Février 2026

# Mise en place technique
# Entreprise GSB

BELLIOT Anne-Juliette

# Sommaire

# Contexte de l'entreprise

L'entreprise GSB (Galaxy Swiss Bourdin) est une entreprise provenant de la fusion du groupe américain Galaxy, spécialisé dans le secteur des maladies virales (sida, hépatite…), et du groupe européen Swiss Bourdin, qui lui travaille sur des médicaments plus traditionnels.
Ces deux entreprises pharmaceutiques ont fusionné en 2009 afin de devenir GSB, le leader de leur secteur.
Le siège social de l'entreprise se trouve à Philadelphia, en Pennsylvanie, aux Etats-Unis, tandis que le siège administratif européen se situe à Paris.

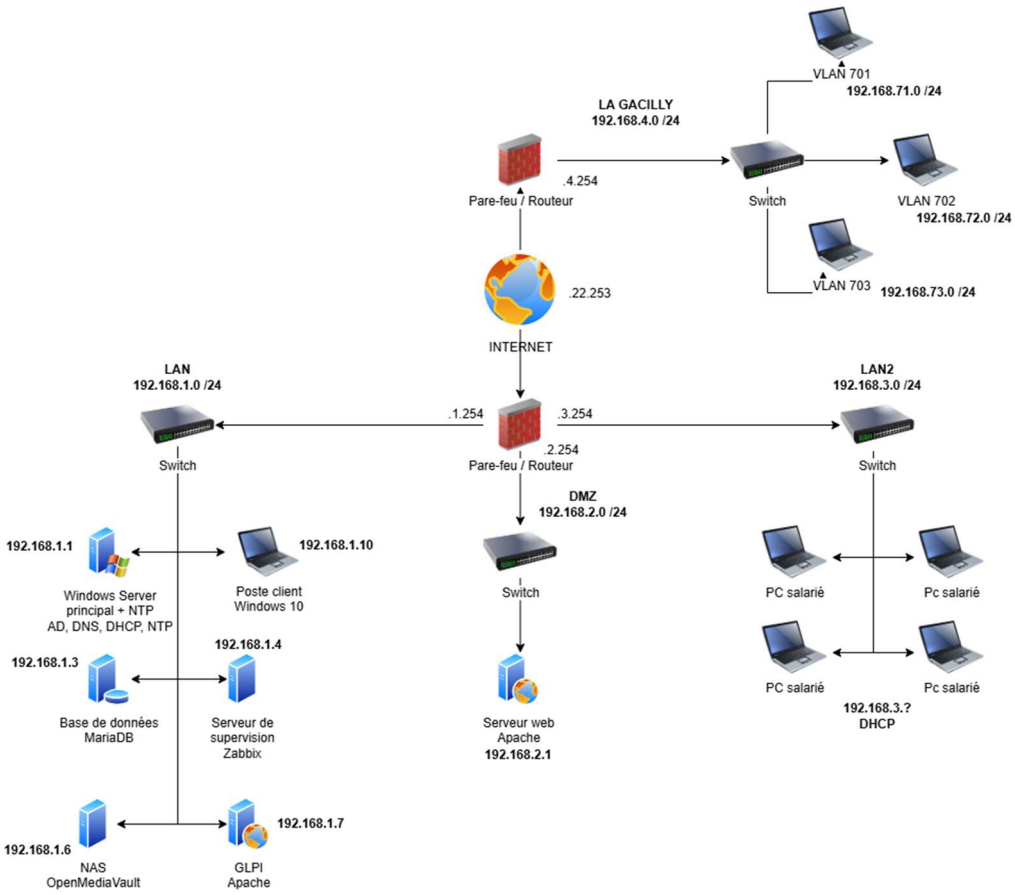
GSB emploie 480 visiteurs médicaux en France métropolitaine et dans les DROM-COM.
Les visiteurs médicaux sont des salariés qui ont pour mission non pas de vendre des médicaments, mais de les présenter à des professionnels de santé, par exemple des médecins, afin d'informer de leur bon usage ou bien simplement de les promouvoir.

Suite à la fusion de ces deux entreprises, GSB souhaite optimiser son fonctionnement.
C'est pourquoi elle désire mettre à disposition de ses salariés une application web, "Appli-Frais", leur permettant de centraliser les comptes-rendus de leur visite, mais aussi de faciliter la gestion des frais de déplacement des visiteurs médicaux. Elle aura également d'autres utilités, par exemple le service comptable disposera d'une page pour effectuer les remboursements.

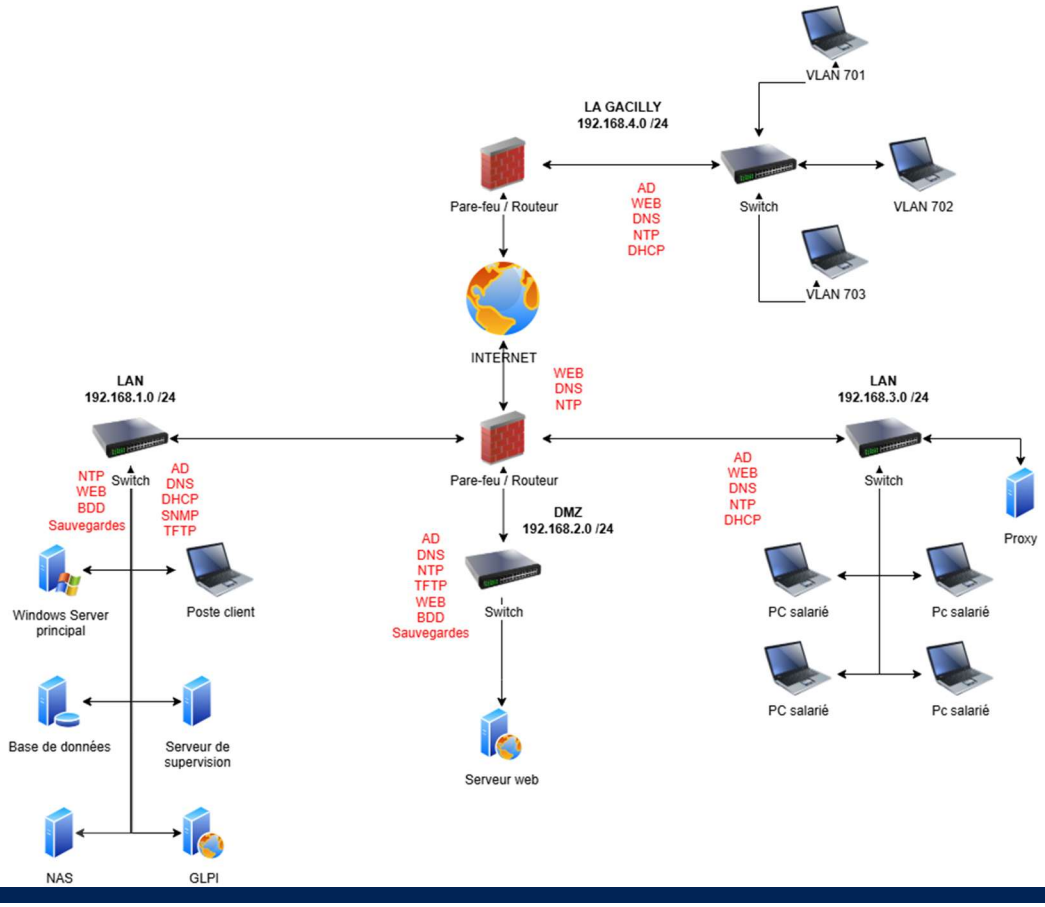
C'est dans ce cadre qu'un cahier des charges a été établi, afin de lister les besoins de l'entreprise pour la mise en place de cette application.
Elle sera soumise à de nombreuses exigences, notamment en termes de cybersécurité.
L'analyse suivante permettra de documenter la mise en place technique attendue, recetter les services déjà installés ainsi que montrer l'avancée du projet.

