SLEEPING FOREST

RAPPORT D'ACTIVITÉ DE MON PROJET E7

Mise en place d'une infrastructure systèmes et réseaux sécurisée

Fêmy LADELEH

BTS SIO option SISR — Épreuve E7

Introduction

En tant qu'étudiant en deuxième année de BTS SIO (Services Informatiques aux Organisations) option SISR (Solutions d'Infrastructure, Systèmes et Réseaux), j'ai réalisé dans le cadre de l'épreuve E7 un projet complet de mise en place d'une infrastructure systèmes et réseaux pour le compte d'une entreprise fictive : Sleeping Forest. Ce projet consiste à construire, sécuriser et administrer l'ensemble de l'infrastructure informatique de cette organisation : annuaire d'entreprise, partage de ressources, durcissement des systèmes, déploiement automatisé des postes de travail et protection du réseau par un pare-feu.

L'ensemble de l'infrastructure a été virtualisé sur un hyperviseur Proxmox mis à disposition par mon établissement. Elle s'articule autour d'un contrôleur de domaine Windows Server 2022 nommé SRVSLFOREST (192.168.2.10), qui héberge les rôles Active Directory, DNS, DHCP, WDS et MDT, d'un pare-feu pfSense (192.168.2.1) faisant office de passerelle, et de postes clients Windows 11 déployés automatiquement au sein du domaine sleepingforest.local.

Ce document a pour vocation de faire le bilan de mon projet E7, avec dans un premier temps une présentation du contexte et de l'environnement technique, puis une présentation détaillée des réalisations effectuées sur la partie SYSTÈME et sur la partie RÉSEAU, avant de conclure sur les difficultés rencontrées et les perspectives d'évolution de cette infrastructure.

Table des matières

Partie 1 : Présentation du contexte et de l'environnement du projet

Sleeping Forest (SF) est une entreprise fictive composée de plusieurs services : la Direction, les Ressources Humaines, les Finances, le service Juridique et le service des Systèmes d'Information (SI). Dans le cadre de ce projet, j'interviens en tant que technicien support informatique mandaté pour mettre en place l'intégralité de l'infrastructure informatique du client.

Sleeping Forest m'a confié plusieurs missions :

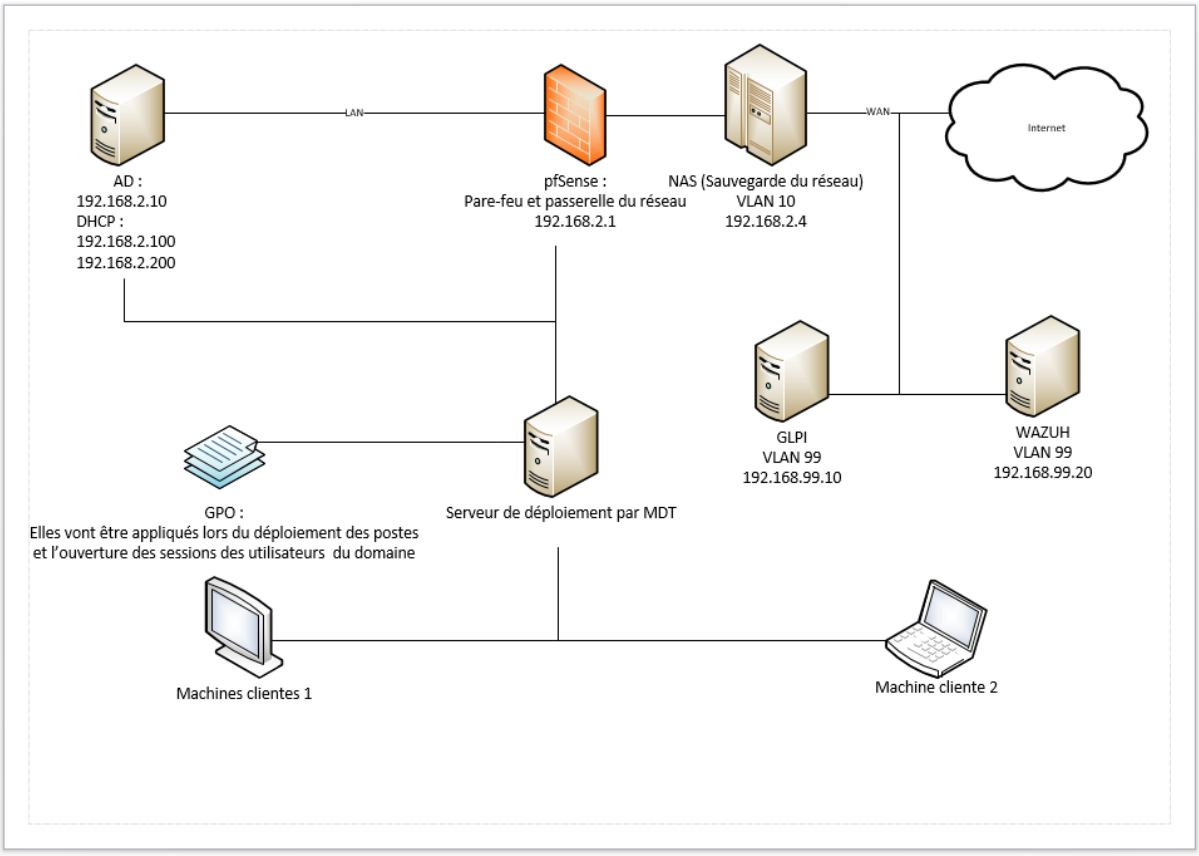
- La **création d'un annuaire d'entreprise** centralisant l'ensemble des salariés, organisés par services, avec une gestion fine de leurs droits d'accès ;
- La **mise à disposition de ressources partagées** (lecteurs réseaux) accessibles selon le service d'appartenance de chaque collaborateur ;
- Le **durcissement des systèmes** (postes clients et serveur) selon les référentiels de sécurité reconnus (CIS, Microsoft Security Baseline) ;
- La **mise en place d'un serveur de déploiement** permettant d'installer automatiquement des postes Windows 11 sécurisés et intégrés au domaine ;
- La **protection du réseau** par un pare-feu constamment actif filtrant les flux de l'infrastructure.

L'environnement technique du projet repose sur les éléments suivants :

Élément	Description
Hyperviseur	Proxmox VE (administration des droits gérée par le professeur)
Contrôleur de domaine	SRVSLFOREST — Windows Server 2022 — 192.168.2.10 (AD DS, DNS, DHCP, WDS, MDT)
Domaine	sleepingforest.local
Pare-feu / passerelle	pfSense — LAN : 192.168.2.1/24 — WAN : réseau 172.16.2.0/24 (bridge Proxmox vmbr111)
Postes clients	Windows 11 (VM de référence durcie, puis postes déployés via MDT)
Outils de sécurité	HardeningKitty, Microsoft Security Baseline (Policy Analyzer, LGPO)

Schéma général de l'infrastructure **(1)**

Cf capture écran ci-dessous



Capture 1 — Schéma de l'infrastructure Sleeping Forest

Partie 2 : Réalisations effectuées dans le cadre du projet E7

2.1. SYSTÈME

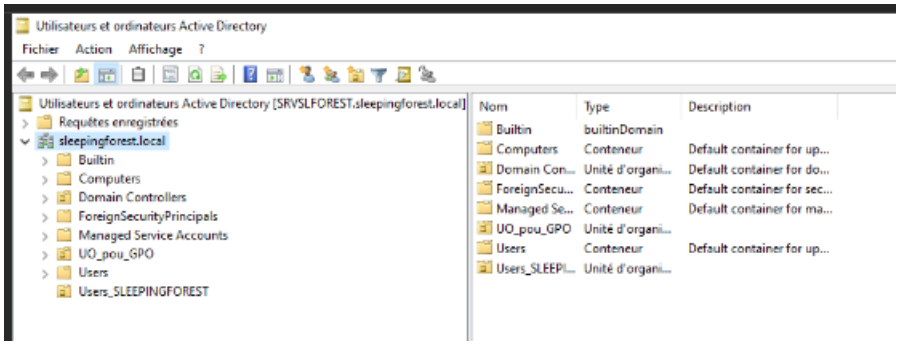
2.1.1. Création de l'Active Directory : groupes de sécurité et utilisateurs

La première étape du projet a consisté à installer le rôle Active Directory Domain Services (AD DS) sur le serveur SRVSLFOREST et à promouvoir celui-ci en contrôleur de domaine du domaine sleepingforest.local. L'Active Directory constitue l'annuaire central de l'entreprise : il recense l'ensemble des salariés, des services et du matériel informatique de Sleeping Forest.

Afin de refléter l'organisation réelle de l'entreprise, j'ai structuré l'annuaire de la manière suivante :

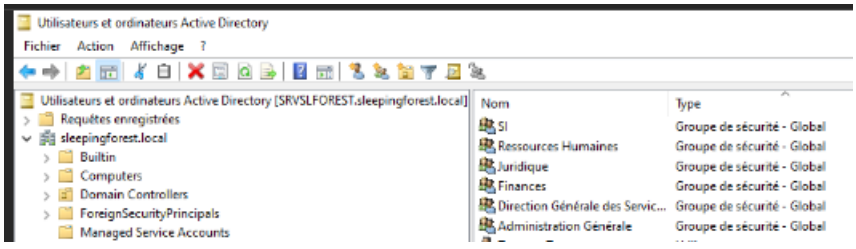
- **Création des unités d'organisation (OU)** correspondant aux services de l'entreprise : Direction, Ressources Humaines, Finances, Juridique et Systèmes d'Information **(2)** ;
- **Création des groupes de sécurité** portant le nom de chaque service (SI, Finances, Ressources Humaines, etc.). Ces groupes constituent la pierre angulaire de la gestion des droits : c'est l'appartenance à un groupe, et non le compte individuel, qui détermine les accès **(3)** ;
- **Création des comptes utilisateurs** (les employés fictifs de Sleeping Forest, par exemple Audrey Hepburn — ahepburn, Diana Themyscira — dthemyscira, Barry Allen ou Oliver Queen pour le service SI), placés dans l'OU de leur service et ajoutés au groupe de sécurité correspondant **(4)**.

Cf capture écran ci-dessous



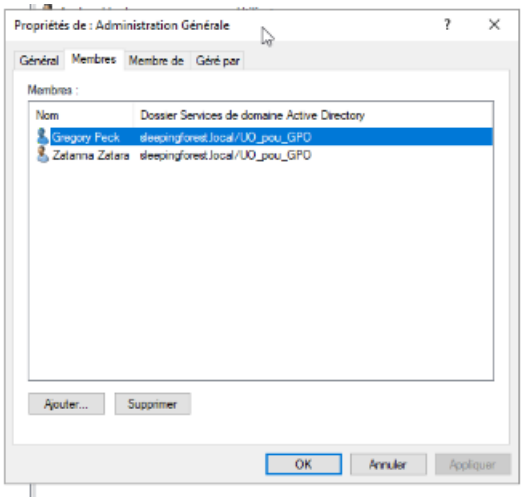
Capture 2 — Arborescence des OU dans Utilisateurs et ordinateurs Active Directory

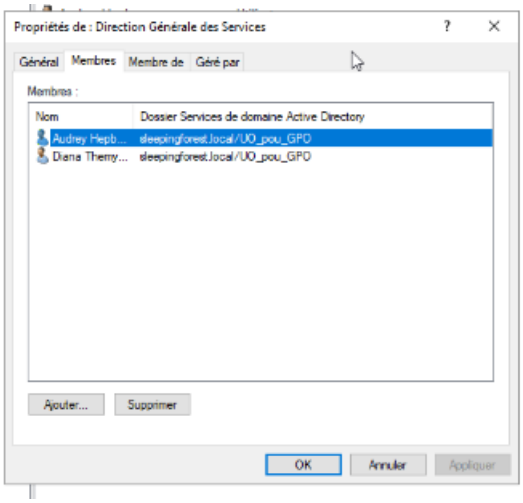
Cf capture écran ci-dessous

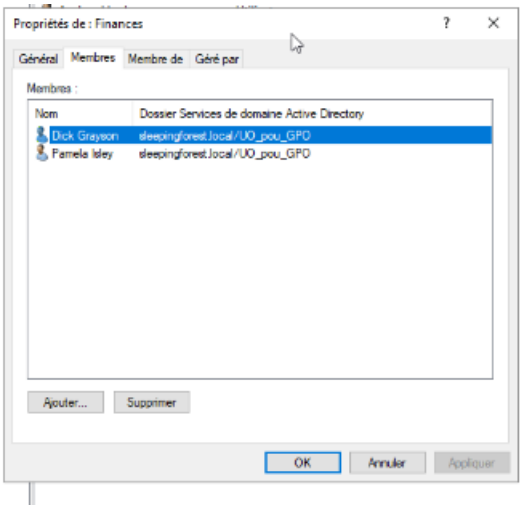


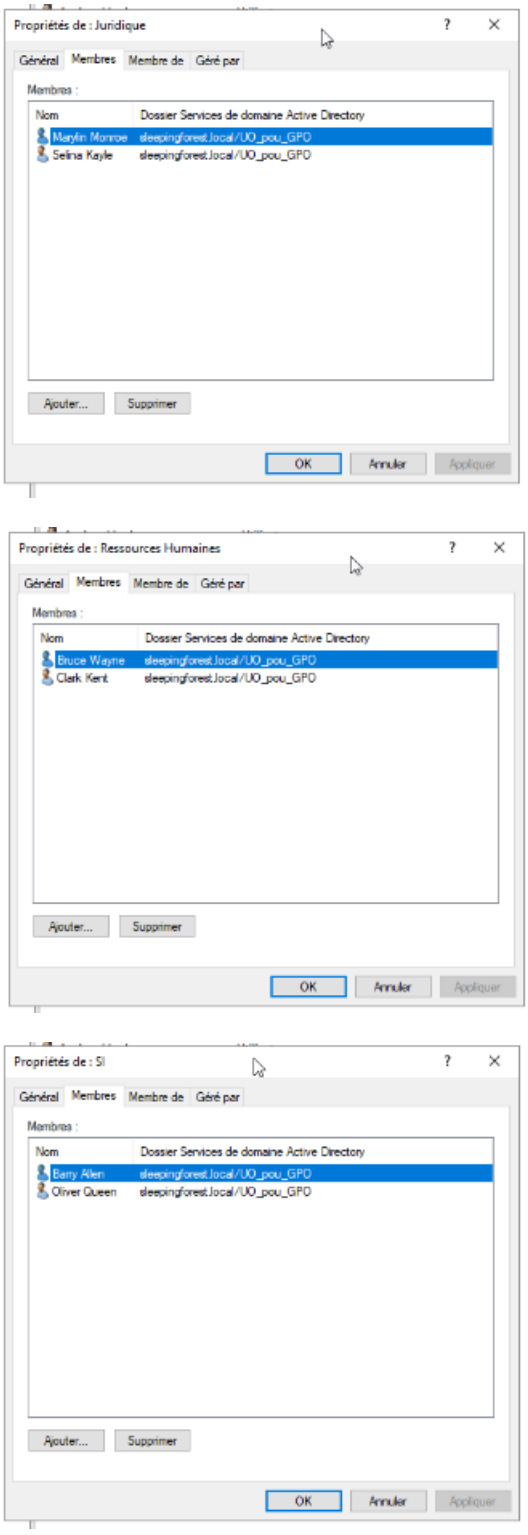
Capture 3 — Groupes de sécurité des services de l'entreprise

Cf capture écran ci-dessous









Capture 4 — Comptes utilisateurs et appartenance aux groupes de sécurité

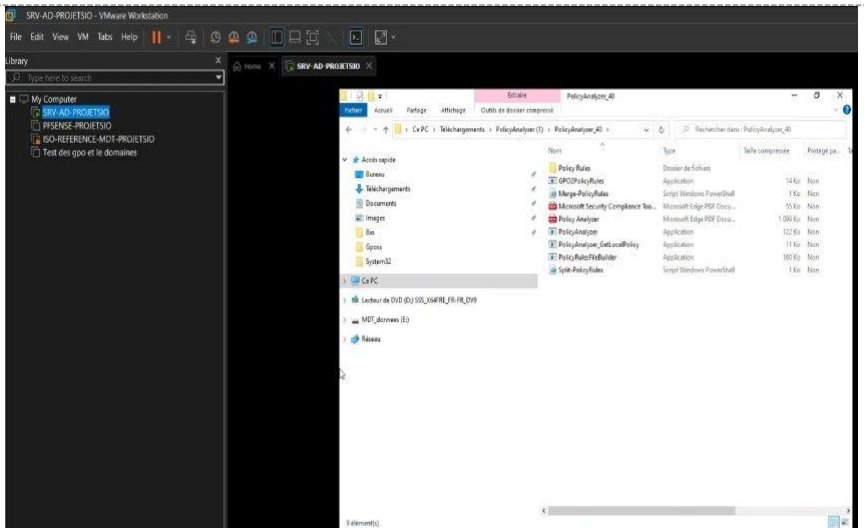
Cette organisation me permet de donner — ou de ne pas donner — des droits aux employés de façon simple et évolutive : pour qu'un nouvel arrivant aux Finances obtienne tous les accès de son service, il suffit de l'ajouter au groupe Finances. Les membres du groupe SI disposent quant à eux de droits étendus d'administration, tandis que les autres services sont volontairement restreints. Ce principe de moindre privilège est au cœur de la politique de sécurité que j'ai mise en place pour Sleeping Forest.

