

|  |
| --- |
| 02 |

|  |
| --- |
| 03 |

|  |
| --- |
| 01 |

Table des matières

### PRÉSENTATION GÉNÉRALE

Introduction p2

### CONNEXION AU DOMAINE

Jonction au domaine p2

Connexion à la session dʼun utilisateur p3

Vérification de lʼintégration du poste à lʼannuaire Active Directory p4

### TESTS DES SERVICES DU SERVEUR AD

Test du service DNS p4

Test du service DHCP p4

|  |
| --- |
| 04 |

### TEST DES STRATÉGIES DE GROUPE (GPO)

GPO - Fond dʼécran p5

GPO - Regedit p6

GPO - CMD p6

GPO - PowerShell p7

GPO - Panneau de configuration p7

GPO - Mappage lecteur réseau p7

|  |
| --- |
| 05 |

### TEST DU SERVEUR ACTIVE DIRECTORY REDONDANT

Simulation dʼune panne p8

|  |
| --- |
| 06 |

### TEST DE LA CONNECTIVITÉ À INTERNET (PFSENSE)

Vérification en lignes de commandes p9

Vérification à lʼaide de lʼaccès au webconfigurator p10

Vérification à lʼaide dʼun navigateur internet p10

|  |
| --- |
| 07 |

### TEST DE VEEAM BACKUP

Vérification de l’installation p13

Vérification de la sauvegarde p15

|  |
| --- |
| 08 |

### CONCLUSION **P17**

## I. Présentation Générale

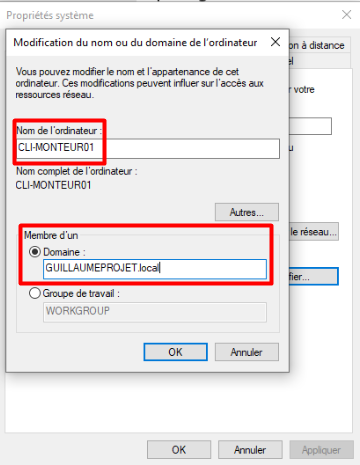
Introduction

Je souhaite vous présenter dans cette documentation les **différents tests** que j'ai réalisés pour valider les configurations effectuées. Les points suivants seront abordés : nous avons vérifié notamment l'intégration au domaine **Active Directory**, le bon fonctionnement des services réseau **(DNS, DHCP)**, l'application des **stratégies de groupe**, ainsi que la **connectivité réseau**, en particulier via le **routeur PFSense**. De plus, nous avons testé la liaison entre notre système et le logiciel de gestion des services informatiques **GLPI**. Je vous souhaite une agréable lecture.

## II. Connexion au domaine

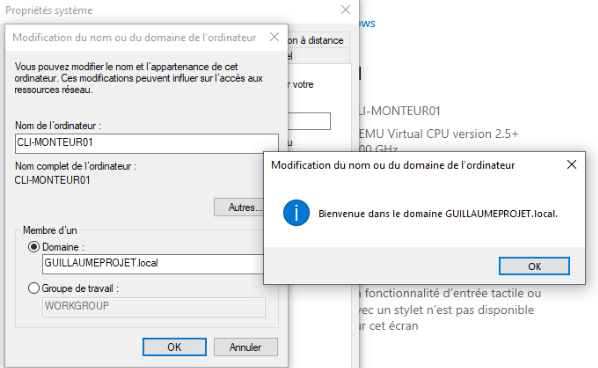
Jonction au domaine

Je dois ensuite accéder à **Système** dans les **Paramètres** de Windows pour joindre la machine au domaine. En cliquant sur **Renommer ce PC (avancé)** puis sur **Modifier**, j'accède à la fenêtre où il faut entrer le **nom de l'ordinateur** et spécifier le **domaine**.

