



NBRD

SOLUTION INFORMATIQUE

DOCUMENTATION RAPPORT DE TESTS

Épreuve E6 : Administration des systèmes et des réseaux

DATE

02/06/2025

RÉDACTEUR

Nohan BROCHARD

07 80 40 96 63

83 Rue André Le Notre, 30900 Nîmes, France

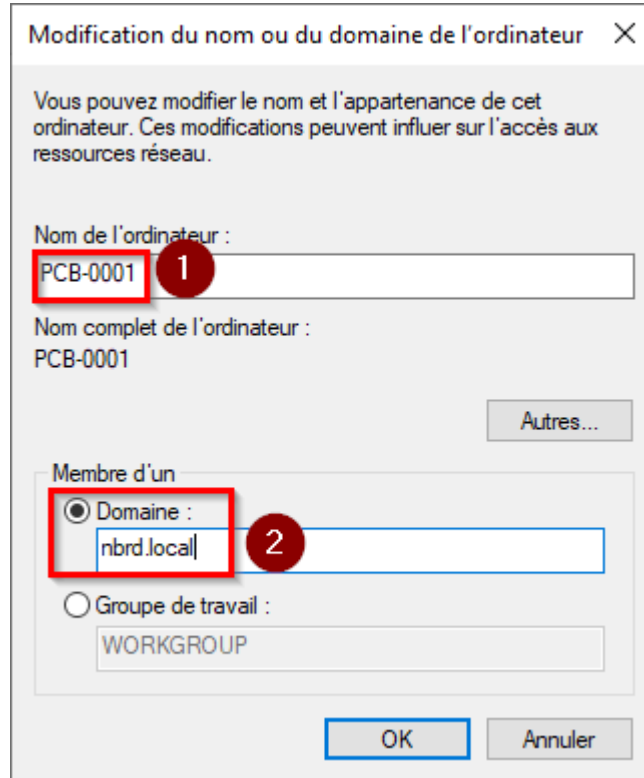
Sommaire

Sommaire.....	2
Connexion au domaine	3
Jonction au domaine	3
Connexion à la session d'un utilisateur	4
Vérification de l'intégration du poste à l'annuaire Active Directory	4
Tests des services du serveur AD	5
Test du service DNS.....	5
Test du service DHCP	5
Test des Stratégies de Groupe (GPO).....	6
GPO – Fond d'écran.....	6
GPO – Raccourci GLPI	6
Test du serveur Active Directory Redondant.....	7
Simulation d'une panne	8
Test de la connectivité à internet (PFSense)	9
Vérification en lignes de commandes.....	9
Vérification à l'aide de l'accès au WebConfigurator	10
Vérification à l'aide d'un navigateur internet.....	10
Test du serveur GLPI.....	11
Test d'accès au serveur	11
Conclusion	12

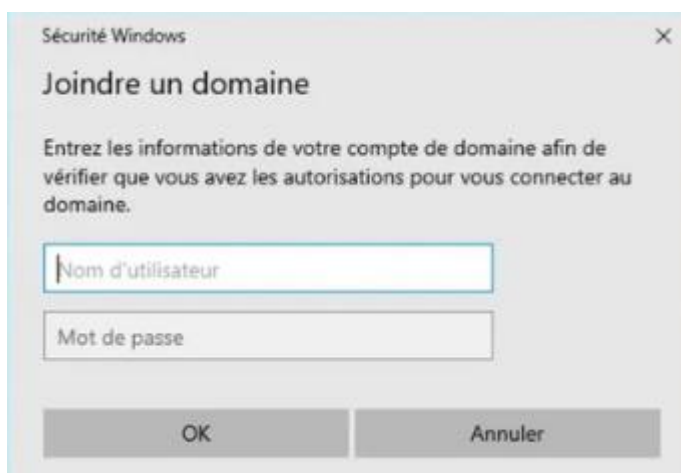
Connexion au domaine

Jonction au domaine

Je dois me rendre dans **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**.



