

1. Présentation du contexte (GSB) : .....	3
2. Liste des besoins (sujet) : .....	4
3. Cahier des charges incluant une estimation financière des investissements .....	5
3.1 Introduction et Contexte du projet.....	5
3.2 Objectif du projet .....	5
3.3 informations sur les services .....	5
3.4 Estimation financière .....	7
4. Schémas des processus de l'entreprise modifiés par le projet.....	8
5. Diagramme de Gantt.....	9
5.1 Durée prévisionnelle du projet .....	9
5.2 Durée effective du projet .....	9
5.3 Diagramme des ressources montrant la répartition des taches .....	10
6. Description de la réalisation étape par étape.....	11
6.1 Mise en place d'un outil de gestion de parc informatique : GLPI.....	11
6.2 Mise en place d'un outil de sauvegarde : Veeam Backup.....	13
6.3 Mise en place d'un outil de supervision : Zabbix .....	13
6.4 Configuration des mises à jour automatisés avec windows server .....	14
6.5 Configuration Pfsense .....	18
6.6 Configuration Portail captif .....	19
6.7 Configuration d'un Active Directory.....	21
6.8 Déploiement automatisé avec Docker .....	23
7. Jeu de tests .....	24
7.1 Ajout d'une machine à un parc informatique: GLPI .....	24
7.2 Test de restauration de fichier : Veeam Backup .....	27
7.3 Ajout d'une machine à la solution de superviseur: Zabbix .....	32
7.4 Automatisation de deux containers :Docker.....	35
7.5 filtrage proxy avec squid .....	37
7.6 test de déploiement automatisé avec lstp.....	38
8. Manuel technique.....	39
8 .1 Mise en place d'un outil de gestion de parc informatique : GLPI.....	39
8.2 Mise en place d'un outil de sauvegarde : VeeamBackup .....	43

8.3 Mise en place d'un outil de supervision : Zabbix .....	44
8.4 Configuration des mises à jour automatisés avec windows server .....	46
8.5 Configuration Pfsense .....	69
8.6 Configuration Portail captif .....	71
8.7 Configuration d'un Active Directory .....	77
8.8 Déploiement automatisé avec LSTP .....	78
8.9 Mise en place d'un proxy : Squid .....	81
9. Manuel utilisateur .....	82
9 .1 Mise en place d'un outil de gestion de parc informatique : GLPI.....	82
9.2 Mise en place d'un outil de sauvegarde : Veeam Backup.....	91
9.3 Utilisation de Zabbix.....	95
9.4 Utilisation du portail captif.....	100
9.5 Déploiement automatisé avec Docker .....	102
9.6 Ajoute de mises à jour approuvés avec WSUS .....	103
9.7 Utilisation du proxy squid .....	105
9.8 Utilisation de LSTP .....	107
10. Références bibliographiques (liste des sources documentaires) .....	108
11. Conclusion sur le travail réalisé ou restant à faire .....	109

## 1. Présentation du contexte (GSB) :

GSB est une entreprise exerçant dans le domaine pharmaceutique et qui fait face à un défi de grande envergure : moderniser et optimiser son infrastructure informatique. Cela est crucial pour plusieurs raisons : maintenir sa compétitivité dans un secteur dynamique comme celui de la pharmacie, optimiser la sécurisation des données sensibles pour éviter les fuites d'informations et les cyberattaques, et offrir des services de haute qualité à la clientèle en répondant mieux à leurs besoins avec des services plus rapides, fiables et personnalisés. Même pour une entreprise comme GSB, qui n'exerce pas directement dans le domaine de l'informatique, disposer d'une infrastructure informatique opérationnelle et optimisée est indispensable. Cela permet non seulement de soutenir les opérations quotidiennes, mais aussi de favoriser l'innovation et l'amélioration continue des services offerts. En investissant dans des technologies de pointe et en formant son personnel aux outils numériques, GSB peut ainsi renforcer sa position sur le marché et garantir une satisfaction client optimale.

## 2. Liste des besoins (sujet) :

1. **Mise en place Routeur et pare-feu logiciel** : Assurent la gestion du trafic réseau et protègent contre les menaces externes en filtrant les données entrantes et sortantes.
2. **Portail captif** : Permet de contrôler l'accès au réseau en redirigeant les utilisateurs vers une page de connexion avant de leur accorder l'accès.
3. **Segmenter efficacement le réseau et isoler (VLAN, DMZ)** : Utilise des VLAN pour séparer les segments de réseau et une DMZ pour isoler les services accessibles depuis l'extérieur, augmentant ainsi la sécurité.
4. **Contrôleur de domaine** : Gère les identités et les accès des utilisateurs au sein du réseau, centralisant l'authentification et les autorisations.
5. **Services DNS et DHCP** : Le DNS traduit les noms de domaine en adresses IP, tandis que le DHCP attribue automatiquement des adresses IP aux appareils du réseau.
6. **Gestion centralisée des mises à jour Windows** : Permet de déployer et de gérer les mises à jour de sécurité et de fonctionnalité sur tous les ordinateurs du réseau de manière centralisée.
7. **Outil de gestion de parc et de tickets** : Facilite la gestion des actifs informatiques et le suivi des demandes de support technique, améliorant ainsi l'efficacité du service informatique.
8. **Outil de supervision** : Surveille en temps réel les performances et la disponibilité des systèmes et des réseaux, permettant une détection rapide des problèmes.
9. **Déploiement automatisé** : Standardise les installations de logiciels et de systèmes, réduit les erreurs humaines et accélère la mise en service de nouveaux équipements.
10. **Solution de sauvegarde et de restauration** : Assure la protection des données en réalisant des copies de sauvegarde régulières et permet une récupération rapide en cas de perte de données.

### 3. Cahier des charges incluant une estimation financière des investissements

#### 3.1 Introduction et Contexte du projet

GSB est une société spécialisée dans le domaine pharmaceutique, dont l'infrastructure informatique nécessite une modernisation pour répondre aux exigences actuelles du marché. À l'ère du numérique, il est crucial pour GSB d'adopter des technologies modernes afin de rester compétitive et efficace. En améliorant leurs systèmes informatiques, GSB pourra offrir de meilleurs services à ses clients, assurer une meilleure gestion des données et sécurisé davantage son infrastructure pour lutter contre les cyber-attaques.

#### 3.2 Objectif du projet

L'objectif de ce projet est de mettre en place divers services pour améliorer l'infrastructure informatique de GSB. En modernisant leur infrastructure, GSB pourra non seulement améliorer son efficacité opérationnelle mais aussi la qualité de ses services. Cela permettra également de renforcer la productivité, d'assurer une meilleure sécurité des données et d'intégrer des solutions de cybersécurité robustes. Le projet vise à adapter les technologies aux besoins spécifiques de GSB pour soutenir sa croissance et son développement futur, tout en protégeant l'entreprise contre les menaces des cyberattaquants.

#### 3.3 Informations sur les services

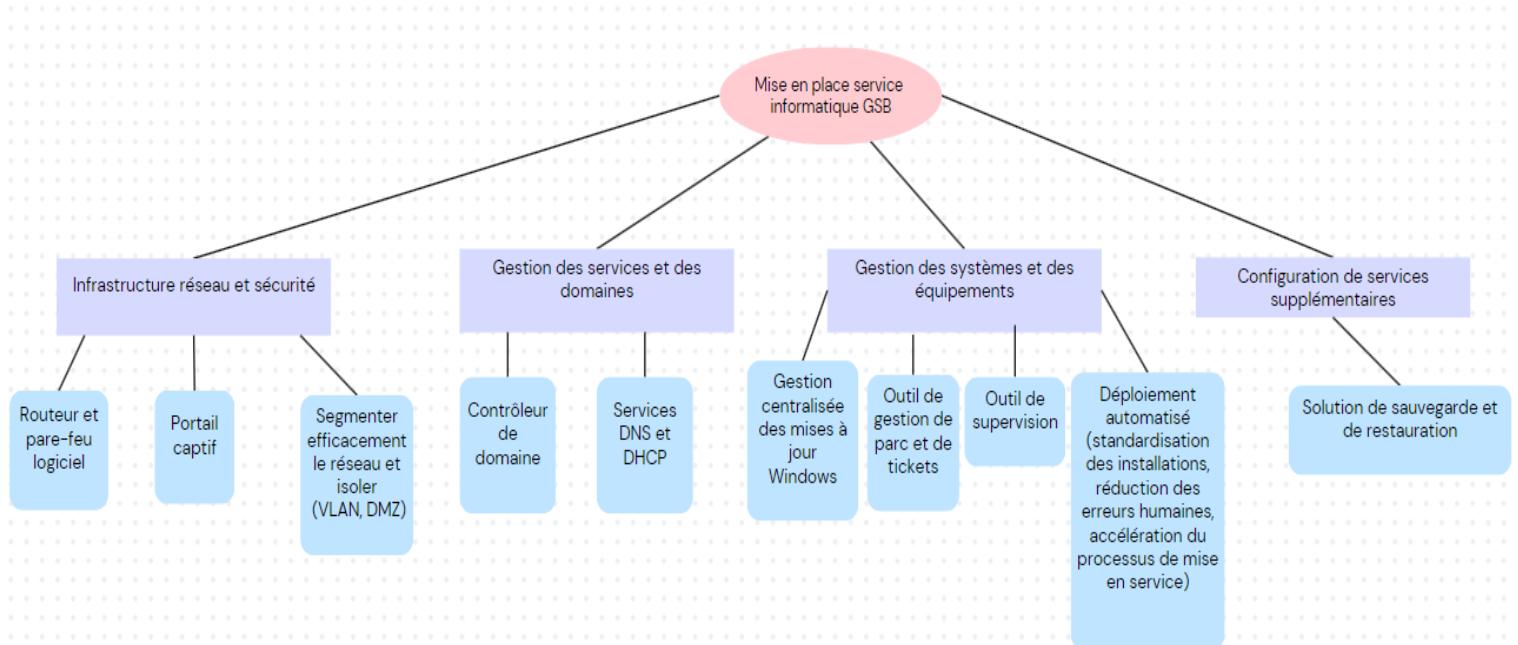
Liste des services	Logiciel/Solution utilisé	Description
Mise en place Routeur et pare-feu logiciel	PfSense	Service qui va permettre d'ajouter des règles sécurité pour sécuriser davantage le réseau
Portail captif	PfSense	Service qui va demander aux utilisateurs du réseau wifi de s'authentifier afin de contrôler l'accès au réseau
Segmenter efficacement le réseau et isoler (VLAN, DMZ)	PfSense	L'isolement du réseau est une couche supérieure de sécurité qui permet d'isoler au sein du réseau même pour limiter les risques en cas d'infrastructure compromise

Contrôleur de domaine	Windows Server 2016	Système permettant de centraliser dans un annuaire tous les utilisateurs de l'entreprise mais aussi d'appliquer des gestions de stratégie de groupe
Services DNS et DHCP	PfSense	Service permettant d'automatiser attribuer une adresse ip pour le dhcp et de résoudre un nom de domaine pour le DNS.
Gestion centralisée des mises à jour Windows	Windows Server 2016/WSUS	Service permettant de centraliser les mises à jour et de les filtrer selon les besoins.
Outil de gestion de parc et de tickets	GLPI	Outil permettant la centralisation des appareils du parc informatique et des tickets.
Outil de supervision	Zabbix	Service permettant de surveiller les appareils du parc et de s'assurer de leur bon fonctionnement
Déploiement automatisé	Docker	Outil permettant de déployer automatiquement divers services et outils bénéfiques à l'infrastructure informatique.
Solution de sauvegarde et de restauration	Veeam Backup	Outil permet de sauvegarder des données importantes et de les restaurer en cas de cyber-attaque ou d'erreur humaine/matériel.

### 3.4 Estimation financière

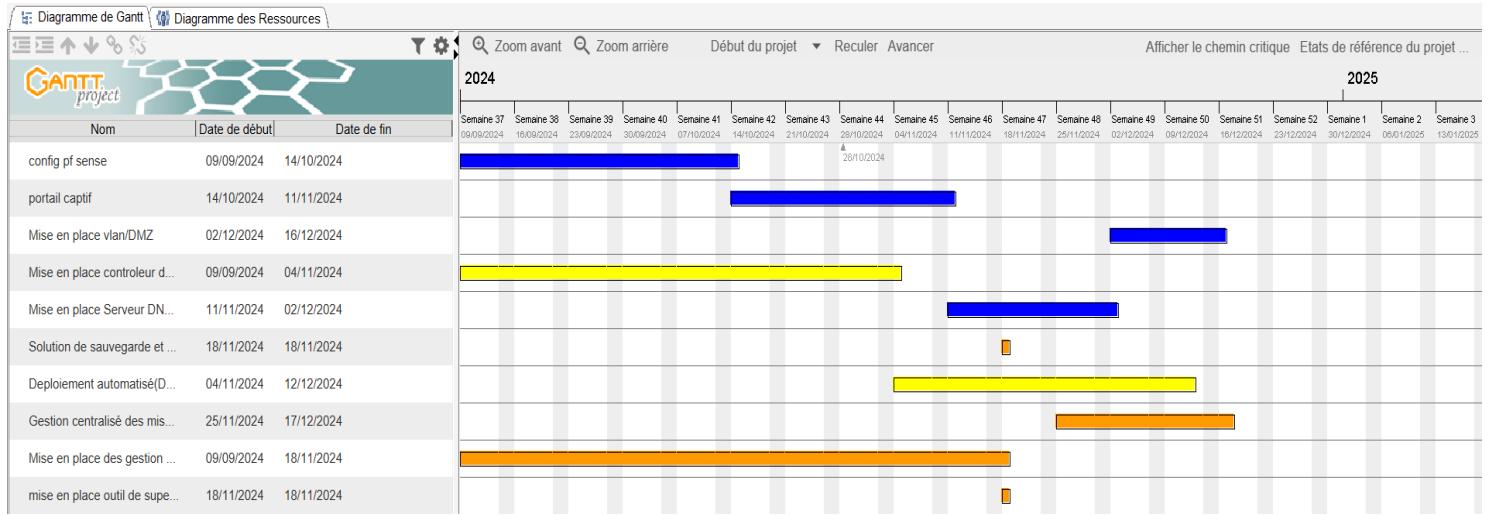
Iso/matériel nécessaire à la mise en place des services	Services concernés	Prix
Serveur	Tous les services sont mis en place sur le serveur	Entre 3 000 € et 10 000 €
PfSense	Mise en place Routeur et pare-feu logiciel, Portail captif, Segmenter efficacement le réseau et isoler (VLAN, DMZ), Services DNS et DHCP	Gratuit
Linux(Ubuntu/Debian)	Outil de gestion de parc et de tickets , Outil de supervision , Déploiement automatisé, Solution de sauvegarde et de restauration	Gratuit
Windows 10	Contrôleur de domaine, Gestion centralisée des mises à jour Windows, service nécessitant l'accès à l'interface web(PfSense, GLPI, Zabbix)	Gratuit
Windows Server	Contrôleur de domaine, Gestion centralisée des mises à jour Windows	Gratuit

#### 4. Schémas des processus de l'entreprise modifiés par le projet



## 5. Diagramme de Gantt

### 5.1 Durée prévisionnelle du projet

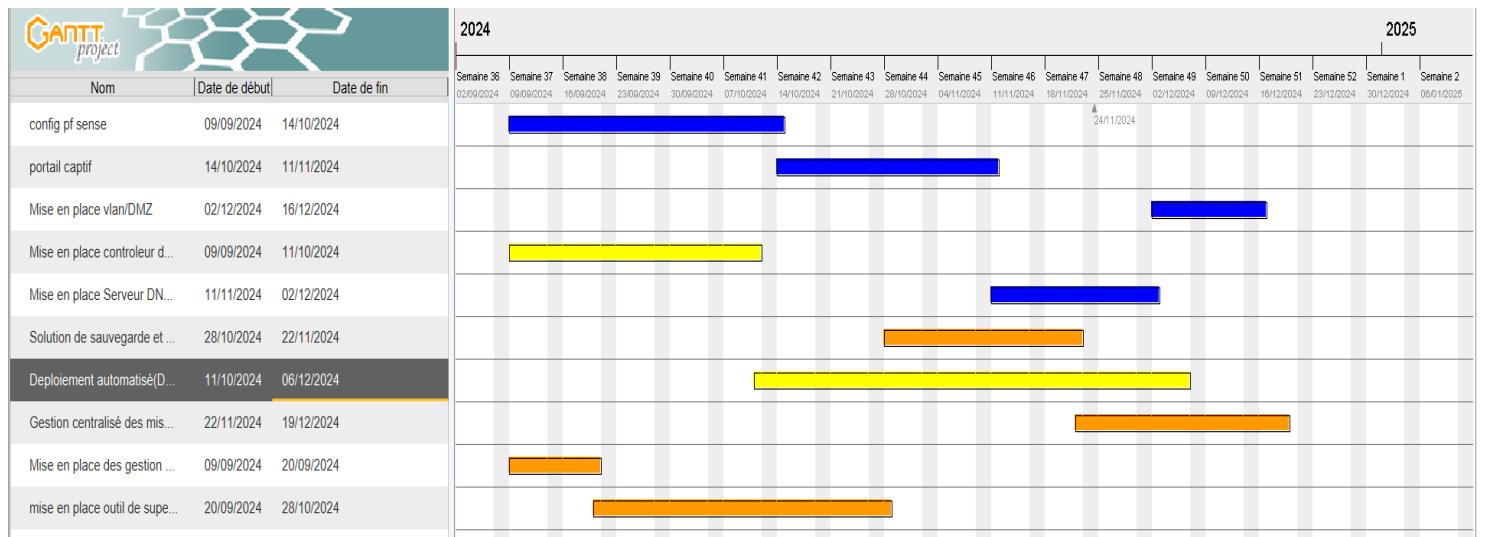


Mathéo en Orange

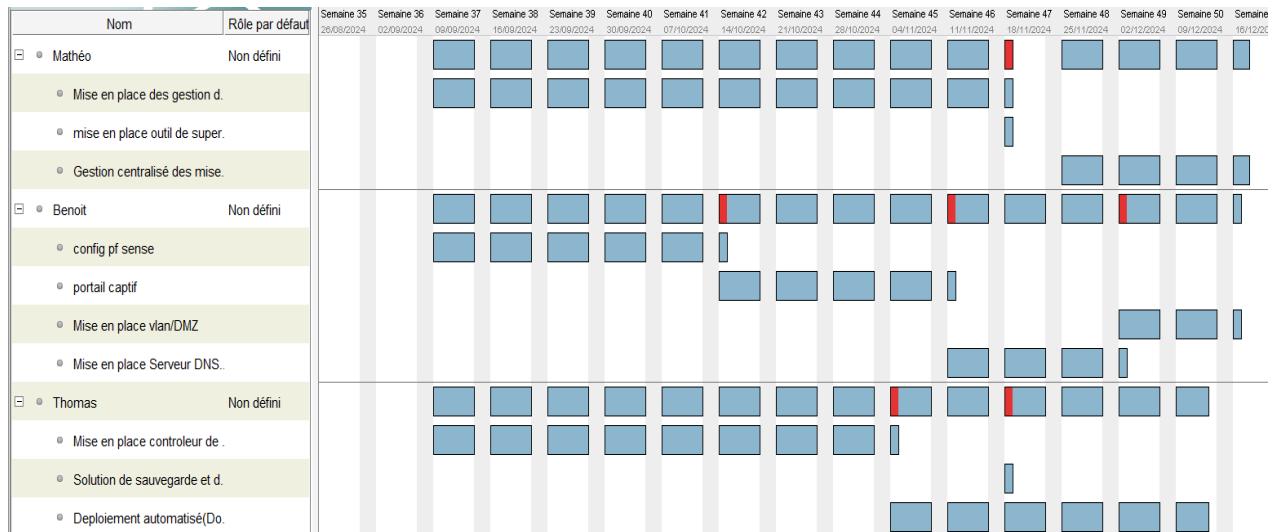
Thomas en Jaune

Benoit en Bleu

### 5.2 Durée effective du projet



## 5.3 Diagramme des ressources montrant la répartition des tâches



## 6. Description de la réalisation étape par étape

### 6.1 Mise en place d'un outil de gestion de parc informatique : GLPI

#### **ETAPE 1 : Installation de MySQL**

##### **1. Mettre à jour la liste des paquets**

- Utiliser la commande apt-get update.