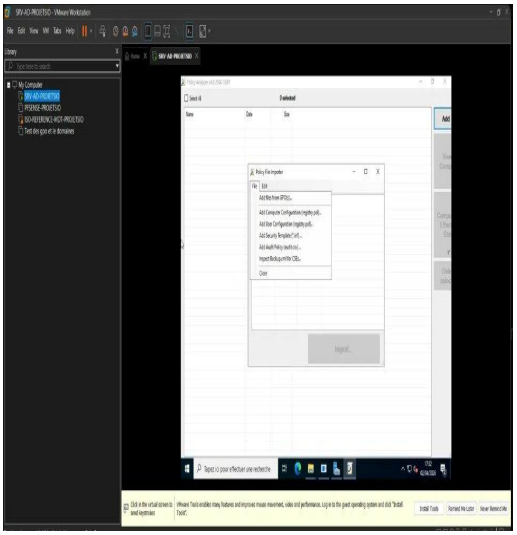
2.1.2. Montage des lecteurs réseaux selon l'appartenance aux groupes de sécurité

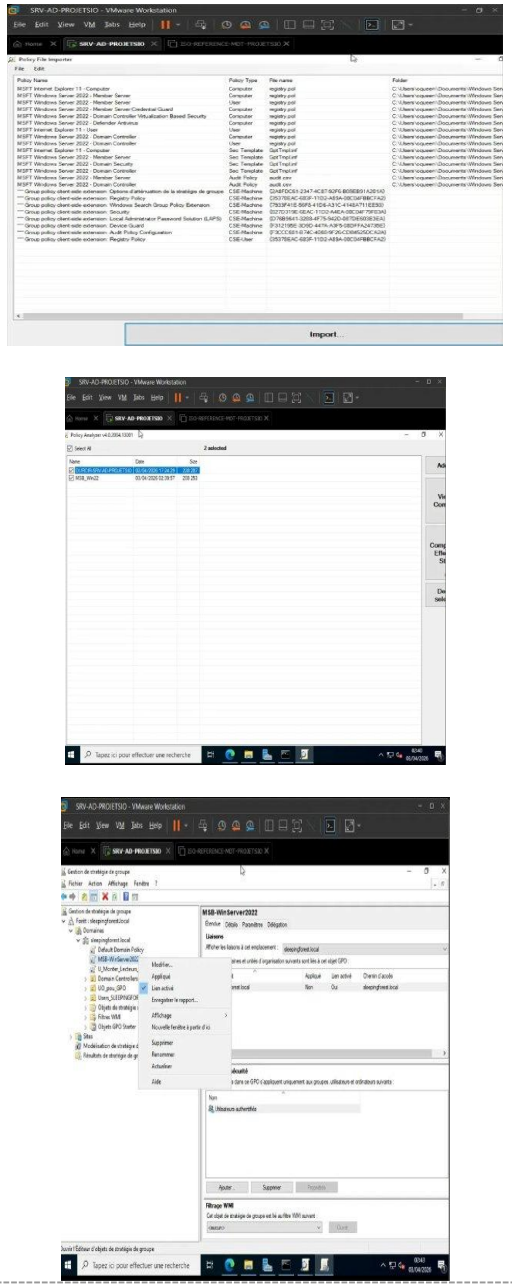
Une fois l'annuaire en place, Sleeping Forest souhaitait que chaque service dispose de son propre espace de stockage réseau, accessible uniquement par ses membres, ainsi que d'un espace commun à toute l'entreprise.

Pour cela, j'ai d'abord créé sur le serveur les dossiers partagés de chaque service (Commun, Direction, Ressources_Humaines, Finances, Juridique, Systèmes_Informatiques) avec des autorisations NTFS et de partage alignées sur les groupes de sécurité de l'AD **(5)**.

Cf capture écran ci-dessous



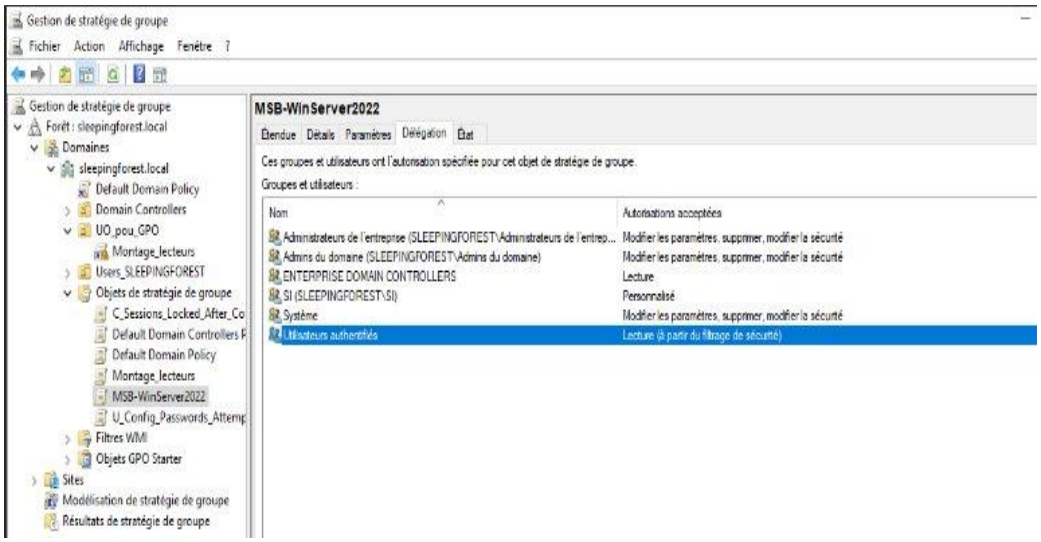




Capture 5 — Dossiers partagés et autorisations sur SRVSLFOREST

Le montage automatique des lecteurs sur les postes clients a ensuite été mis en place par une **GPO** dédiée, **Montage_lecteurs**, liée à l'OU contenant les utilisateurs du domaine. Cette GPO est configurée dans Configuration utilisateur → Stratégies → Paramètres Windows → Scripts → **Ouverture de session** : elle exécute à chaque connexion le script **monter_lecteurs.bat**, déposé dans le partage **NETLOGON** du contrôleur de domaine (\\SRVSLFOREST\netlogon), ce qui le rend automatiquement accessible à tous les postes du domaine **(6)**.

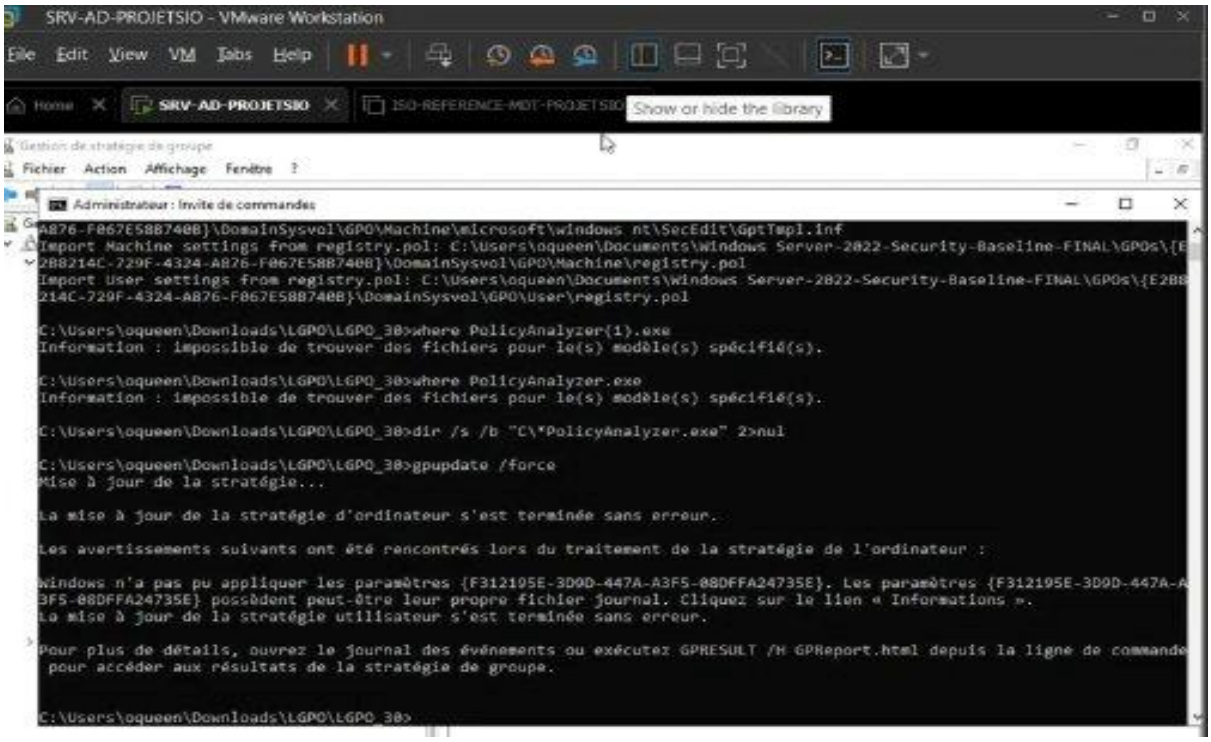
Cf capture écran ci-dessous



Capture 6 — GPO Montage_lecteurs : script d'ouverture de session dans NETLOGON

Le point clé de cette réalisation est que la sélection des lecteurs est gérée directement par le script : à l'ouverture de session, celui-ci teste l'**appartenance de l'utilisateur aux groupes de sécurité** de l'Active Directory et ne monte que les lecteurs correspondant à son service. Ainsi, un membre du service Finances voit apparaître à sa connexion le lecteur Commun et le lecteur Finances, mais jamais celui des Ressources Humaines **(7)**.

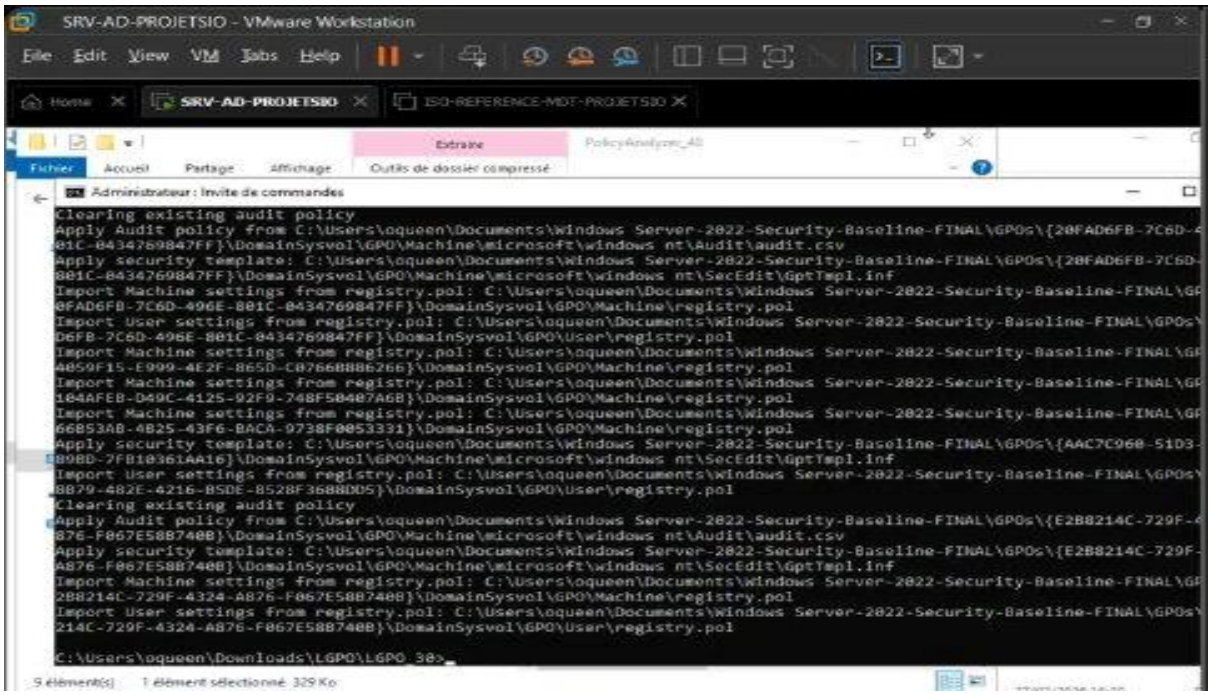
Cf capture écran ci-dessous



Capture 7 — Contenu du script monter_lecteurs.bat (conditions par groupe de sécurité)

La mise au point de ce script m'a appris une subtilité importante : les conditions du script échouaient à cause des **caractères accentués** des noms de groupes français, que l'interpréteur de commandes gérait mal. Le remplacement des caractères accentués dans les conditions du script a permis un fonctionnement fiable du montage pour tous les utilisateurs du domaine **(8)**.

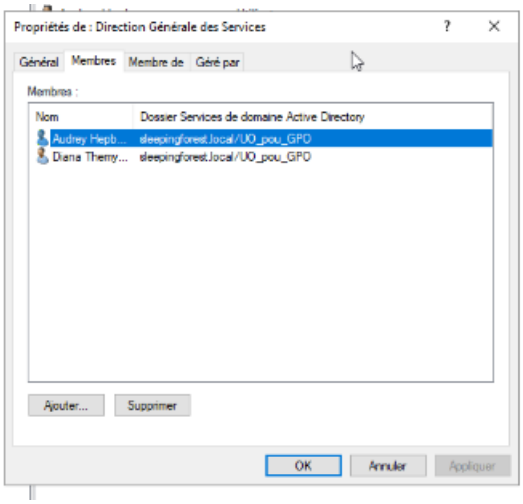
Cf capture écran ci-dessous

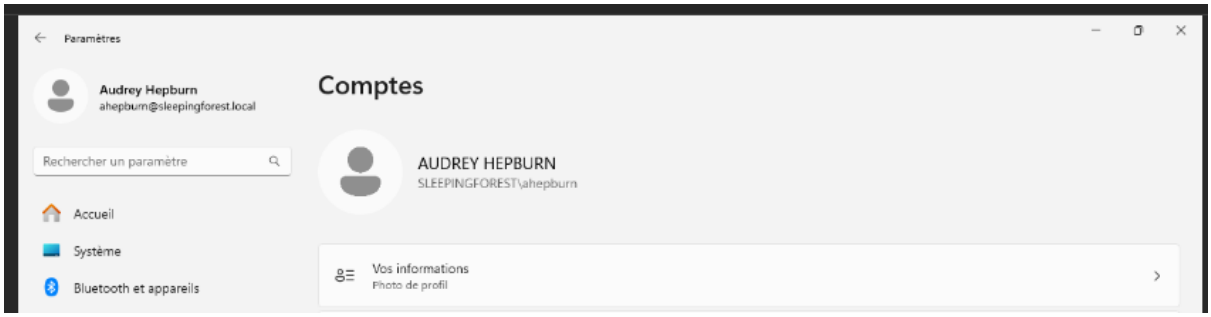


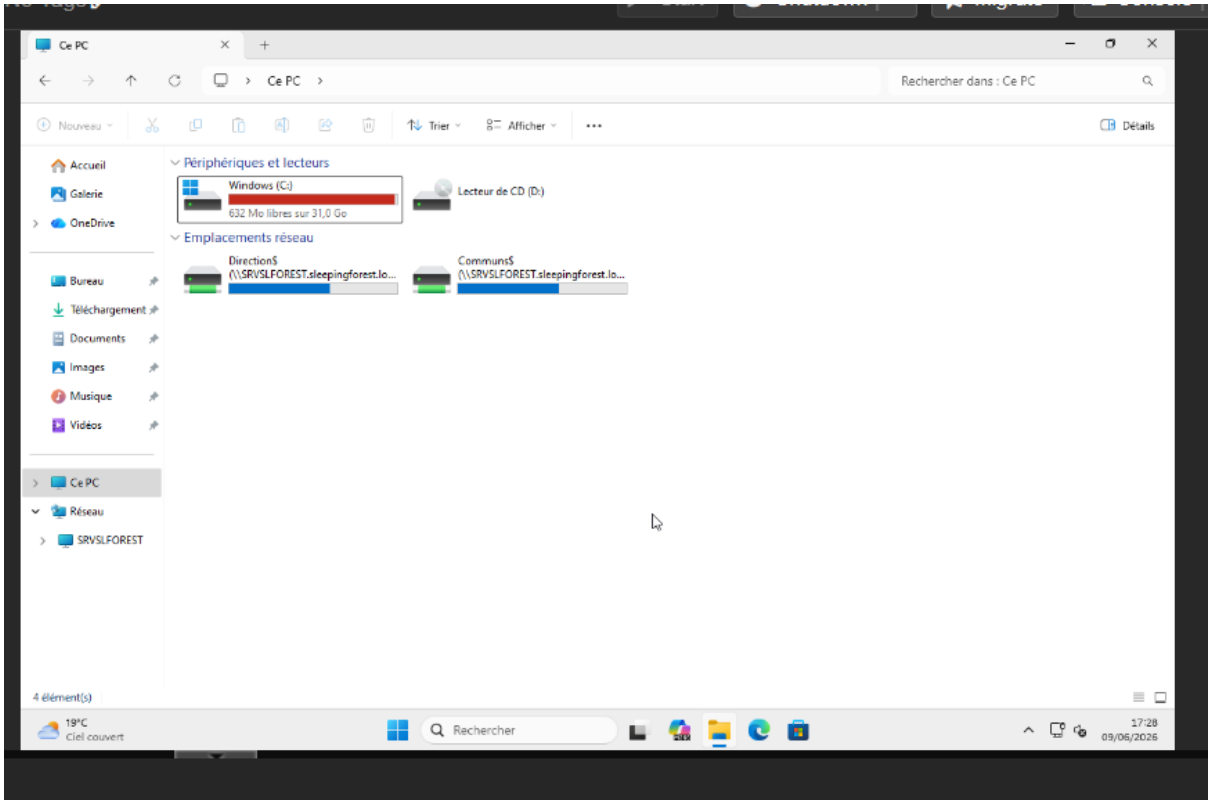
Le résultat final a été validé en ouvrant une session avec des comptes de différents services sur un poste client : chaque utilisateur ne voit que les lecteurs auxquels son service lui donne droit **(9)**.