# Architecture réseau

## Schéma de l'infrastructure du réseau GSB




## Schéma des flux de l'infrastructure



# Services mis en place

| nom machine | système d'exploitation | adresse ip | services | description | login | mot de passe |
|---|---|---|---|---|---|---|
| SRV-AD1-AJB-1.1 | Windows Server 2022 | 192.168.1.1 | ad, dns, dhcp, ntp | serveur ad principal | Administrateur | Chevrollier23 |
| SRV-WEB-AJB-2.1 | Linux Debian | 192.168.2.1 | apache | serveur web pour l'appli | root | root |
| SRV-GLPI-AJB-1.7 | Linux Debian | 192.168.1.7 | apache | serveur web pour glpi | root | root |
| SRV-BDD-AJB-1.3 | Linux Debian | 192.168.1.3 | mariadb | serveur bdd pour web, glpi, zabbix | userGsb | admin_glpi \| Admin_glpi |
| SRV-NAS-AJB-1.6 | OpenMediaVault | 192.168.1.6 | openmediavault | nas pour les sauvegardes | test | MDPomv17! |
| MACHINE-CLIENTE-AJB-1.10 | Windows 10 | 192.168.1.10 | | machine cliente pour configurer serveurs | dandre | MDPuser17! \| oppg5 |
| SRV-PFSENSE-AJB-22.253 | pfSense | 192.168.22.253 (wan) | pfsense | pare-feu central pour filtrage et vpn | admin | pfsense |
| SRV-SUPERVISION-AJB-1.4 | Linux Debian | 192.168.1.4 | zabbix | serveur pour surveiller l'infra | | MDPzabbix17! |
| MACHINE-CLIENTE-AJB-3.XXX | Windows 11 | 192.168.3.XXX (dhcp) | | machine pour tester le dhcp | admin \| dandre | azerty \| MDPuser17! \| oppg5 |
| SRV-PROXY-1.5 | Linux Debian | 192.168.1.5 | squid | | | |

## Windows Server 1

Nous allons mettre en place un Windows Server afin de créer un domaine Active Directory, un DNS et un DHCP. Notre domaine sera gsb.coop, nous créerons un alias visite pour le site web.
Le DHCP permettra à nos machines du LAN utilisateur d'avoir des IP automatiquement.

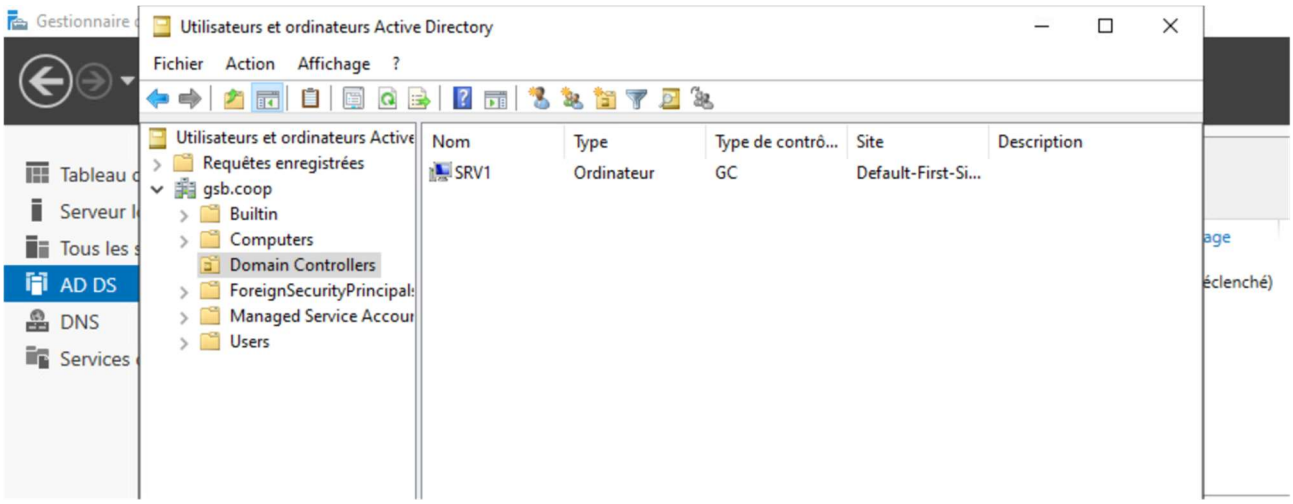
Nous pourrons aussi centraliser nos utilisateurs, bien gérer nos comptes.

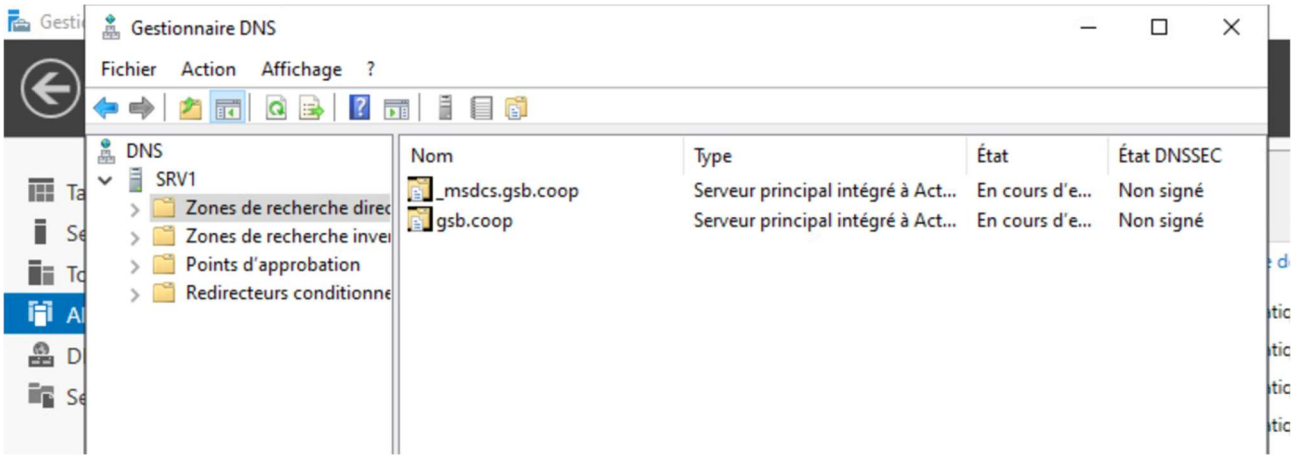
Notre serveur sera dans notre LAN.