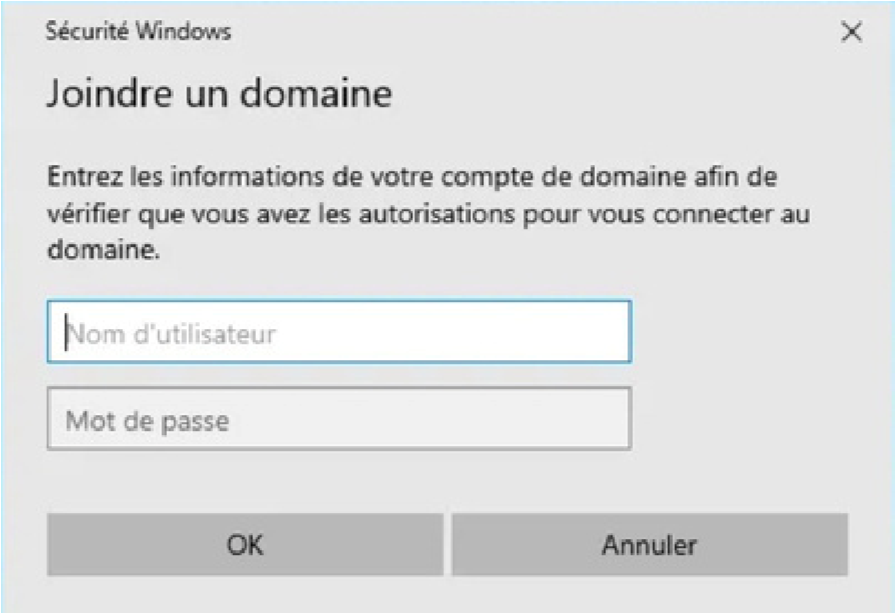


Une fois le **nom de domaine** et le **nom de l'ordinateur** renseignés, une fenêtre s'ouvre pour demander l'authentification avec un compte autorisé à joindre le domaine. Il faut entrer les **identifiants de connexion** d’un utilisateur du groupe **Admins du domaine** (j’utilise ici les informations de connexion du responsable informatique).

Une fenêtre apparait alors pour nous approuver le **succès de la jonction au domaine**. Il faut maintenant **redémarrer** le poste.



Connexion à la session dʼun utilisateur

Après redémarrage du poste, je me connecte avec un utilisateur du domaine, en l'occurrence **John White**, afin de valider l'**authentification** et la **configuration** du serveur. Une fois cette étape réalisée, je peux définir un **nouveau mot de passe** pour l'utilisateur et me connecter avec ce dernier sans **problème**.

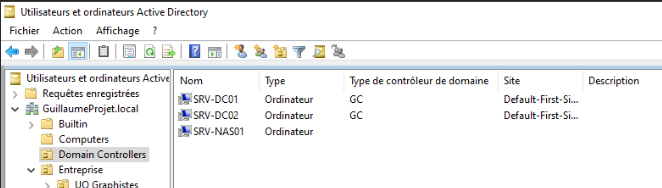


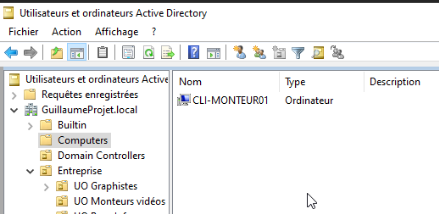
Après avoir changé le **mot de passe**, je peux accéder au **bureau Windows** de la session de l'utilisateur **John White** sans difficulté.



Vérification de lʼintégration du poste à lʼannuaire Active Directory

On peut également vérifier la bonne **intégration du client au domaine** en consultant l'outil **Utilisateurs et ordinateurs Active Directory** sur le **contrôleur de domaine**. Nous reproduisons le même schéma pour la bonne intégration des trois serveurs.

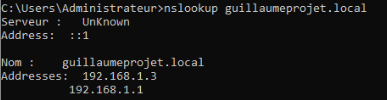




## III. Tests des services du serveur AD

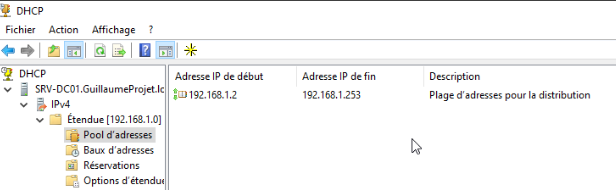
Test du service DNS

Après avoir ouvert une **Invite de commandes**, il faut entrer la commande **nslookup** pour vérifier le fonctionnement du service **DNS**.

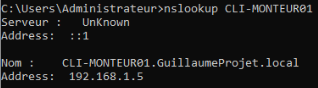


Test du service DHCP

Pour vérifier le service **DHCP**, je me connecte à une machine Windows client avec un utilisateur de mon **annuaire LDAP**. Ensuite, j'exécute la commande **nslookup CLI-MONTEUR01** dans l'invite de commandes **(CMD) de l’AD** pour m'assurer que l'adresse IP attribuée automatiquement fait bien partie de l'étendue configurée sur le **serveur DHCP**.



L'adresse IP attribuée correspond bien à la plage d'adresses configurée dans les **pools d'adresses** du serveur **Active Directory**.