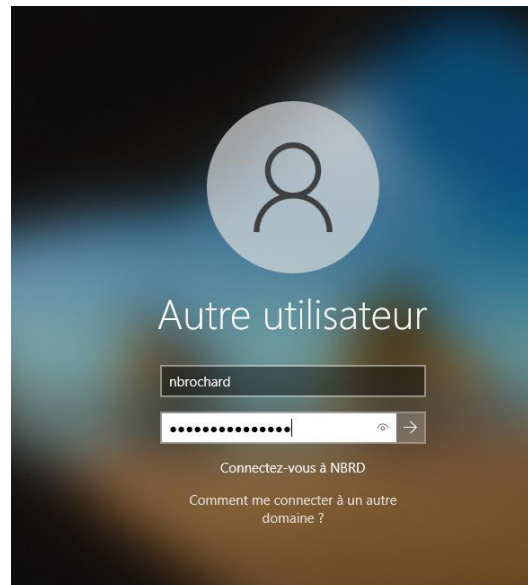
Une fois le **nom de domaine** et le **nom de l'ordinateur** renseignés, une fenêtre s'ouvre pour demander l'authentification avec un compte autorisé à joindre le domaine. Il faut entrer les **identifiants de connexion** d'un utilisateur du groupe **Admins du domaine** (j'utilise ici les informations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



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

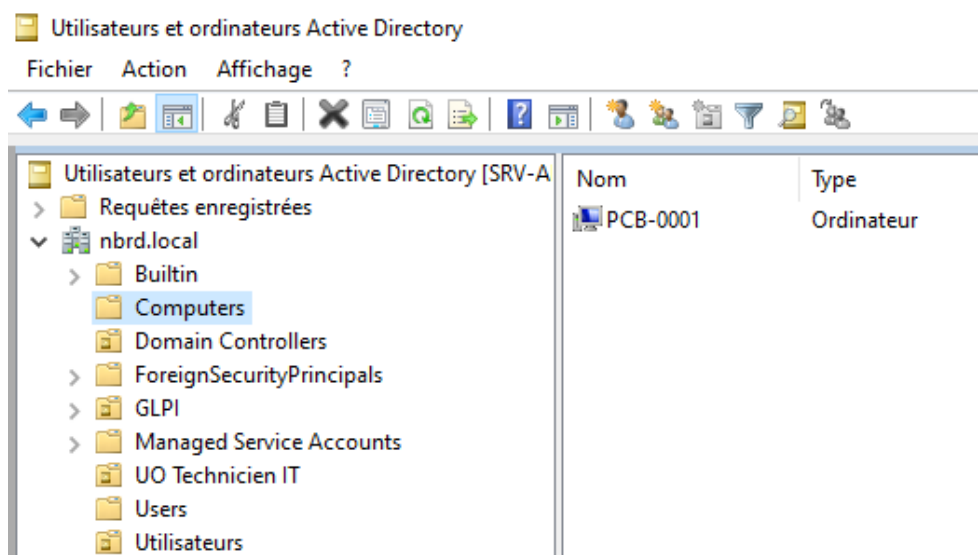
Connexion à la session d'un utilisateur

Après redémarrage du poste, je me connecte avec un utilisateur du domaine, en l'occurrence **Nohan BROCHARD**, afin de valider l'**authentification** et la **configuration** du serveur.



Vérification de l'intégration du poste à l'annuaire 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.



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**.

```

C:\Users\nbrochard>nslookup nbrd.local
Serveur : UnKnown
Address: 192.168.10.254

Nom : nbrd.local
Addresses: 192.168.10.253
           192.168.10.254
  
```

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 **ipconfig** dans l'invite de commandes (**CMD**) pour m'assurer que l'adresse IP attribuée automatiquement fait bien partie de l'étendue configurée sur le **serveur DHCP**.

```

C:\Users\nbrochard>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : nbrd.local
    Adresse IPv6 de liaison locale. . . . : fe80::cf29:dde2:d1b2:e742%6
    Adresse IPv4. . . . . : 192.168.10.13
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.10.1

Carte Ethernet Connexion réseau Bluetooth :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :
  