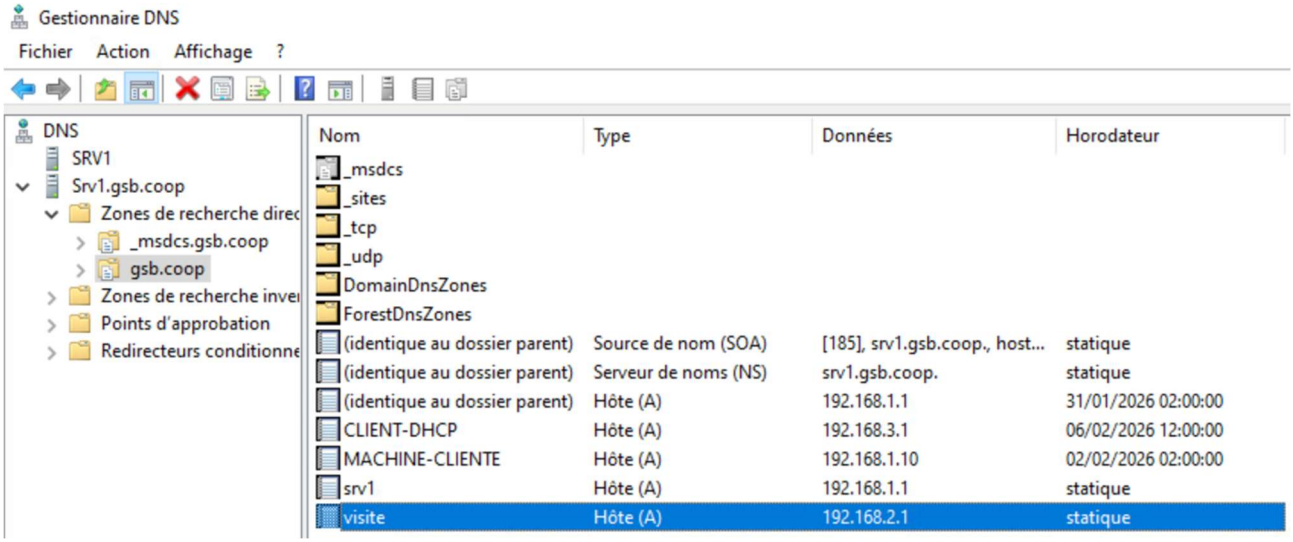
Adresse ip : 192.168.1.1

Nom d'utilisateur : Administrateur
Mot de passe : Chevrollier23

Nom de domaine : gsb.coop






## Serveur WEB

Notre serveur web est une machine Debian, sous Linux, sans interface graphique.
Il va héberger notre site web.
Nous installerons le service Apache pour que cela fonctionne correctement.
Apache représente le meilleur choix. C'est l'outil le plus largement utilisé, donc il est très documenté, il est fiable et très simple à installer et à configurer.

Nous allons utiliser une machine Debian sous Linux pour ce serveur. En effet, celle-ci sera plus adaptée que Windows pour plusieurs raisons :

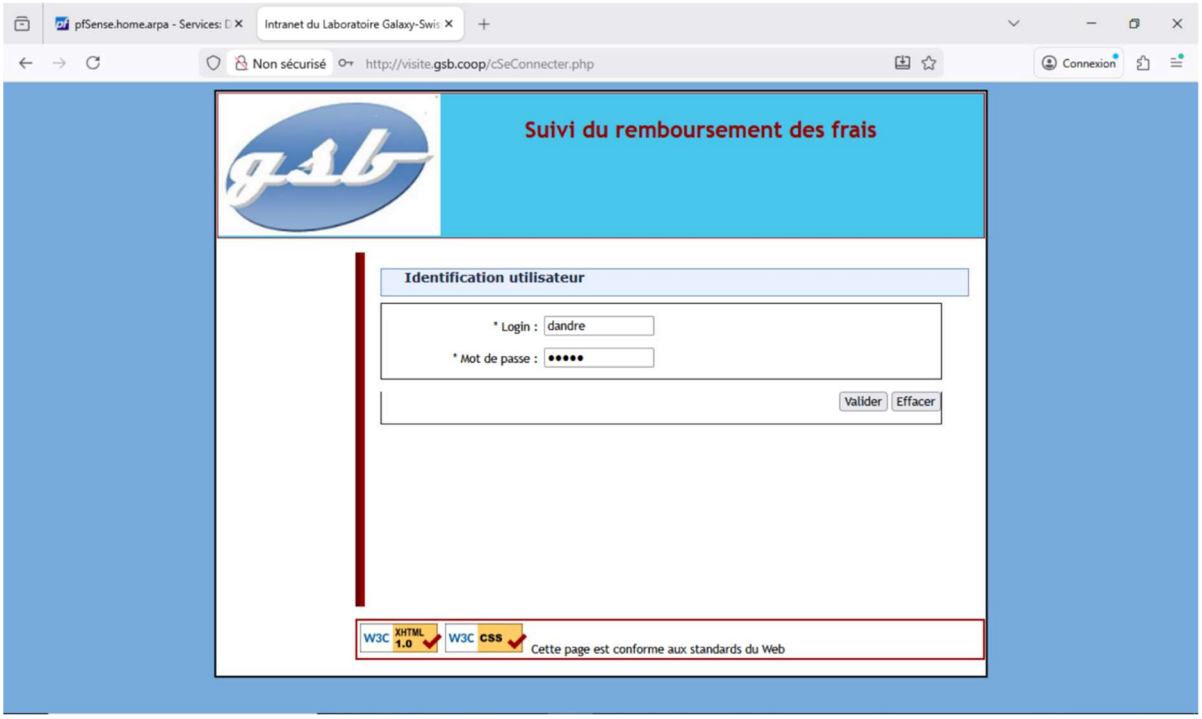
- Debian est gratuit alors qu'une licence Windows est payante
- Debian sans interface graphique consomme beaucoup moins, notamment en termes de mémoire ou de processeur, qu'un serveur Windows
- Installer Apache sur une machine Debian est plus simple et rapide
- Linux est mieux sécurisé que Windows

Le serveur web sera placé dans une DMZ afin qu'il ne soit pas directement relié aux autres machines internes, et il ne sera accessible qu'en http/s (donc ports 80 ou 443).

Adresse ip : 192.168.2.1

Nom d'utilisateur machine : root
Mot de passe : root

Nom d'utilisateur utilisateur : dandre
Mot de passe : oppg5



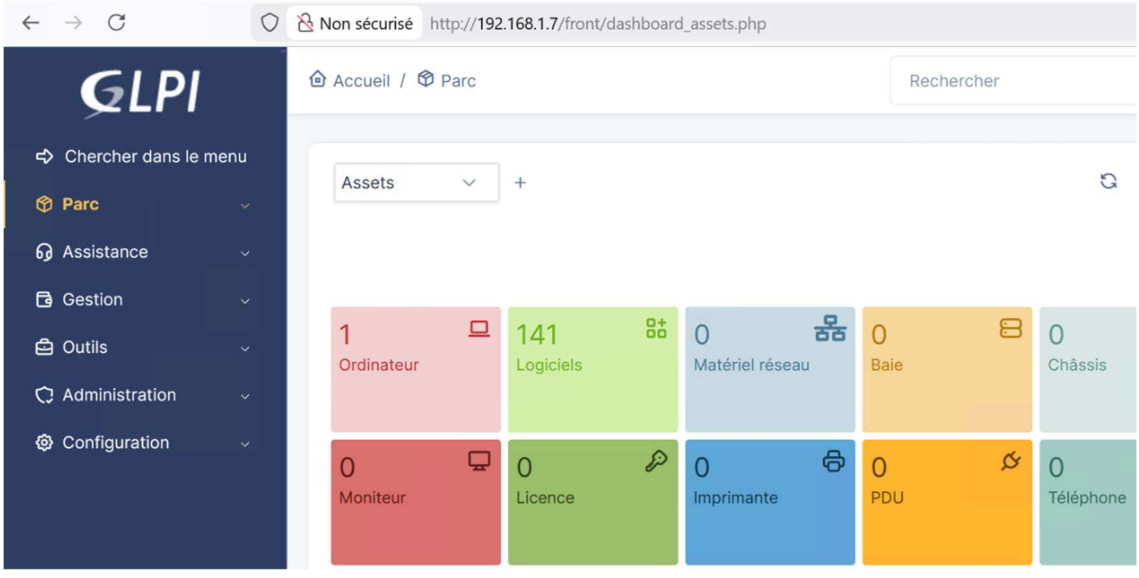

## Serveur GLPI

Nous installerons un GLPI dans notre LAN afin de pouvoir gérer les incidents et le matériel. On le placera avec nos autres serveurs car il n'a pas besoin d'être exposé à l'extérieur. De plus, il servira à gérer le matériel, les logiciels et les tickets utilisateurs internes seulement.