##### **2. Installer MariaDB-Server**

- Utiliser la commande apt-get install -y mariadb-server.

##### **3. Lancer l'installation sécurisée**

- Utiliser la commande mysql\_secure\_installation.

##### **4. Configurer les options de sécurité**

- Répondre **y** (yes) à toutes les options de sécurité sauf pour celle concernant le changement de mot de passe root. Modifier ce mot de passe plus tard avec la commande ALTER.

#### **ETAPE 2 : Prérequis avant d'installer GLPI**

##### **1. Installer Apache2 et les modules PHP nécessaires**

- Utiliser les commandes appropriées pour installer Apache2 et les modules PHP.

##### **2. Configurer MySQL pour GLPI**

- Créer un utilisateur glpi et une base de données glpi.
- Donner tous les droits à l'utilisateur glpi sur la base de données glpi.

#### **ETAPE 3 : Installation de GLPI**

##### **1. Télécharger et installer GLPI**

- Se rendre dans le répertoire /var/www/html.
- Télécharger l'archive GLPI depuis GitHub en utilisant wget.
- Extraire l'archive avec la commande tar.

##### **2.Modifier les droits propriétaires des fichiers**

- Utiliser la commande chown pour modifier les droits de propriétaire.

## **ETAPE 4 : Finalisation sur l'interface web**

### **1. Accéder à l'interface web**

- Aller sur [http://adresse\\_ip\\_du\\_serveur\\_glpi](http://adresse_ip_du_serveur_glpi).

### **2. Configurer GLPI via l'interface web**

- Entrer le port sur lequel est hébergé le serveur SQL ainsi que les identifiants.
- Sélectionner la base de données à utiliser pour GLPI.

## **Étape 5 : Installation de Agent-GLPI**

### **1. Installez le paquet 'perl' :**

- Pour pouvoir exécuter le script d'installation, vous devez installer le paquet 'perl'. Ce paquet est nécessaire pour exécuter le script d'installation de l'agent GLPI.

### **2. Téléchargez le script d'installation :**

- Utilisez wget pour télécharger le fichier script d'installation .pl de la version de votre choix de l'agent GLPI. Assurez-vous d'avoir accès à l'URL du fichier .pl.

## **Étape 6 : Exécution et configuration**

### **4. Exécutez le script d'installation :**

- Avec perl, exécutez le script téléchargé. Utilisez l'option -s pour spécifier le serveur GLPI. La commande ressemblera à perl script.pl -s [http://adresse\\_du\\_serveur](http://adresse_du_serveur).

### **5. Redémarrez agent-glpi :**

- Une fois l'installation terminée, redémarrez l'agent GLPI pour appliquer les modifications et commencer à collecter des données sur les appareils du parc informatique.

## 6.2 Mise en place d'un outil de sauvegarde : Veeam Backup

### **Étape 1 : Installation des paquets nécessaires pour Veeam**

1. Télécharger le dépôt .deb de Veeam.
2. Ajouter le dépôt à la liste des paquets en utilisant la commande `dpkg -i ./veeam-release*`.

### **Étape 2 : Mise à jour et installation des paquets**

1. Mettre à jour la liste des paquets disponibles avec la commande `apt-get update`.
2. Installer les paquets principaux en utilisant `apt-get install blksnap veeam -y`.
3. Ajouter le paquet complémentaire avec `apt-get install veeam-nosnap -y`.

### **Étape 3 : Vérification de l'installation**

1. Pour vérifier que l'installation s'est bien déroulée, exécuter `veeamconfig ui`

## 6.3 Mise en place d'un outil de supervision : Zabbix

## **Étape 1 : Sélection de la distribution Linux**

1. L'utilisateur doit indiquer son mot de passe root pour le serveur SQL.
2. Il sélectionne sa distribution Linux : Debian ou Ubuntu.

## **Étape 2 : Installation des paquets nécessaires**

1. Mettre à jour la liste des paquets disponibles.
2. Installer les composants essentiels de Zabbix

## **Étape 3 : Configuration de la base de données**

1. Création de la base de données zabbix.
2. Définition d'un utilisateur zabbix avec les droits nécessaires.

## **Étape 4 : Finalisation de l'installation**

1. Génération d'un fichier de configuration pour le démarrage des services Zabbix.
2. Activation et redémarrage des services (zabbix-server, zabbix-agent, apache2).
3. Modification manuelle du fichier /etc/zabbix/zabbix\_server.conf pour définir le mot de passe de la base de données.
4. Une fois cette modification effectuée, il faut redémarrer zabbix.

## 6.4 Configuration des mises à jour automatisés avec windows server

### **1. Installer le service wsus :**

- Sur le gestionnaire des serveurs sélectionner « ajouter des rôles et des fonctionnalités » puis sur « service wsus » pour l'installer

## **2. Créer et lier un objet GPO :**

- Ouvrez la fenêtre "Exécuter" avec win+r et tapez gpmc.msc.
- Accédez à Forest\Domains\Votre\_Domaine et sélectionnez Crée un objet GPO dans ce domaine et le lier ici.
- Nommez le nouvel objet GPO "WSUS - Emplacement du service de mise à jour automatique et intranet".
- Cliquez avec le bouton droit sur l'objet GPO précédemment créé puis sélectionnez Modifier.

## **3. Configurer les mises à jour automatiques :**

- Dans l'éditeur de gestion des stratégies de groupe, accédez à : Configuration ordinateur\Stratégies\Modèles d'administration\Composants Windows\Windows Update.
- Cliquez avec le bouton droit sur le paramètre Configurer les mises à jour automatiques, puis sélectionnez Modifier.
- Dans la boîte de dialogue Configurer les mises à jour automatiques, sélectionnez Activer.
- Sous Options, dans la liste Configurer la mise à jour automatique, sélectionnez 3 - Téléchargement automatique et notification pour l'installation, puis sélectionnez OK.

## **4. Spécifier l'emplacement du service de mise à jour intranet :**

- Cliquez avec le bouton droit sur le paramètre Spécifier l'emplacement du service de mise à jour Microsoft intranet, puis sélectionnez Modifier.
- Dans la boîte de dialogue Spécifier l'emplacement du service de mise à jour Microsoft intranet, sélectionnez Activer.
- Sous Options, dans les options Définir le service de mise à jour intranet pour la détection des mises à jour et Définir le serveur de statistiques intranet, saisissez [http://Votre\\_Adresse\\_IP:8530](http://Votre_Adresse_IP:8530), puis sélectionnez OK.
- Si cela n'est pas déjà fait rajouter une règle de pare feu entrant autorisant le port 8530

## **5. Créez les groupes d'ordinateurs sur la console wsus :**

- Tapez Ring 2 Pilot Business Users comme nom, puis sélectionnez Ajouter.

- Répétez ces étapes pour les groupes Ring 3 Broad IT et Ring 4 Broad Business Users.
- Une fois terminé, vous devez avoir trois groupes d'anneaux de déploiement.

## **6. Configurer WSUS pour autoriser le ciblage côté client à partir de la stratégie de groupe :**

- Ouvrez la console d'administration WSUS, accédez à Nom\_serveur\Options, puis sélectionnez Ordinateurs.
- Dans la boîte de dialogue Ordinateurs, sélectionnez Utiliser la stratégie de groupe ou les paramètres de registre sur les ordinateurs, puis sélectionnez OK.

## **7. Configurer WSUS pour autoriser le ciblage côté client :**

- Ouvrez la console de gestion des stratégies de groupe (gpmc.msc).
- Développez Forest\Domains\Votre\_Domaine.
- Cliquez avec le bouton droit sur Votre\_Domaine, puis sélectionnez Créez un objet GPO dans ce domaine et le lier ici.
- Dans la boîte de dialogue Nouvel objet GPO, saisissez WSUS - Ciblage client - Ring 4 Broad Business Users comme nom du nouvel objet GPO.
- Cliquez avec le bouton droit sur l'objet GPO WSUS - Client Targeting - Ring 4 Broad Business Users, puis sélectionnez Modifier.
- Sélectionnez l'anneau WSUS 4 et modifiez-le dans la stratégie de groupe.
- Dans l'éditeur de gestion des stratégies de groupe, accédez à : Configuration ordinateur\Stratégies\Modèles d'administration\Composants Windows\Windows Update.
- Cliquez avec le bouton droit sur Activer le ciblage côté client, puis sélectionnez Modifier.
- Dans la boîte de dialogue Activer le ciblage côté client, sélectionnez Activer.
- Créez 3 unités d'organisation, une pour chaque groupe d'ordinateur.
- Fermez l'éditeur de gestion des stratégies de groupe.

## **8. Étendre l'objet GPO à un groupe :**

- Dans GPMC, sélectionnez la stratégie WSUS - Ciblage client - Ring 4 Broad Business Users.
- Sélectionnez l'onglet Portée.

- Appliquer à l'unité d'organisation

## **9. Approuver et déployer automatiquement les mises à jour des fonctionnalités :**

- Dans la console d'administration WSUS, accédez à Services de mise à jour\Nom\_serveur\Options, puis sélectionnez Approbations automatiques.
- Dans l'onglet Mettre à jour les règles, sélectionnez Nouvelle règle.
- Dans la boîte de dialogue Ajouter une règle, cochez les cases Lorsqu'une mise à jour concerne une classification spécifique, Lorsqu'une mise à jour concerne un produit spécifique et Définir une date limite pour l'approbation.
- Dans la zone Modifier les propriétés, sélectionnez une classification. Désélectionnez tous les éléments sauf Mises à niveau, puis sélectionnez OK.
- Dans la zone Modifier les propriétés, sélectionnez le lien de n'importe quel produit. Décochez toutes les cases sauf Windows 10, puis sélectionnez OK.
- Dans la zone Modifier les propriétés, sélectionnez le lien Tous les ordinateurs. Décochez toutes les cases du groupe d'ordinateurs, à l'exception de Ring 3 Broad IT, puis sélectionnez OK.
- Laissez le délai fixé à 7 jours après l'approbation à 3h00 du matin.
- Dans la zone Étape 3 : Spécifier un nom, saisissez Approbation automatique de la mise à niveau de Windows 10 pour Ring 3 Broad IT, puis sélectionnez OK.
- Dans la boîte de dialogue Approbations automatiques, sélectionnez OK.

## **10. Approuver et déployer manuellement les mises à jour des fonctionnalités :**

- Dans la console d'administration WSUS, accédez à Update Services\Server\_Name\Updates.
- Dans le volet Action, sélectionnez Nouvelle vue de mise à jour.
- Dans la boîte de dialogue Ajouter une vue de mise à jour, sélectionnez Les mises à jour sont dans une classification spécifique et Les mises à jour concernent un produit spécifique.
- À l'étape 2 : Modifier les propriétés, sélectionnez une classification. Décochez toutes les cases sauf Mises à niveau, puis sélectionnez OK.
- À l'étape 2 : Modifier les propriétés, sélectionnez un produit. Décochez toutes les cases sauf Windows 10, puis sélectionnez OK.
- Dans la zone Étape 3 : Spécifier un nom, saisissez Toutes les mises à niveau de Windows 10, puis sélectionnez OK.

- Dans la console d'administration WSUS, accédez à Update Services\Server\_Name\Updates\All Windows 10 Upgrades.
- Cliquez avec le bouton droit sur la mise à jour de fonctionnalité que vous souhaitez déployer, puis sélectionnez Approuver.  
(Dans la boîte de dialogue Approuver les mises à jour, dans la liste Utilisateurs professionnels Ring 4 Broad, sélectionnez Approuvé pour l'installation.)
- Dans la boîte de dialogue Approuver les mises à jour, dans la liste Utilisateurs professionnels Ring 4 Broad, sélectionnez Date limite, sélectionnez Une semaine, puis sélectionnez OK.
- Si la boîte de dialogue Termes du contrat de licence du logiciel Microsoft s'ouvre, sélectionnez Accepter.
- Si le déploiement réussit, vous devriez recevoir un rapport de progression réussi.
- Dans la boîte de dialogue Progression de l'approbation, sélectionnez Fermer.

## 6.5 Configuration Pfsense

La solution pfSense a été déployée au sein de l'infrastructure réseau virtualisée via une machine virtuelle dédiée. Pour cela, une image ISO de pfSense a été installée, permettant ensuite la configuration des différentes interfaces réseau : **WAN**, **LAN** et **DMZ**.

Une fois le pare-feu pfSense opérationnel, l'accès à l'interface web d'administration a été réalisé depuis une machine Windows du même réseau, via l'adresse IP par défaut (dans notre cas : 192.168.2.1). L'ensemble des services et paramètres suivants ont ensuite été configurés :

- **Interfaces réseau** : attribution des plages d'adresses aux interfaces WAN, LAN et DMZ.
- **Règles de pare-feu** : mise en place de règles de filtrage pour contrôler les flux entre les différentes zones (LAN, DMZ, SERVEURS). Par exemple :
  - Blocage des flux DMZ → LAN et DMZ → SERVEURS.
  - Autorisation des ports 80 (HTTP), 443 (HTTPS), et 53 (DNS) en sortie depuis la DMZ.
  - Blocage des communications SERVEURS ↔ DMZ.
- **Règles NAT** : configuration des accès distants :
  - **Accès RDP** vers un serveur Windows.
  - **Accès SSH** vers une machine Ubuntu.
- **Services activés** :
  - **DHCP** sur les interfaces nécessaires pour l'attribution automatique des adresses IP.
  - **Ping** autorisé pour des raisons de diagnostic et de supervision.
- **VLAN** : création du VLAN 300, dédié à la zone SERVEURS, pour une meilleure isolation et segmentation du réseau.

## 6.6 Configuration Portail captif

Une fois le serveur DHCP et DNS mis en place, l'entreprise nous a demandé de mettre en place un portail captif ce qui permet aux administrateurs réseau de mettre en place des mécanismes d'authentification tels que les noms d'utilisateur et les mots de passe pour permettre une sécurité plus accrue du réseau de l'entreprise.

### Étape 1 : Accéder à la Configuration du Portail Captif

1. Accédez à l'interface web de PfSense. 1.2. Allez dans Status > Captive Portal.

### **Étape 2 : Ajouter une Nouvelle Zone de Portail Captif**

1. Cliquez sur Add (ou Ajouter si votre interface est en français).

2. Suivez les instructions suivantes :

- Zone Name : Entrez un nom pour la zone.
- Zone Description : Entrez une description pour la zone.

3. Cochez la case Enable Captive Portal.

4. Configurez les paramètres suivants :

- Description : Entrez un nom pour la description.
- Interfaces : Sélectionnez LAN.

5. Cliquez sur Save pour appliquer les modifications.

### **Étape 3 : Configurer les Autorisations Utilisateurs**

1. Accédez à System > User Manager > Groups.

2. Cliquez sur Add (ou Ajouter).

3. Créez un groupe :

- Group Name : Entrez un nom pour le groupe.
- Description : Ajoutez une description.

4. Cliquez sur Save.

5. Modifiez les droits du groupe :

- Cliquez sur l'icône du stylo à côté du groupe nouvellement créé.
- Faites défiler vers le bas et ajoutez des privilèges.
- Sélectionnez les privilèges nécessaires pour les administrateurs du portail captif.
- Cliquez sur Save pour appliquer les modifications.

### **Étape 4 : Créer un Utilisateur Administrateur**

1. Allez dans System > User Manager > Users.

2. Cliquez sur Add (ou Ajouter).

3. Créez un utilisateur administrateur :

- Username : Entrez un nom d'utilisateur.
- Password : Entrez un mot de passe sécurisé.
- Group Memberships : Ajoutez l'utilisateur au groupe AdminCaptivePortal.

4. Cliquez sur Save.

#### **Étape 5 : Créer un Groupe pour les Utilisateurs du Portail**

1. Allez dans System > User Manager > Groups.

2. Cliquez sur Add (ou Ajouter).

3. Créez un groupe pour les utilisateurs du portail :

- Group Name : Entrez un nom pour le groupe.
- Description : Ajoutez une description.

4. Cliquez sur Save.

5. Modifiez les privilèges du groupe :

- Cliquez sur l'icône du stylo à côté du groupe nouvellement créé.
- Faites défiler vers le bas et ajoutez les privilèges nécessaires.
- Cliquez sur Save pour appliquer les modifications.

#### **Étape 6 : Créer un Utilisateur Test**

1. Retournez dans System > User Manager > Users.

2. Cliquez sur Add (ou Ajouter).

3. Créez un utilisateur test :

- Username : Entrez un nom d'utilisateur.
- Password : Entrez un mot de passe sécurisé.
- Group Memberships : Ajoutez l'utilisateur au groupe UsersCaptivePortal.

6.4. Cliquez sur Save

#### **6.7 Configuration d'un Active Directory**

#### **Étape 1 : Installation des rôles et des fonctionnalités**

1. Cliquez sur Ajouter des rôles et des fonctionnalités.

#### **Étape 2 : Sélection des services**

1. Cochez le service AD DS (Active Directory Domain Services), qui installera le service Active Directory.
2. Redémarrez le serveur Windows après l'installation.

### **Étape 3 : Activation d'Active Directory**

1. Après le redémarrage, le service Active Directory sera actif.
2. Commencez à créer des groupes, des utilisateurs et des partages réseaux.

## 6.8 Déploiement automatisé avec Docker

### **Étape 1 : Mise à jour du serveur**

1. On met à jour le serveur.

### **Étape 2 : Installation des dépendances nécessaires**

1. Installer les dépendances nécessaires.

### **Étape 3 : Ajout de la clé GPG de Docker**

1. Ajouter la clé GPG de Docker.

### **Étape 4 : Ajout du dépôt Docker**

1. Ajouter le dépôt Docker.

### **Étape 5 : Mise à jour du serveur**

1. On remet à jour le serveur.

### **Étape 6 : Installation de Docker**

1. On peut installer Docker.

### **Étape 7 : Vérification de l'installation de Docker**

1. Pour vérifier s'il est installé.

## 7. Jeu de tests

### 7.1 Ajout d'une machine à un parc informatique: GLPI

Pour tester l'efficacité du glpi, nous allons utiliser 2 machines linux :

-1 ubuntu server 192.168.1.52 qui est le serveur GLPI

-1 debian 192.168.1.45 qui est la machine cliente et qui va envoyer ses données au serveur grâce à agent-glpi

The screenshot shows the GLPI web interface on a Windows desktop. The browser title is "Interface standard - GLPI" and the address bar shows "192.168.1.52/glpi/front/central.php". The page displays a dashboard with various statistics: 0 Logiciel, 0 Ordinateur, 0 Matériel réseau, 0 Téléphone, 0 Licence, 0 Moniteur, 0 Baie, and 0 Imprimante. A prominent orange warning box contains the following text:

- Pour des raisons de sécurité, veuillez changer le mot de passe par défaut pour le(s) utilisateur(s) : glpi post-only tech normal
- Pour des raisons de sécurité, veuillez supprimer le fichier : install/install.php
- La configuration du dossier racine du serveur web n'est pas sécurisée car elle permet l'accès à des fichiers non publics. Référez-vous à la documentation d'installation pour plus de détails.
- La directive PHP "session.cookie\_httponly" devrait être définie à "on" pour prévenir l'accès aux cookies depuis les scripts côté client.

Below the dashboard, there is a section titled "Statuts des tickets par mois" which states "Aucune donnée trouvée". The bottom of the screen shows the Windows taskbar with various icons and the date/time "14/12/2024 15:38".

Voici le serveur glpi au début, aucun ordinateur n'est présent dans le gestionnaire de parc informatique.