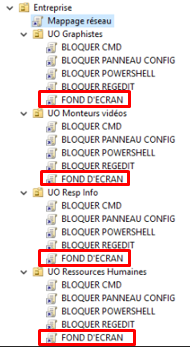


## IV. Test des Stratégies de Groupe (GPO)

Ce rapport présente les **sept GPO** que j'ai configurées, chacune ayant pour objectif de gérer des paramètres spécifiques dans l'environnement **Active Directory**. Ces stratégies de groupe centralisent la gestion des configurations et garantissent une application cohérente des règles au sein de l'infrastructure. Nous analyserons en détail chaque **GPO**, en mettant en lumière leur fonction et l'impact qu'elles ont sur les **utilisateurs** et les **systèmes**.

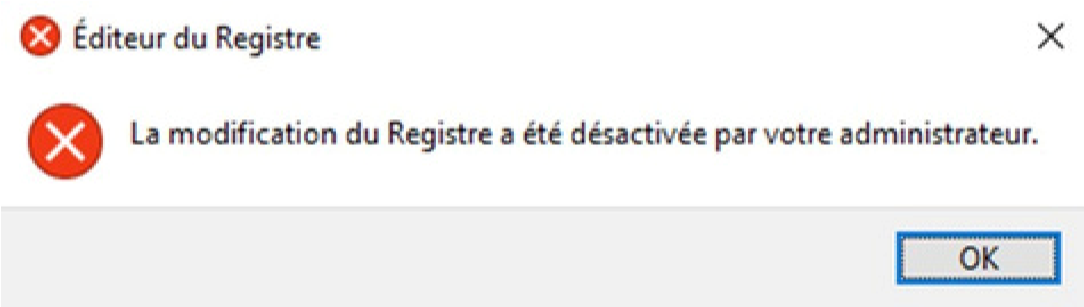
GPO - Fond dʼécran

Je vais donc vérifier l'application de la **GPO** concernant le **fond d'écran**.



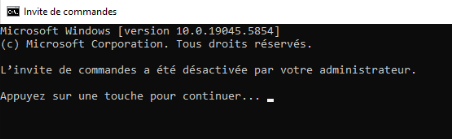
GPO - Regedit

Pour vérifier la **GPO** qui bloque l'accès à l'**Éditeur de Registre**, j'essaie d'exécuter l'outil **Regedit** et je constate si l'accès est **restreint** conformément à la configuration de la GPO.



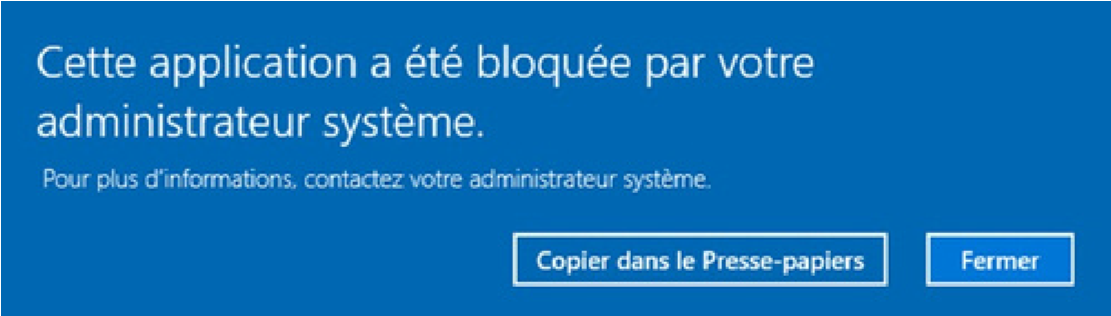
GPO - CMD

Pour tester la **GPO** bloquant l'accès à l'**invite de commandes**, je tente d'exécuter le programme **cmd** et je vérifie si l'accès est bien **restreint** conformément à la configuration de la GPO.



GPO - PowerShell

Pour tester la **GPO** bloquant l'accès à l'invite de commandes **PowerShell**, j'essaie d'exécuter le programme PowerShell et je vérifie si l'accès est correctement **restreint** conformément à la configuration de la GPO.