Adresse ip : 192.168.1.7

Nom d'utilisateur machine : root
Mot de passe machine : root

Nom d'utilisateur et mot de passe GLPI : glpi



## Serveur MariaDB

Notre serveur de base de données sera dans notre LAN avec le reste des serveurs. Il ne sera accessible qu'avec le port 3306 depuis le serveur web, le glpi et notre serveur Zabbix, pour des raisons de sécurité.
Nous utiliserons MariaDB. C'est un outil très fiable, simple et stable. Il est donc parfaitement adapté pour l'entreprise GSB.
Des sauvegardes seront effectuées vers le NAS tous les jours.
Pour cela, nous mettrons en place des scripts automatisés dans notre machine.
Notre serveur contient 2 bases de données.

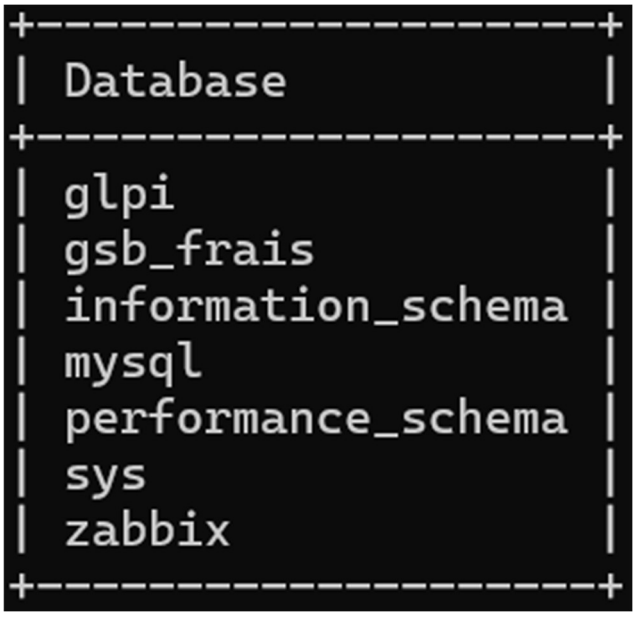
Adresse ip : 192.168.1.3

Nom d'utilisateur : root
Mot de passe : root

Utilisateur web : admin_web
Mot de passe : MDPweb17!

Utilisateur glpi : admin_glpi
Mot de passe : MDPglpi17!

Utilisateur zabbix : admin_glpi
Mot de passe : MDPzabbix17!



| Database |
|---|
| glpi |
| gsb_frais |
| information_schema |
| mysql |
| performance_schema |
| sys |
| zabbix |

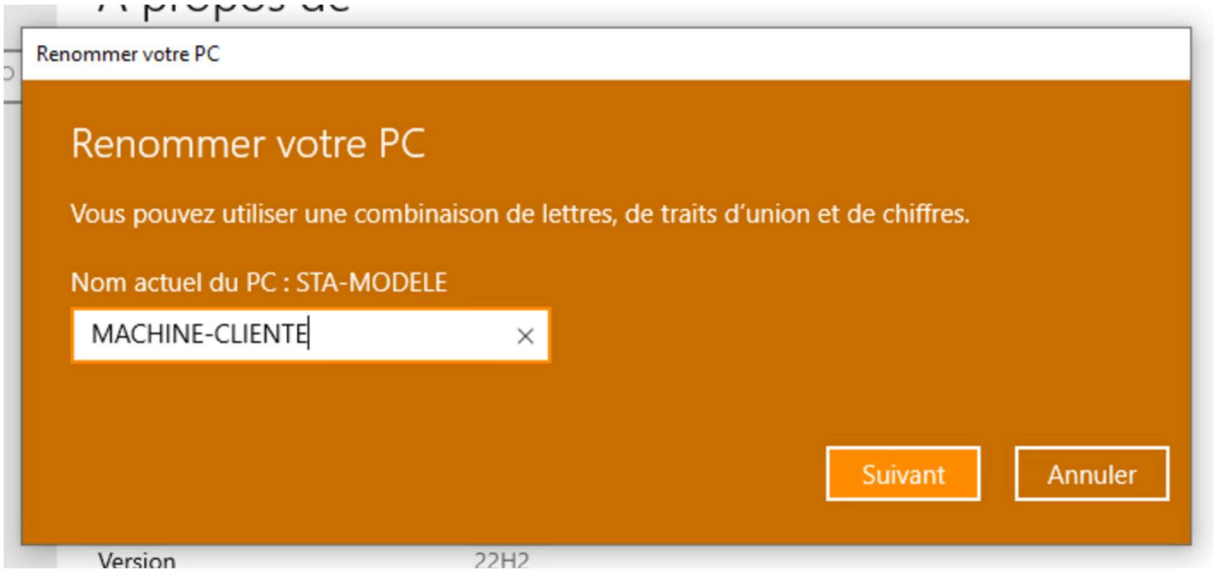
| User |
|---|
| admin_zabbix |
| Admin_glpi |
| Admin_glpi |
| admin_glpi |
| admin_web |
| userGsb |
| userGsb |
| admin_glpi |
| admin_web |
| admin_zabbix |
| mariadb.sys |
| mysql |
| root |