Nous allons donc installer agent-glpi avec le script « agent-glpi.sh »

```
Debian GNU/Linux 12 debian tty1
debian login: root
Mot de passe:
Linux debian 6.1.0-27-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.115-1 (2024-11-01) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~# wget https://agentglpi.onrender.com/script/projet/agent-glpi.sh
--2024-12-14 15:38:55-- http://agentglpi.onrender.com/script/projet/agent-glpi.sh
Résolution de agentglpi.onrender.com (agentglpi.onrender.com)... 216.24.57.252, 216.24.57.4
Connexion à agentglpi.onrender.com (agentglpi.onrender.com)|216.24.57.252|:443... connecté.
requête HTTP transmise, en attente de la réponse... 301 Moved Permanently
Emplacement : https://agentglpi.onrender.com/script/projet/agent-glpi.sh (suivant)
Réponse 301, adresse : https://agentglpi.onrender.com/script/projet/agent-glpi.sh
Connexion à agentglpi.onrender.com (agentglpi.onrender.com)|216.24.57.252|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 566 [text/x-sh]
Sauvegarde en : 0 agent-glpi.sh
agent-glpi.sh          100%[=====] 566 --.-kB/s   ds 0s
En-tête de dernière modification incorrect – ignoré.
2024-12-14 15:38:57 (2,15 Mo/s) - « agent-glpi.sh » sauvé [566/566]
root@debian:~# chmod +x agent-glpi.sh
root@debian:~#
```

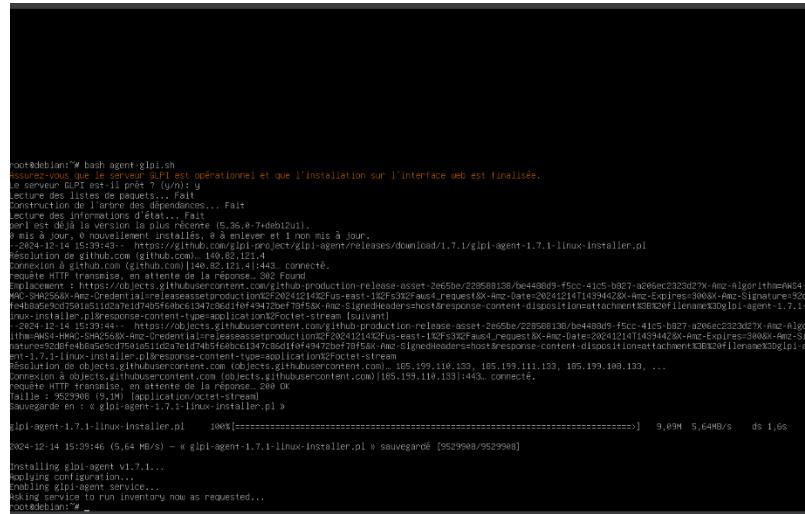
Avant d'exécuter le script on va modifier légèrement pour entrer la bonne adresse du serveur, particulièrement cette ligne-là :

```
perl glpi-agent-1.7.1-linux-installer.pl -s http://192.168.1.52/glpi --runnow --install
```

Maintenant que nous avons correctement indiqué l'adresse ip du serveur glpi, nous pouvons exécuter le script avec « bash » :

```
root@debian:~# bash agent-glpi.sh
Assurez-vous que le serveur GLPI est opérationnel et que l'installation sur l'interface web est finalisée.
Le serveur GLPI est-il prêt ? (y/n): y
```

Lorsque l'installation sera finalisée, nous verrons ça :



```
root@debian:~# bash agent-glpi.sh
Assurez-vous que le serveur GLPI est opérationnel et que l'installation sur l'interface web est finalisée.
Le serveur GLPI est-il prêt ? (y/n): y
Lecture des listes de paquets... Fait
construction de l'arbre des dépendances... Fait
les dépendances sont toutes satisfaites.
perl est déjà la version la plus récente (5.35.0-7+deb12u1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
root@debian:~# curl https://github.com/glpi-project/glpi/releases/download/1.7.1/glpi-agent-1.7.1-linux-installer.pl
résolution de github.com (github.com)|140.82.121.4|:443... connecté.
requête HTTP transmise, en attente de la réponse... 382 Found
... redirection... 200 OK
... lecture de /glpi-agent-1.7.1-linux-installer.pl?product=release-agent_2055ba238988129_be498d9_fcc-41c5-b927-a296ec2329d7X_amz-algoisshashW44A
amz-SHA256Amz-Credential|amz-releaseasset|production|F2024121402fus-east-1|2Cf532fAusl|request|8X-Amz-Date|20241214T14934423X-Amz-Expires|3000X-Amz-Signature|32d
fe48bb8e0d7501a510d79e1d74b5f6a0c61347c08d1ff494720ef79f58X-Amz-SignedHeaders|host&response-content-disposition|attachment;filename=d3glpi-agent-1.7.1-1
... téléchargement de /glpi-agent-1.7.1-linux-installer.pl?product=release-agent_2055ba238988129_be498d9_fcc-41c5-b927-a296ec2329d7X_amz-algo
isshashW44A
amz-SHA256Amz-Credential|amz-releaseasset|production|F2024121402fus-east-1|2Cf532fAusl|request|8X-Amz-Date|20241214T14934423X-Amz-Expires|3000X-Amz-Sig
nature|920f941d408a59101ca7a1d74b5f6a0c61347c08d1ff494720ef79f58X-Amz-SignedHeaders|host&response-content-disposition|attachment;filename=d3glpi-agent-1.7.1-1
... téléchargement de /glpi-agent-1.7.1-linux-installer.pl?product=release-agent_2055ba238988129_be498d9_fcc-41c5-b927-a296ec2329d7X_amz-algo
isshashW44A
amz-SHA256Amz-Credential|amz-releaseasset|production|F2024121402fus-east-1|2Cf532fAusl|request|8X-Amz-Date|20241214T14934423X-Amz-Expires|3000X-Amz-Sig
nature|920f941d408a59101ca7a1d74b5f6a0c61347c08d1ff494720ef79f58X-Amz-SignedHeaders|host&response-content-disposition|attachment;filename=d3glpi-agent-1.7.1-1
... téléchargement de objects.githubusercontent.com (objects.githubusercontent.com)|105.199.110.130, 105.199.111.130, 105.199.108.130, ...
... connexion à objects.githubusercontent.com (objects.githubusercontent.com)|105.199.110.130|1443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
taille : 35000000 (5.1M) en attente de la réponse...
sauvegarde en 1 : < glpi-agent-1.7.1-linux-installer.pl >
glpi-agent-1.7.1-linux-installer.pl 100%[=====] 9,09M 5,64MB/s ds 1,6s
0x24-12-14 15:39:41 (5,64 MB/s) - < glpi-agent-1.7.1-linux-installer.pl > sauvegardé [9529988/9529988]

Installing glpi-agent v1.7.1...
  applying configuration...
  enabling glpi-agent service...
  asking glpi-agent to run inventory now as requested...
root@debian:~#
```



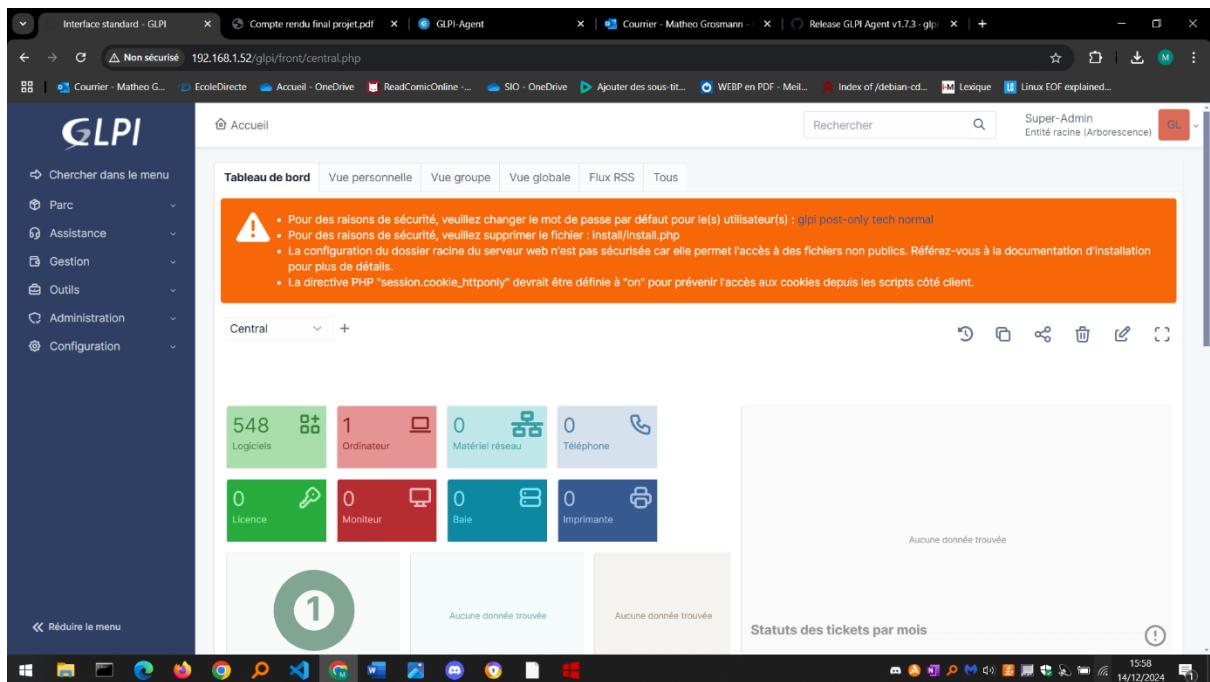
This is GLPI Agent 1.7.1-1

The current status is waiting

Next server target execution planned for:  
• server0: Sat Dec 14 15:43:42 2024

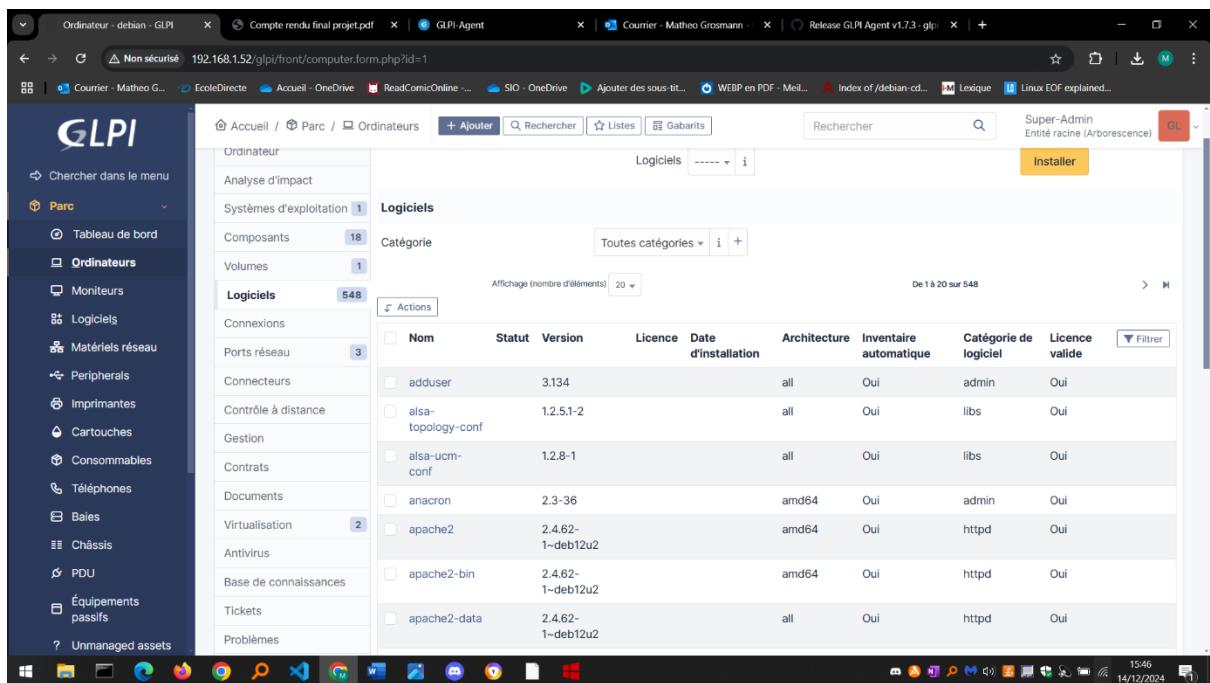
C'est bon signe bien que ce ne soit pas instantané et qu'il faut un peu de patience pour que la machine debian soit ajouté au serveur glpi.

Si nous patientons un peu lorsque nous retournons sur le serveur glpi, nous pouvons constater un changement.



L'ordinateur Debian a bien été ajouté

Dans l'onglet ordinateur vous pouvez accéder au détail de la debian.



Le serveur glpi est donc opérationnel

## 7.2 Test de restauration de fichier : Veeam Backup

Pour ce jeu de test nous allons faire une backup de notre répertoire html contenant

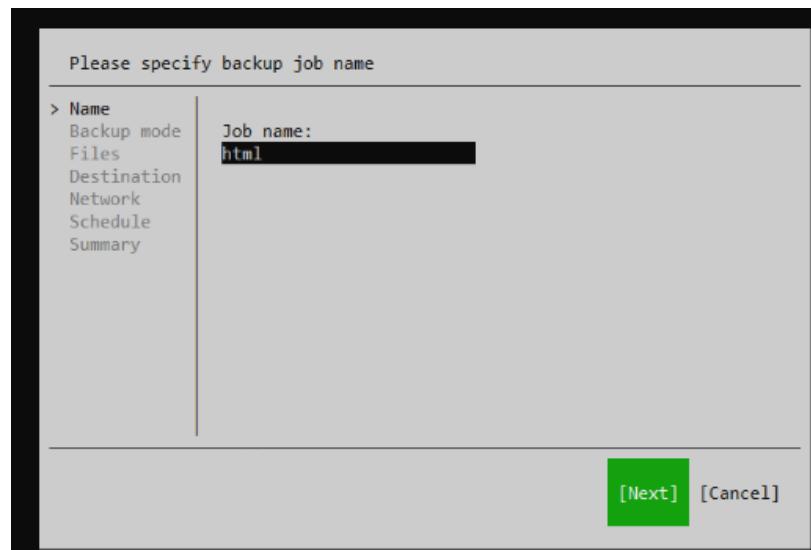
-un index.html

-fog

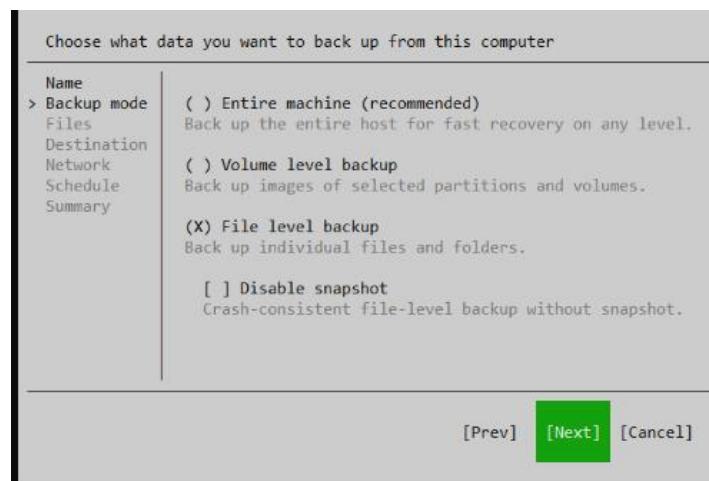
-glpi

```
mgrosmann@debian10-www: ~
root@debian:~# ls /var/www/html/
fog  glpi  glpi-10.0.17.tgz  index.html
root@debian:~#
```

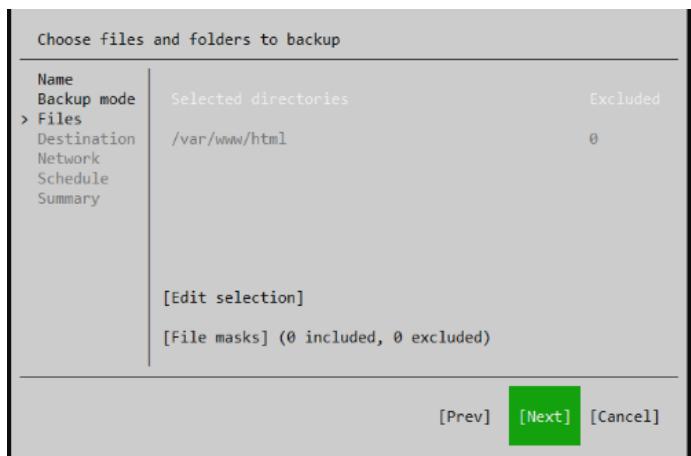
Pour cela on va configurer un nouveau job que l'on va appeler « html »



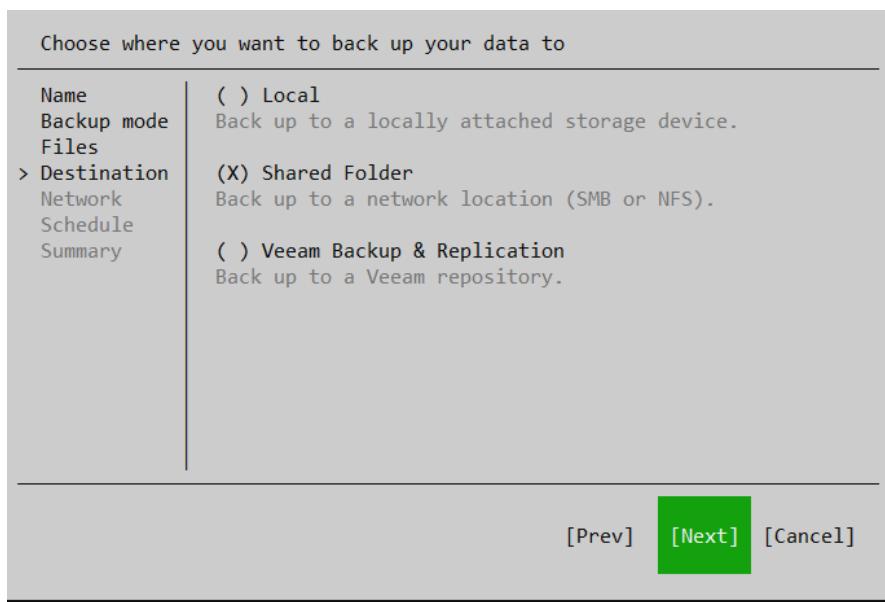
Nous allons sélectionner « file level backup » pour sauvegarder uniquement un dossier



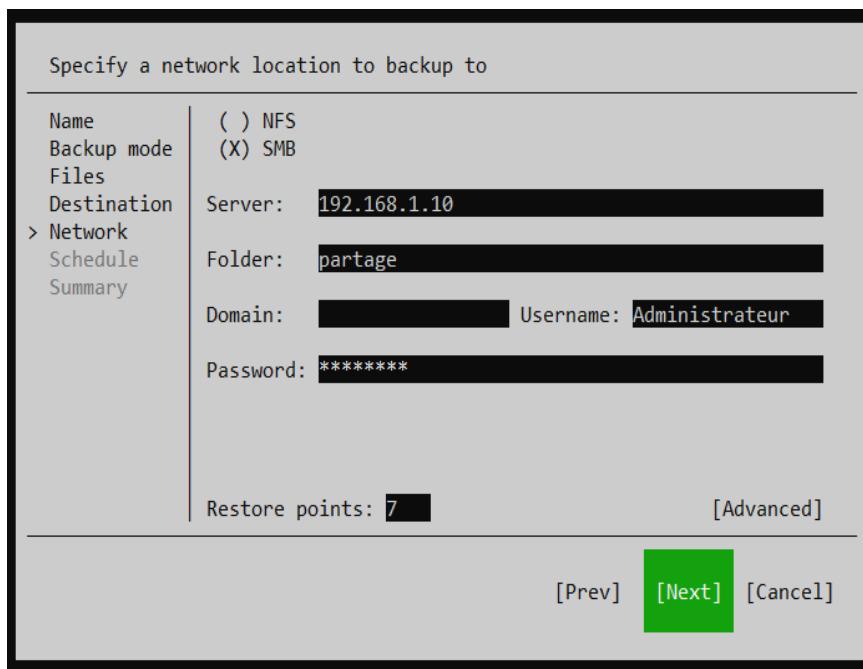
Nous allons sélectionner le répertoire « /var/www/html »