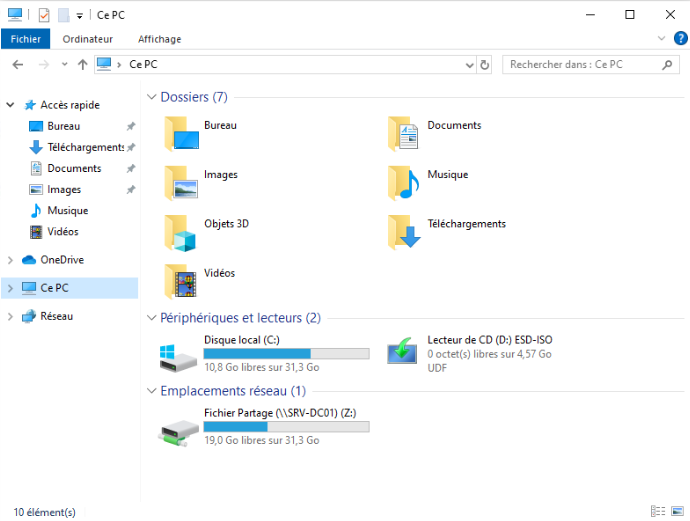
GPO - Panneau de configuration

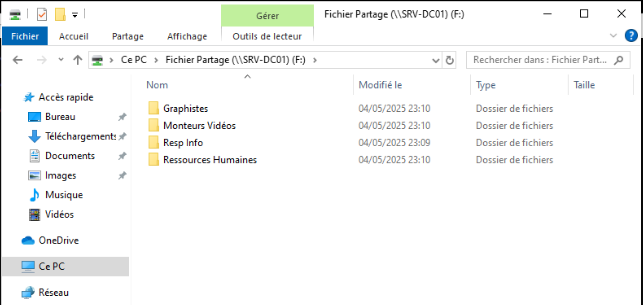
Pour tester la **GPO** bloquant l'accès au **Panneau de configuration**, j'essaie de l'exécuter et je vérifie si l'accès est correctement **bloqué** conformément à la configuration de la GPO.



GPO - Mappage lecteur réseau

Pour vérifier le **mappage réseau**, j'ouvre l'**explorateur de fichiers** et accède à **"Ce PC"** afin de m'assurer que l'**emplacement réseau** est correctement mappé et visible.

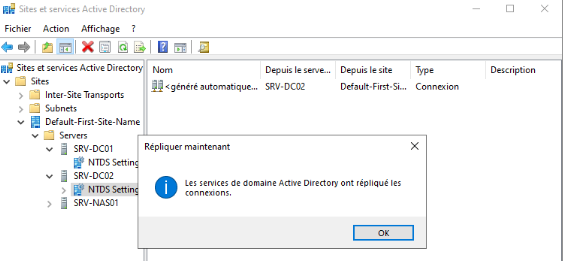


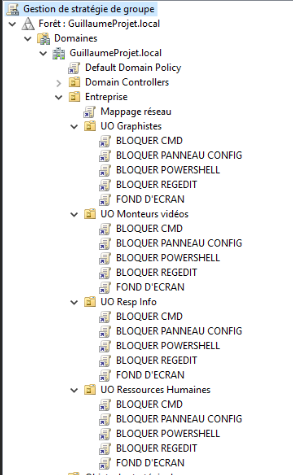
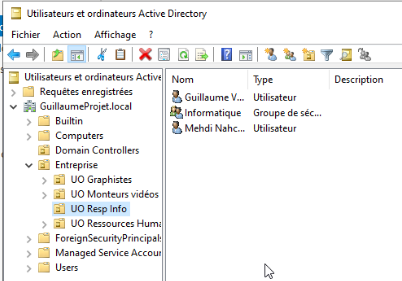


La session **Windows** de **Mehdi Nahceri** a bien accès au partage général **"Fichier Partage"** ainsi qu'au service spécifique associé à son **domaine d'activité**.

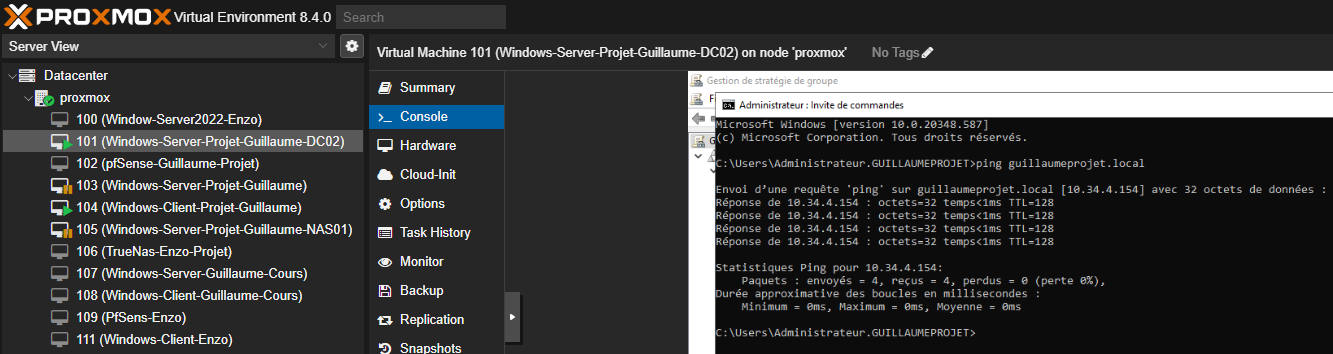
# V. Test du serveur active directory redondant

Dans un premier temps, pour vérifier la redondance de mon **Active Directory**, je vais effectuer une **réplication manuelle** et m'assurer que les **GPO** ainsi que les **utilisateurs** sont correctement répliqués sur le contrôleur de domaine redondant.