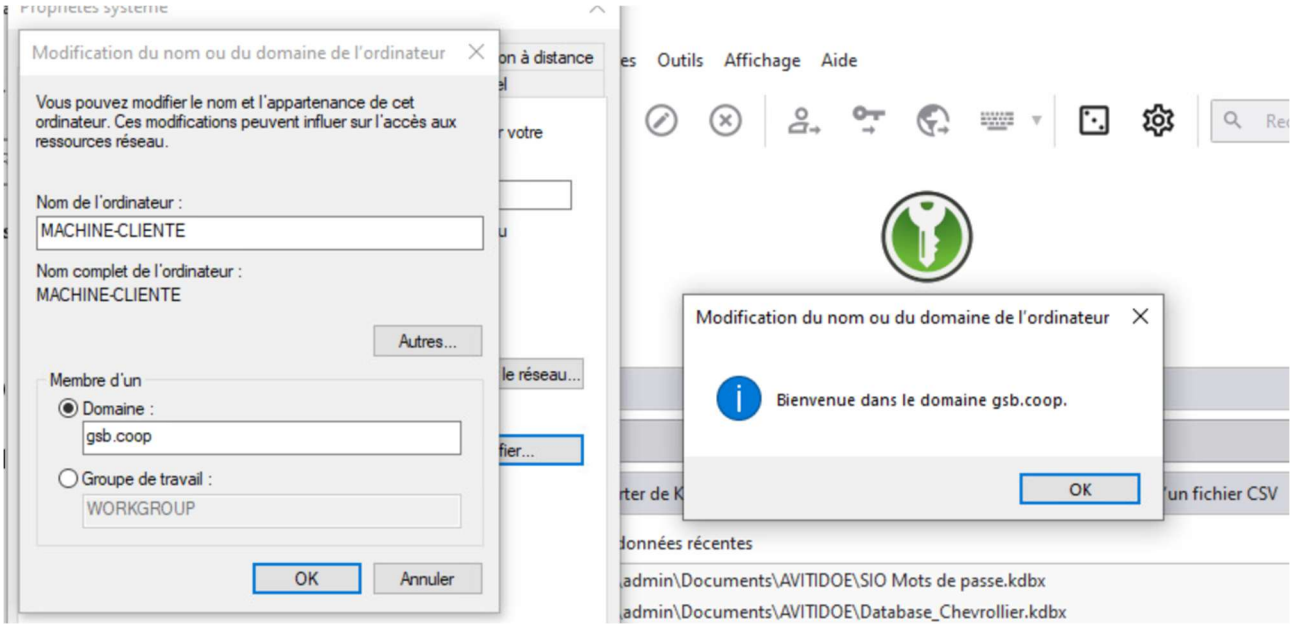
## Machine cliente

Création de la machine cliente pour tester le domaine, le DNS, ainsi que pour pouvoir configurer nos serveurs.

Adresse ip : 192.168.1.10

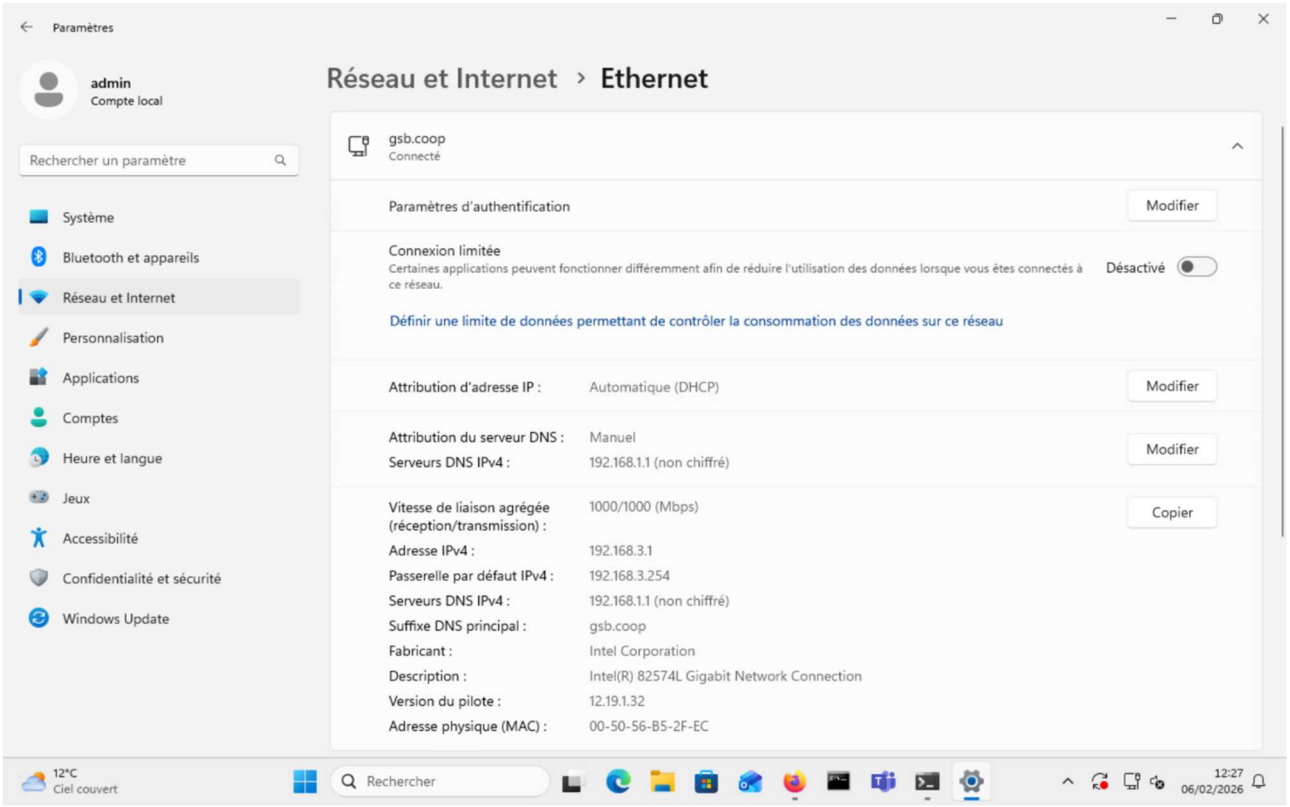
Nom d'utilisateur : admin
Mot de passe : azerty