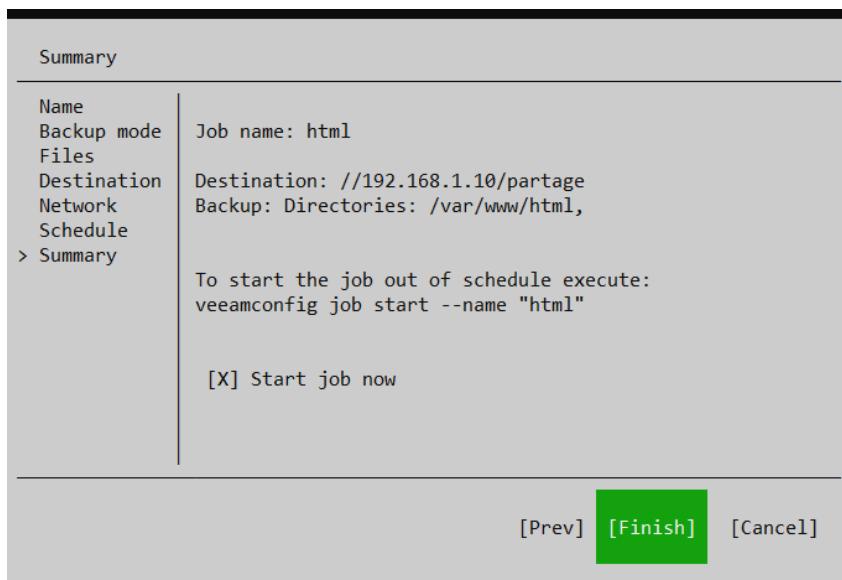
On sélectionne ensuite shared folder pour que la backup soit stocké sur notre serveur smb windows server



On précise les infos sur le serveur SMB



On lance ensuite le job



Une fois fini on observe sa présence sur le partage du windows server

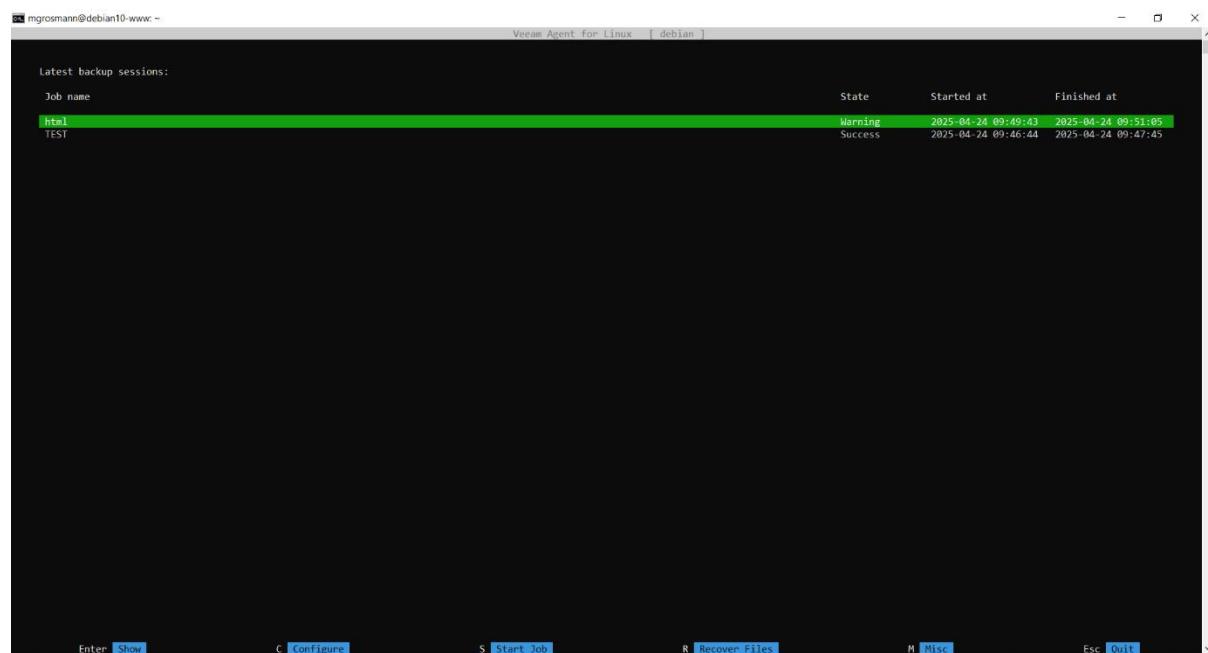
C > Partage (\\\TBM-AD) (P:) >			
Nom	Modifié le	Type	Taille
autres	31/03/2025 14:45	Dossier de fichiers	
backup	31/03/2025 14:45	Dossier de fichiers	
debian html	24/04/2025 09:50	Dossier de fichiers	
logiciel	31/03/2025 21:10	Dossier de fichiers	
raccourci	31/03/2025 17:05	Dossier de fichiers	
script.ps1	02/04/2025 14:19	Script Windows Po...	34 Ko

> Partage (\\\TBM-AD) (P:) > debian html			
Nom	Modifié le	Type	Taille
html.vbm	24/04/2025 09:50	Fichier VBM	8 Ko
html_2025-04-24T094957.vbk	24/04/2025 09:50	Fichier VBK	314 840 Ko

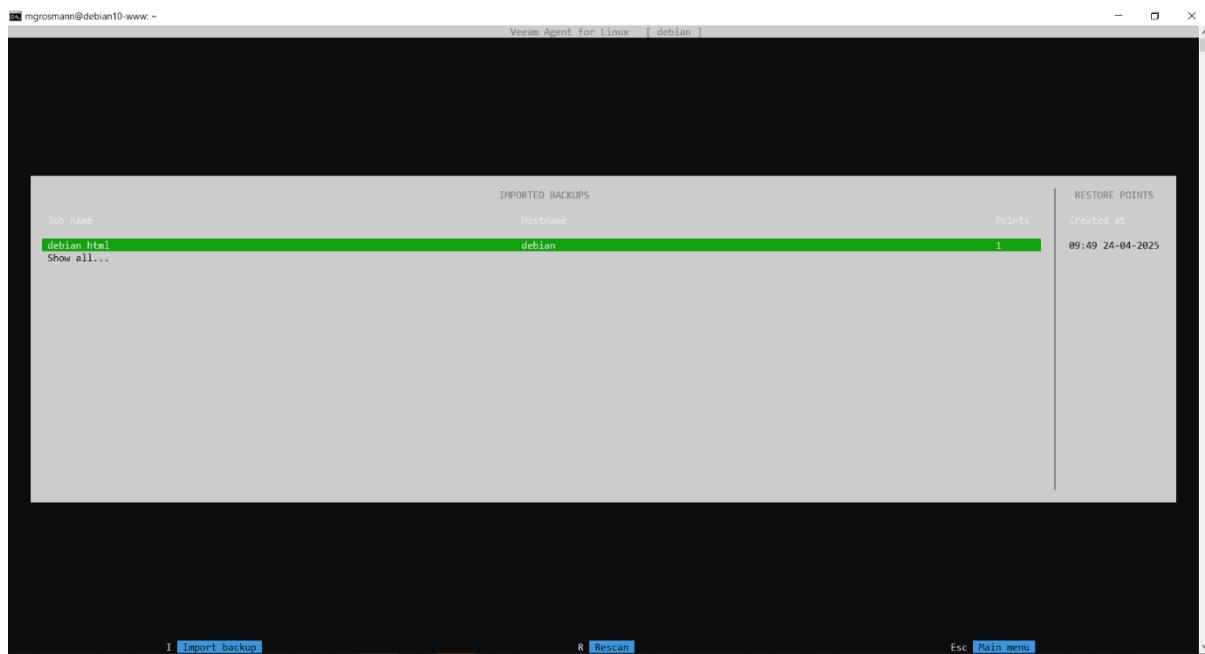
Pour tester son efficacité on va supprimer le répertoire /var/www/html

```
root@debian:~# rm -rf /var/www/html/
root@debian:~#
```

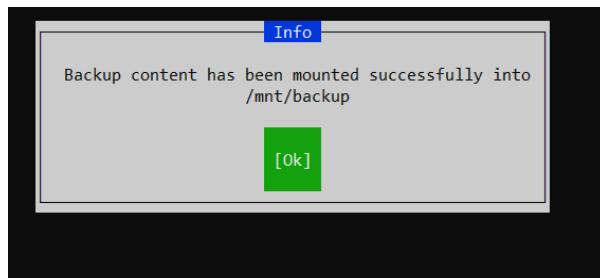
On lance l'interface avec « veeam » puis on appuie sur « R » pour restaurer une backup



On sélectionne « debian html »



Un message nous informe que le dossier a été restauré dans « /mnt/backup »



On vérifie avec ls et on observe que la restauration a marché

```
mgrosmann@debian10-www: ~
root@debian:~# ls /var/www/html/
fog glpi glpi-10.0.17.tgz index.html
root@debian:~# veeam
root@debian:~# veeam
root@debian:~# rm -rf /var/www/html/
root@debian:~# veeam
root@debian:~# ls /mnt/backup/var/www/html/
fog glpi glpi-10.0.17.tgz index.html
root@debian:~#
```

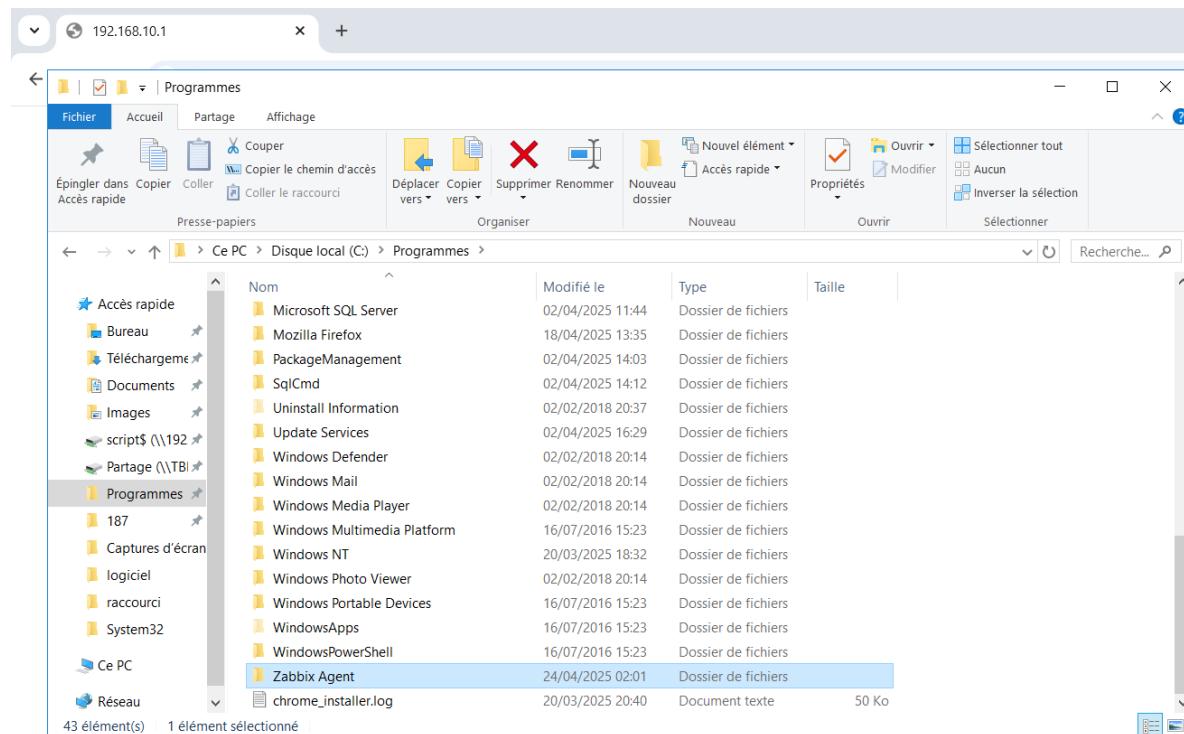
### 7.3 Ajout d'une machine à la solution de superviseur: Zabbix

Pour ce test on va ajouter le windows server 192.168.1.10 au serveur zabbix 192.168.1.11

Pour cela sur le windows server on va exécuter ce script bat

```
zabbix.bat - Bloc-notes
Fichier Edition Format Affichage ?
@ECHO OFF
if exist "C:\Program Files\zabbix agent\" (
exit
)
set zabbix="\\192.168.1.10\script$\zabbix_agent-7.2.5-windows-amd64-openssl.msi"
set server="192.168.1.11"
set hostname="zabbix-agent"
msiexec /i %zabbix% /qn SERVER=%server% SERVERACTIVE=%server% HOSTNAME=%hostname%
```

Une fois le script exécuté on vérifie dans C:\Program Files que Zabbix agent existe bien



Sur l'interface web de zabbix on va dans « collecte de données -> hôtes »

The screenshot shows the Zabbix web interface with the following details:

- Top Left:** A sidebar with navigation links: Tableaux de bord, Surveillance, Services, Inventaire, Raports, Collecte de données (selected), Groupes de modèles, Modèles, Hôtes, Maintenance, Corrélation d'événement, Découverte, Alertes, Utilisateurs, Administration, Support, Intégrations, Aide, and Paramètres utilisateur.
- Top Center:** A performance monitor section with a chart showing "2.01 ↑ Zabbix server Values per second". Below it are three graphs: CPU usage (1.44 %), Memory usage (0.10), and Disk usage (0.09). A table titled "Information système" provides system statistics.
- Top Right:** A large digital clock displaying "10:28" with the location "Paris".
- Middle Left:** A "Problèmes par严重性" (Problems by Severity) bar chart with categories: Majeur (0), Inconnu (0), Total (1), Catastrophe (0), Haut (0), Moyen (1), Avertissement (0), Information (0), and Non classé (0).
- Middle Center:** A table titled "Problème > Sévérité" showing a single entry: "Linux. Number of installed packages has been changed" (Severity: Catastrophe, Duration: 57m 17s, Last updated: Actualiser).
- Middle Right:** A "Carte géographique" (Geographic Map) showing a map of Riga, Latvia, with various monitoring points marked.

On sélectionne « créer une hôte » puis on ajoute les infos du windows server

The screenshot shows the "Nouvel hôte" (New Host) configuration dialog with the following fields:

- Hôte Tab:** Contains:
  - \* Nom de l'hôte: windows server
  - Nom visible: windows server
  - Modèles: Windows by Zabbix agent (selected)
  - \* Groupes d'hôtes: Virtual machines (selected)
- Interfaces Tab:** Contains:
  - Type: adresse IP
  - Agent: 192.168.1.11
  - Nom DNS:
  - Connexion à: IP
  - Port: 10050
  - Défaut:
  - Supprimer button
- Description:** A text area labeled "Ajouter" (Add) with placeholder text "Description".
- Surveillé par:** Buttons for Serveur (selected), Proxy, and Groupe de proxy.
- Activé:** A checked checkbox.
- Buttons:** Ajouter (Add) and Annuler (Cancel).

Si on attend quelques minutes et qu'on clique sur « graphique » on a des infos sur le windows server

Hôtes

Créer un hôte Importer Filtre

Groupes hôtes : taper ici pour rechercher Sélectionner État : Tous Actif Désactivé

Modèles : taper ici pour rechercher Sélectionner Surveillé par : Tous Serveur Proxy Groupe de proxy

Nom : DNS : IP : Port :

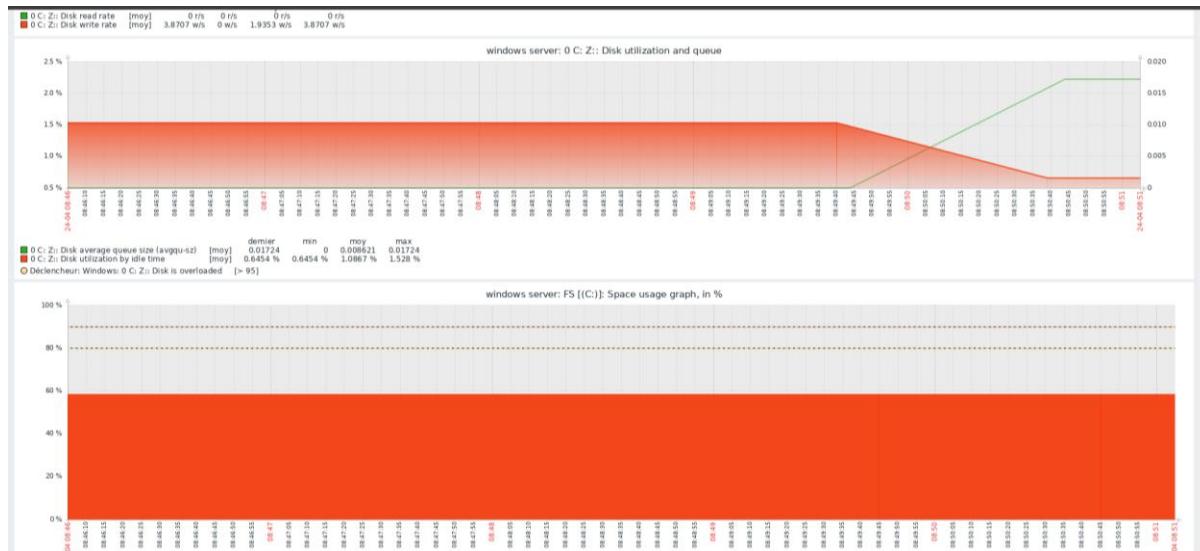
Tags : ET OU tag : Content : valeur : Supprimer Ajouter

Appliquer Réinitialiser

	Éléments	Déclencheurs	Graphiques	Découverte	Web	Interface	Proxy	Modules	État	Disponibilité	Chiffrement sur l'agent	Info	Tags
<input type="checkbox"/> Windows server	Éléments 34	Déclencheurs 13	Graphiques 5	Découverte 4	Web 192.168.1.10 10050			Windows by Zabbix agent	Actif	Aucun			
<input type="checkbox"/> Zabbix server	Éléments 175	Déclencheurs 102	Graphiques 24	Découverte 6	Web 127.0.0.1 10050			Linux by Zabbix agent, Zabbix server health	Actif	Aucun			

Affichage de 2 sur 2 trouvés

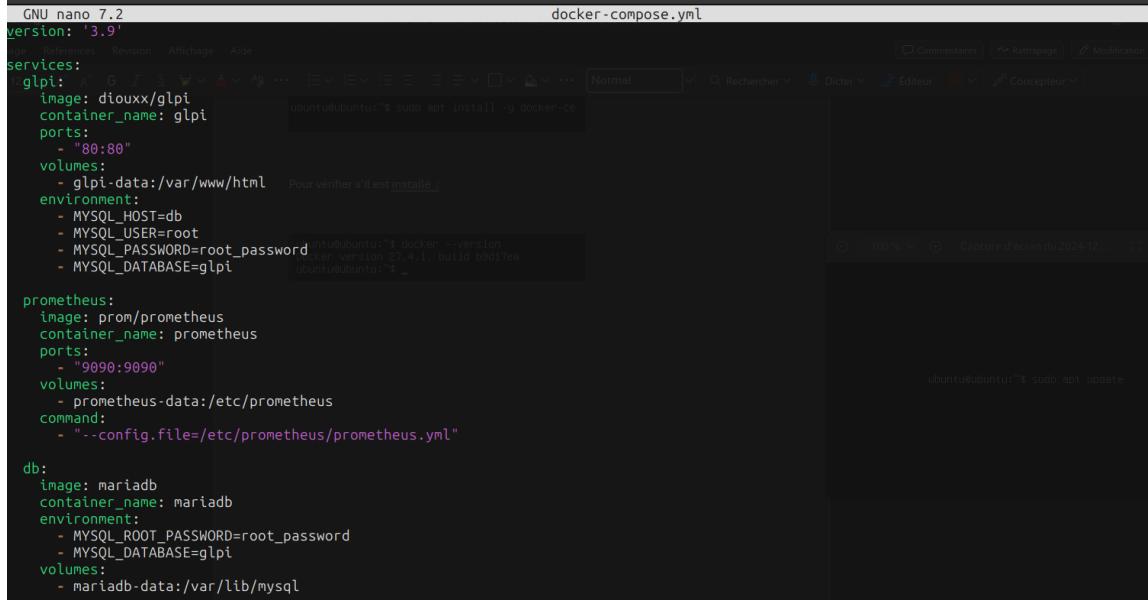
0 sélectionné Activer Désactiver Exporter Modification collective Supprimer



## 7.4 Automatisation de deux containers :Docker

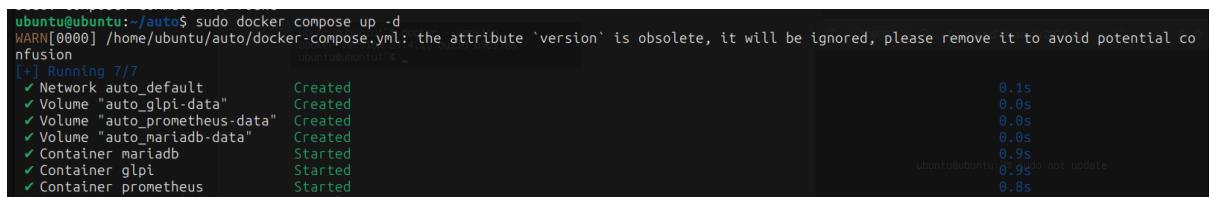
Pour tester l'efficacité de docker on va lancer automatiquement 2 container(GLPI et Prometheus) à l'aide d'un fichier compose.yml. ).Les container doivent être souvent les mettre à jour manuellement. Watchtower automatise cette tâche.