Capture 8 — Script monter_lecteurs.bat : correction des caractères accentués

Cf capture écran ci-dessous







Capture 9 — Lecteurs réseaux montés sur le poste client selon le service de l'utilisateur

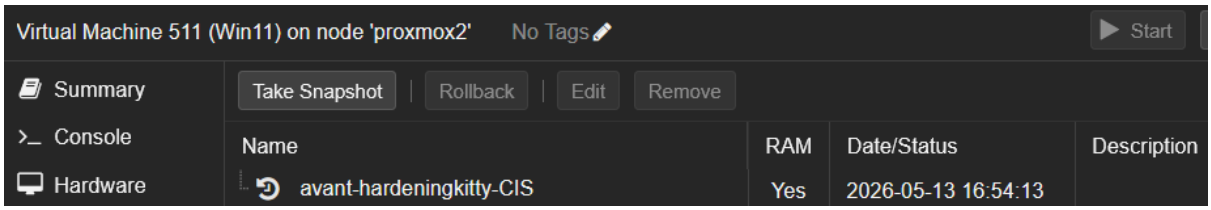
2.1.3. Sécurisation de l'ISO de référence Windows 11 avec HardeningKitty

Avant de déployer Windows 11 sur les postes de Sleeping Forest, il était essentiel de durcir l'image de référence afin que tous les postes issus du déploiement soient sécurisés dès leur installation. Pour cela, j'ai utilisé **HardeningKitty**, un outil PowerShell qui audite et applique les recommandations de durcissement issues notamment des référentiels **CIS (Center for Internet Security)**.

Ma démarche a été la suivante :

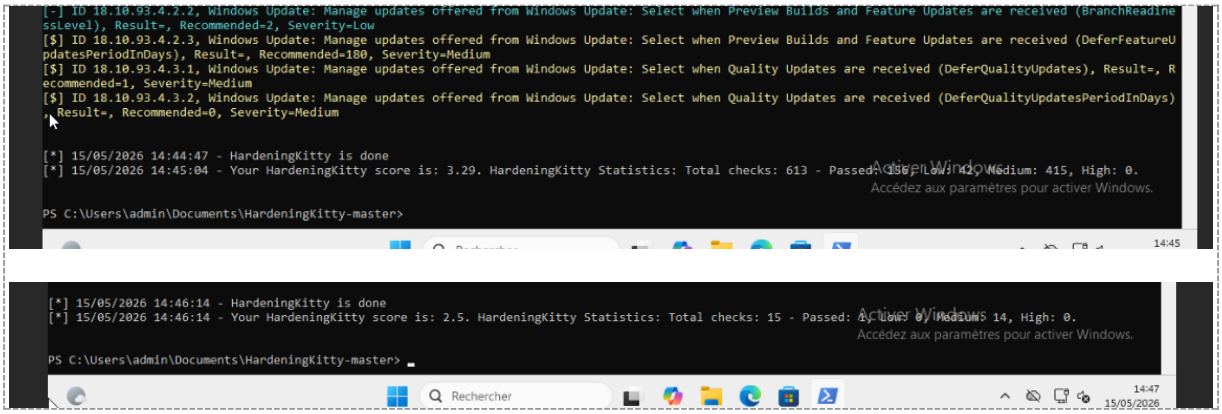
- Création d'une **VM de référence Windows 11** sur Proxmox et réalisation d'un **snapshot** avant toute modification, afin de pouvoir revenir en arrière en cas de blocage **(10)** ;
- Exécution d'un premier **audit HardeningKitty** pour mesurer le niveau de sécurité initial du système **(11)** ;
- Application du durcissement à partir de la liste de paramètres CIS, puis nouvel audit de contrôle : le score obtenu après durcissement est quasi parfait, ce qui valide la conformité de l'image aux recommandations **(12)**.

Cf capture écran ci-dessous



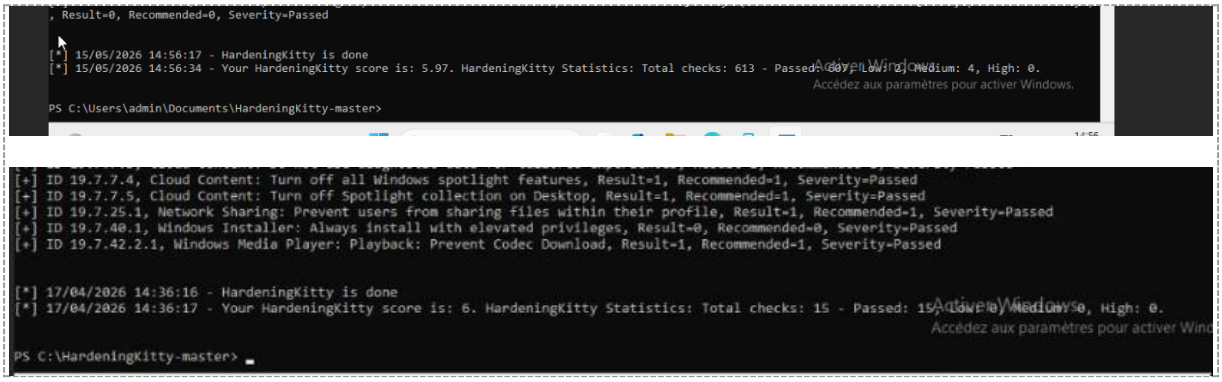
Capture 10 — Snapshot Proxmox de la VM Windows 11 de référence

Cf capture écran ci-dessous



Capture 11 — Audit HardeningKitty initial (avant durcissement)

Cf capture écran ci-dessous



Capture 12 — Audit HardeningKitty final (après durcissement)

Ce durcissement a néanmoins eu des effets de bord qu'il a fallu diagnostiquer et corriger : certains paramètres bloquaient l'accès aux navigateurs (verrouillages, AppLocker bloquant Edge). Cette phase m'a appris qu'un durcissement ne s'applique jamais aveuglément : il doit être testé, et chaque blocage doit être analysé pour trouver l'équilibre entre sécurité et utilisabilité. C'est cette image durcie qui a ensuite servi de base à la capture et au déploiement MDT décrits plus loin.

2.1.4. Sécurisation de l'AD avec les Microsoft Security Baseline (GPO)

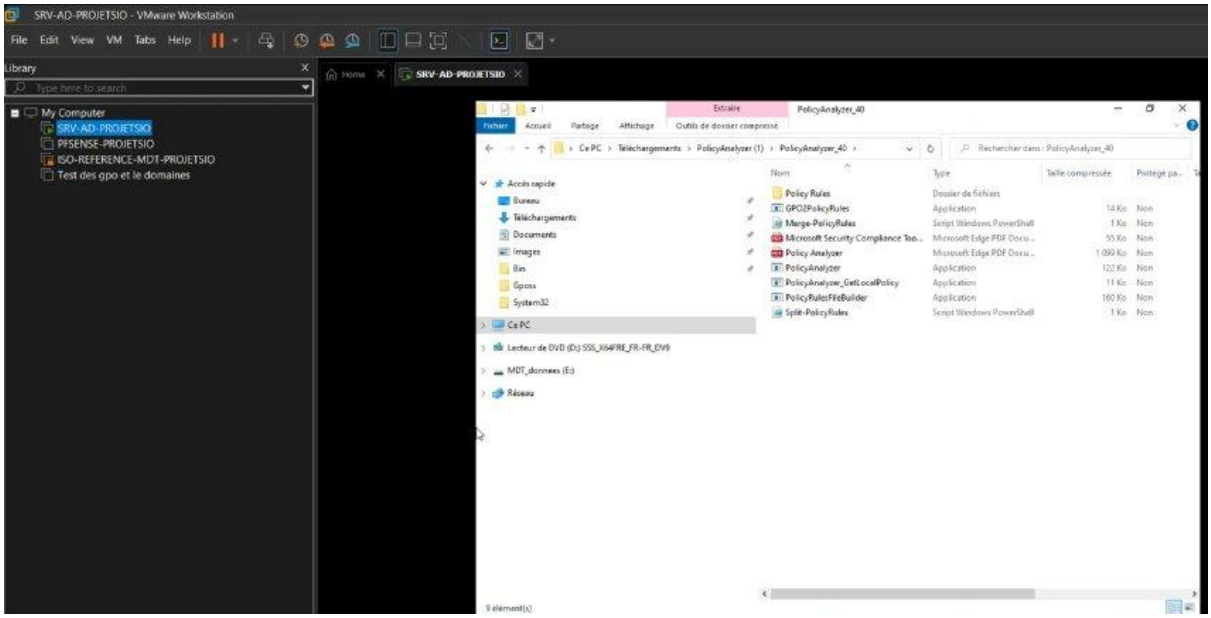
Après les postes clients, j'ai sécurisé le serveur et le domaine en déployant les **Microsoft Security Baseline (MSB)**, c'est-à-dire l'ensemble des GPO de sécurité recommandées par Microsoft pour Windows Server 2022.

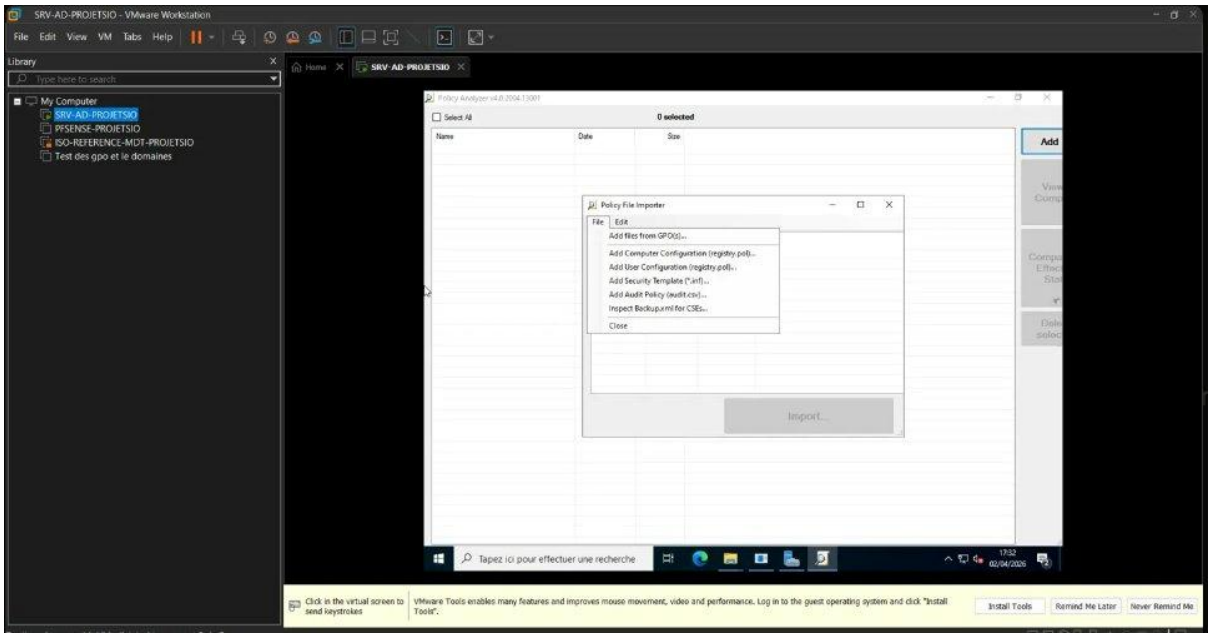
La mise en place s'est déroulée en plusieurs étapes :

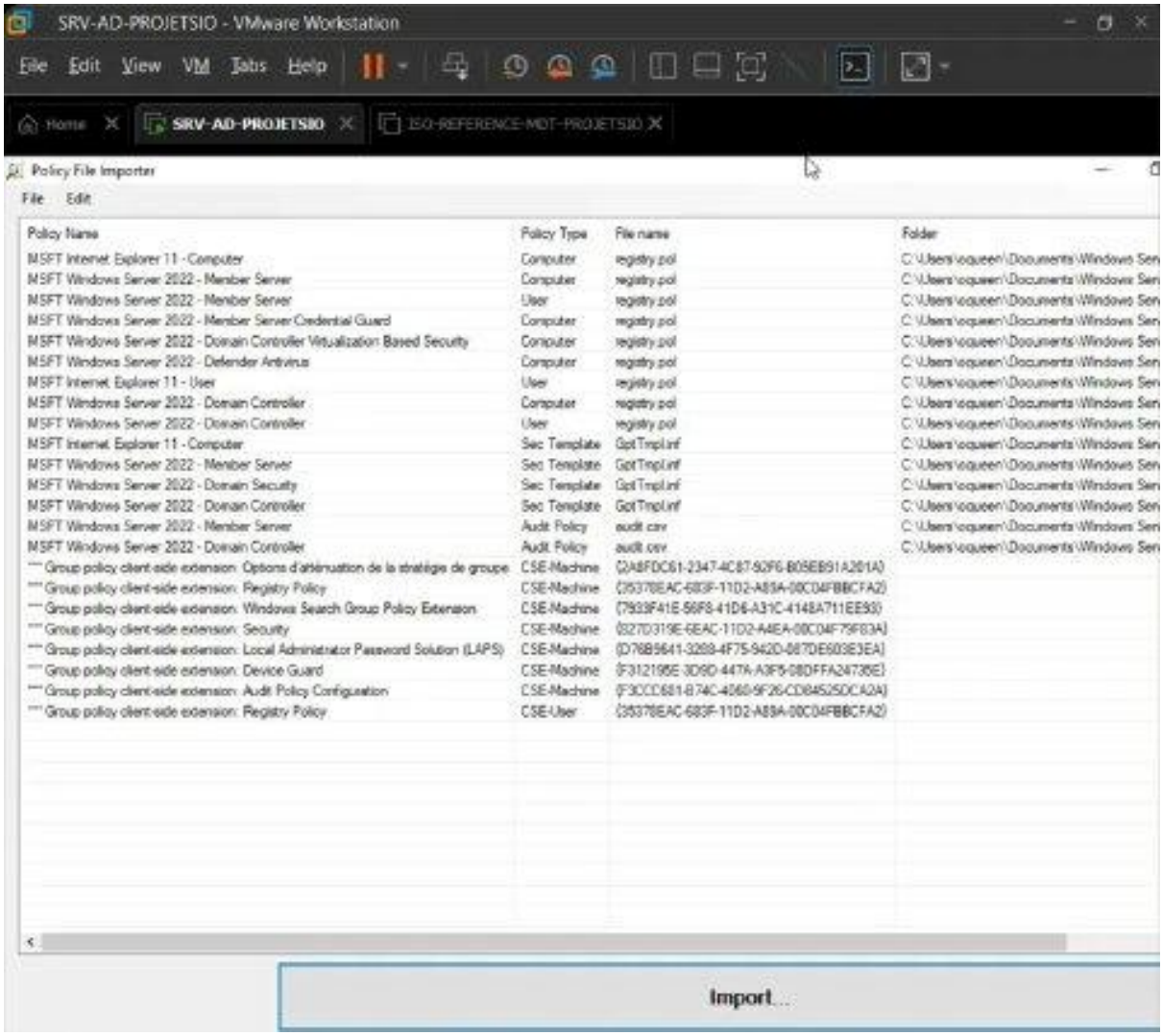
- Analyse des baselines avec **Policy Analyzer**, qui permet d'importer et de comparer les paramètres MSFT Windows Server 2022 — Member Server avec la configuration existante **(13)** ;

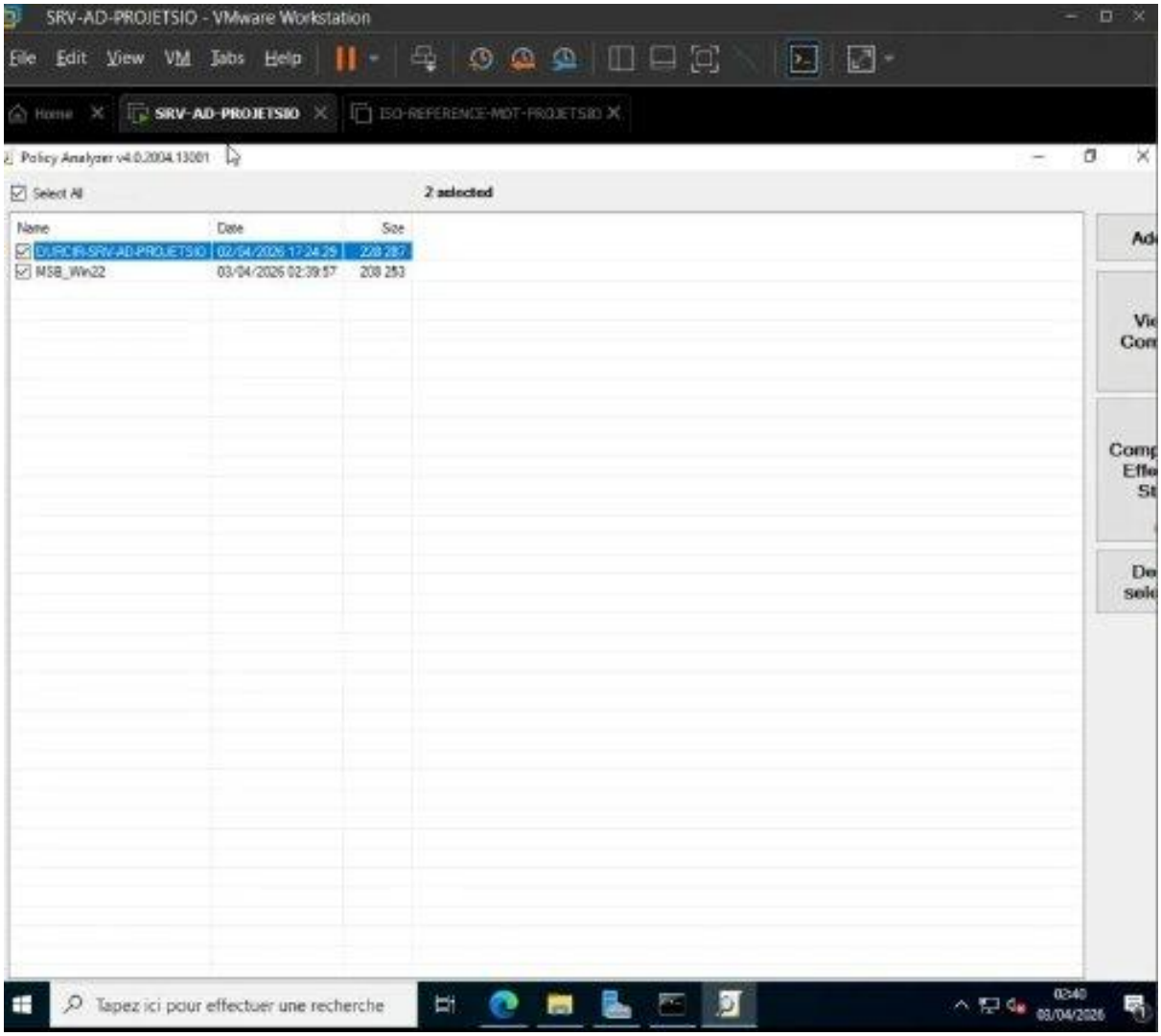
- Application locale des stratégies avec l'outil **LGPO** sur le serveur **(14)** ;
- Import de la baseline dans la **console de gestion des stratégies de groupe (GPMC)** sous la forme d'une GPO nommée MSB-WinServer2022, liée au domaine sleepingforest.local **(15)**.