## Machine cliente 2

Seconde machine cliente pour tester le DHCP

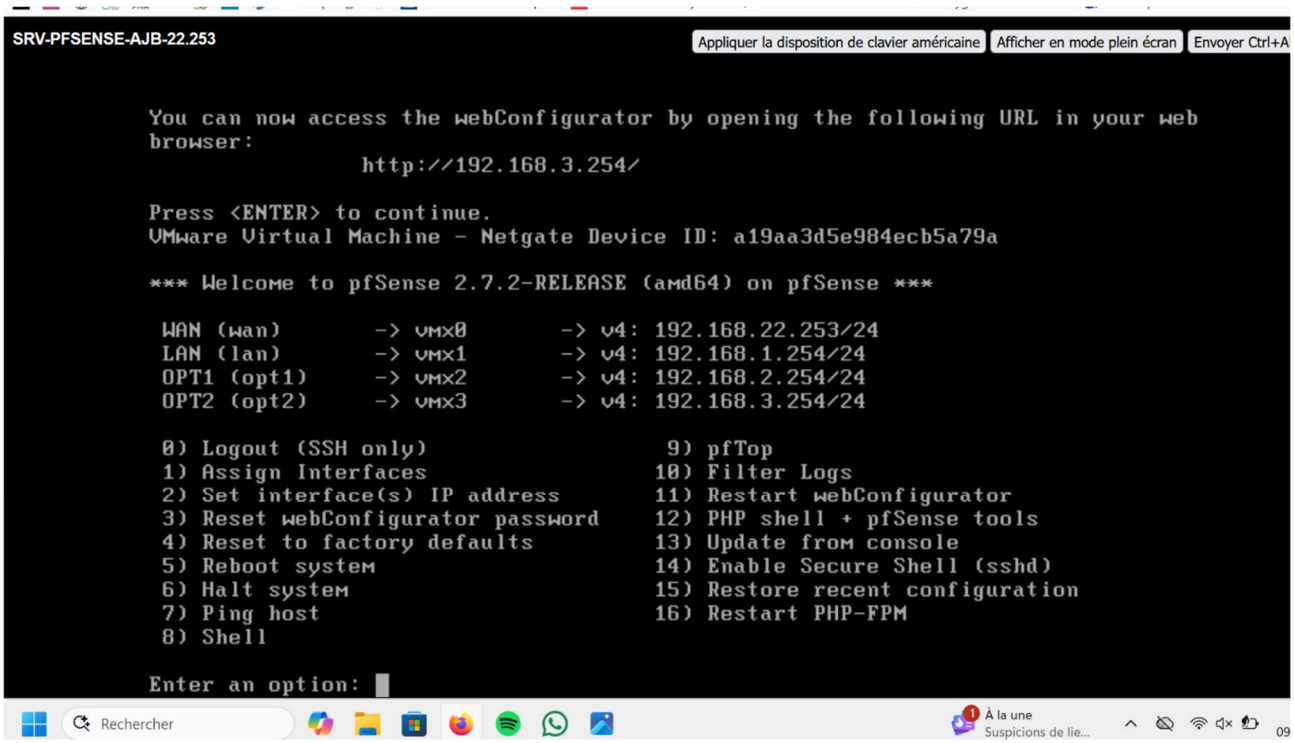



## Pare-feu pfSense

Notre pare-feu sera également notre routeur. Il aura pour rôle de sécuriser et de filtrer l'ensemble des flux entrants et sortants. Le NAT permettra de masquer les adresses privées du réseau interne. Des règles seront mises en place : depuis Internet vers la DMZ, seuls les flux HTTP/S seront autorisés ; depuis la DMZ vers le LAN, seuls les flux nécessaires entre le serveur Web et la base de données seront autorisés. Enfin, tous les accès seront journalisés afin de conserver une trace des flux. Nous utiliserons l'outil pfSense car c'est un outil majoritairement utilisé en entreprise, et il contient une interface graphique, ce qui est plus simple qu'un outil en ligne de commandes comme nftables. De plus, il permettra de mettre en place notre VPN.
Les règles n'ont pas été encore configurées, seules les interfaces sont paramétrées.

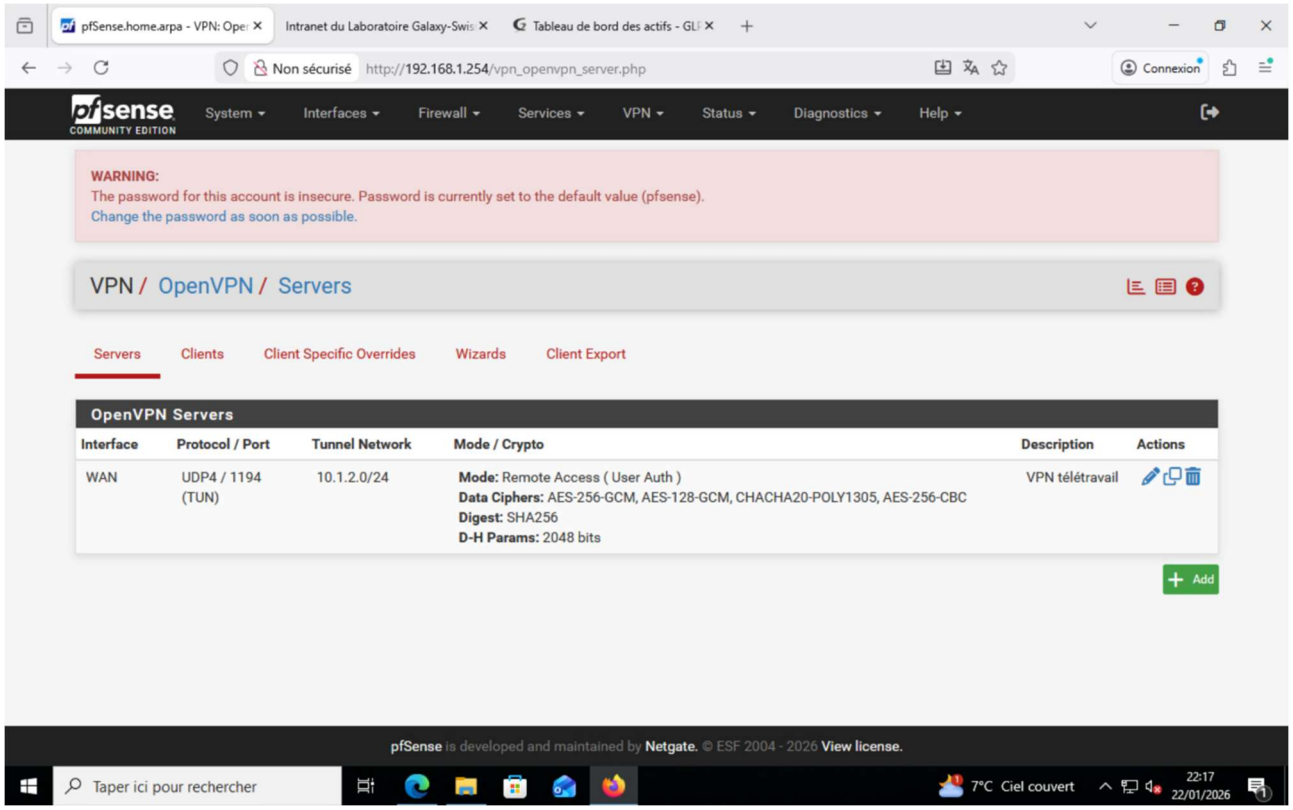
Nom d'utilisateur machine : root
Mot de passe machine : root

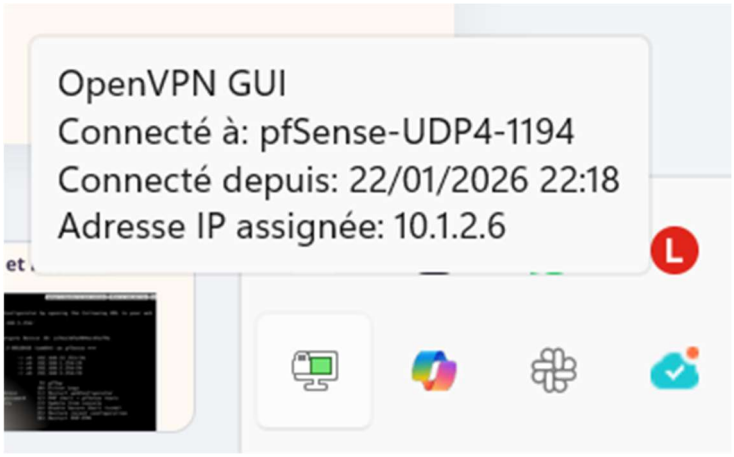
Nom d'utilisateur admin pfsense : admin
Mot de passe : pfsense