Le fichier compsose est le suivant :



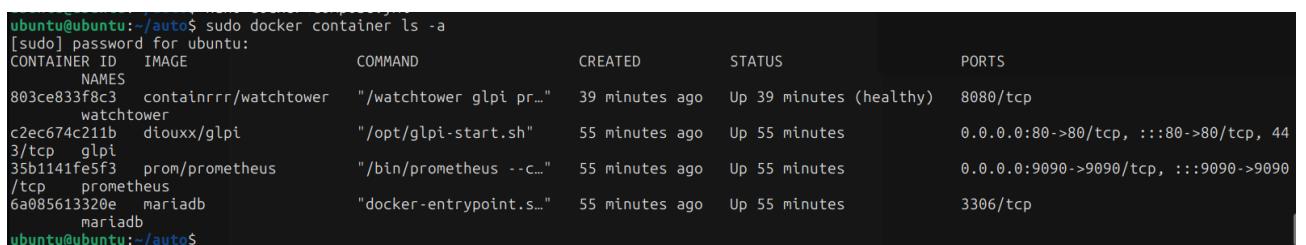
```
GNU nano 7.2                                            docker-compose.yml
version: '3.9'
services:
  glpi:
    image: diouxx/glpi
    container_name: glpi
    ports:
      - "80:80"
    volumes:
      - glpi-data:/var/www/html    Pour vérifier s'il est installé :
    environment:
      - MYSQL_HOST=db
      - MYSQL_USER=root
      - MYSQL_PASSWORD=root_password
      - MYSQL_DATABASE=glpi
  prometheus:
    image: prom/prometheus
    container_name: prometheus
    ports:
      - "9090:9090"
    volumes:
      - prometheus-data:/etc/prometheus
    command:
      - "--config.file=/etc/prometheus/prometheus.yml"
  db:
    image: mariadb
    container_name: mariadb
    environment:
      - MYSQL_ROOT_PASSWORD=root_password
      - MYSQL_DATABASE=glpi
    volumes:
      - mariadb-data:/var/lib/mysql
```

Ensuite avec la commande Docker compose up -d



```
ubuntu@ubuntu:~/auto$ sudo docker compose up -d
WARN[0000] /home/ubuntu/auto/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Running 7/7
  ✓ Network auto_default          Created
  ✓ Volume "auto_glpi-data"       Created
  ✓ Volume "auto_prometheus-data" Created
  ✓ Volume "auto_mariadb-data"     Created
  ✓ Container mariadb             Started
  ✓ Container glpi                Started
  ✓ Container prometheus          Started
ubuntu@ubuntu:~/auto$
```

Les containers se lancent

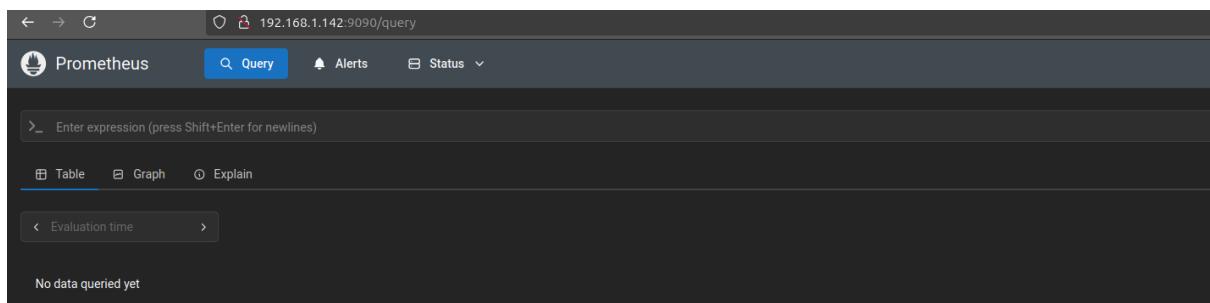


```
ubuntu@ubuntu:~/auto$ sudo docker container ls -a
[sudo] password for ubuntu:
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS
 NAMES
803ce833fb8c3    containrrr/watchtower   "/watchtower glpi pr..."   39 minutes ago    Up 39 minutes (healthy)   8080/tcp
c2ec674c211b    diouxx/glpi           "/opt/glpi-start.sh"    55 minutes ago    Up 55 minutes      0.0.0.0:80->80/tcp, :::80->80/tcp, 44
3/tcp            glpi                "/opt/glpi-start.sh"    55 minutes ago    Up 55 minutes      0.0.0.0:9090->9090/tcp, :::9090->9090
35b1141fe5f3    prom/prometheus      "/bin/prometheus --c..."   55 minutes ago    Up 55 minutes      0.0.0.0:9090->9090/tcp, :::9090->9090
/tcp             prometheus          "docker-entrypoint.s..."   55 minutes ago    Up 55 minutes      3306/tcp
6a085613320e    mariadb             "mariadb"                55 minutes ago    Up 55 minutes      3306/tcp
ubuntu@ubuntu:~/auto$
```

Donc la redirection de port sur l'adresse ip du serveur avec le port 80 correspond à la page de glpi



Et la redirection de port 9090 c'est prometheus



Pour le déploiement automatique, je vais utiliser Watchtower, qui permettra la mise à jour des images Docker, leur lancement et redémarrage automatique. Avec le fichier donné il est installé, pour qu'il fonctionne, on regarde dans les logs.

C'est cette commande qui va lancer un conteneur Watchtower :

```
sudo docker run -d \ --name watchtower \ -v  
/var/run/docker.sock:/var/run/docker.sock \ containrrr/watchtower  
glpi prometheus mariadb
```

L'installation de Watchtower est terminée

## 7.5 filtrage proxy avec squid

```
GNU nano 7.2                         blacklist.txt
twitter.com                                          man GNU/Linux system are free software;
facebook.com                                           terms and conditions program are described in the
                                                       /usr/share/doc/copyright.
```

Voici la liste des sites internet interdits.



Pour vérifier que le proxy fonctionne, nous allons donc le mettre dans la navigateur comme ceci :

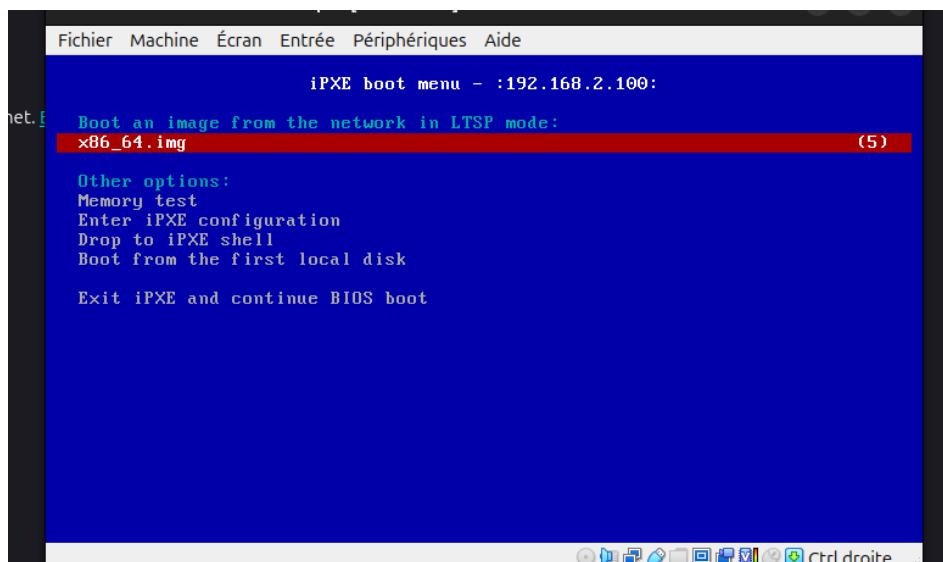
192.168.1.162 étant l'adresse du Proxy et le port 3128.



On peut voir que le proxy bloque bel et bien la connexion.

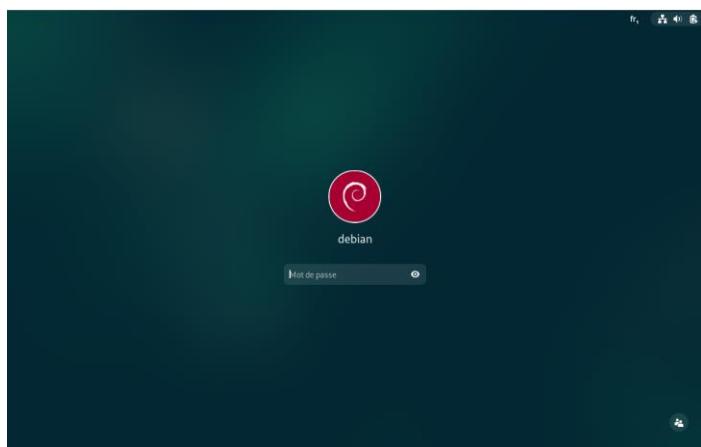
## 7.6 test de déploiement automatisé avec lstp

Pour vérifier que le serveur LTSP fonctionne il suffit seulement de lancer une machine en mode PXE et voir si elle trouve bien le serveur :



On peut voir que le serveur et bien trouvé et l'image également.

L'image se lance bel et bien.



## 8. Manuel technique

Tous les scripts shell sont disponibles sur

<https://github.com/mgrosman/mgrosmann/tree/main/script/projet>

### 8.1 Mise en place d'un outil de gestion de parc informatique : GLPI

Tout d'abord avant d'installer GLPI, il faudra installer un serveur mysql afin que glpi puisse l'utiliser.

```
1  #!/bin/bash
2  apt update
3  apt install mariadb-server -y
4  mysql_secure_installation <<EOF
5  y
6  n
7  y
8  y
9  y
10 y
11 EOF
12 mysql <<EOF
13 ALTER USER 'root'@'localhost' IDENTIFIED BY 'root';
14 CREATE USER 'mgrosmann'@'localhost' IDENTIFIED BY 'password';
15 CREATE DATABASE test;
16 GRANT ALL PRIVILEGES ON test.* TO 'root'@'localhost';
17 FLUSH PRIVILEGES;
18 EOF
```

Maintenant que les prérequis ont été installé nous pouvons commencer l'installation de GLPI.

Voici le script utilisé :

```
1  #!/bin/bash
2  apt update
3  apt install -y apache2 php php-{apcu,cli,common,curl,gd,imap,ldap,mysql,xmlrpc,xml,mbstring,bcmath,intl,zip,redis,bz2} libapache2-mod-php php-soap php-cas
4  mysql <<EOF
5  CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'glpi';
6  CREATE DATABASE glpi;
7  GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost';
8  GRANT SELECT ON `mysql`.\`time_zone_name\` TO 'glpi'@'localhost';
9  FLUSH PRIVILEGES;
10 EOF
11 cd /var/www/html
12 wget https://github.com/glpi-project/glpi/releases/download/10.0.17/glpi-10.0.17.tgz
13 tar -xvzf glpi-10.0.17.tgz
14 chown root:root /var/www/html/glpi/
15 chown www-data:www-data /var/www/html/glpi/ -R
```

Tout d'abord on met à jour la liste des paquets avec apt-get update et on s'assure qu'ils soient sous leur dernière version avec apt-get upgrade

Ensuite on installe le paquet « apache2 » afin de pouvoir héberger un site web sur notre adresse IP, puis on installe divers module PHP nécessaire au fonctionnement de GLPI.

```
2 apt update
3 apt install -y apache2 php php-{apcu,cli,common,curl,gd,imap,ldap,mysql,xmllrpc,xml,mbstring,bcmath,intl,zip,redis,bz2} libapache2-mod-php php-soap php-cas
```

Ensuite on utilisera la commande « mysql » suivi de la commande « EOF » précédemment cité, puis on créer la base de données glpi, puis l'utilisateur glpi plus on lui donne tous les droits sur la base de données afin que glpi puisse s'en servir. Il ne reste plus qu'à redémarrer les droits avec « flush privileges »

```
4 mysql <<EOF
5 CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'glpi';
6 CREATE DATABASE glpi;
7 GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost';
8 GRANT SELECT ON `mysql`.\`time_zone_name\` TO 'glpi'@'localhost';
9 FLUSH PRIVILEGES;
10 EOF
```

On se rend dans le répertoire « /var/www/html » installe glpi en téléchargeant l'archive sur GitHub en utilisant la commande wget suivi de l'url du dépôt.

En extraira ensuite l'archive avec la commande tar.

```
11 cd /var/www/html
12 wget https://github.com/glpi-project/glpi/releases/download/10.0.17/glpi-10.0.17.tgz
13 tar -xvf glpi-10.0.17.tgz
```

On modifie les droits de propriétaire grâce à « chown » avec l'user root et www-data.

```
14 chown root:root /var/www/html/glpi/
15 chown www-data:www-data /var/www/html/glpi/ -R
```

Ensuite on continue l'installation sur l'interface web sur

[http://adresse\\_ip\\_du\\_server\\_glpi](http://adresse_ip_du_server_glpi)

```
46 systemctl restart apache2
```

Tout d'abord il faudra entrer le port sur lequel est héberger le serveur sql ainsi que les identifiants.



Puis on sélectionnera la base de données à utiliser pour glpi



L'installation du serveur glpi est maintenant finalisée.

Maintenant que le serveur glpi est correctement installé, il faut installer agent-glpi pour pouvoir collecter des données sur les appareils du parc informatique.

Le script suivant sera utilisé :

```
1 #!/bin/bash
2 echo -e "\e[33mAssurez-vous que le serveur GLPI est opérationnel et que l'installation sur l'interface web est finalisée.\e[0m"
3 read -p "Le serveur GLPI est-il prêt ? (y/n): " confirm
4 if [[ $confirm != "y" ]]; then
5     echo "Veuillez finaliser l'installation du serveur GLPI avant de continuer."
6     exit 1
7 fi
8 apt install perl
9 wget https://github.com/glpi-project/glpi-agent/releases/download/1.7.1/glpi-agent-1.7.1-linux-installer.pl
10 perl glpi-agent-1.7.1-linux-installer.pl -s http://192.168.1.78/glpi --runnow --install
11 systemctl enable glpi-agent
```

Premièrement le script demandera donc si le serveur glpi est prêt.

```
2     echo -e "\e[33mAssurez-vous que le serveur GLPI est opérationnel et que l'installation sur l'interface web est finalisée.\e[0m"
3     read -p "Le serveur GLPI est-il prêt ? (y/n): " confirm
4     if [[ $confirm != "y" ]]; then
5         echo "Veuillez finaliser l'installation du serveur GLPI avant de continuer."
6         exit 1
7     fi
```

Si c'est le cas vous pourrez passer à l'installation du paquet « perl » pour exécuter le script d'installation « .pl » de agent glpi et utiliser wget pour télécharger le « .pl » de la version de votre choix.

```
8     apt install perl
9     wget https://github.com/glpi-project/glpi-agent/releases/download/1.7.1/glpi-agent-1.7.1-linux-installer.pl
```

Ensuite on execute le script avec perl et on utilise -s pour spécifier le serveur.

```
10    perl glpi-agent-1.7.1-linux-installer.pl -s http://192.168.1.78/glpi --runnow --install
```

Une fois que c'est fait il ne reste qu'à redémarrer agent glpi

```
11    systemctl enable glpi-agent
```

## 8.2 Mise en place d'un outil de sauvegarde : VeeamBackup

Pour installer Veeam Backup à l'aide de ce script

```
#!/bin/bash
wget https://download2.veeam.com/VAL/v6/veeam-release-deb_1.0.9_amd64.deb
dpkg -i ./veeam-release* && apt-get update
apt-get install blksnap veeam -y
apt-get install veeam-nosnap -y
echo "effectuez 'veeamconfig ui' pour vérifier si l'installation a réussi"
```

```
 wget https://download2.veeam.com/VAL/v6/veeam-release-deb_1.0.9_amd64.deb
dpkg -i ./veeam-release* && apt-get update
```

Cette partie la télécharge le package .deb puis utiliser la commande « dpkg -i » afin d'ajouter les paquets pour installer veam.