```

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

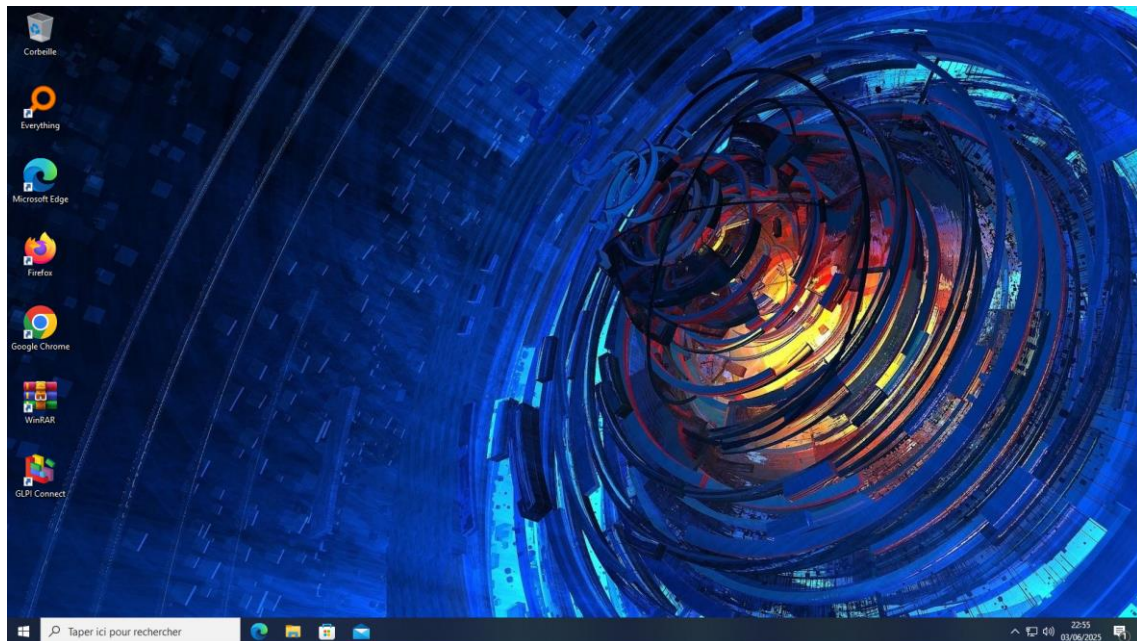
DHCP			
Fichier Action Affichage ?			
<div> <div> <div>DHCP</div> <div> <div>srv-ad.nbrd.local</div> <div>IPv4</div> <div>Étendue [192.168.10.0] NBRD - PROD</div> <div>Pool d'adresses</div> <div>Baux d'adresses</div> <div>Réservations</div> <div>Options d'étendue</div> <div>Stratégies</div> <div>Options de serveur</div> <div>Stratégies</div> <div>Filtres</div> <div>IPv6</div> </div> </div> </div>			
Adresse IP de début	Adresse IP de fin	Description	
192.168.10.10	192.168.10.200	Plage d'adresses pour la distribution	
192.168.10.100	192.168.10.110	Adresses IP exclues de la distribution	

Test des Stratégies de Groupe (GPO)

Ce rapport présente les **deux 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 d'écran

Tout d'abord, je vais vérifier l'application de la **GPO** concernant le **fond d'écran**. Pour cela, je me connecterai à une **machine du réseau** avec l'utilisateur **Nohan BROCHARD** et m'assurerai que la GPO est correctement appliquée.



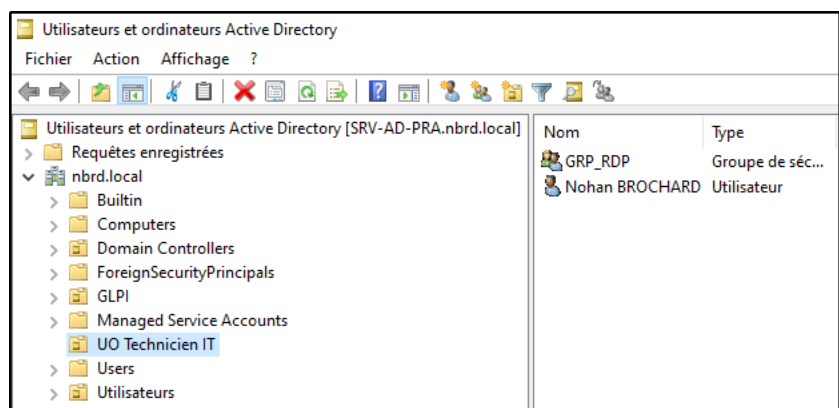
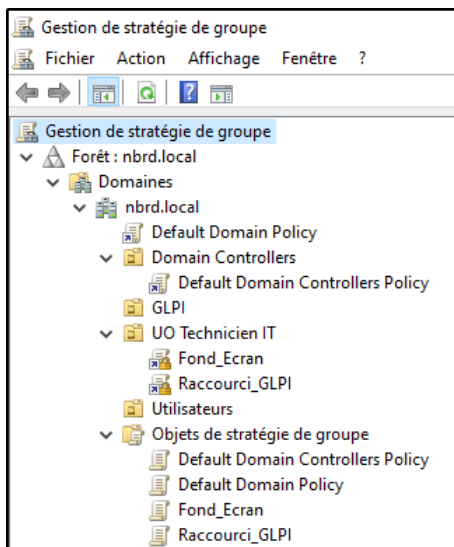
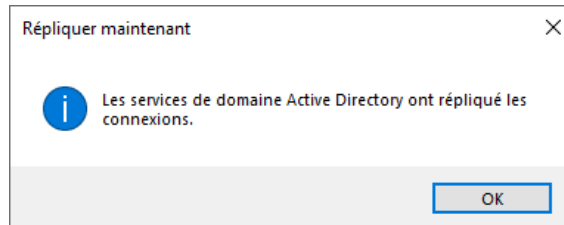
GPO – Raccourci GLPI