## VPN

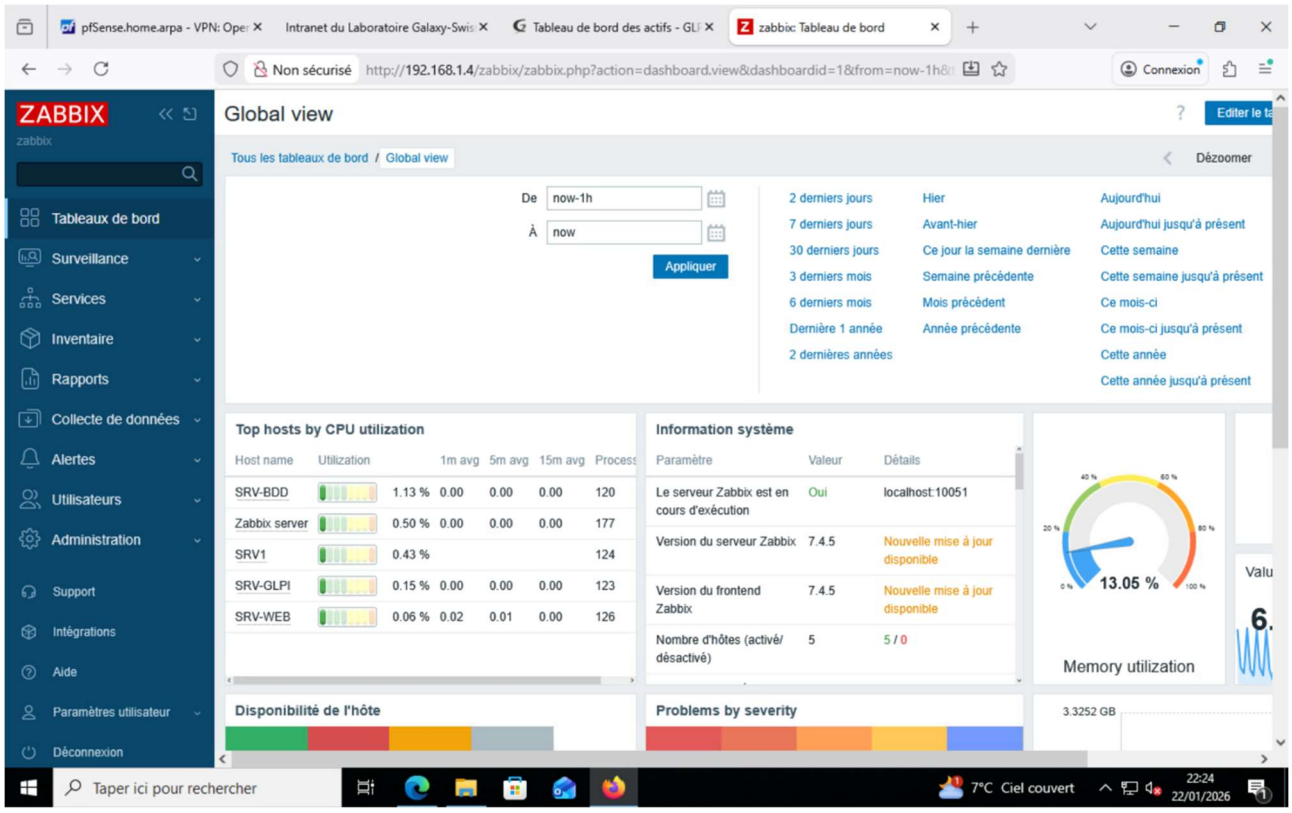
Le VPN servira aux télétravailleurs afin de pouvoir avoir accès aux serveurs à distance. On installe OpenVPN directement sur le pfSense. C'est le meilleur type de VPN pour un site à client.