Une fois cela fait, on pourra installer les paquets nécessaires pour installer veeam backup et lancer l'interface avec « veeam » ou « veeamconfig ui »

```
apt-get install blksnap veeam -y
apt-get install veeam-nosnap -y
echo "effectuez 'veeamconfig ui' pour vérifier si l'installation a réussi"
```

Veeam Backup est maintenant installé

### 8.3 Mise en place d'un outil de supervision : Zabbix

Pour installer zabbix on va utiliser ce script

```
#!/bin/bash
echo "quel est le mot de passe root du serveur sql ? "
read -s pass
read -p "quel est votre distrib linux ? (1 pour debian 2 pour ubuntu) " linux
if [[ $linux == 1 ]]; then
    wget https://repo.zabbix.com/zabbix/7.2/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.2+debian12_all.deb
    dpkg -i zabbix-release_latest_7.2+debian12_all.deb
elif [[ $linux == 2 ]]; then
    wget https://repo.zabbix.com/zabbix/7.2/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.2+ubuntu24.04_all.deb
    dpkg -i zabbix-release_latest_7.2+ubuntu24.04_all.deb
else
    echo "choix incorrect, veuillez réessayer"
fi
apt update
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y
echo "create database IF NOT EXISTS zabbix character set utf8mb4 collate utf8mb4_bin;" > zbx.sql
echo "create user IF NOT EXISTS zabbix@localhost identified by 'zabbix';" >> zbx.sql
echo "grant all privileges on zabbix.* to zabbix@localhost;" >> zbx.sql
echo "set global log_bin_trust_function_creators = 1;" >> zbx.sql
echo "flush privileges;" >> zbx.sql
mysql -uroot -p$pass < zbx.sql
zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz > zbx.sql
echo "set global log_bin_trust_function_creators = 0;" >> zbx.sql
mysql -uroot -p$pass zabbix < zbx.sql
rm zbx.sql
echo "systemctl restart zabbix-server zabbix-agent apache2" > zbx.sh
echo "systemctl enable zabbix-server zabbix-agent apache2" >> zbx.sh
echo "nano /etc/zabbix/zabbix_server.conf pour DBPASSWORD, une fois fait, 'bash zbx.sh'"
```

Pour cette partie du script on va recueillir la distribution linux utilisé (si elle pris en compte) ainsi que le mot de passe root du serveur sql.

```
#!/bin/bash
echo "quel est le mot de passe root du serveur sql ? "
read -s pass
read -p "quel est votre distrib linux ? (1 pour debian 2 pour ubuntu) " linux
if [[ $linux == 1 ]]; then
```

En fonction de la distribution linux on va installer les paquets zabbix

```
if [[ $linux == 1 ]]; then
    wget https://repo.zabbix.com/zabbix/7.2/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.2+debian12_all.deb
    dpkg -i zabbix-release_latest_7.2+debian12_all.deb
elif [[ $linux == 2 ]]; then
    wget https://repo.zabbix.com/zabbix/7.2/release/ubuntu/pool/main/z/zabbix-release/zabbix-release_latest_7.2+ubuntu24.04_all.deb
    dpkg -i zabbix-release_latest_7.2+ubuntu24.04_all.deb
else
    echo "choix incorrect, veuillez réessayer"
fi
apt update
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y
echo "create database IF NOT EXISTS zabbix character set utf8mb4 collate utf8mb4_bin;" > zbx.sql
```

On va ensuite exécuter un mini-script sql qui va créer la base de données zabbix ainsi que l'utilisateur zabbix qui aura tous les droits sur cette dernière mais aussi exécuter le script sql de zabbix présent dans /usr/share/zabbix/sql-scripts/

```
echo "create database IF NOT EXISTS zabbix character set utf8mb4 collate utf8mb4_bin;" > zbx.sql
echo "create user IF NOT EXISTS zabbix@localhost identified by 'zabbix';" >> zbx.sql
echo "grant all privileges on zabbix.* to zabbix@localhost;" >> zbx.sql
echo "set global log_bin_trust_function_creators = 1;" >> zbx.sql
echo "flush privileges;" >> zbx.sql
mysql -uroot -p$pass < zbx.sql
zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz > zbx.sql
echo "set global log_bin_trust_function_creators = 0;" >> zbx.sql
mysql -uroot -p$pass zabbix < zbx.sql
rm zbx.sql
```

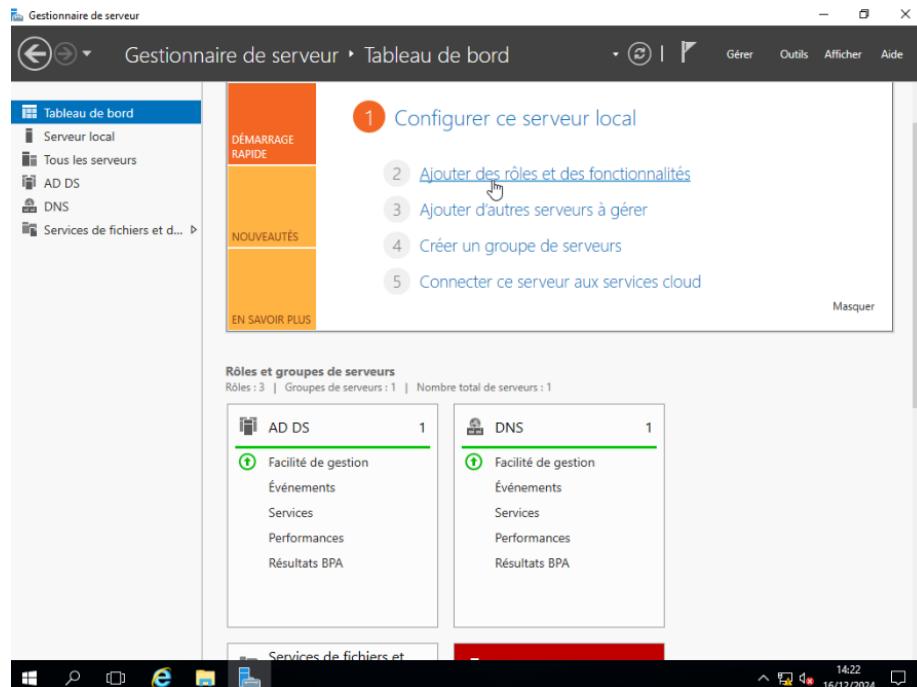
Ensuite il faudra redémarrer le serveur zabbix mais pas avant d'avoir renseigné le « DB\_password » dans /etc/zabbix/zabbix\_server.conf

```
echo "systemctl restart zabbix-server zabbix-agent apache2" > zbx.sh
echo "systemctl enable zabbix-server zabbix-agent apache2" >> zbx.sh
echo "nano /etc/zabbix/zabbix_server.conf pour DBPASSWORd, une fois fait, 'bash zbx.sh'"
```

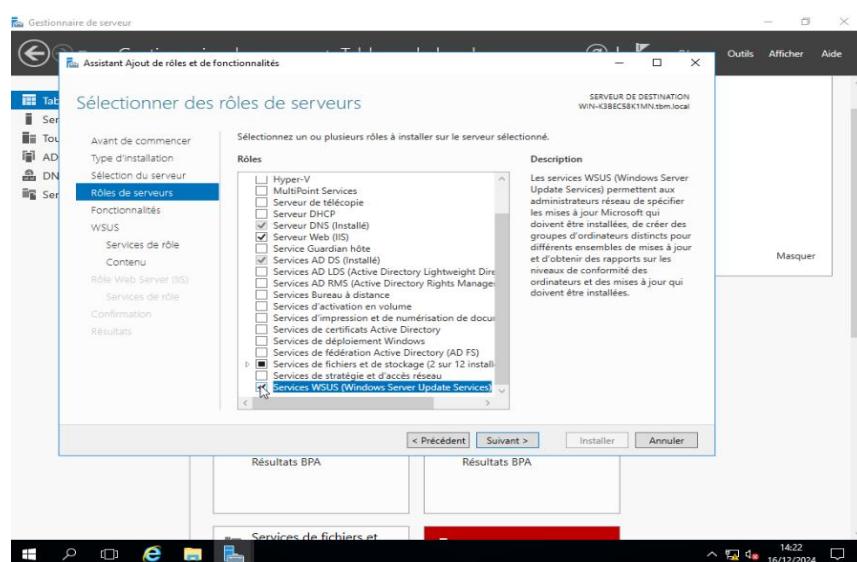
## 8.4 Configuration des mises à jour automatisés avec windows server

Tout d'abord il va falloir se rendre sur le gestionnaire de serveur, afin d'y installer le service WSUS.

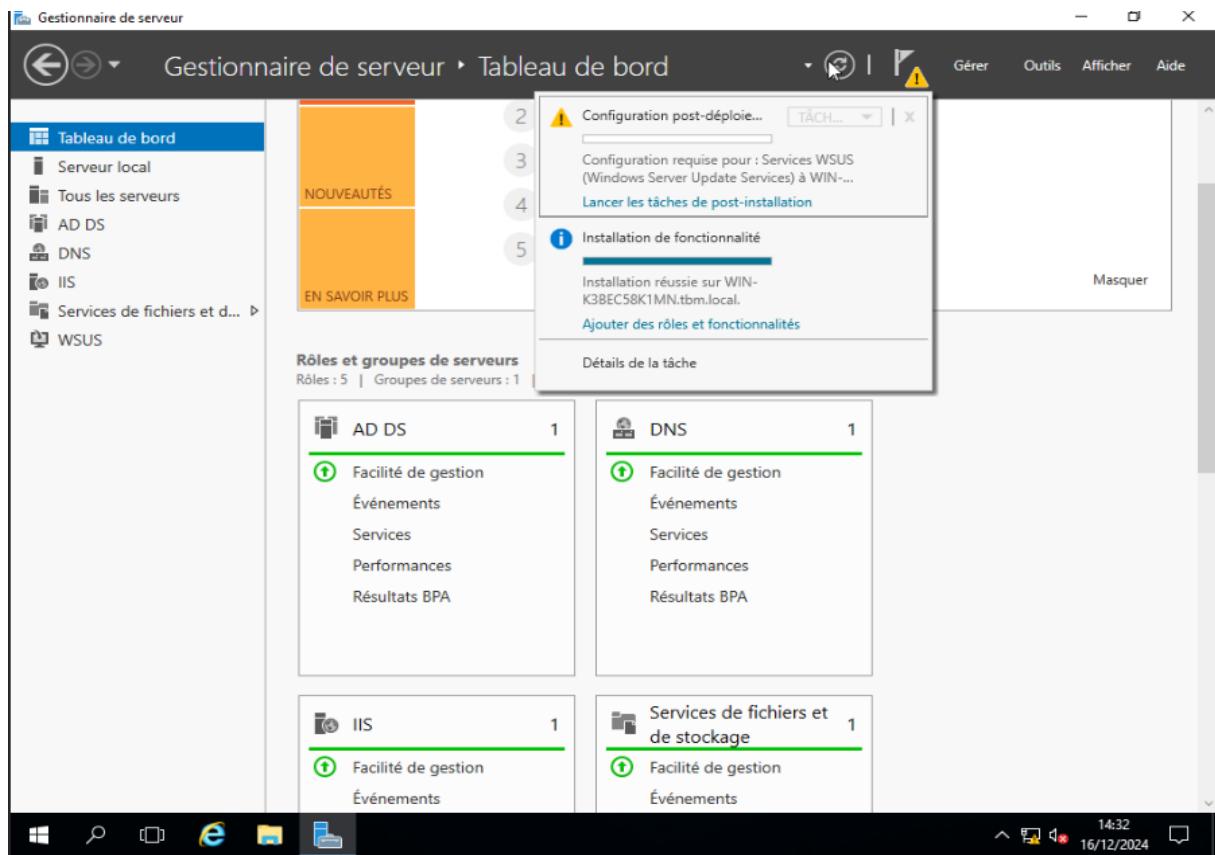
Pour cela il faudra sélectionner « Ajouter des rôles et des fonctionnalités ».



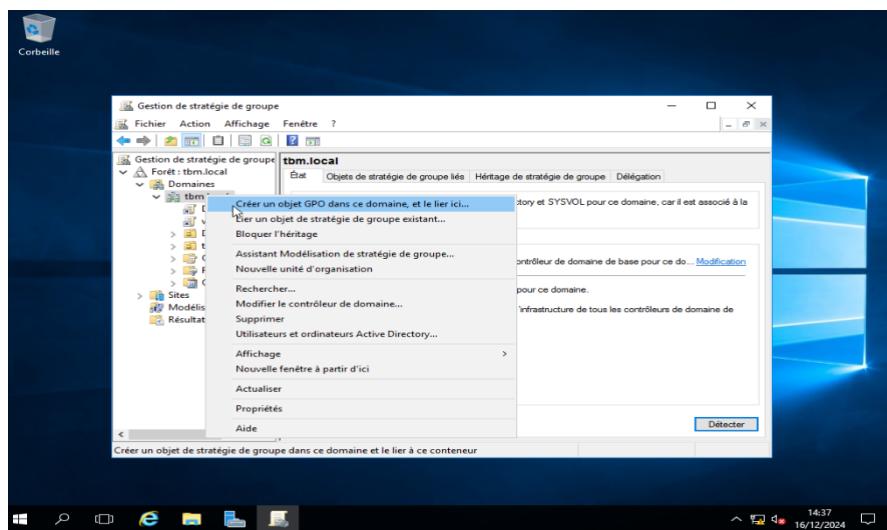
Ensuite dans les services, il faudra sélectionner « Services WSUS » puis confirmer l'installation.



Une fois que l'installation sera finie on aura une image ressemblant à ça :

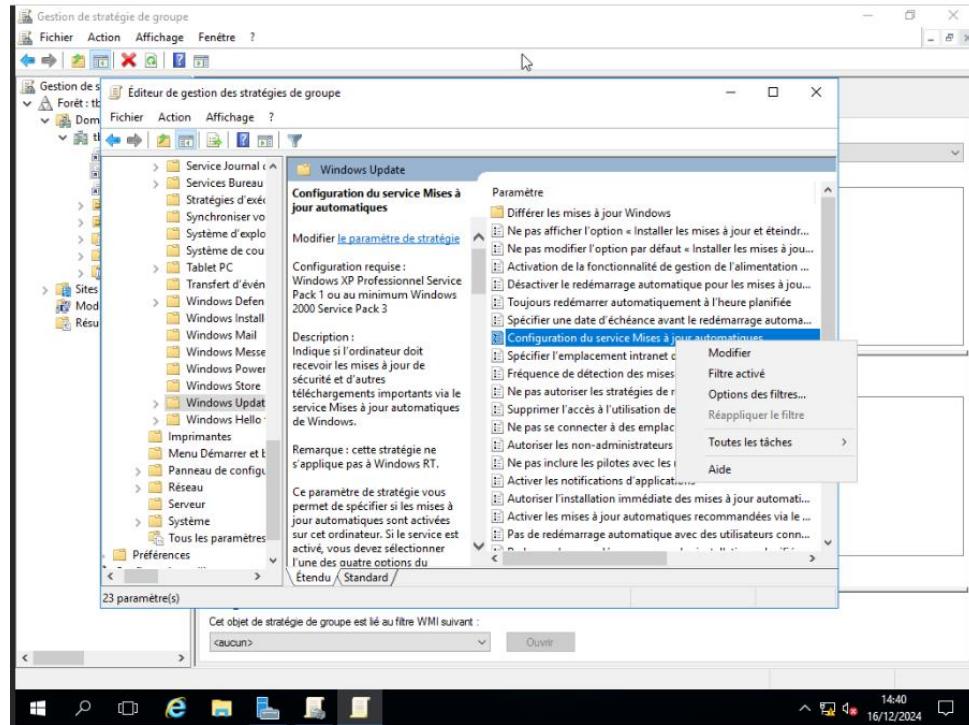


On va ensuite se rendre sur la gestion de stratégie de groupe, puis sur `foret\domaine` et créer une po pour wsus.

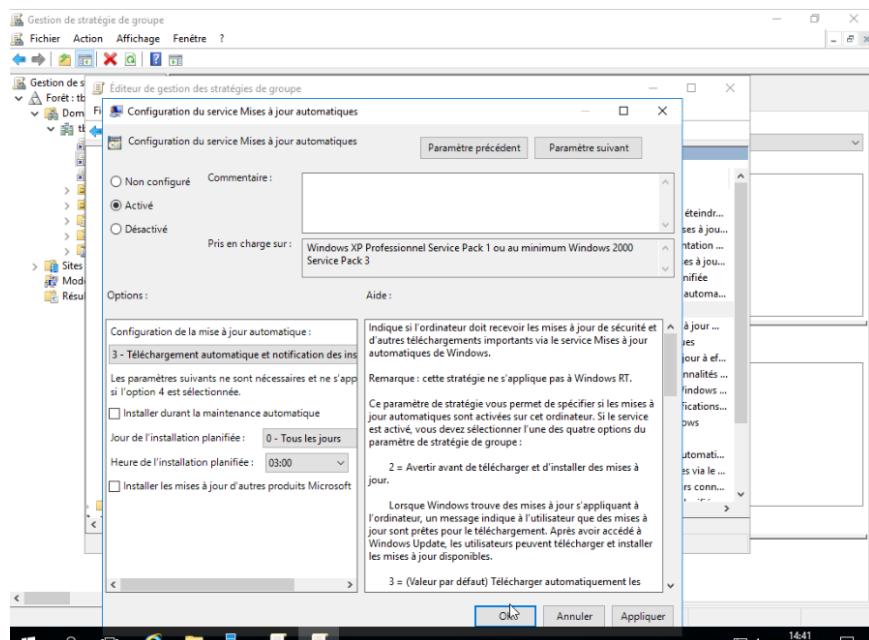


Nous allons ensuite modifier la gpo puis nous rendre dans les paramètres « Configuration ordinateur\Stratégies\Modèles d'administration\Composants Windows\Windows Update. »

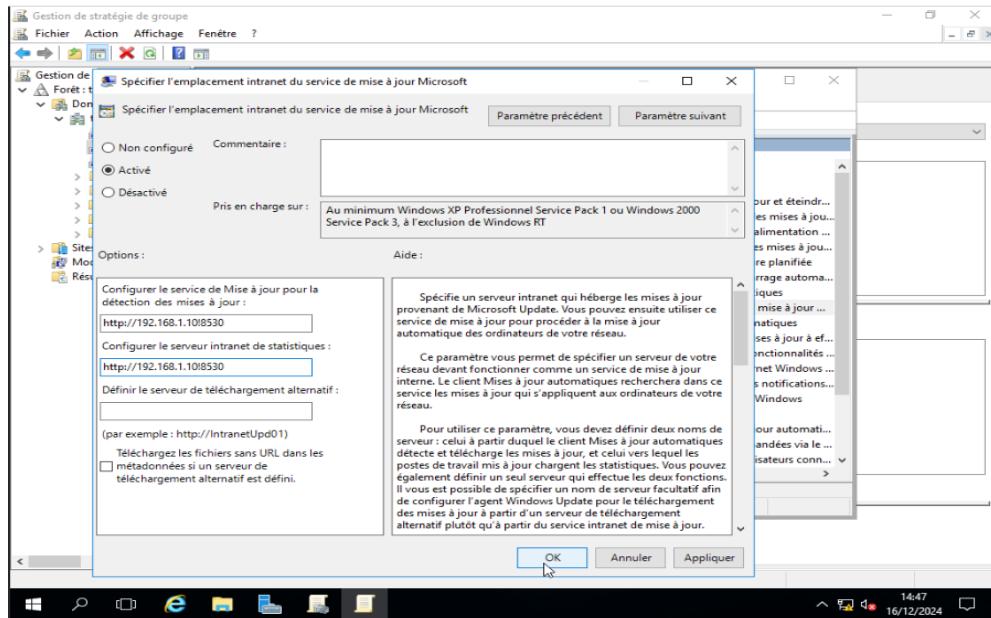
Puis modifier le paramètre « Configurer les mises à jour automatiques »



Il va falloir cocher la case « Activé » pour activer les GPO et dans les options choisir l'option « 3 » pour configurer les mises à jour automatiquement

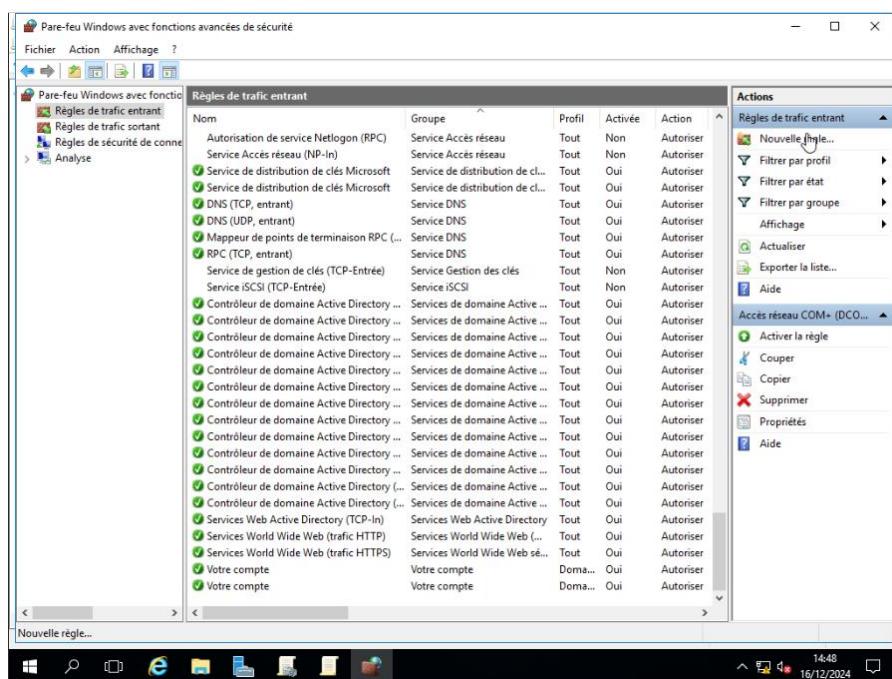


Ensuite, il va falloir modifier le paramètre « Spécifier l'emplacement du service de mise à jour Microsoft intranet », dans un premier temps il va falloir l'activer et dans un second temps spécifier pour « Définir le service de mise à jour intranet pour la détection des mises à jour » et « Définir le serveur de statistiques intranet » votre adresse pi ainsi que le port utilisé par sus (8530).

