :

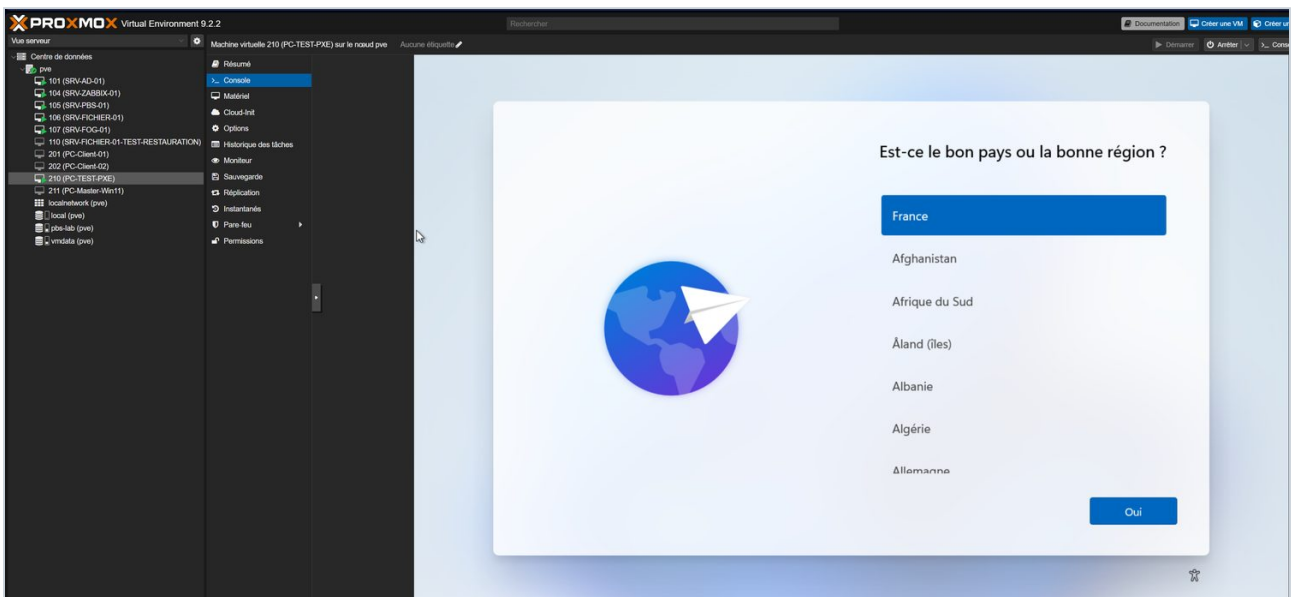


Figure 22 — OOB sur un poste déployé — les paramètres régionaux de l'unattend.xml sont appliqués

8.4 Liste de contrôle

Point	Contrôle
Client FOG	FOGService actif, démarrage automatique différé
Régionalisation	fr-FR sur les trois blocs d'intl.cpl
Fichier de réponses	Présent dans Panther, XML valide
Instantané	Point pré-sysprep disponible
Sysprep	Sysprep_succeeded.tag présent
Image	Répertoire présent dans /images, taille cohérente
Déclaration	Image listée dans Image Management
Amorçage	PXE conservé sur le master (tests) ; disque en tête sinon