Cf capture écran ci-dessous



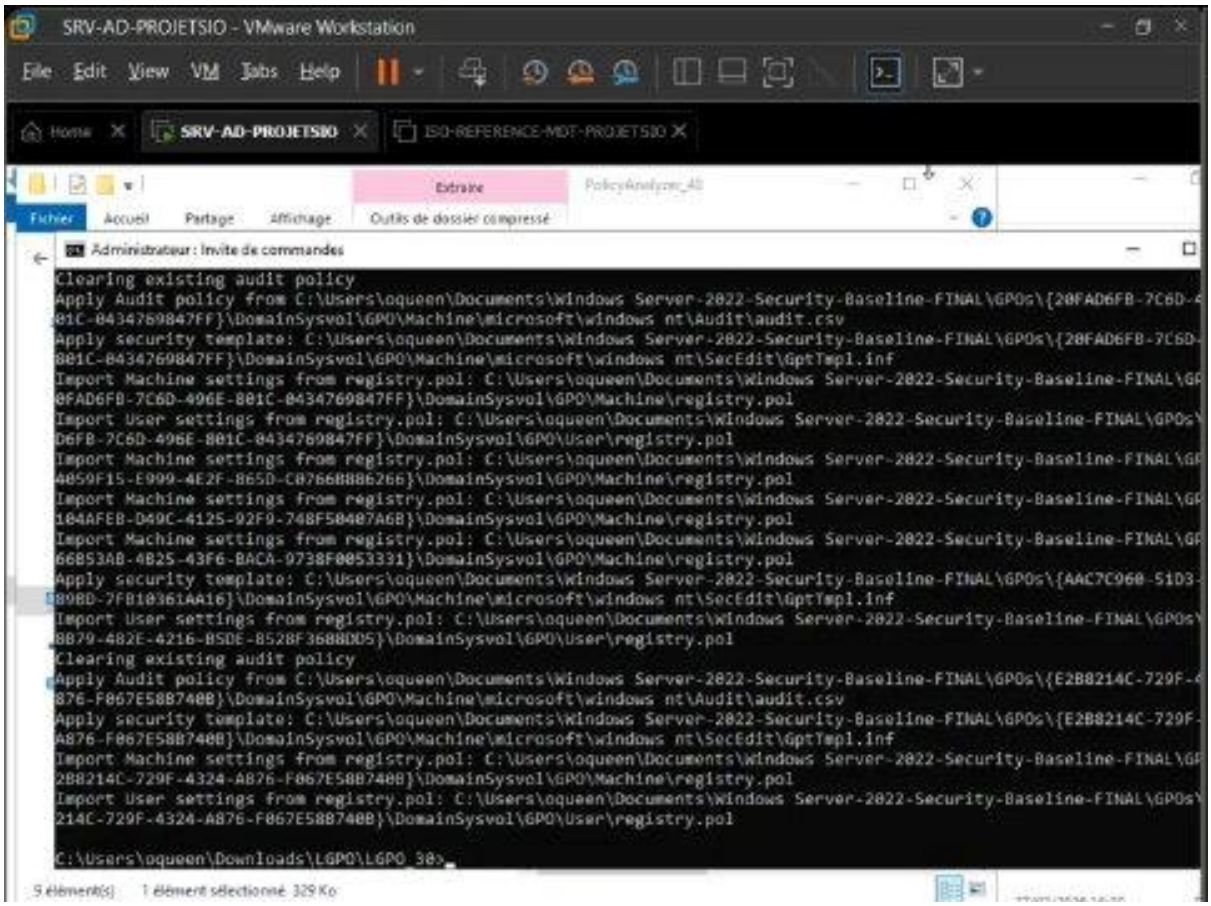



SRV-AD-PROJETSIO - VMware Workstation
File Edit View VM Tabs Help
Home
SRV-AD-PROJETSIO
ISO-REFERENCE-MDT-PROJETSIO
Policy File Importer
File Edit
Policy Name
Policy Type
File name
Folder
MSFT Internet Explorer 11 - Computer
Computer
registry.pol
MSFT Windows Server 2022 - Member Server
Computer
registry.pol
MSFT Windows Server 2022 - Member Server
User
registry.pol
MSFT Windows Server 2022 - Member Server Credential Guard
Computer
registry.pol
MSFT Windows Server 2022 - Domain Controller Virtualization Based Security
Computer
registry.pol
MSFT Windows Server 2022 - Defender Antivirus
Computer
registry.pol
MSFT Internet Explorer 11 - User
User
registry.pol
MSFT Windows Server 2022 - Domain Controller
Computer
registry.pol
MSFT Windows Server 2022 - Domain Controller
User
registry.pol
MSFT Internet Explorer 11 - Computer
Sec Template
GptTmpl.inf
MSFT Windows Server 2022 - Member Server
Sec Template
GptTmpl.inf
MSFT Windows Server 2022 - Domain Security
Sec Template
GptTmpl.inf
MSFT Windows Server 2022 - Domain Controller
Sec Template
GptTmpl.inf
MSFT Windows Server 2022 - Member Server
Audit Policy
audit.csv
MSFT Windows Server 2022 - Domain Controller
Audit Policy
audit.csv
*** Group policy client-side extension: Options d'atténuation de la stratégie de groupe
CSE-Machine
{2A8FDC61-2347-4C87-92F6-B05EB91A261A}
*** Group policy client-side extension: Registry Policy
CSE-Machine
{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
*** Group policy client-side extension: Windows Search Group Policy Extension
CSE-Machine
{7933F41E-56F8-41D6-A31C-4148A711EE93}
*** Group policy client-side extension: Security
CSE-Machine
{827D319E-6EAC-11D2-A4EA-00C04F79F83A}
*** Group policy client-side extension: Local Administrator Password Solution (LAPS)
CSE-Machine
{D76B9641-3288-4F75-942D-087DE603E3EA}
*** Group policy client-side extension: Device Guard
CSE-Machine
{F312195E-3D9D-447A-A3F5-08DFFA24735E}
*** Group policy client-side extension: Audit Policy Configuration
CSE-Machine
{F3CCC681-B74C-4060-9F26-CD84525DCA2A}
*** Group policy client-side extension: Registry Policy
CSE-User
{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
Import...



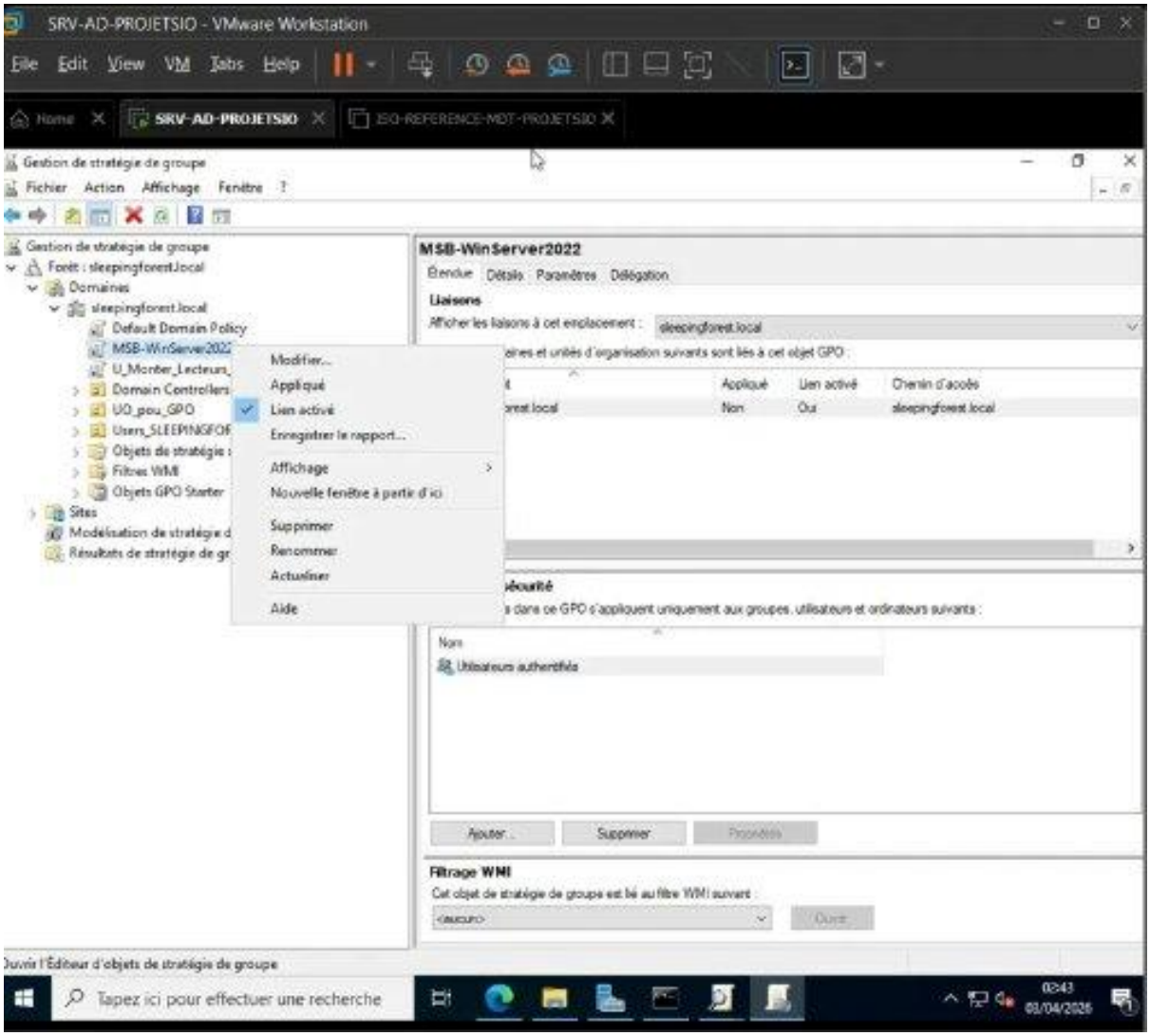
Capture 13 — Import et comparaison des baselines dans Policy Analyzer

Cf capture écran ci-dessous



Capture 14 — Application des stratégies avec LGPO

Cf capture écran ci-dessous

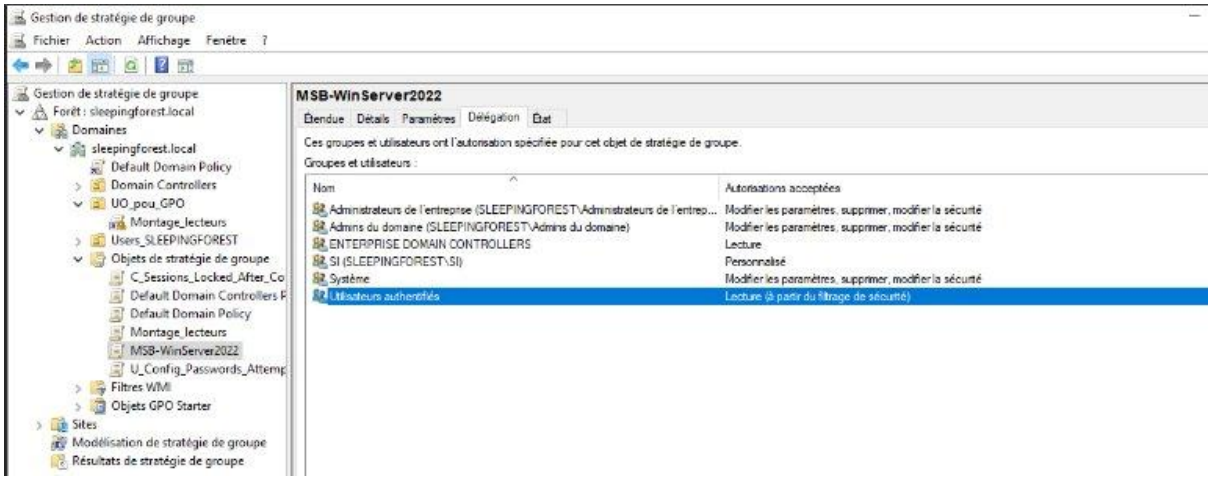


Capture 15 — GPO MSB-WinServer2022 dans la GPMC

Un point important de cette réalisation concerne le **filtrage de sécurité** de la GPO. Pour que la baseline s'applique à l'ensemble des employés tout en préservant les capacités d'administration de l'équipe informatique, j'ai configuré :

- « **Utilisateurs authentifiés** » dans le filtrage de sécurité, afin que la GPO s'applique à tout le monde ;
- Une autorisation « **Refuser — Appliquer la stratégie de groupe** » sur le groupe **SI** dans l'onglet Délégation : le « Refuser » étant toujours prioritaire dans Active Directory, les administrateurs sont automatiquement exclus de la baseline **(16)**.

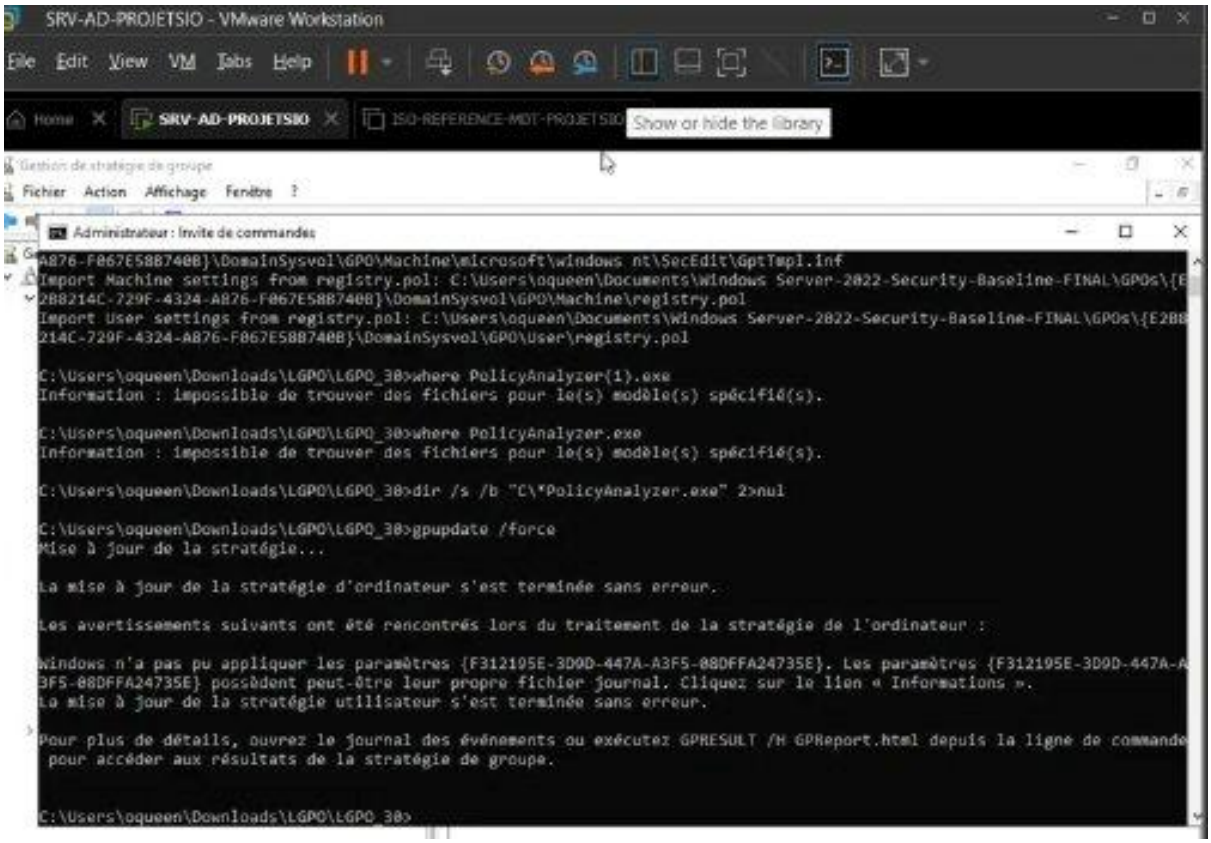
Cf capture écran ci-dessous



Capture 16 — Filtrage de sécurité et délégation (Refuser pour le groupe SI)

Après un gpupdate /force, la mise à jour des stratégies d'ordinateur et d'utilisateur s'est terminée sans erreur sur l'ensemble du domaine **(17)**. J'ai également constaté que la baseline bloquait volontairement **Internet Explorer** : il ne s'agissait pas d'une GPO mal configurée mais d'une mesure de sécurité intentionnelle de Microsoft, ce navigateur obsolète devant être remplacé par Edge. Ce diagnostic m'a permis de comprendre en profondeur l'ordre d'application et la portée (utilisateur ou ordinateur) des stratégies de groupe.