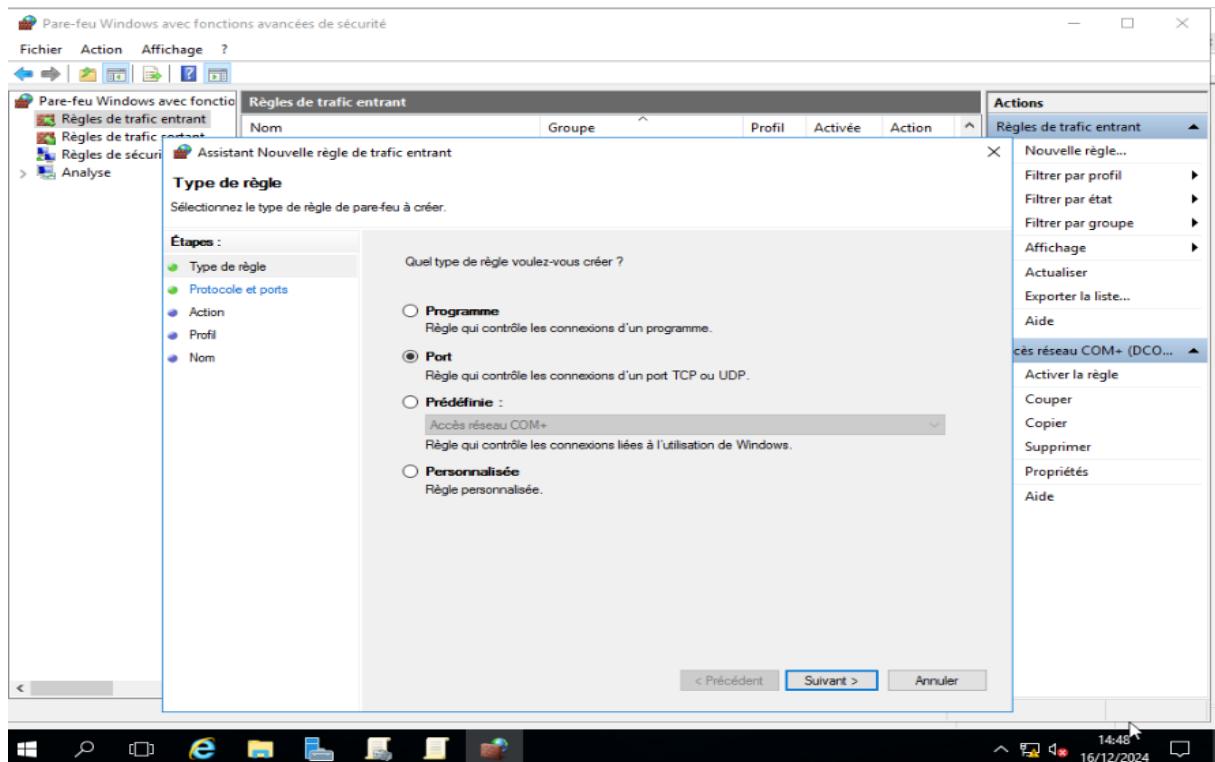


Si ce n'est pas déjà fait il va falloir rajouter une règle de pare feu pour ouvrir le port 8530.

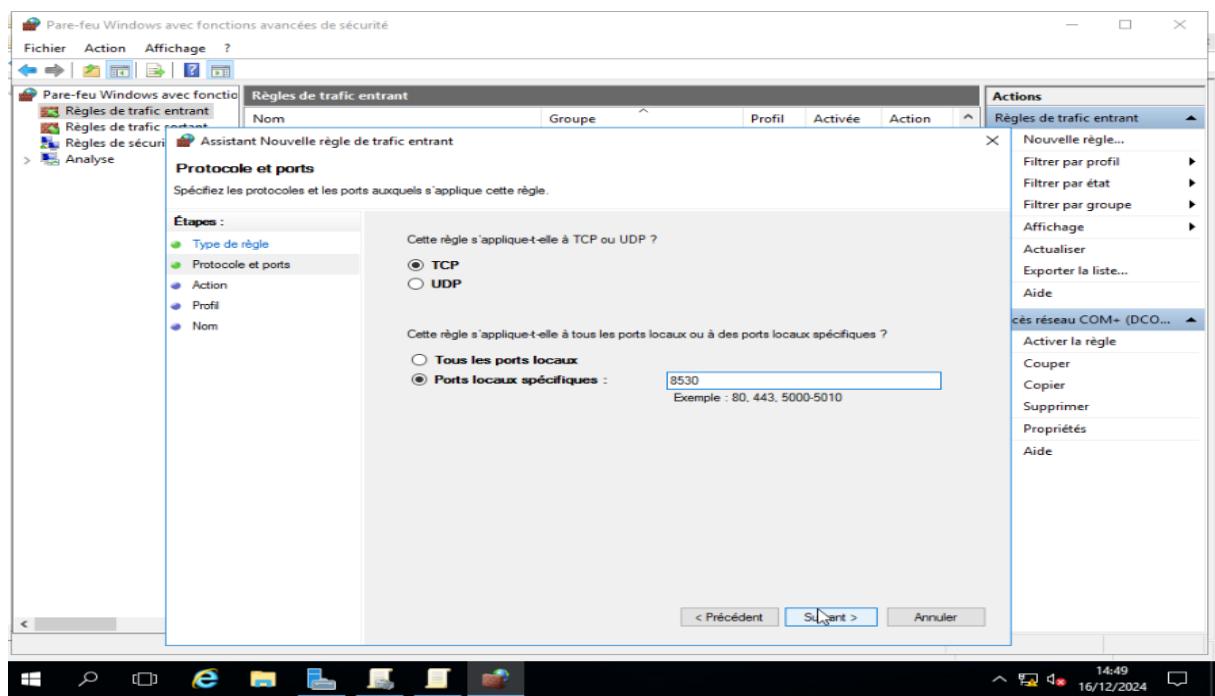
Dans les règles de trafic entrant il faut sélectionner « nouvelle règle ».



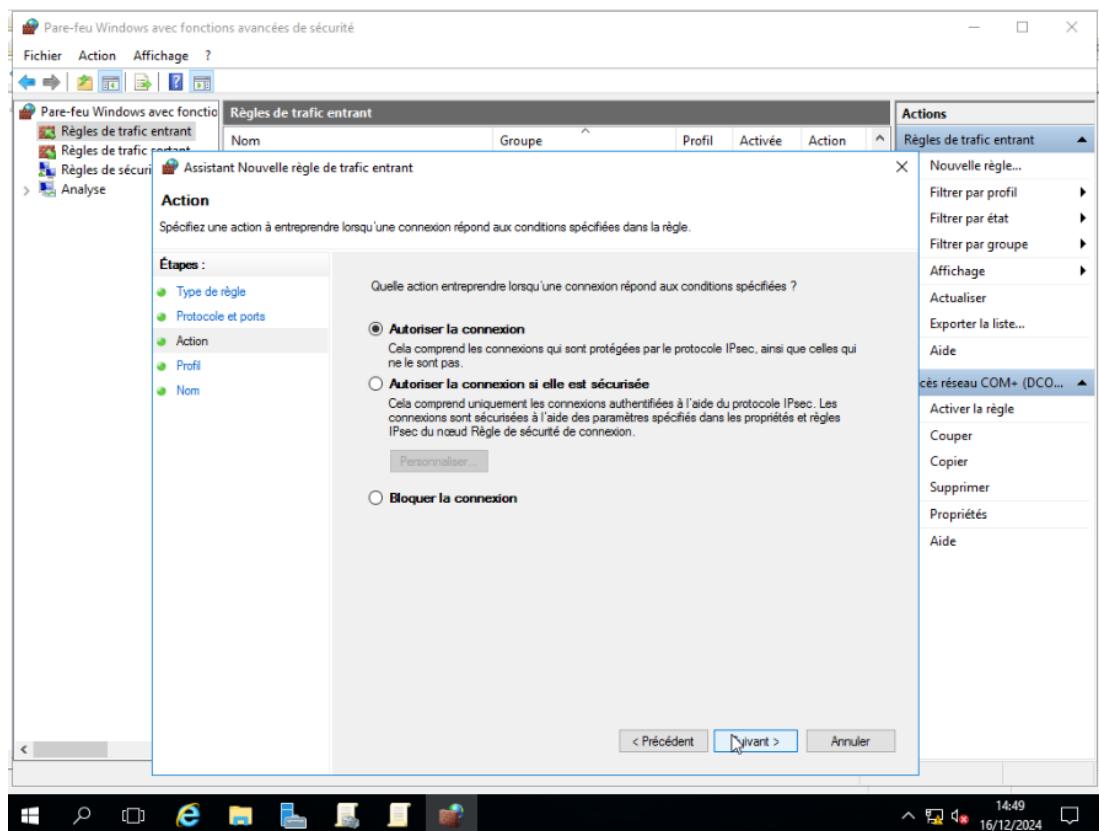
Dans le type de règle, sélectionnez « port »



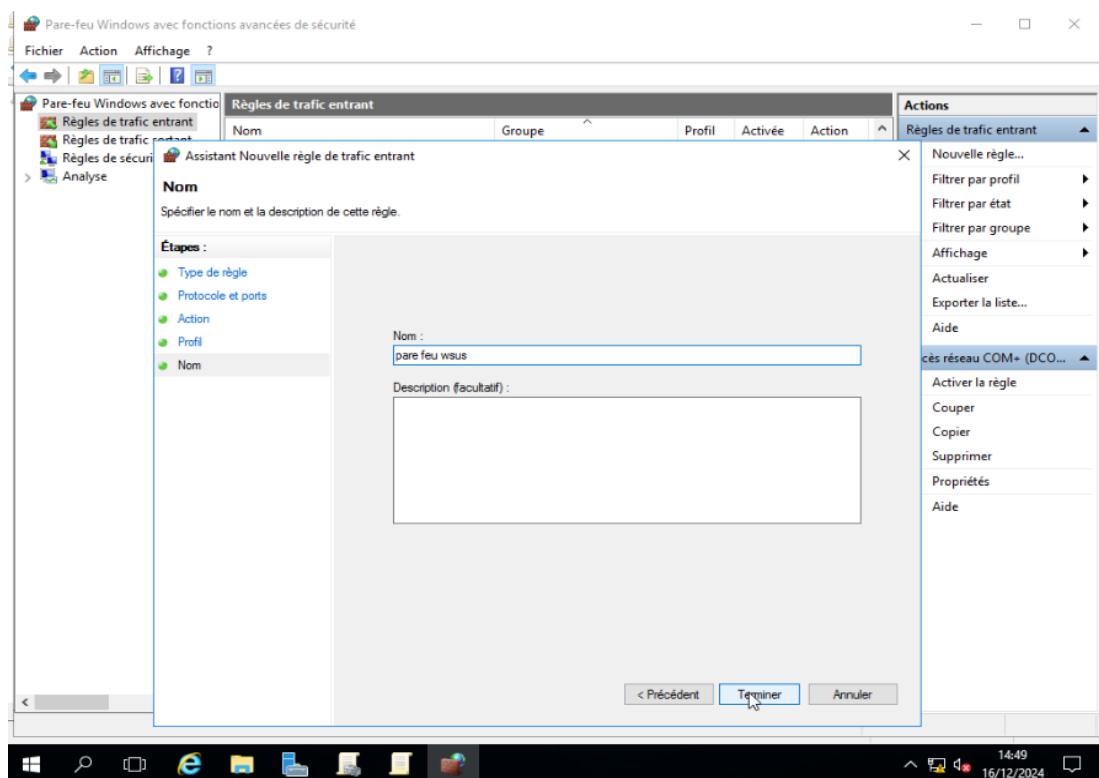
Ensuite entrez comme port « 8530 »



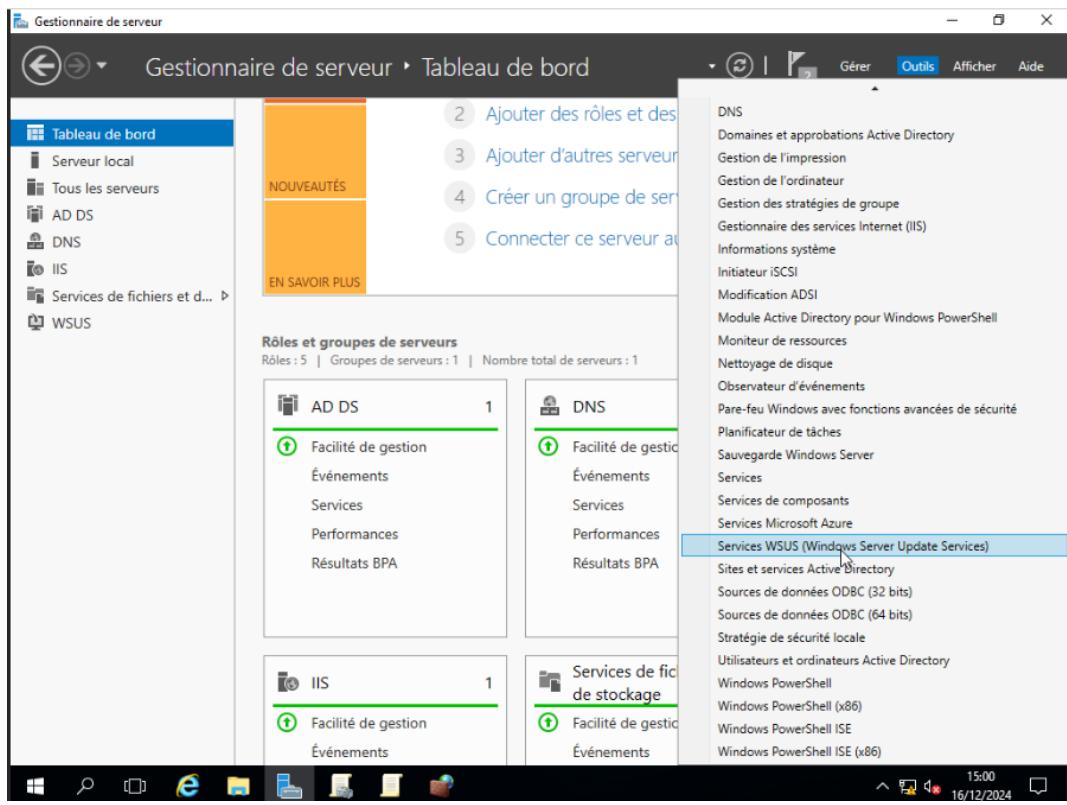
Ensuite il faudra sélectionner « autoriser la connexion »



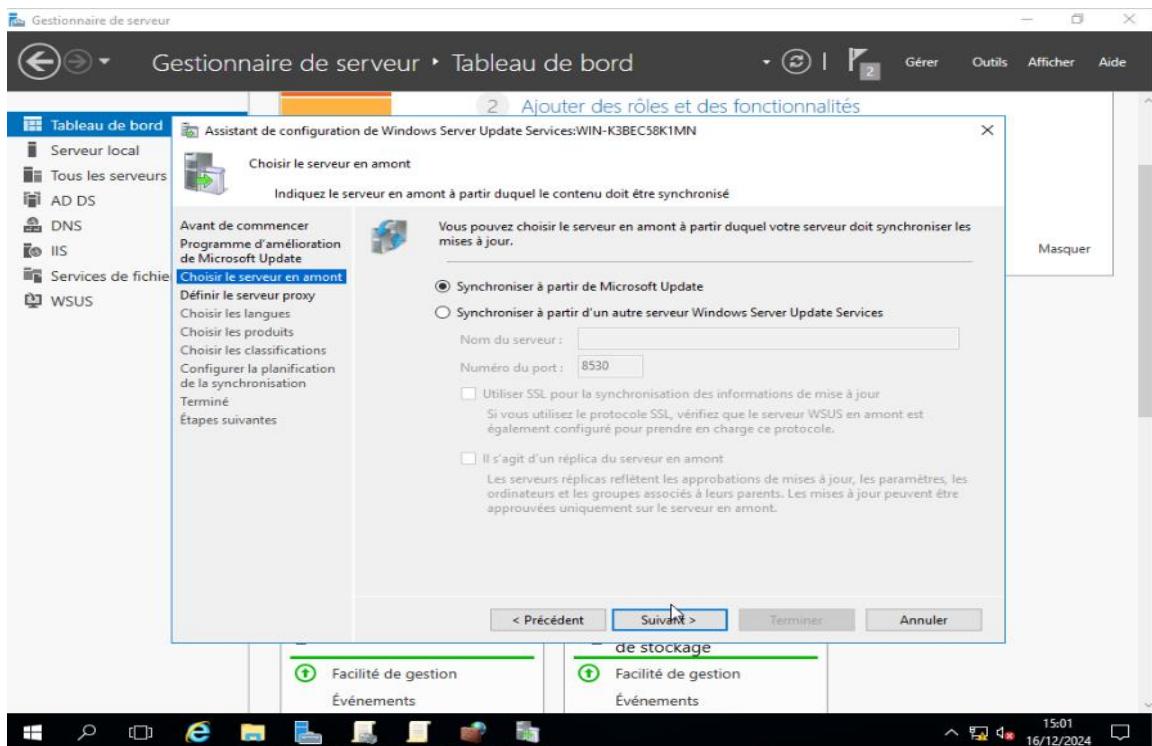
Puis pour finalisez la règle, il faudra lui donner un nom.



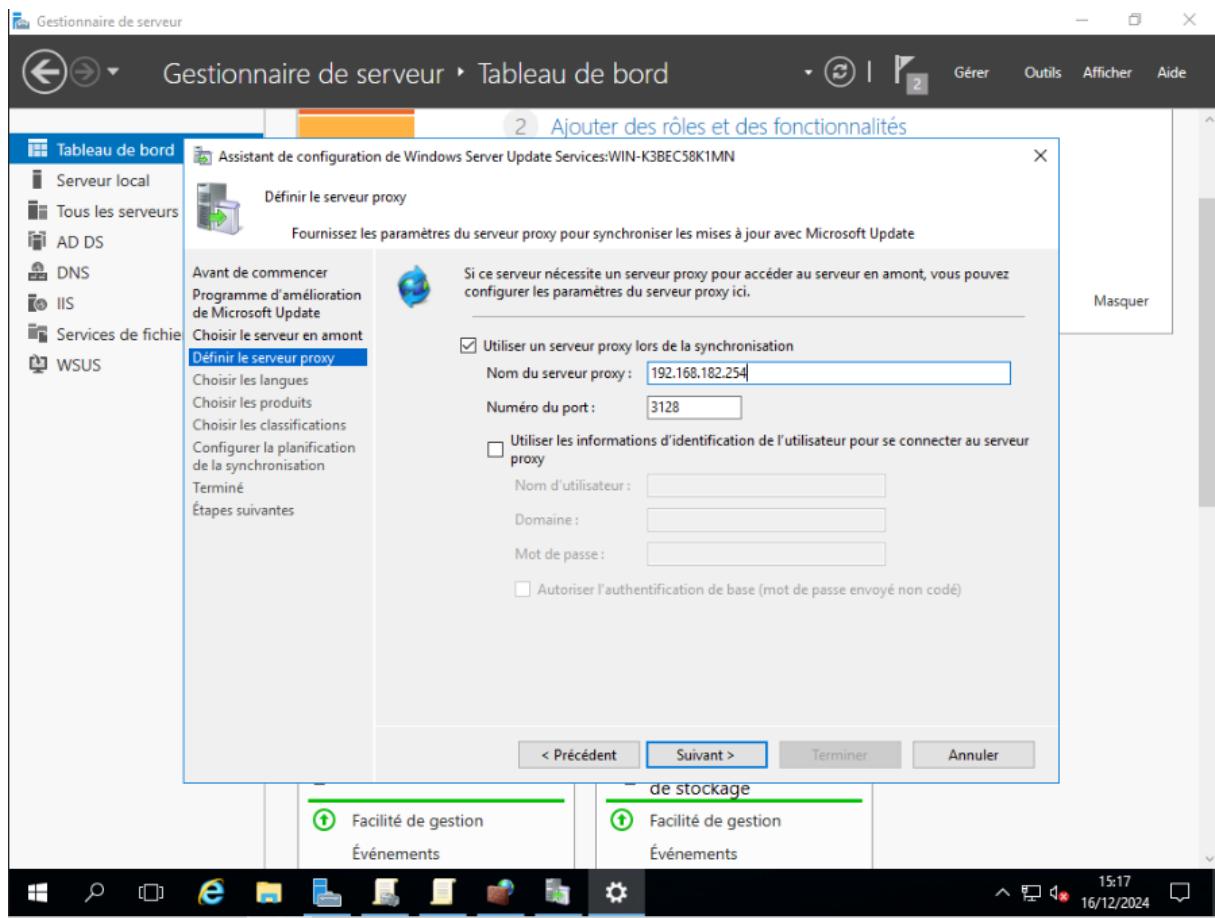
Ensuite nous pourrons nous rendre sur le gestionnaire de serveur pour lancer WSUS.