Sur le **bureau Windows**, une icône intitulée « **GLPI Connect** » est située en haut à gauche. Cette icône permet d'accéder directement à l'interface web de **GLPI**, offrant ainsi la possibilité de **créer un incident**.



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.



Simulation d'une panne

Pour tester la redondance de l'**Active Directory**, je vais simuler une panne sur le contrôleur de domaine principal (adresse IP **192.168.10.254**) et vérifier si le contrôleur redondant (adresse IP **192.168.10.253**) prend bien le relais. Ce test sera effectué depuis une **machine cliente** en lançant un simple test de **ping** vers **nbrd.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.

```
Invite de commandes
Microsoft Windows [version 10.0.19045.5854]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\nbrochard>ping nbrd.local

Envoi d'une requête 'ping' sur nbrd.local [192.168.10.254] avec 32 octets de données :
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.10.254 : octets=32 temps<1ms TTL=128
Réponse de 192.168.10.254 : octets=32 temps<1ms TTL=128
Réponse de 192.168.10.254 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.10.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\nbrochard>ping nbrd.local

Envoi d'une requête 'ping' sur nbrd.local [192.168.10.254] avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.10.254:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\nbrochard>ping nbrd.local

Envoi d'une requête 'ping' sur nbrd.local [192.168.10.254] avec 32 octets de données :
Ctrl+C
^C
C:\Users\nbrochard>ping nbrd.local

Envoi d'une requête 'ping' sur nbrd.local [192.168.10.254] avec 32 octets de données :
Réponse de 192.168.10.14 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 192.168.10.254:
    Paquets : envoyés = 1, reçus = 1, perdus = 0 (perte 0%),
Ctrl+C
^C
C:\Users\nbrochard>ping nbrd.local

Envoi d'une requête 'ping' sur nbrd.local [192.168.10.253] avec 32 octets de données :
Réponse de 192.168.10.253 : octets=32 temps<1ms TTL=128
Réponse de 192.168.10.253 : octets=32 temps<1ms TTL=128
Réponse de 192.168.10.253 : octets=32 temps<1ms TTL=128
Réponse de 192.168.10.253 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.10.253:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```


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 d'autres appareils du réseau et accéder à Internet. Les tests permettront de vérifier la **connectivité**, le **routing** et la **sécurité réseaux** assurés par PFSense.

```
FreeBSD/amd64 (pfSense.nbrd) (ttyv0)

VMware Virtual Machine - Netgate Device ID: bdc293576f6520e26537

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)          -> le0          -> v4/DHCP4: 192.168.118.150/24
LAN (lan)           -> le1          -> v4: 192.168.10.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option:
```

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 **routing réseau** et l'**accès externe** via PFSense.

```
Administrateur : Invite de commandes

C:\Users\Administrateur>ping 192.168.10.1

Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.10.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.10.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.10.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>ping 8.8.8.8