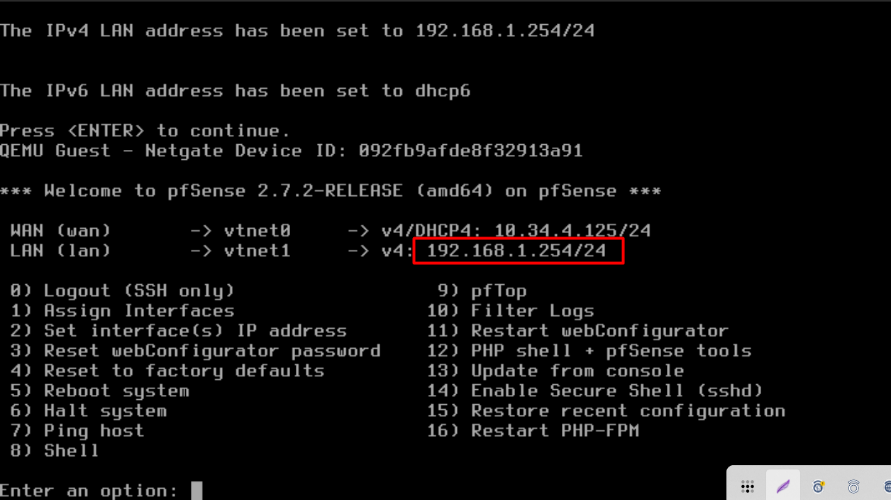


Pour tester la redondance de l'**Active Directory**, je vais simuler une panne sur le contrôleur de domaine principal (adresse IP **192.168.1.1**) et vérifier si le contrôleur redondant (adresse IP **192.168.1.3**) prend bien le relais. Ce test sera effectué depuis le serveur redondant lui-même en lançant un simple test de **ping** vers **guillaumeprojet.local**, qui est le domaine configuré. L'objectif est de valider que, même en cas de défaillance du contrôleur principal, le contrôleur secondaire prend en charge les demandes d'authentification et que la communication avec le domaine reste fonctionnelle.



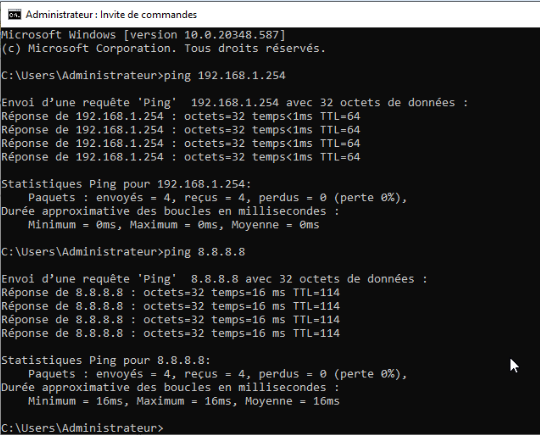
# VI. Test de la connectivité à internet (PFSense)

Lors du test de **PFSense**, la machine virtuelle est configurée avec deux interfaces réseau : l'une pour le **WAN**, recevant une **adresse IP publique**, et l'autre pour le **LAN**, attribuée comme **passerelle** du réseau interne. Cette configuration permet de relier le **serveur Active Directory** au réseau interne via l'**IP LAN de PFSense**. En utilisant cette passerelle, le serveur peut communiquer avec dʼautres appareils du réseau et accéder à Internet. Les tests permettront de vérifier la **connectivité**, le **routage** et la **sécurité réseaux** assurés par PFSense.