Cf capture écran ci-dessous



Capture 17 — Résultat du gpupdate /force sans erreur

2.1.5. Mise en place du serveur de déploiement (MDT / WDS)

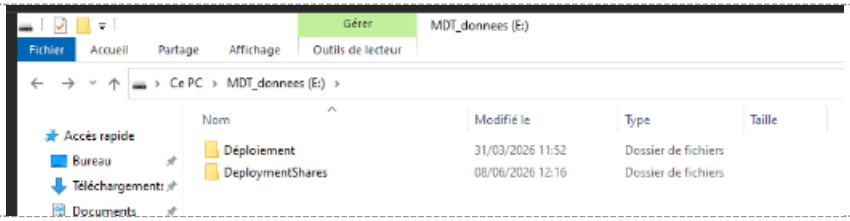
La dernière brique de la partie système est la mise en place d'un **serveur de déploiement** sur le contrôleur de domaine, afin d'installer automatiquement des postes Windows 11 durcis, à jour et directement intégrés au domaine sleepingforest.local. Cette solution repose sur le **Microsoft Deployment Toolkit (MDT)** et son interface **Deployment Workbench**, couplés au rôle **WDS (Windows Deployment Services)** pour le démarrage des postes par le réseau (boot PXE).

La construction de la chaîne de déploiement s'est déroulée ainsi :

- Ajout d'un disque dédié **MDT_Données** sur le serveur, qui héberge le **Deployment Share** : c'est dans cet espace que sont stockés les images .wim, les captures, les pilotes, les applications et les séquences de tâches **(18)** ;
- Import de l'image d'installation Windows 11 dans le Deployment Workbench et **injection des pilotes VirtIO** (contrôleur SCSI) dans l'environnement **WinPE** : sans ces pilotes, l'environnement de préinstallation ne voyait pas les disques des VM Proxmox, ce qui provoquait l'erreur MDT 5456 lors des déploiements **(19)** ;

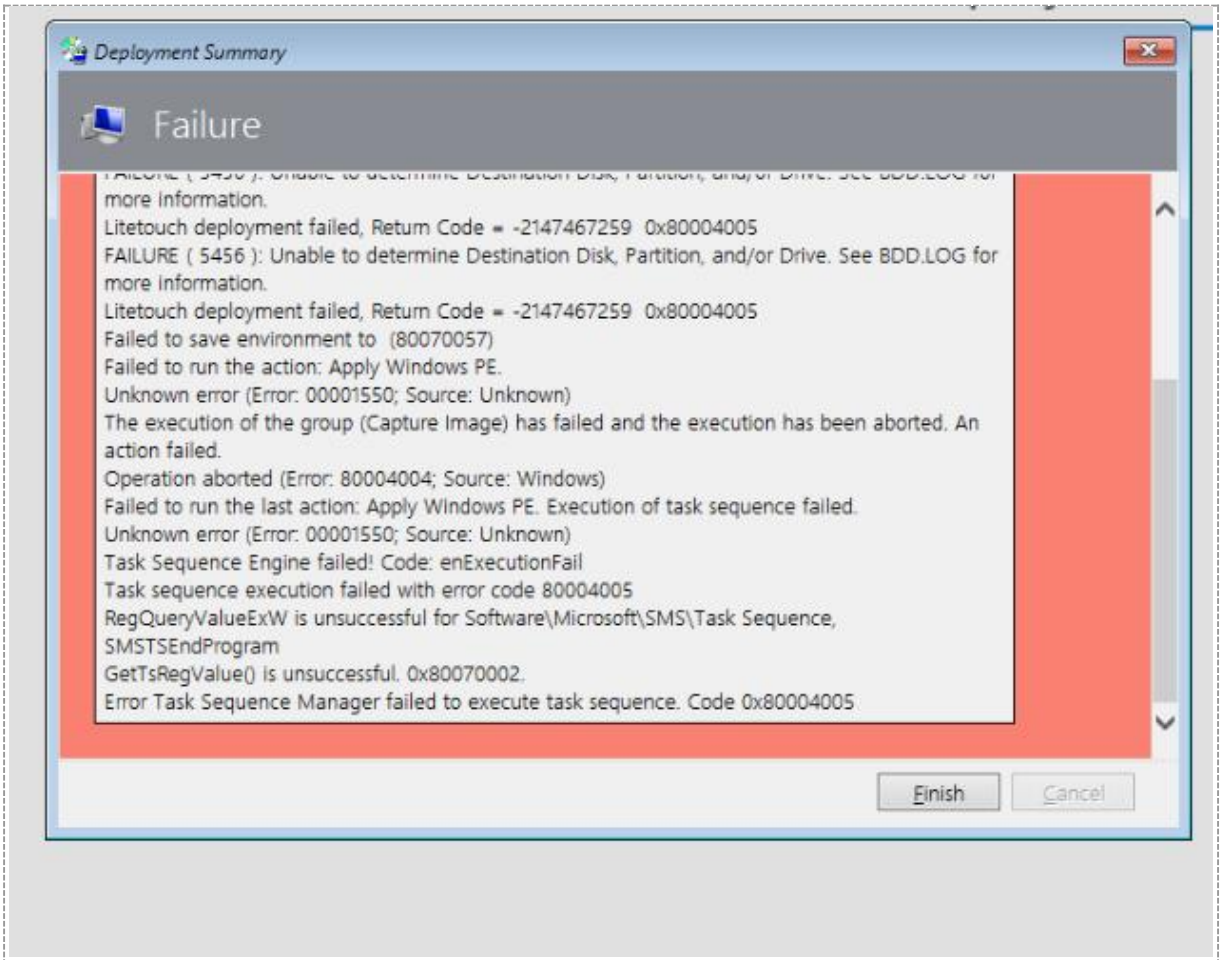
- Régénération des images de boot **LiteTouch** et import de celles-ci dans **WDS** afin de permettre le démarrage PXE des postes clients **(20)** ;

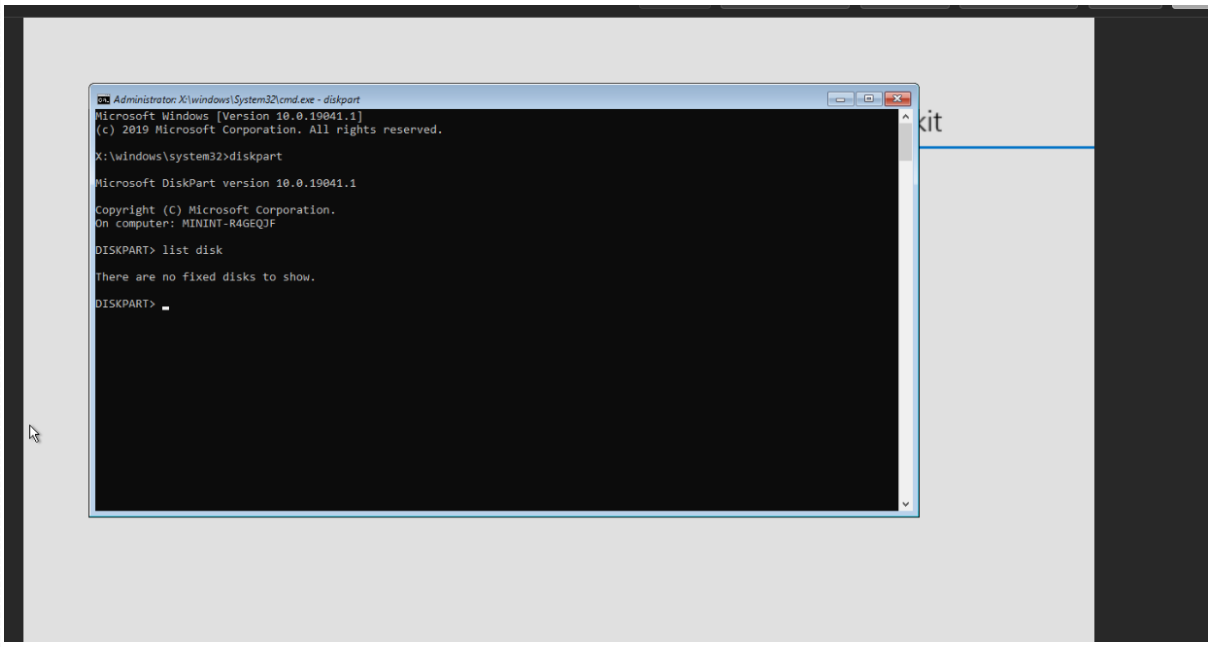
Cf capture écran ci-dessous

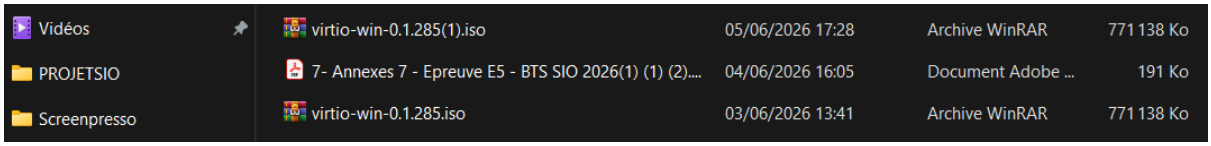


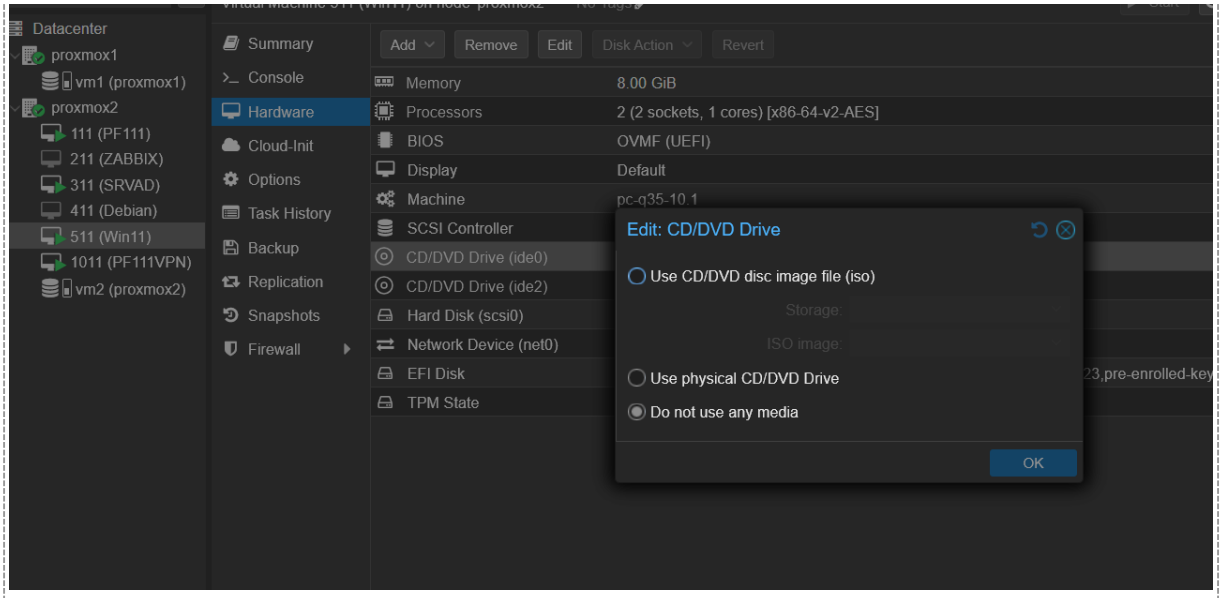
Capture 18 — Deployment Share sur le disque MDT_Données dans le Deployment Workbench

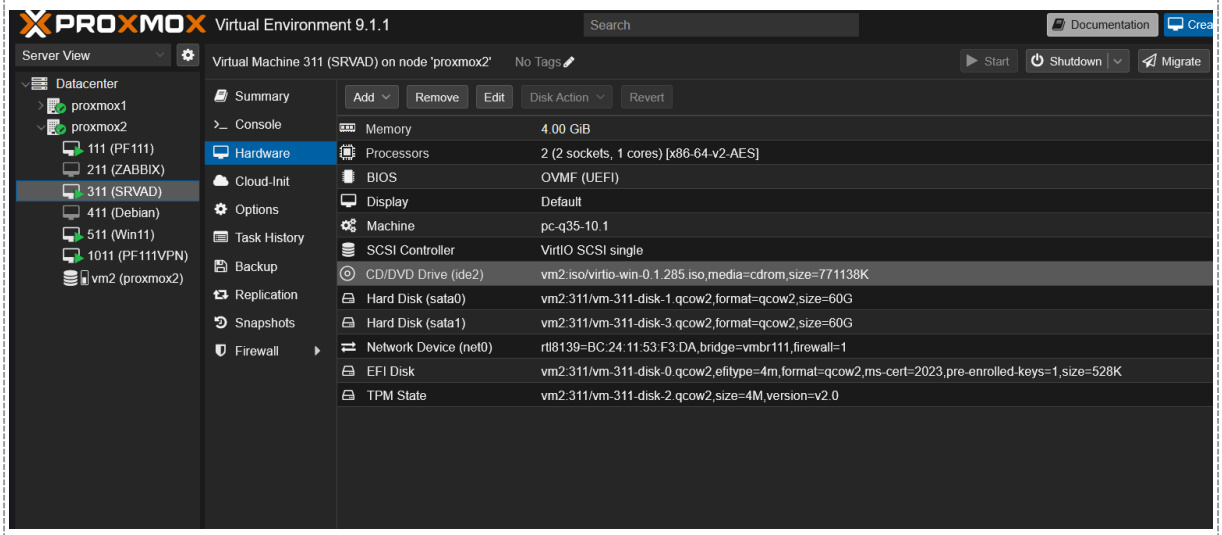
Cf capture écran ci-dessous

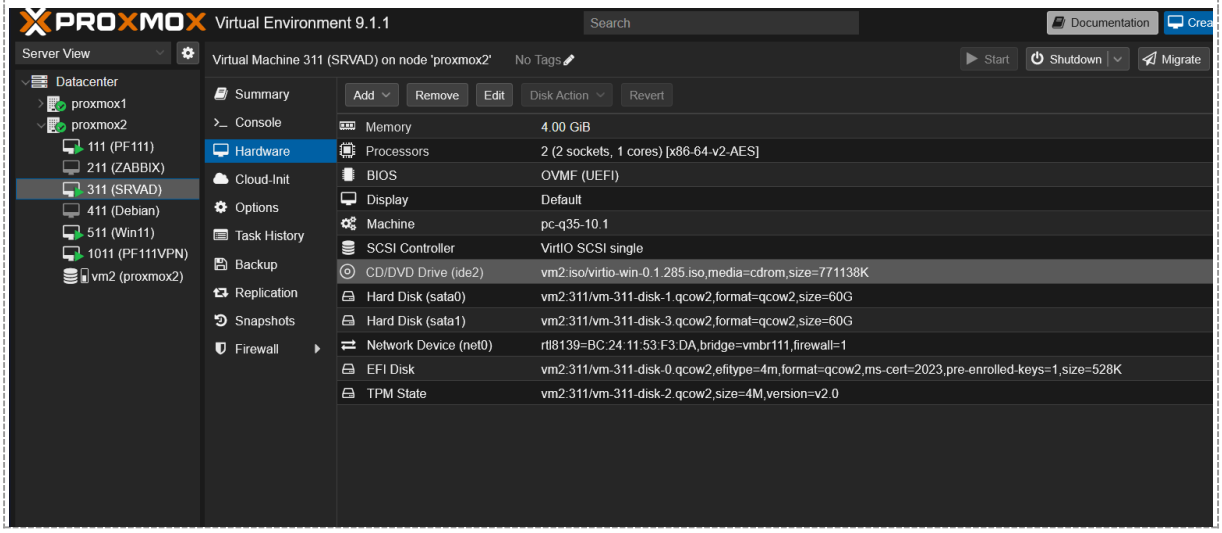






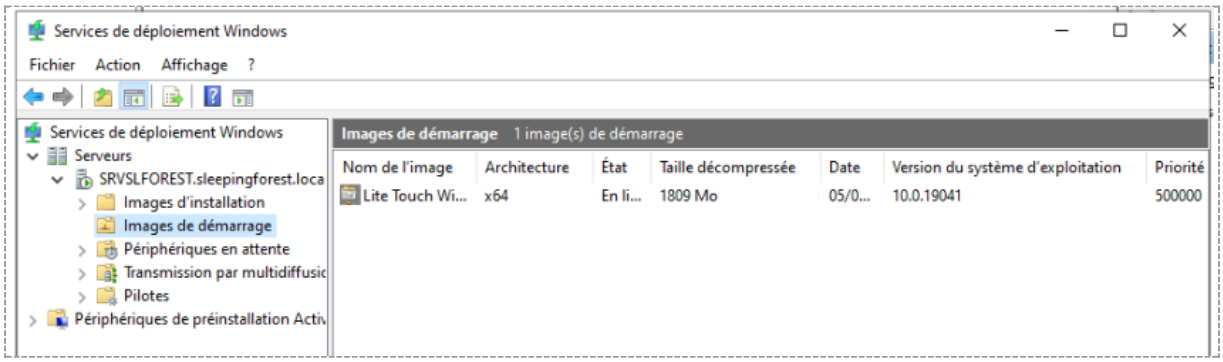






Capture 19 — Import des pilotes VirtIO dans WinPE (Out-of-Box Drivers)