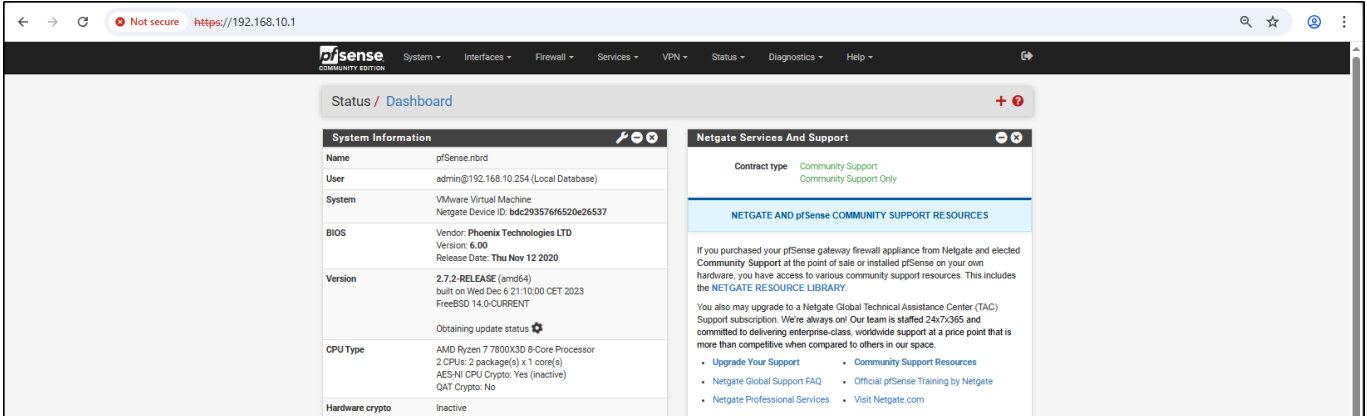
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=127

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 9ms, Maximum = 10ms, Moyenne = 9ms