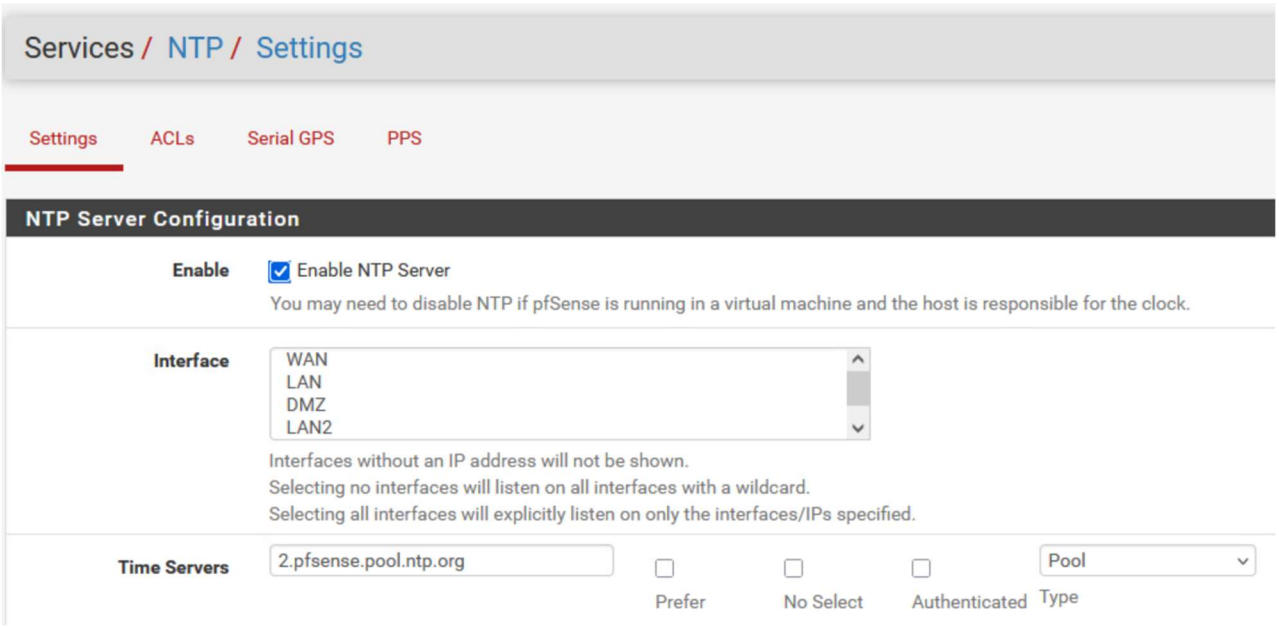

## Zabbix

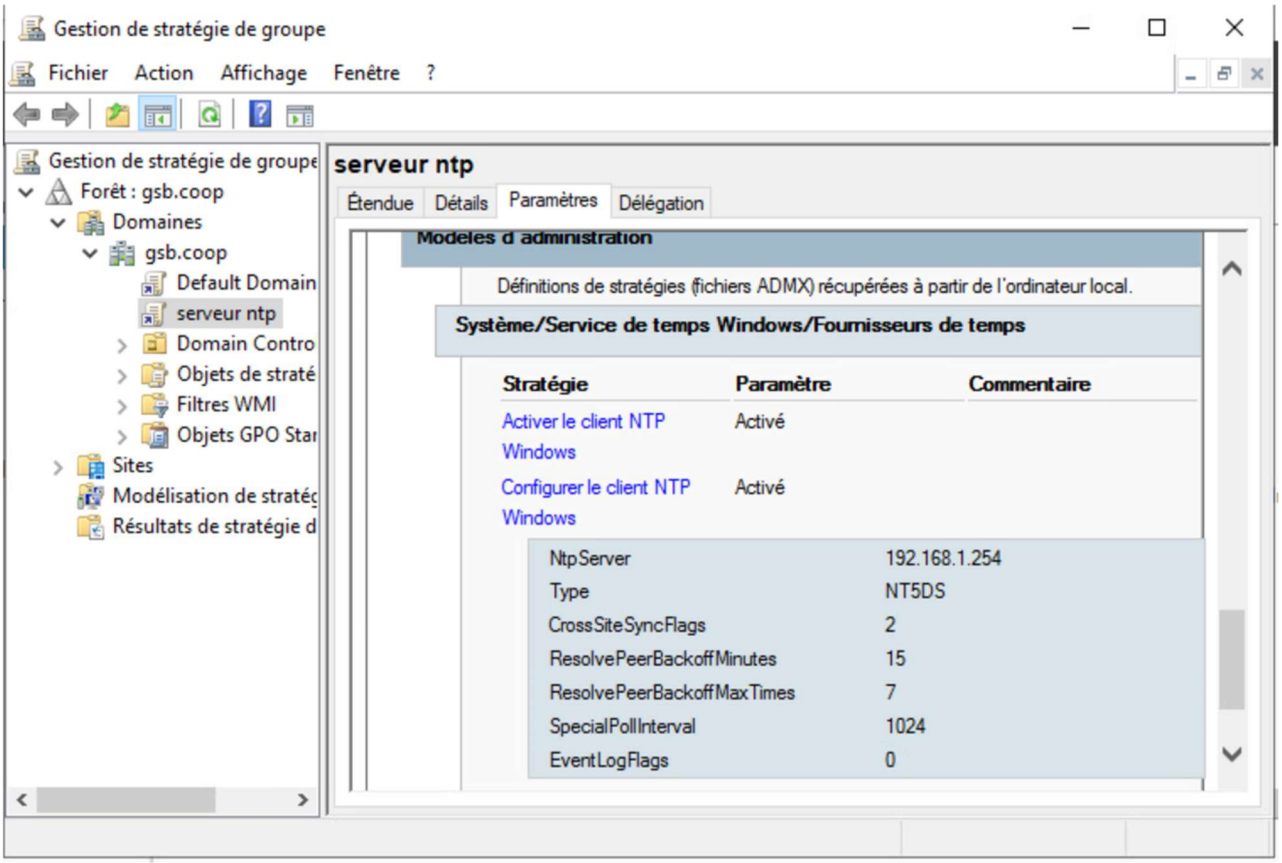
On met en place un serveur de supervision avec le service Zabbix. En effet, ce dernier nous permet de mettre des déclencheurs sur nos agents, qui sont nos autres serveurs. On peut par exemple définir un déclencheur lorsqu'on serveur ne fonctionne plus, ou alors qu'il n'a plus de stockage.



# NTP

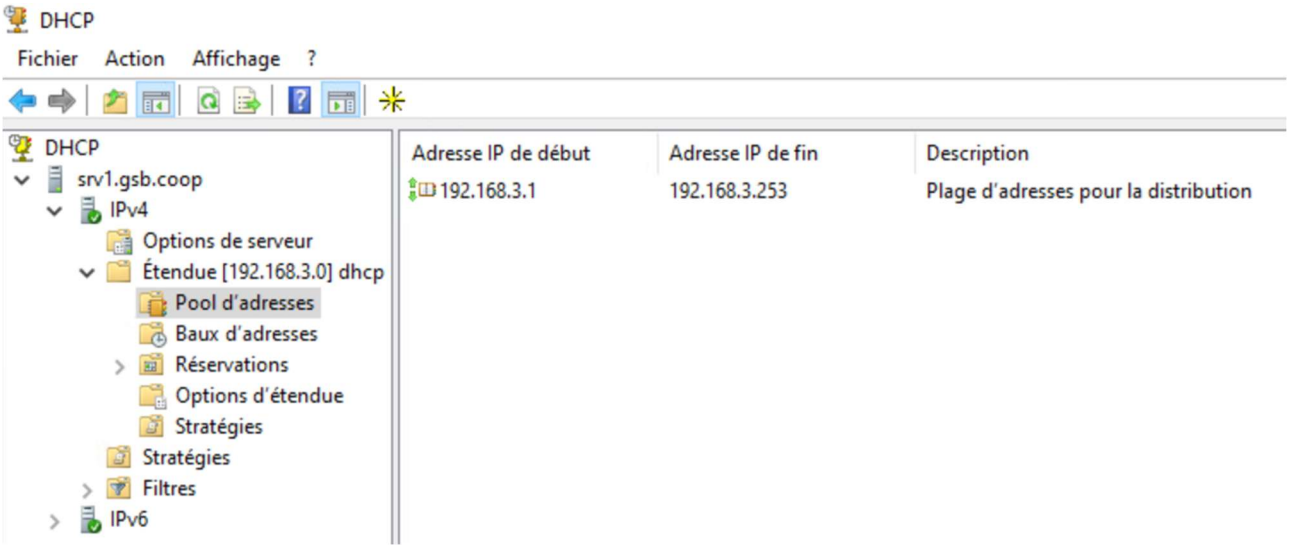
Pour mettre en place un serveur de temps, on peut directement utiliser celui du pfSense, pour ensuite créer une GPO qui fera redescendre l'heure à nos machines. Un serveur de temps est indispensable pour qu'en cas de problèmes, les machines aient toutes la même heure dans les logs.



## DHCP

Pour les utilisateurs, on configure un DHCP qui permettra de donner des adresses IP automatiquement. Cela est utile car on n'aura pas à tout paramétrer à la main, et cela permet que toutes les machines soient dans le même LAN, aient la même passerelle pour pouvoir avoir accès à internet grâce au routeur.




## NAS

Notre NAS servira à sauvegarder les données de nos machines, notamment les données de l'Active Directory, les bases de données ou encore les fichiers des pages web. Pour cela, on peut mettre en place des scripts notamment pour les bases de données.
Notre NAS sera une machine basée sur OpenMediaVault, qui est un serveur de stockage.

# Cybersécurité

La cybersécurité est un élément central de notre infrastructure, car elle garantit la confidentialité, l'intégrité et la disponibilité des données de l'entreprise GSB. Dans un environnement où les informations sont sensibles et où les utilisateurs accèdent à des applications internes via le réseau, il est indispensable de mettre en place des stratégies de cybersécurité.

Pour limiter les risques d'intrusion, tous les services de l'infrastructure sont protégés par des authentifications, gérées par notre domaine Active Directory.
Notre serveur Windows Server centralise tous les comptes utilisateurs et groupes.
Seuls les utilisateurs autorisés pourront se connecter aux services internes, avec un identifiant et un mot de passe.
Les droits d'accès seront gérés de manière à ce que, par exemple, seuls les développeurs puissent modifier les fichiers du serveur web, et seuls les membres du service comptable peuvent mettre à jour certaines données dans la base de données.
Notre Active Directory sera dupliqué pour garantir une haute disponibilité.

Pour l'administration à distance, le télétravail, ou la Gacilly, un VPN sécurisé sera disponible.

Le serveur web sera dans une DMZ. Cela limite l'impact d'une éventuelle intrusion : un hacker ayant accès au serveur web ne pourra pas atteindre directement la base de données interne où les autres serveurs.

Pour La Gacilly, les VLANS seront isolés, et pour le cas contraire nous déciderons au préalable qui peut échanger avec qui.

Un pare-feu/routeur filtre tous les flux entrants et sortants selon une politique stricte :

- Depuis Internet vers la DMZ : seuls les flux HTTP/S sont autorisés.
- Depuis la DMZ vers le LAN : seuls les flux nécessaires entre serveurs sont autorisés
- Tous les accès et tentatives de connexion seront journalisés, permettant la traçabilité et la détection d'activités suspectes.

Enfin, notre NAS permettra de faire des sauvegardes. Avec la règle 3-2-1 et les sauvegardes incrémentielles, les données seront presque imperdables.

# Veille technologique

Pour ma veille, j'utilise les tutos d'It-Connect, ou bien des tutos de Microsoft.
J'utilise également des anciens cours et procédures pour des notions déjà étudiées.