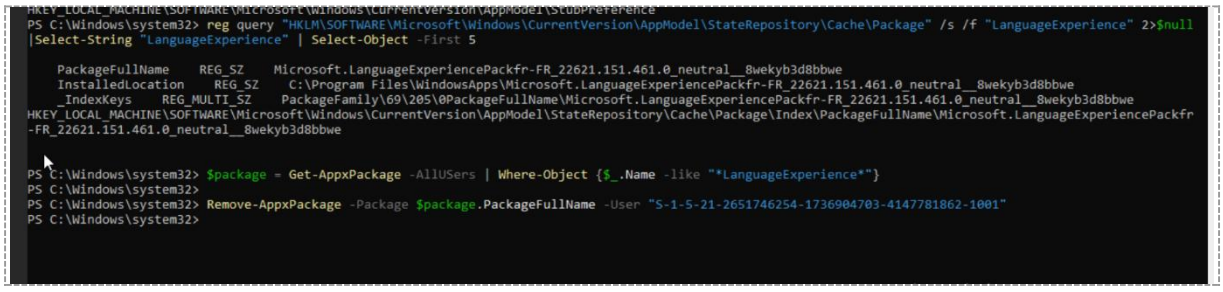
Cf capture écran ci-dessous



Capture 20 — Images de boot LiteTouch importées dans WDS

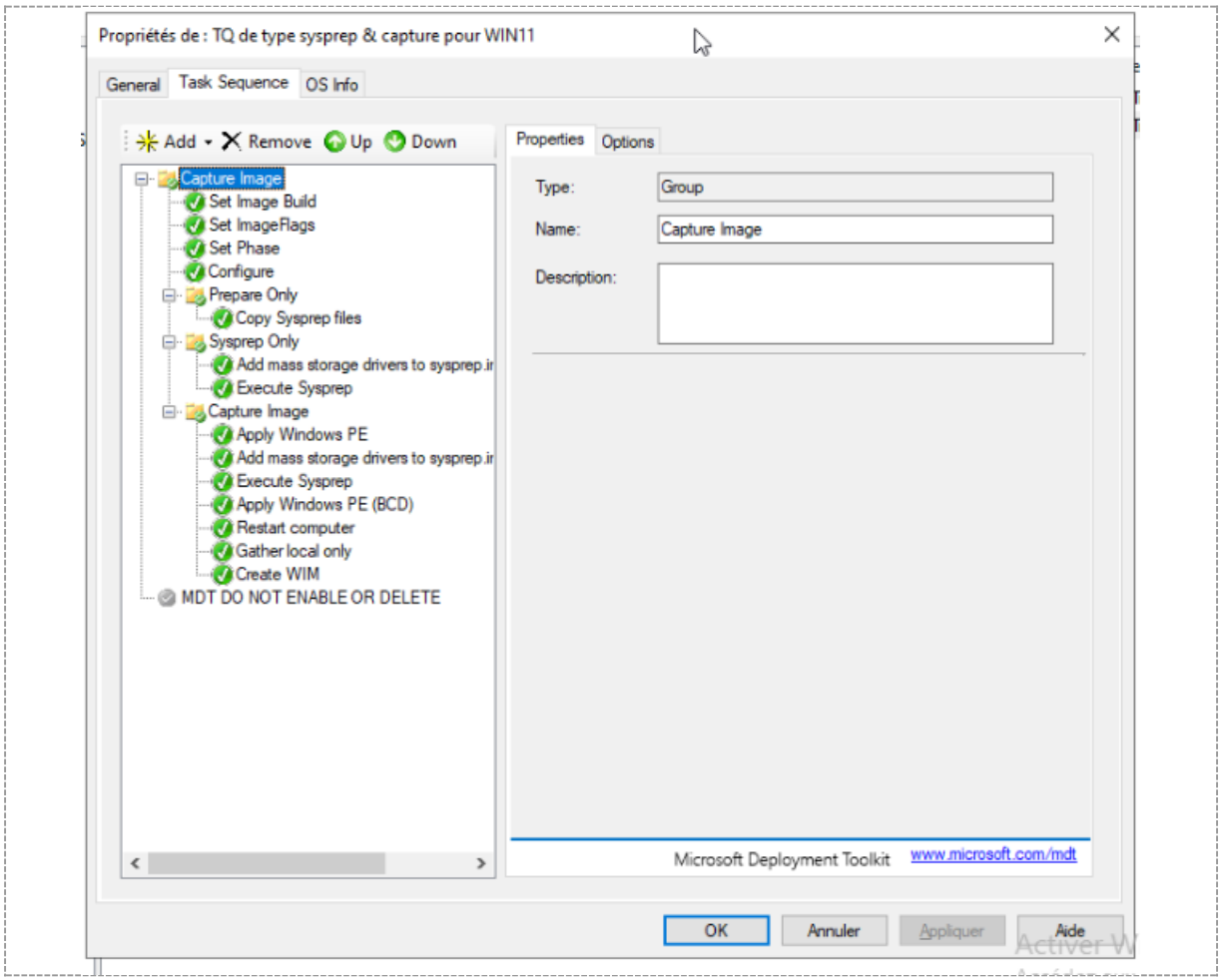
- Préparation de la VM de référence durcie avec **Sysprep** (généralisation de l'image). Cette étape a nécessité un vrai travail de diagnostic : Sysprep échouait à cause de paquets AppX provisionnés pour un seul utilisateur (notamment LanguageExperiencePackfr-FR et WinRAR.ShellExtension) ainsi que d'opérations de renommage de fichiers en attente (PendingFileRenameOperations) générées par les mises à jour automatiques d'Edge. La suppression de ces paquets et le nettoyage des opérations en attente ont permis la généralisation de l'image **(21)** ;
- **Capture de l'image de référence** au format .wim (WIN11-SYSPREP.wim) via une séquence de tâches de capture, l'image étant automatiquement déposée dans le dossier Captures du Deployment Share **(22)** ;
- Création de la séquence de tâches de déploiement **DEPLOY-WIN11-CIS** basée sur l'image capturée, incluant l'installation automatique d'applications (KeePass, PDFGear, VLC) et la **jonction automatique au domaine** sleepingforest.local configurée dans le fichier CustomSettings.ini **(23)**.

Cf capture écran ci-dessous



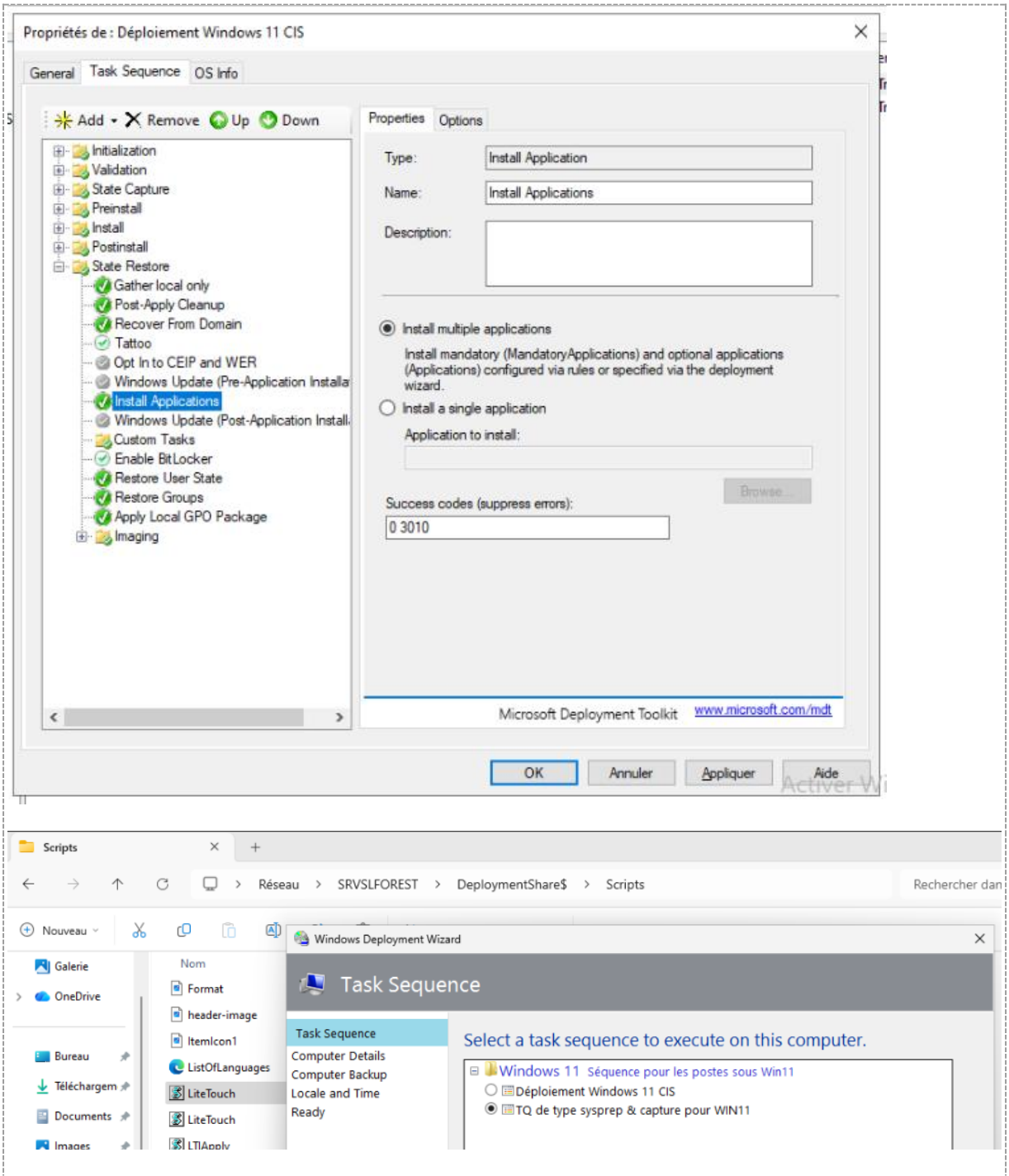
Capture 21 — Résolution des erreurs Sysprep (suppression des paquets AppX)

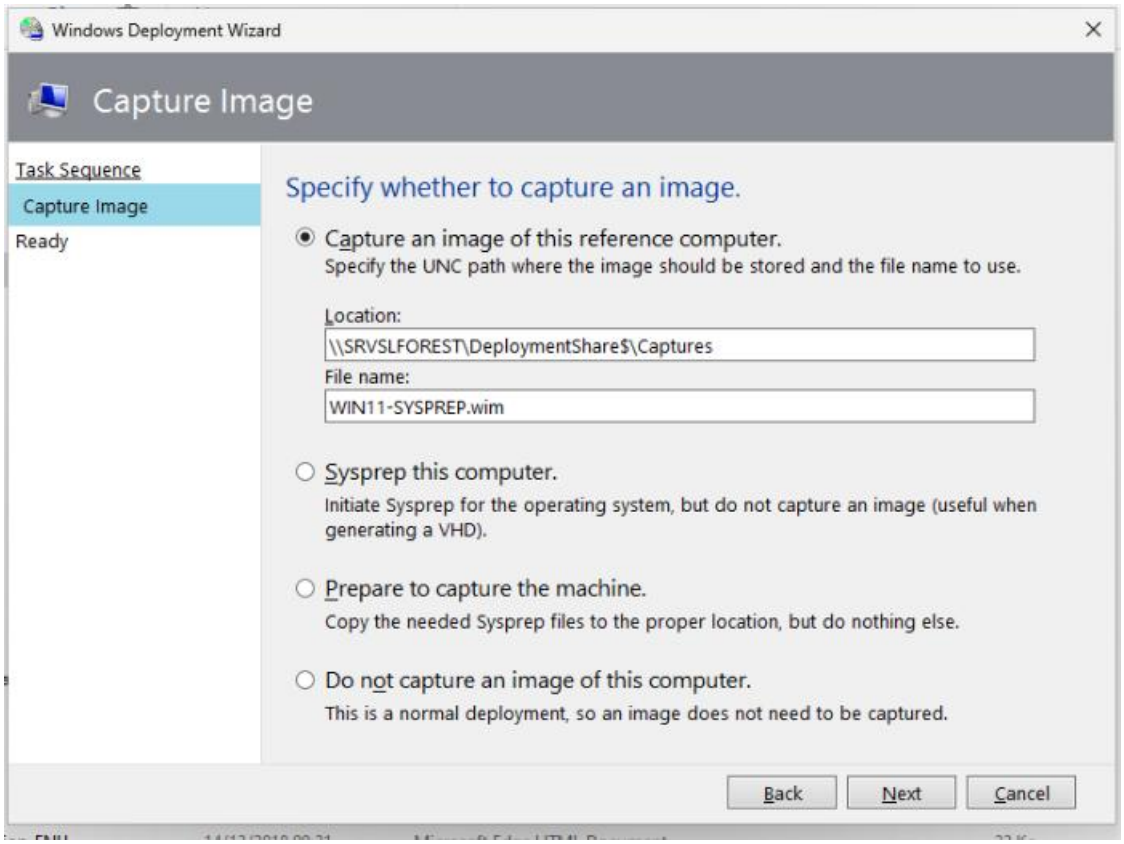
Cf capture écran ci-dessous

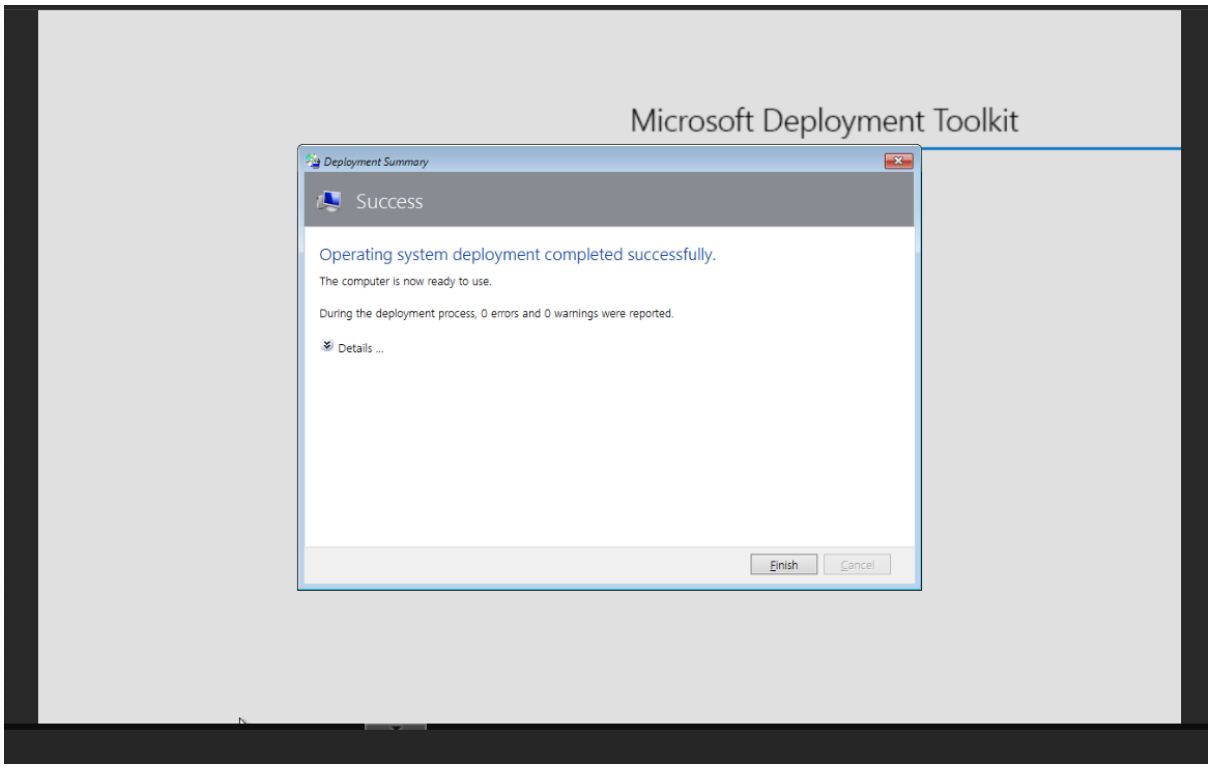


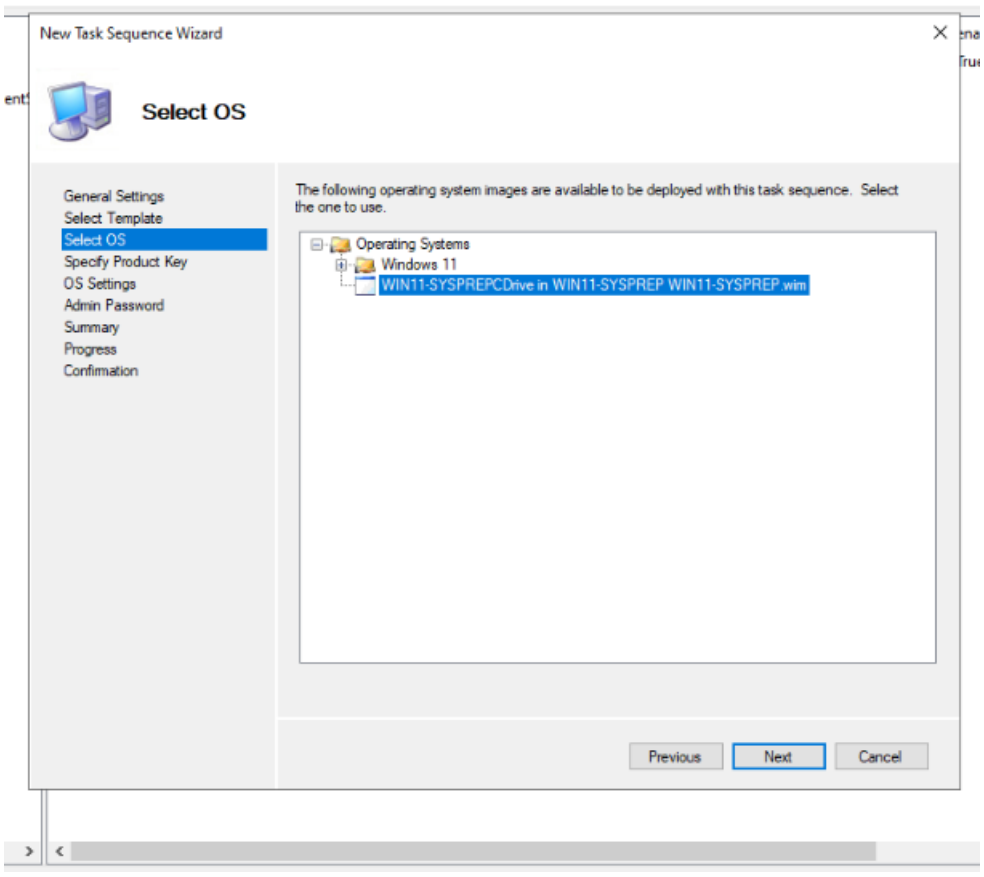
Capture 22 — Capture de l'image WIN11-SYSPREP.wim dans le Deployment Share