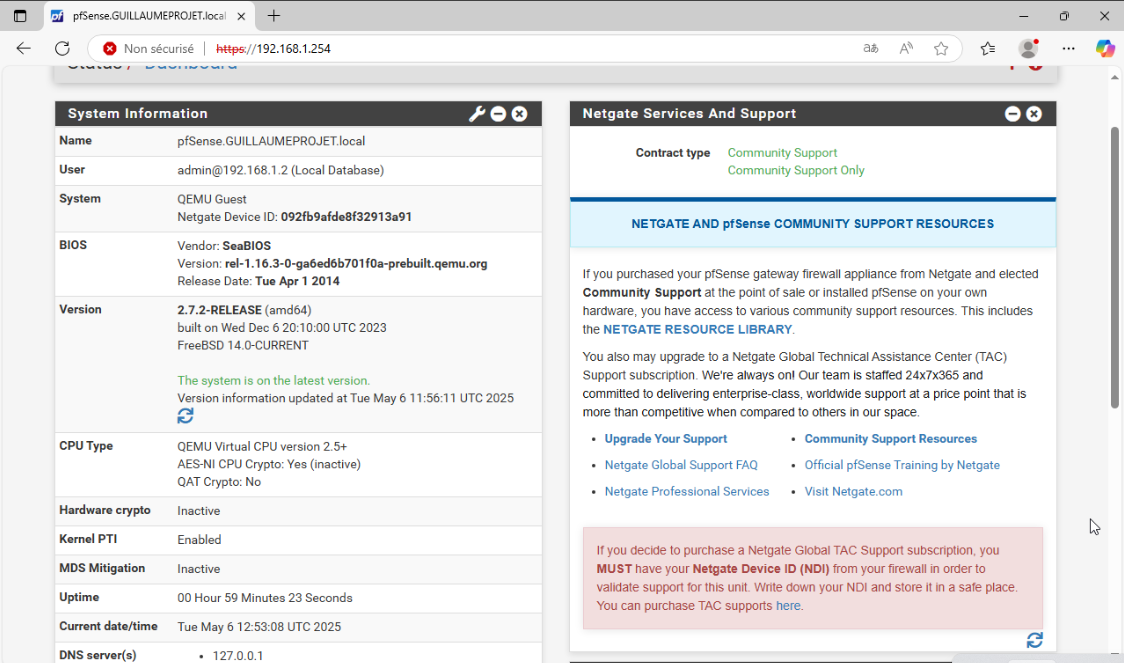
Vérification en lignes de commandes

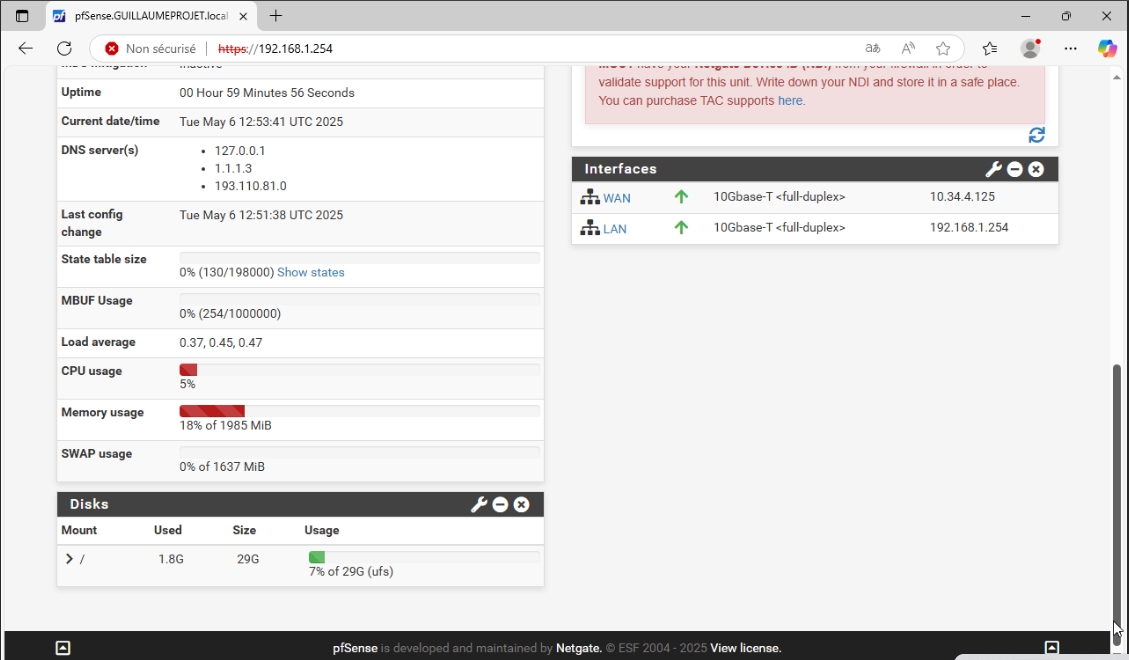
Sur le **serveur Active Directory**, un test de **ping** est d'abord effectué vers l'adresse **IP de la passerelle** (interface **LAN** de PFSense) pour confirmer la communication entre le serveur et PFSense. Une fois cette connexion locale validée, un second test de **ping** est réalisé vers **8.8.8.8**, le DNS public de Google, afin de vérifier que le serveur Active Directory dispose bien d'une connexion Internet en passant par la passerelle PFSense. Ces tests garantissent le bon fonctionnement du **routage réseau** et l'**accès externe** via PFSense.