C:\Users\Administrateur>
```

Vérification à l'aide de l'accès au WebConfigurator

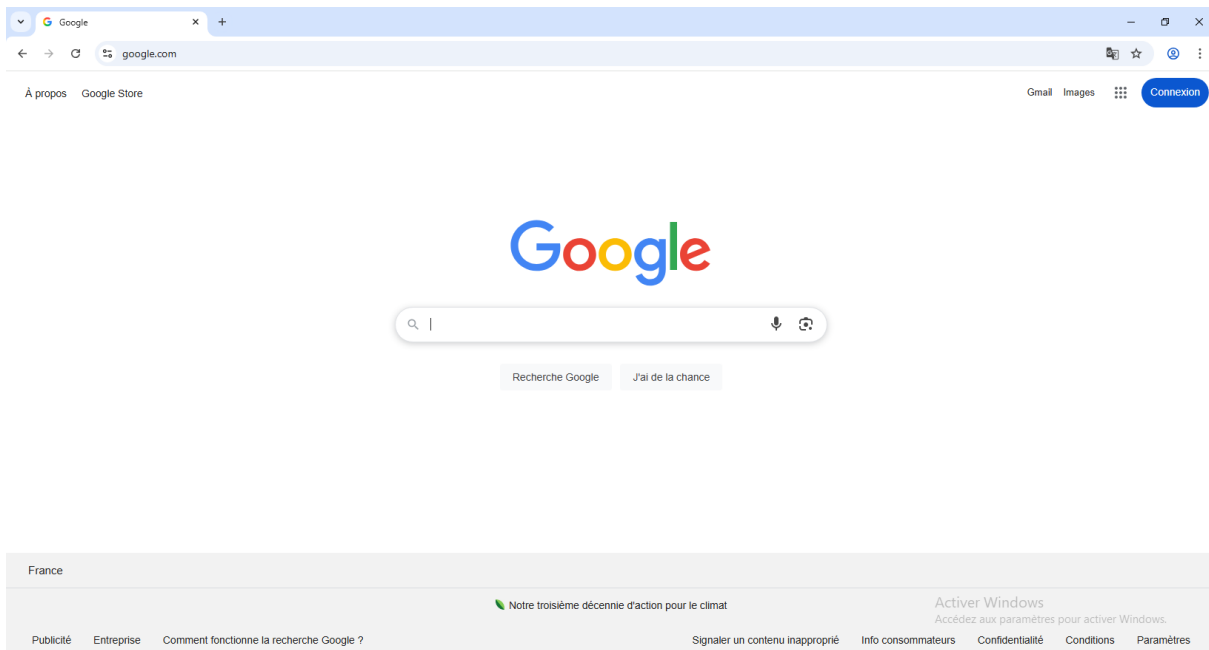
Enfin, depuis le serveur **Active Directory**, j'accède au **WebConfigurator** de PFSense via un navigateur en utilisant l'**adresse IP LAN**. Cela confirme que le serveur communique correctement avec PFSense et permet d'accéder à son interface d'administration.



The screenshot shows the pfSense WebConfigurator interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two panels. The left panel, titled 'System Information', displays details about the pfSense instance, including the user (admin@192.168.10.254), system (VMware Virtual Machine), BIOS (Phoenix Technologies LTD), version (2.7.2-RELEASE), and CPU type (AMD Ryzen 7 7800X3D 8-Core Processor). The right panel, titled 'Netgate Services And Support', provides information about the support contract type (Community Support) and lists various support resources, including upgrade guides, FAQs, and training materials.

Vérification à l'aide d'un navigateur internet

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

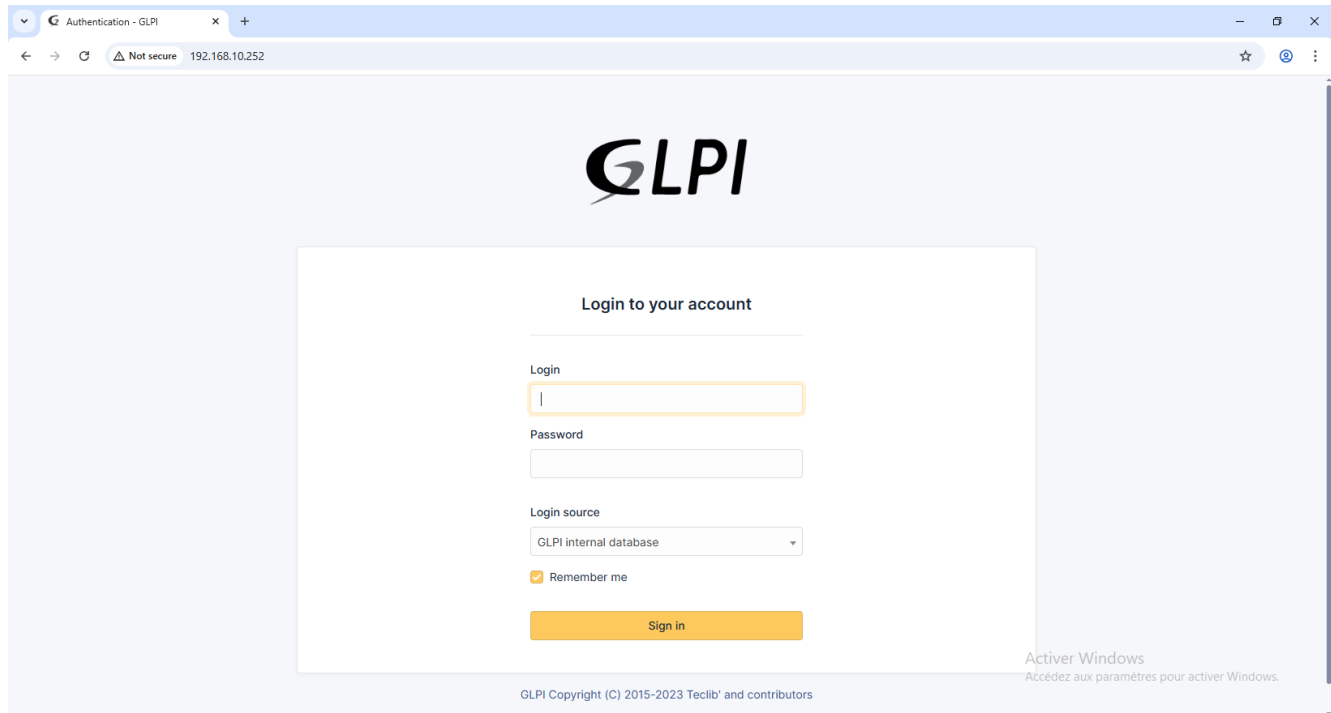


The screenshot shows the Google homepage in a web browser. The address bar displays 'google.com'. The page features the Google logo, a search bar, and a 'Recherche Google' button. The footer includes links for 'A propos', 'Google Store', 'Gmail', 'Images', and 'Connexion'. A banner at the bottom of the page reads 'Notre troisième décennie d'action pour le climat'.

Test du serveur GLPI

Test d'accès au serveur

Depuis le serveur **Active Directory**, j'accède à la page de connexion du serveur **GLPI** en utilisant son adresse IP (**192.168.10.252**).



Authentication - GLPI

Not secure 192.168.10.252

GLPI

Login to your account

Login

Password

Login source

GLPI internal database

☒ Remember me

Sign in

GLPI Copyright (C) 2015-2023 Teclib' and contributors

Activer Windows
Accédez aux paramètres pour activer Windows.

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 NBRD Corporation**.