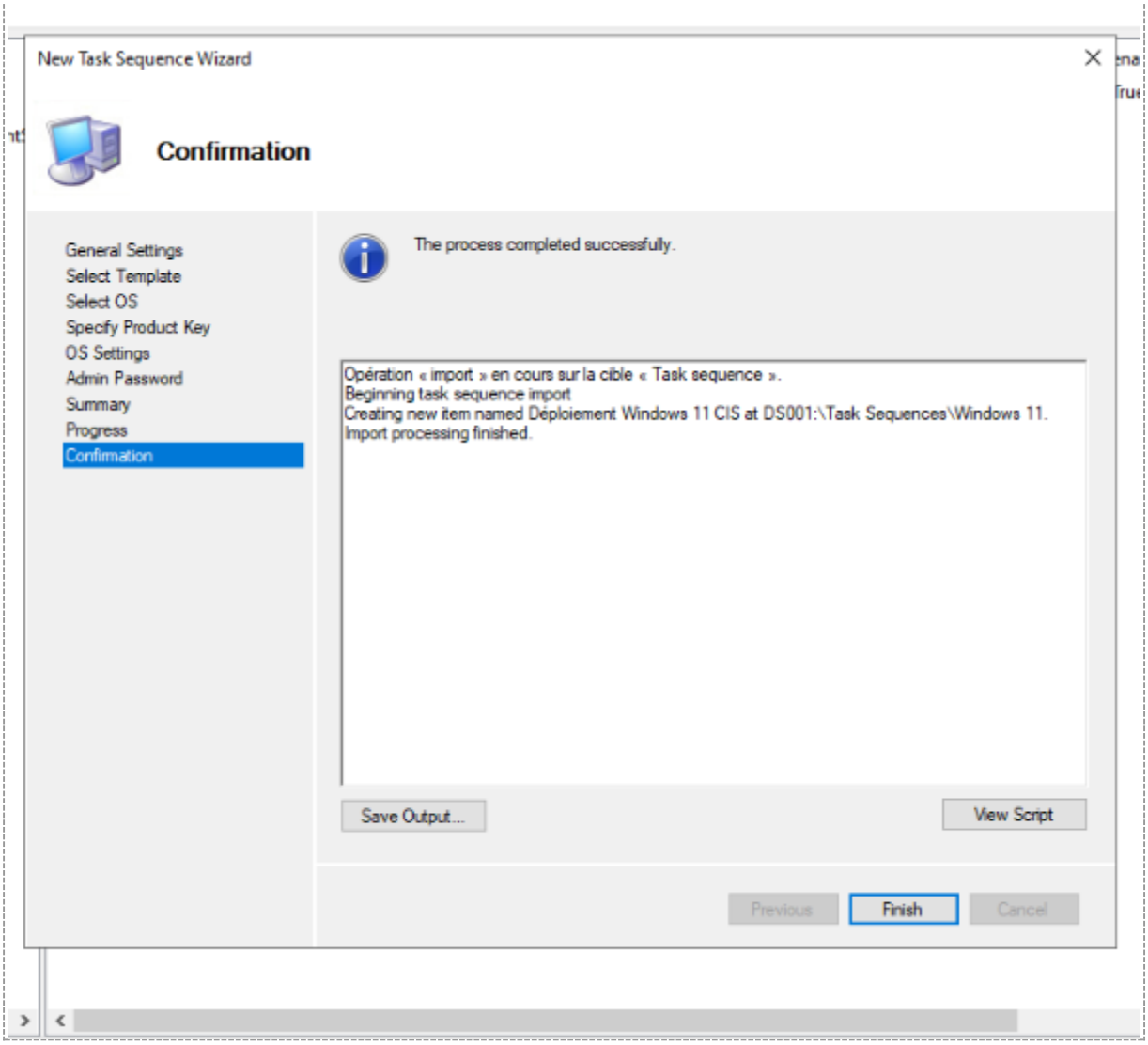
Cf capture écran ci-dessous




Windows Deployment Wizard
Capture Image
Task Sequence
Capture Image
Ready
Specify whether to capture an image.
Capture an image of this reference computer.
Specify the UNC path where the image should be stored and the file name to use.
Location:
\\SRVSLFOREST\DeploymentShare$\Captures
File name:
WIN11-SYSPREP.wim
Sysprep this computer.
Initiate Sysprep for the operating system, but do not capture an image (useful when generating a VHD).
Prepare to capture the machine.
Copy the needed Sysprep files to the proper location, but do nothing else.
Do not capture an image of this computer.
This is a normal deployment, so an image does not need to be captured.
Back
Next
Cancel


Microsoft Deployment Toolkit
Deployment Summary
Success
Operating system deployment completed successfully.
The computer is now ready to use.
During the deployment process, 0 errors and 0 warnings were reported.
Details ...
Finish
Cancel

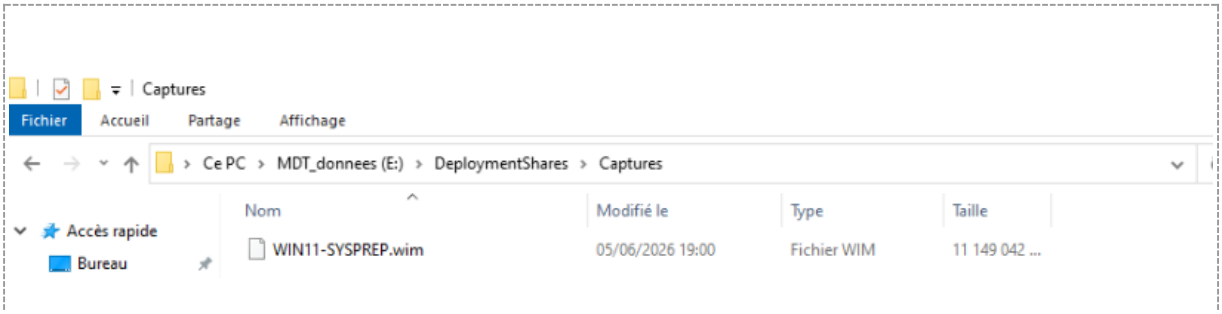

New Task Sequence Wizard
Select OS
General Settings
Select Template
Select OS
Specify Product Key
OS Settings
Admin Password
Summary
Progress
Confirmation
The following operating system images are available to be deployed with this task sequence. Select the one to use.
Operating Systems
Windows 11
WIN11-SYSPREPCDrive in WIN11-SYSPREP WIN11-SYSPREP.wim
Previous
Next
Cancel

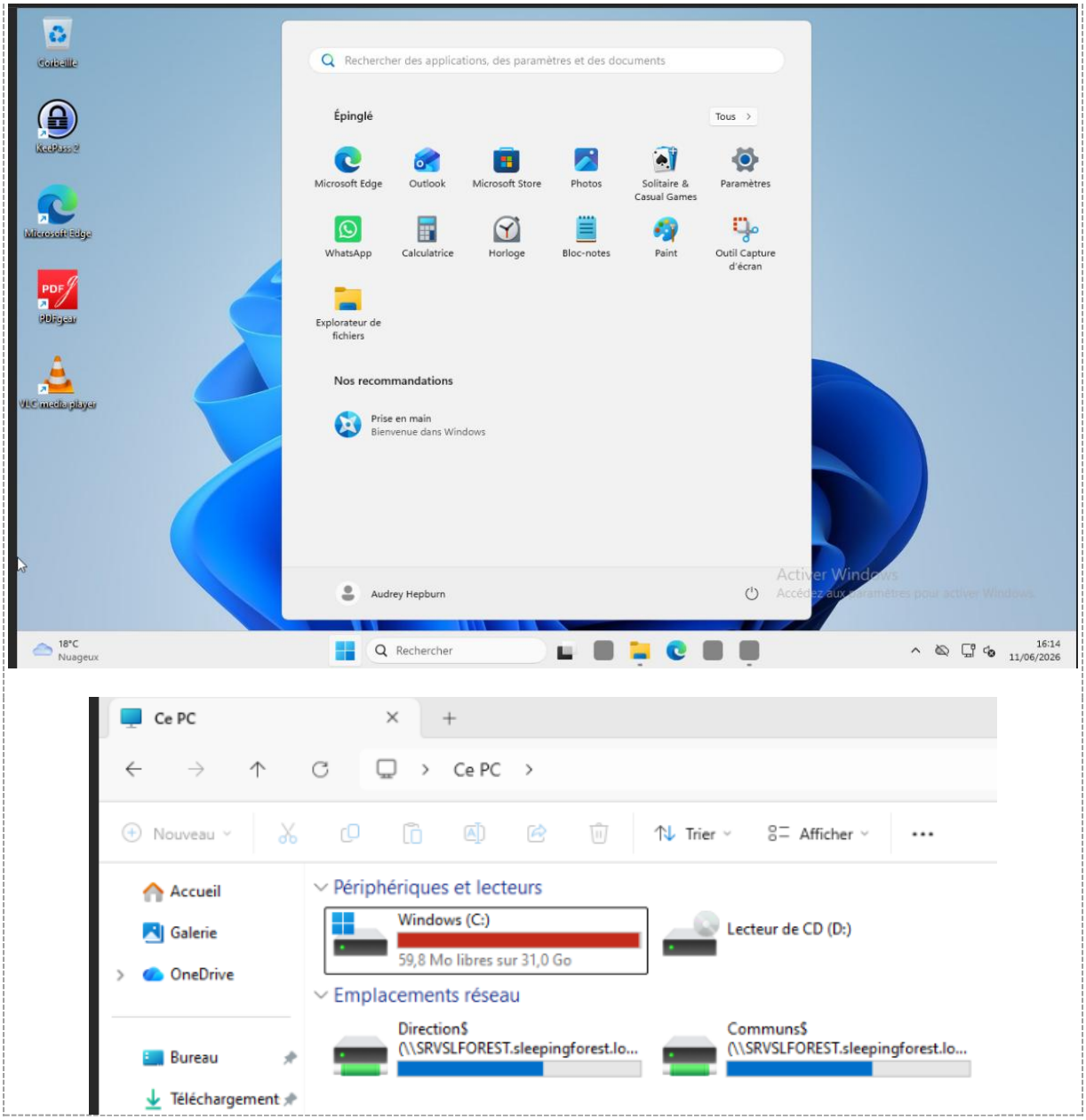


Capture 23 — Séquence de tâches DEPLOY-WIN11-CIS et applications associées

Le test final a consisté à démarrer une nouvelle VM cliente en boot réseau : celle-ci a chargé LiteTouch, exécuté la séquence DEPLOY-WIN11-CIS, installé l'image Windows 11 durcie avec ses applications, puis rejoint automatiquement le domaine. À sa première connexion, l'utilisateur retrouve ses lecteurs réseaux et l'ensemble des GPO de Sleeping Forest **(24)**. L'entreprise dispose ainsi d'une chaîne de déploiement complète, garantissant l'uniformité et la sécurité de tout son parc informatique.

Cf capture écran ci-dessous





Capture 24 — Déploiement LiteTouch réussi sur un poste client et jonction au domaine

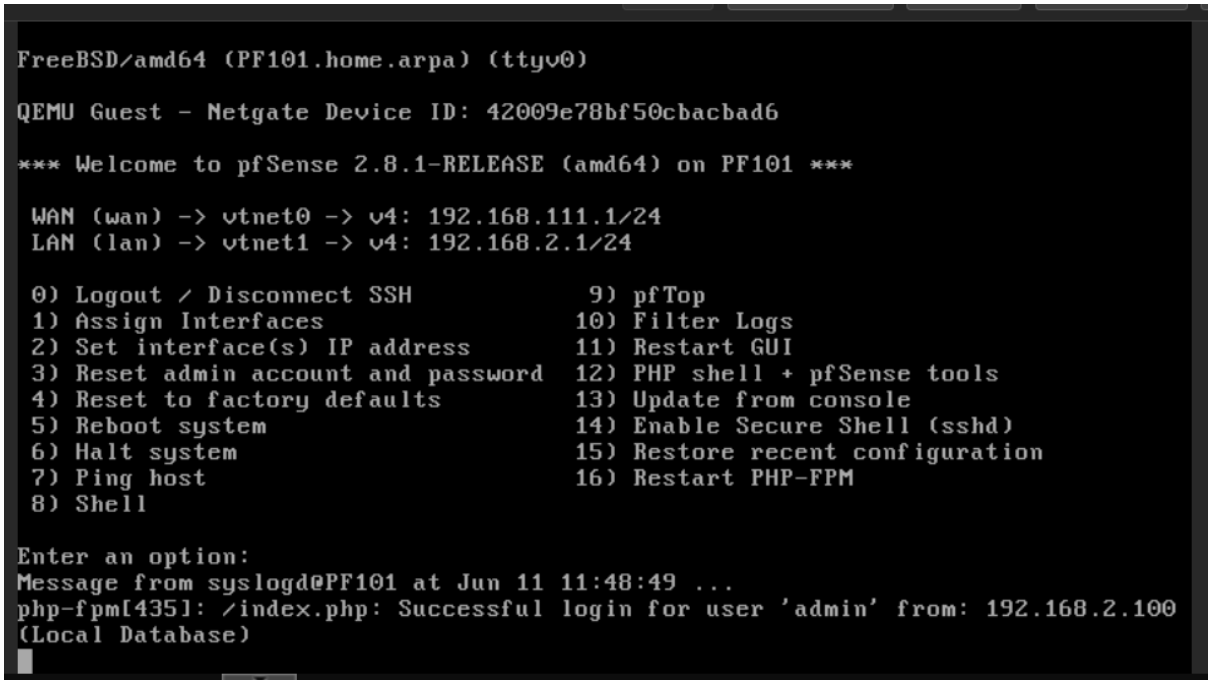
2.2. RÉSEAU

2.2.1. Configuration du pare-feu pfSense et mise en place des règles

Le pare-feu **pfSense** constitue la porte d'entrée et de sortie de toute l'infrastructure de Sleeping Forest : il fait office de **passerelle** entre le réseau interne (LAN 192.168.2.0/24) et l'extérieur (WAN sur le réseau 172.16.2.0/24, relié au bridge Proxmox vmbr111), et de **pare-feu** filtrant l'ensemble des flux.

J'ai d'abord configuré les interfaces de la VM pfSense : assignation des interfaces WAN et LAN, adressage du LAN en 192.168.2.1/24 (passerelle des machines du domaine, dont SRVSLFOREST en 192.168.2.10) et adressage du WAN sur le réseau de l'hyperviseur **(25)**.