Vérification à lʼaide de lʼaccès au webconfigurator

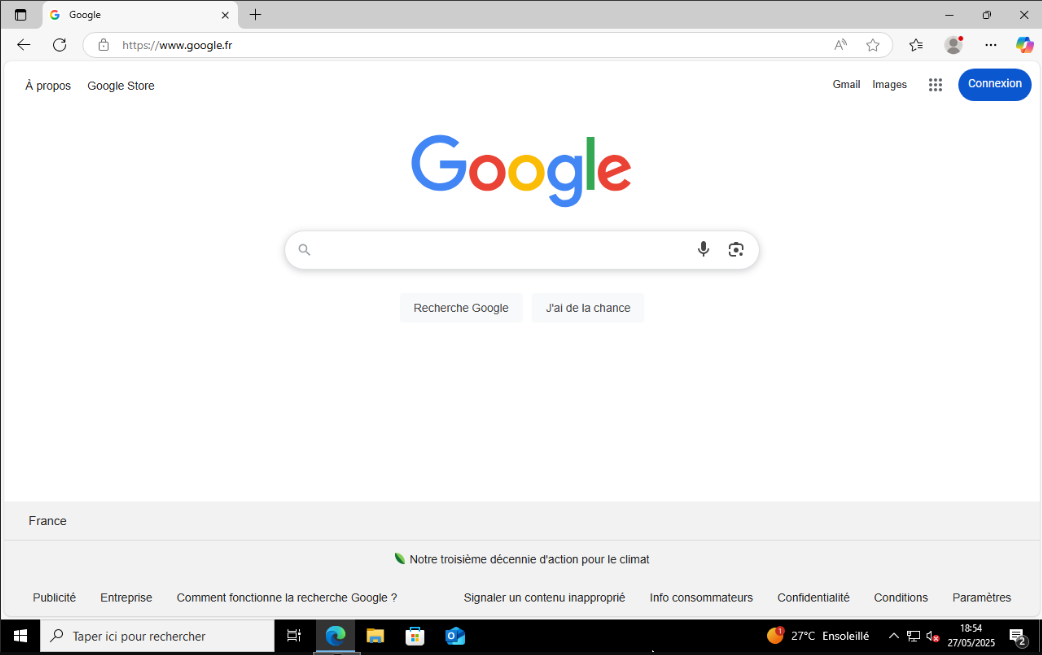
Enfin, depuis le serveur **Active Directory**, j'accède au **WebConfigurator** de PFSense via un navigateur en utilisant l'**adresse IP LAN**. Cela confirme que le serveur communique correctement avec PFSense et permet dʼaccéder à son **interface dʼadministration**.





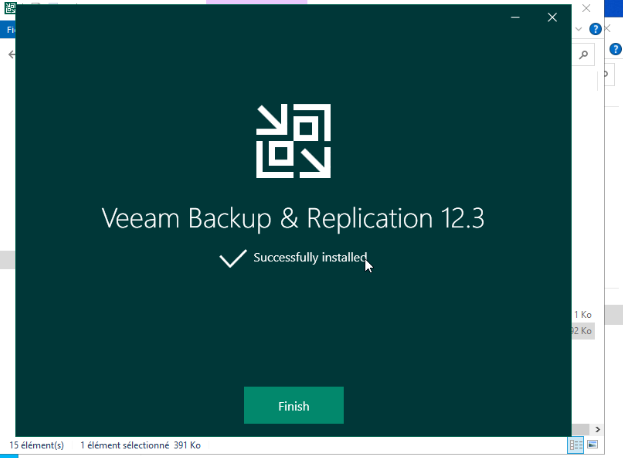
Vérification à lʼaide dʼun navigateur internet

On peut ouvrir un **navigateur internet** et entrer l'adresse “www.google.fr” dans la barre d'URL pour vérifier le fonctionnement d'internet sur le poste client.



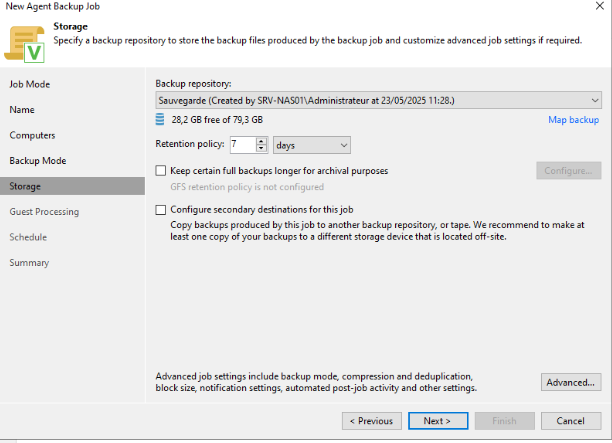
## VII. Test de Veeam Backup

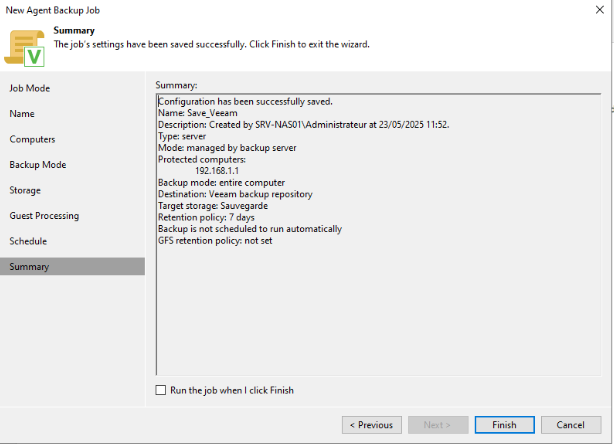
Vérification de l’installation



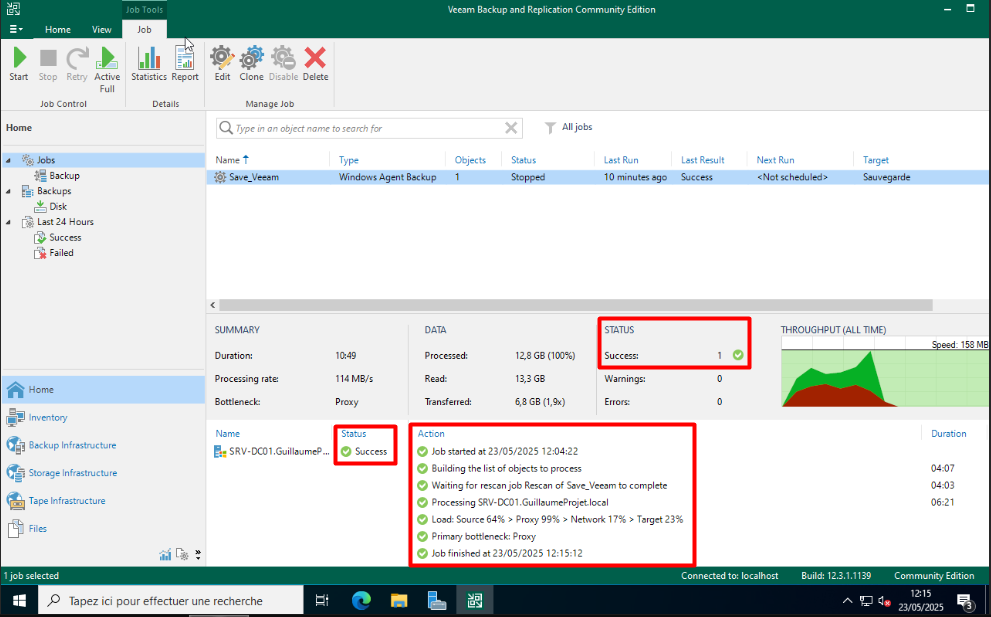
Vérification de la sauvegarde

Création du repository :

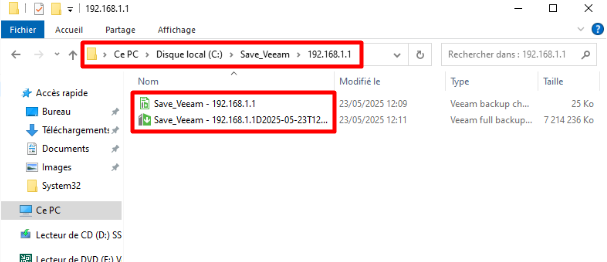




Lancement de la sauvegarde sur le logiciel Veeam Backup :



Vérification dans le dossier repository créé au préalable :



## VIII. Conclusion

**Tous les tests réalisés** ont été **concluants**, confirmant que les configurations et les services fonctionnent correctement sur le poste client et dans l'environnement réseau. Les tests démontrent que l'infrastructure mise en place est **stable**, **fiable** et **prête** à être utilisée dans un **environnement de production de l’entreprise Pixarias Studios**.