Cf capture écran ci-dessous



La construction des règles repose sur les principes fondamentaux d'un pare-feu à états (stateful) :

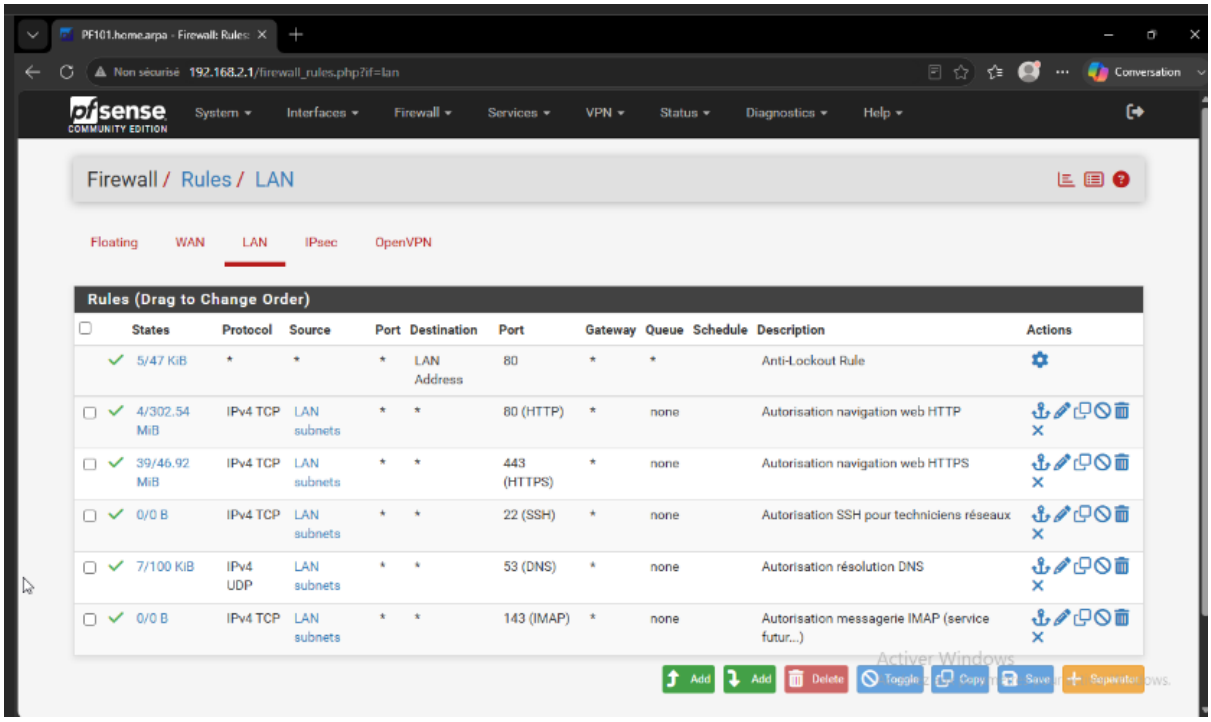
Capture 25 — Interfaces WAN et LAN de pfSense

- pfSense lit les règles **de haut en bas** et s'arrête à la première correspondance ;
- La philosophie appliquée est le **default deny** : tout ce qui n'est pas explicitement autorisé est bloqué ;
- Grâce à la **table d'états**, seul le trafic initiateur doit être autorisé, les réponses étant automatiquement acceptées.

Sur l'interface **LAN**, j'ai mis en place le jeu de règles suivant **(26)** :

- Conservation de la règle **anti-lockout**, qui garantit de ne jamais perdre l'accès à l'interface d'administration de pfSense ;
- Autorisation de l'**ICMP** pour les diagnostics réseau (ping) ;
- Autorisation de la **navigation web**, via deux règles autorisant le trafic TCP du LAN vers les ports 80 (HTTP) et 443 (HTTPS) ;
- Autorisation de la **résolution DNS** (port 53), du **SSH** (port 22) réservé aux interventions des techniciens réseaux, et de la messagerie **IMAP** (port 143), en prévision d'un futur service de messagerie ;
- **Désactivation** (et non suppression) des règles permissives par défaut « Default allow LAN to any », afin de documenter la transition vers une politique de filtrage explicite : tout flux non autorisé tombe désormais dans le deny implicite.

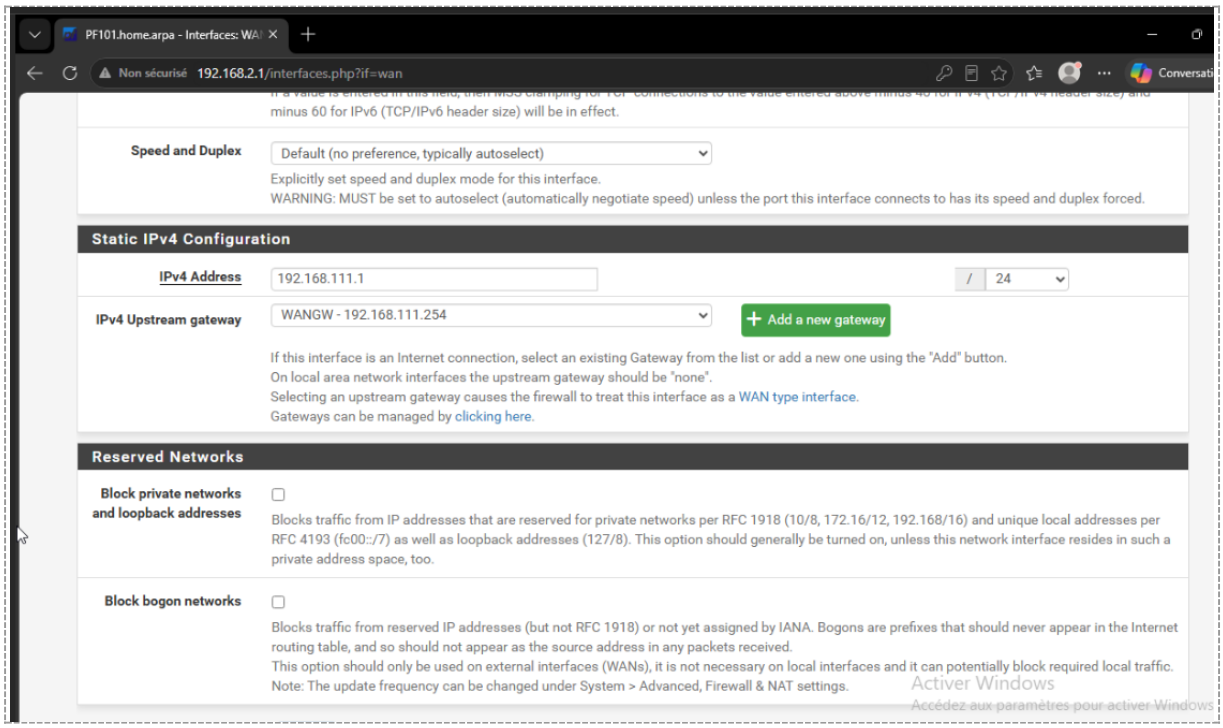
Cf capture écran ci-dessous



Côté **WAN**, la configuration s'appuie sur les protections natives de pfSense : blocage des réseaux privés (**RFC 1918**) et des **bogons** en entrée, aucun flux entrant n'étant autorisé vers l'infrastructure — le deny implicite fait le reste **(27)**. La translation d'adresses (**NAT Outbound**) est restée en mode automatique, pfSense générant lui-même la règle de traduction du réseau 192.168.2.0/24 vers l'adresse WAN **(28)**.

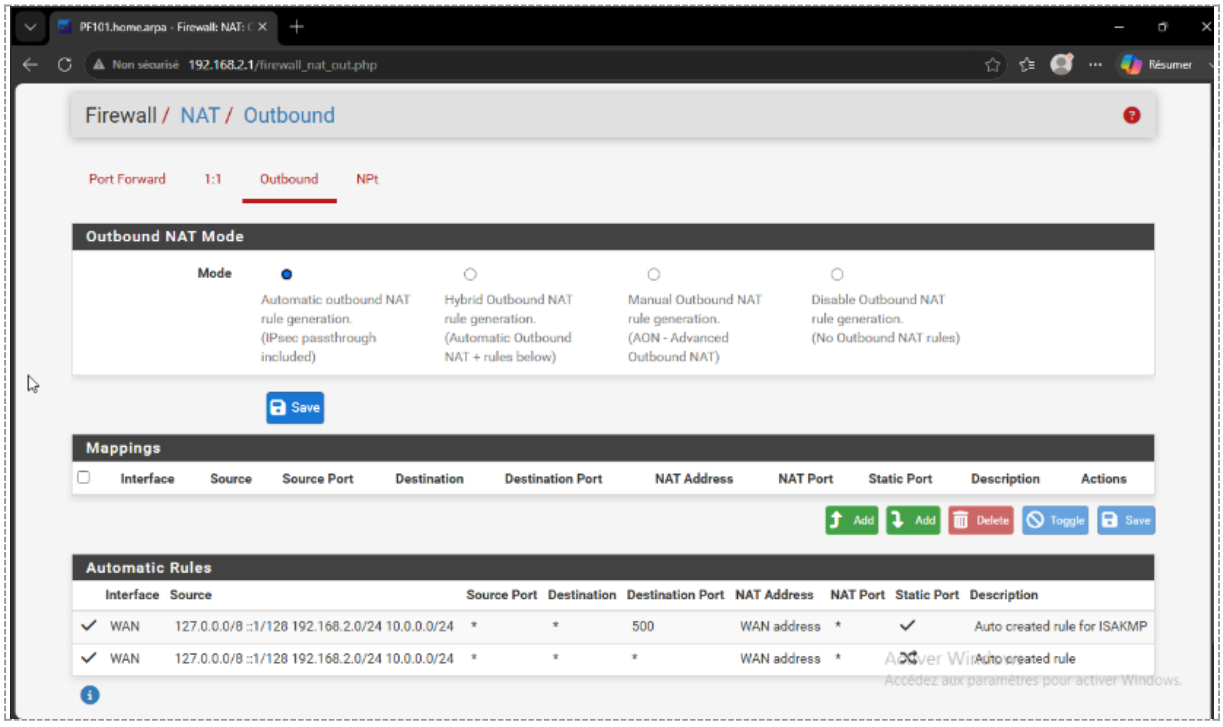
Capture 26 — Règles de filtrage de l'interface LAN

Cf capture écran ci-dessous



Capture 27 — Interface WAN : blocage RFC 1918 et bogons

Cf capture écran ci-dessous

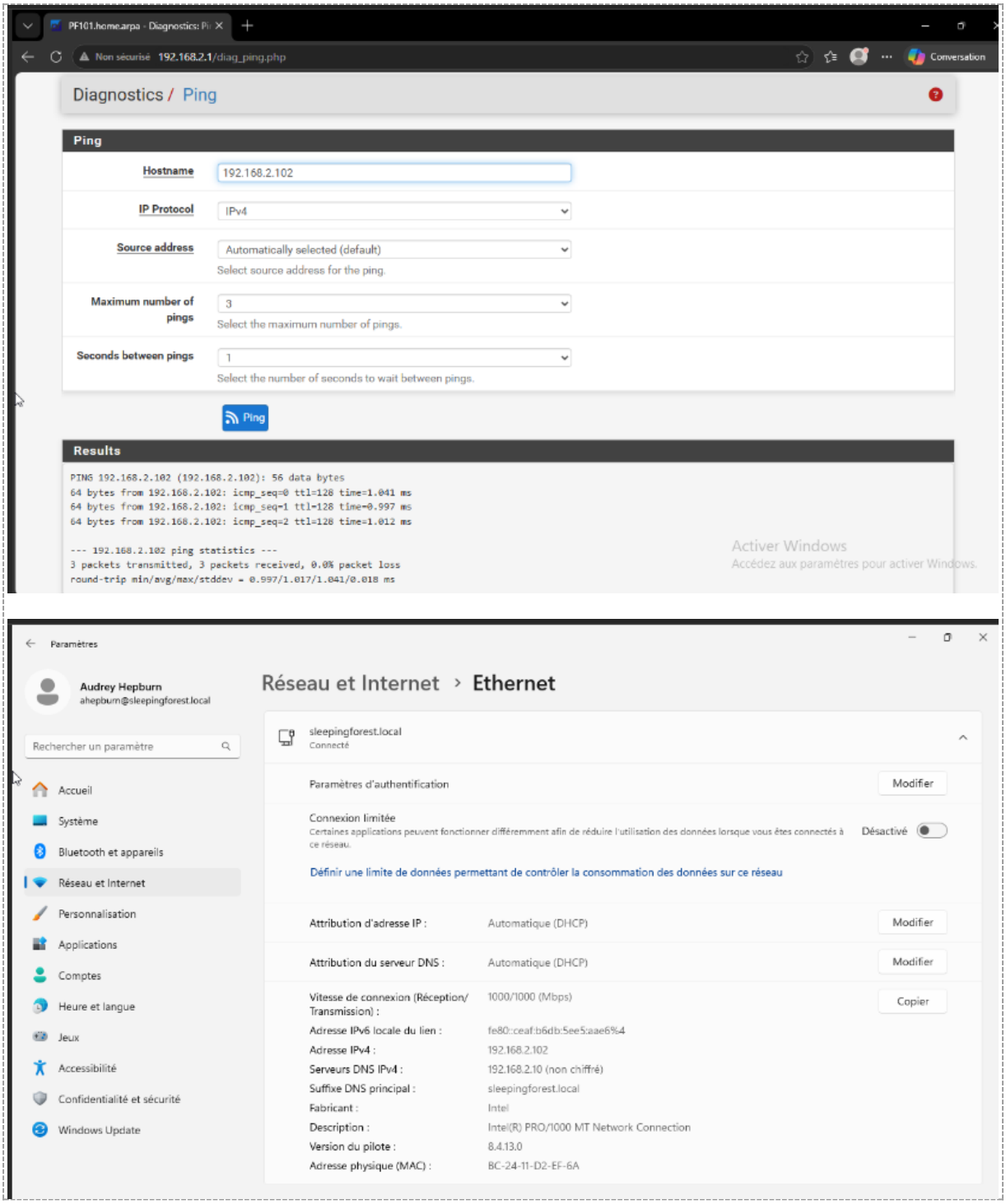


Capture 28 — NAT Outbound automatique pour le réseau 192.168.2.0/24

J'ai validé le bon fonctionnement de l'ensemble à l'aide des outils de diagnostic de pfSense (Diagnostics → Ping depuis les interfaces LAN et WAN) et depuis les postes clients **(29)**. Ce travail de

validation m'a d'ailleurs permis de diagnostiquer des coupures de connectivité qui ne provenaient pas de mes règles mais de la passerelle amont du réseau Proxmox, géré par mon professeur : une bonne illustration de la démarche d'analyse couche par couche (poste → pfSense → réseau amont) qu'un technicien doit appliquer.

Cf capture écran ci-dessous



Capture 29 — Tests de connectivité (Diagnostics Ping pfSense et postes clients)

2.3. Les difficultés que j'ai rencontrées durant ce projet

Ce projet m'a confronté à de nombreuses difficultés techniques qui ont constitué autant d'occasions d'apprentissage. La plus marquante a été la chaîne **Sysprep / capture MDT** : entre les paquets AppX bloquant la généralisation, les opérations de fichiers en attente créées par les mises à jour d'Edge, les pilotes VirtIO absents de WinPE (erreur 5456) et la réapparition du paquet LanguageExperiencePackfr-FR, j'ai dû mener un véritable travail d'enquête, journaux à l'appui (setupact.log, smsts.log), pour fiabiliser chaque maillon de la chaîne de déploiement.

Le **durcissement** a également généré des effets de bord inattendus : blocages de navigateurs par AppLocker après HardeningKitty, blocage d'Internet Explorer par les Microsoft Security Baseline. J'ai appris à distinguer un dysfonctionnement réel d'un comportement de sécurité volontaire, et à toujours travailler avec des snapshots pour pouvoir revenir en arrière.

Enfin, certaines contraintes étaient **extérieures à mon périmètre** : les droits d'administration de Proxmox et la connectivité du réseau amont sont gérés par mon professeur, ce qui m'a parfois imposé d'attendre une intervention ou de réorganiser mon travail pour avancer sur d'autres briques en parallèle. Cette situation reflète la réalité d'une entreprise, où le technicien doit composer avec des périmètres de responsabilité partagés.

2.4. Mon retour personnel et professionnel sur ce projet

Ce projet E7 m'a permis de mettre en pratique, sur une infrastructure complète et cohérente, l'ensemble des compétences SISR travaillées en cours : annuaire et stratégies de groupe, durcissement des systèmes, déploiement automatisé et filtrage réseau. Il m'a surtout appris une démarche : partir du besoin du client (Sleeping Forest), concevoir une solution, la mettre en œuvre, la tester, diagnostiquer méthodiquement les blocages et documenter chaque étape avec des captures d'écran.

Il fait également écho à mon alternance au SIPPEREC : la rigueur acquise dans le suivi des tickets et la rédaction de procédures m'a servi pour structurer ce projet, et inversement, les compétences d'infrastructure développées ici (AD, GPO, déploiement, pare-feu) enrichissent ma compréhension des environnements que je côtoie en entreprise. Des pistes d'évolution restent ouvertes pour renforcer la tolérance aux pannes de l'infrastructure : redondance du serveur de déploiement et réplication DFS des partages notamment.

Conclusion

Au terme de ce projet, l'entreprise Sleeping Forest dispose d'une infrastructure systèmes et réseaux complète, sécurisée et administrable. Sur la partie **SYSTÈME**, l'annuaire Active Directory organise les salariés par services au travers de groupes de sécurité qui pilotent l'ensemble des droits ; les lecteurs réseaux se montent automatiquement sur les postes selon le service de chaque utilisateur ; l'image de référence Windows 11 a été durcie avec HardeningKitty et le domaine sécurisé par les Microsoft Security Baseline ; enfin, le serveur de déploiement MDT/WDS permet d'installer automatiquement des postes durcis, applicatifs compris, directement intégrés au domaine.

Sur la partie **RÉSEAU**, le pare-feu pfSense protège l'infrastructure en appliquant une politique de filtrage explicite fondée sur le default deny, avec des règles organisées, documentées et testées.

Ce projet m'a fait progresser techniquement et méthodologiquement : je sais désormais construire une infrastructure de bout en bout, anticiper les interactions entre ses briques (un durcissement qui impacte un déploiement, une règle de pare-feu qui conditionne l'authentification au domaine) et diagnostiquer des pannes complexes. Il constitue une base solide pour la suite de mon parcours vers les métiers de l'administration systèmes et réseaux et de la cybersécurité.