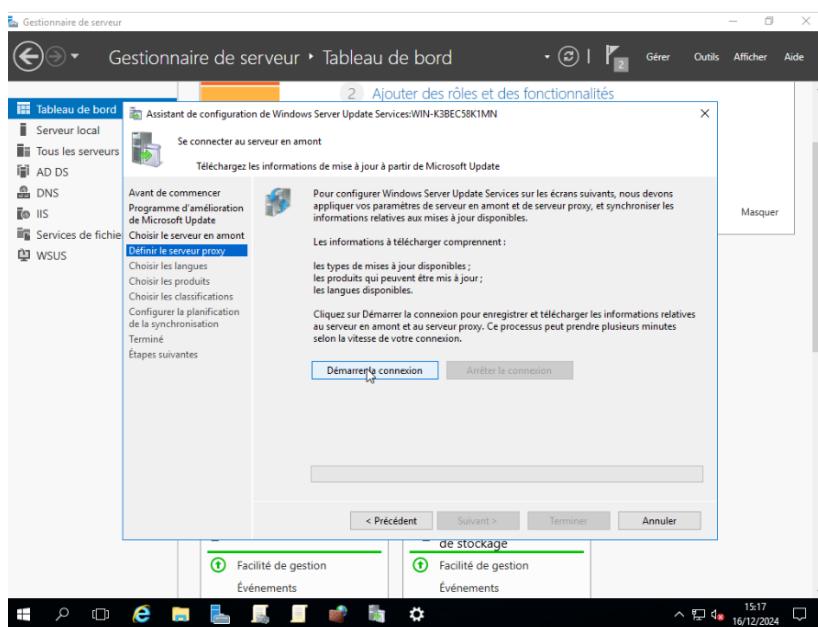
Concernant la synchronisation, on choisira « Microsoft Update »



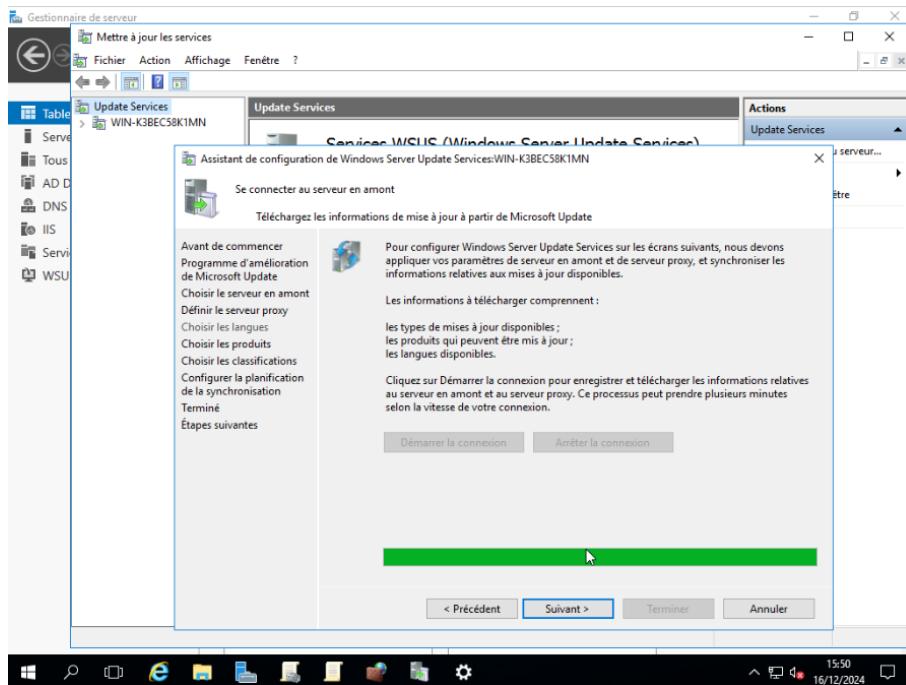
Si vous avez un proxy, il faudra le spécifiez



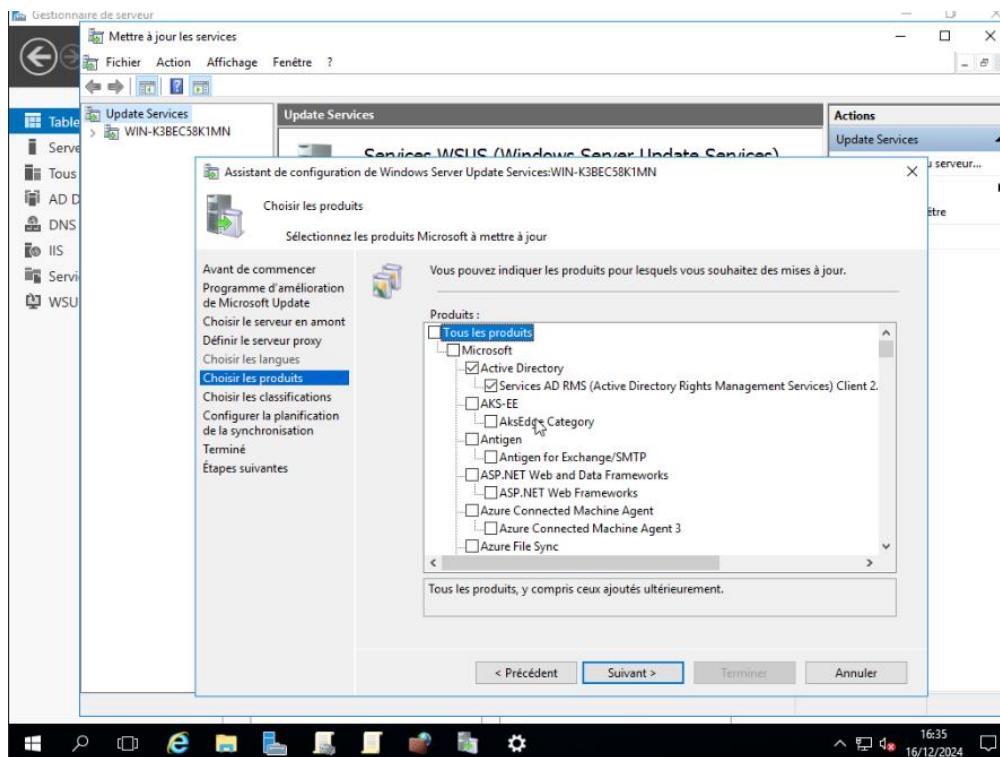
Une fois le proxy renseigné, wsus aura besoin de télécharger des informations relatives quant au serveur proxy et au windows server. Pour continuer il faudra sélectionner « Démarrer la connexion » ce processus peut s'avérer très long et durer jusqu'à 30 minutes environ.



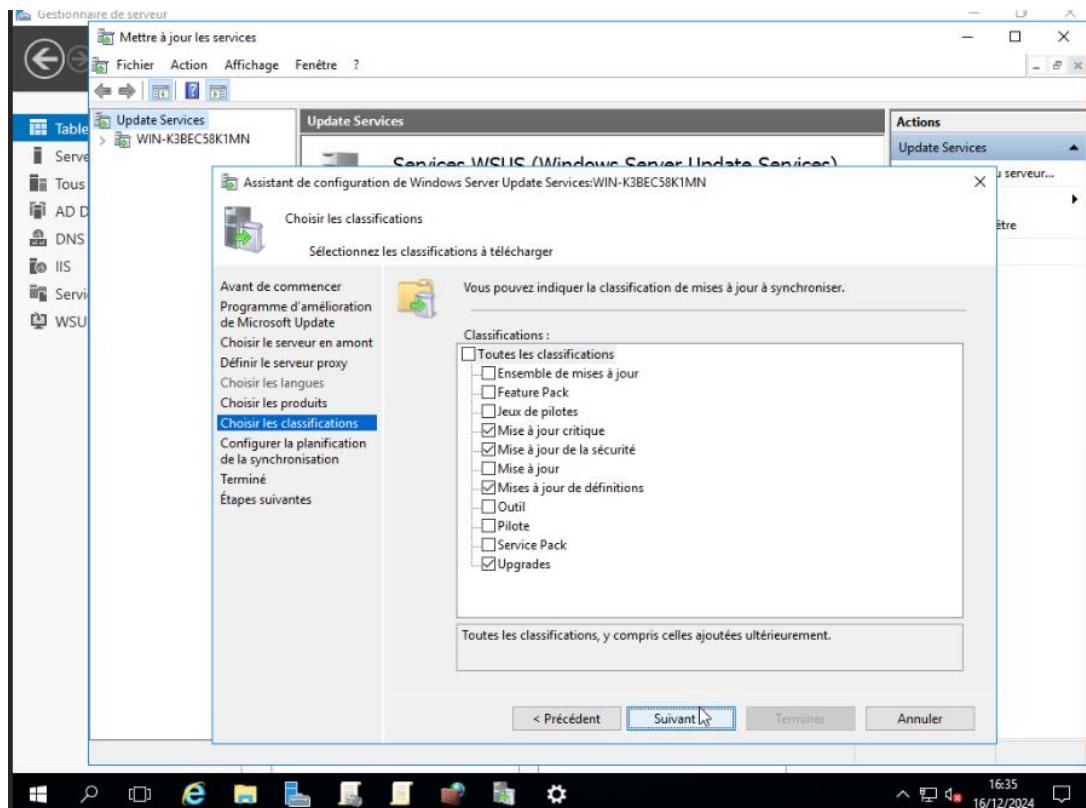
Une fois le processus terminé on pourra procéder à la suite. Vous devriez avoir un écran comme ça :



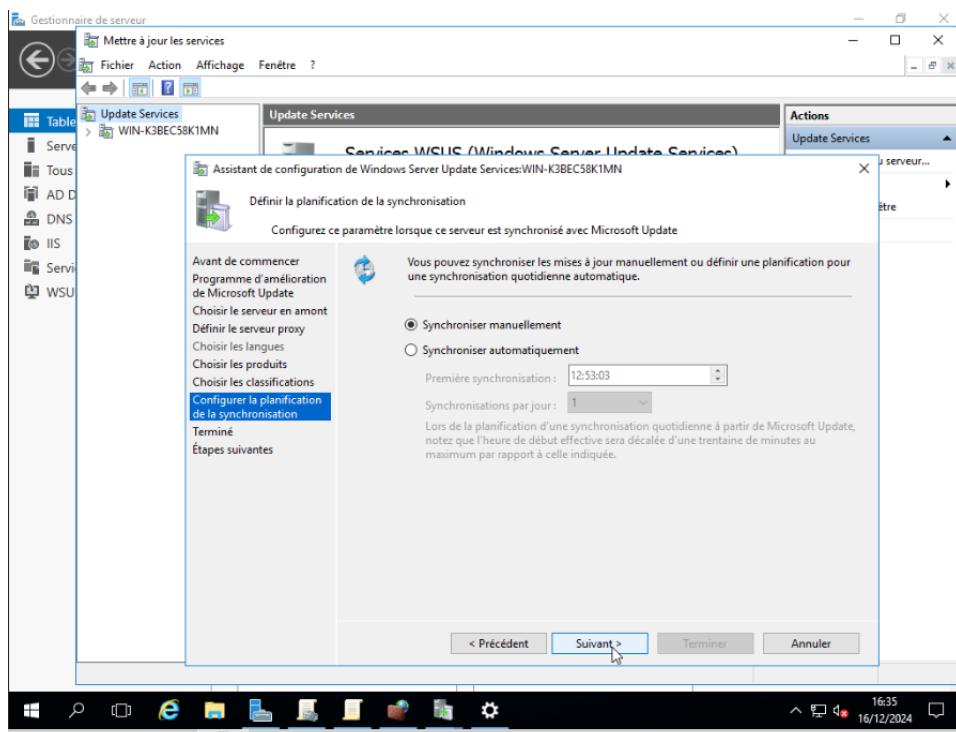
Vous pourrez constater que seuls les produits Microsoft sont cochés, on rajoutera « Active Directory » dans le cas où un autre windows server fera partie du domaine.



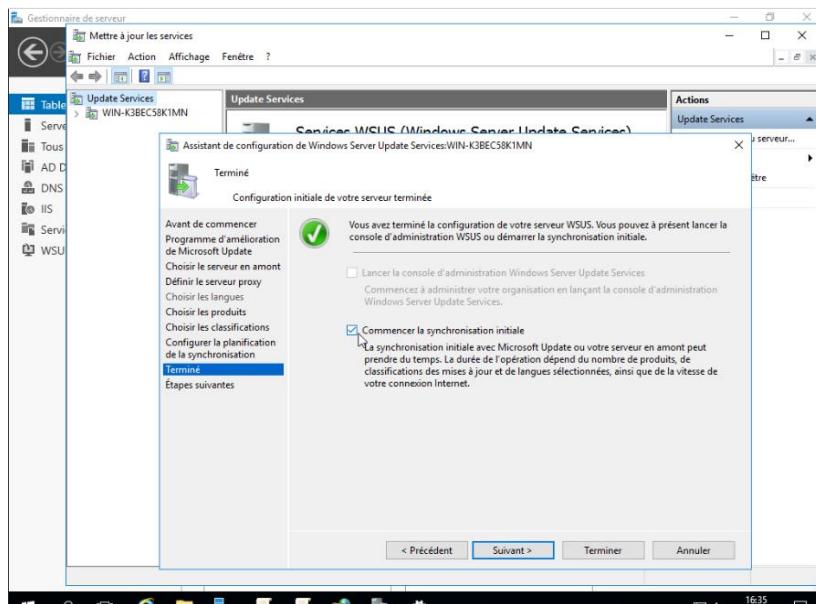
Vous pourrez également choisir les classifications, de notre côté on laissera par défaut afin d'avoir tous les types de mises à jour.



Vous aurez ensuite le choix entre une synchronisation automatique et manuelle. Il faudra choisir manuelle.



Ensuite pour finalisez la configuration wsus commencera la synchronisation.



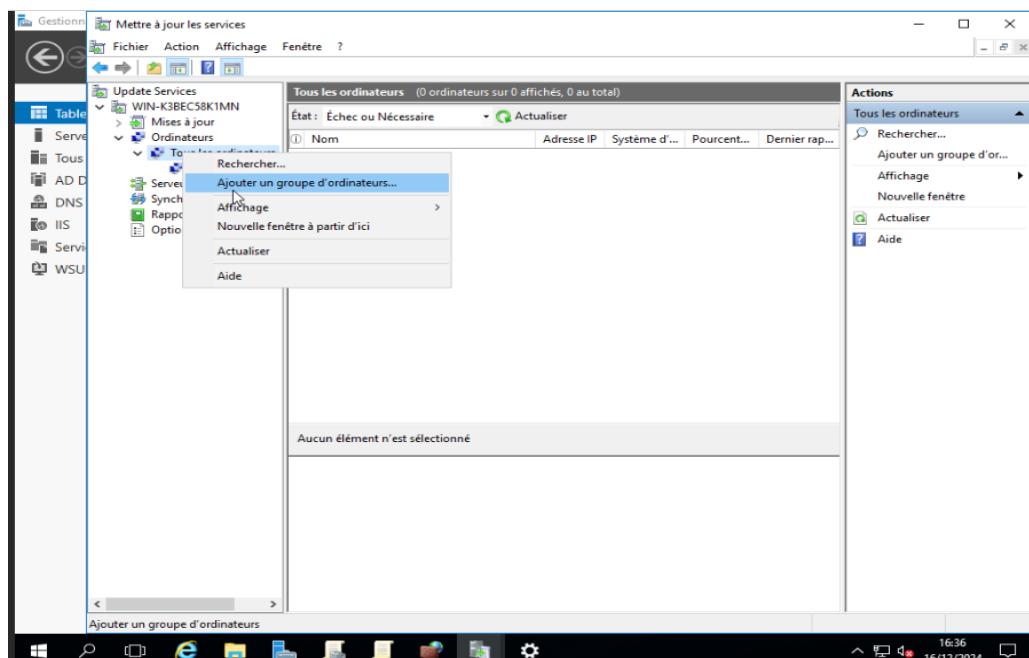
Maintenant que nous pouvons accéder à la console wsus, il faudra créer 3 groupes d'ordinateurs :

-Ring 2 Pilot Business Users

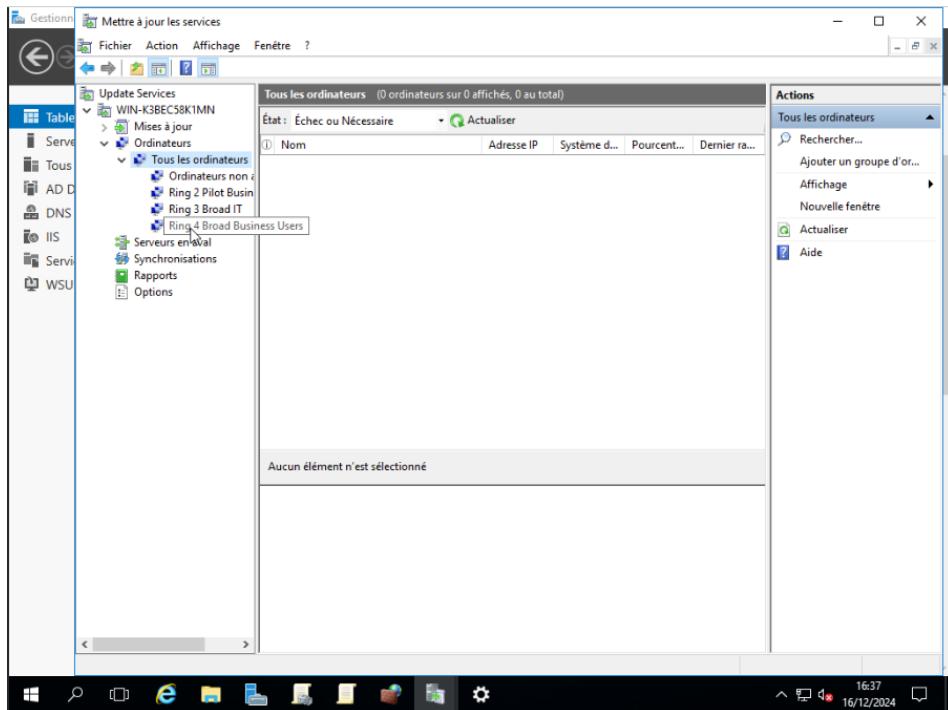
-Ring 3 Broad IT

-Ring 4 Broad Business Users

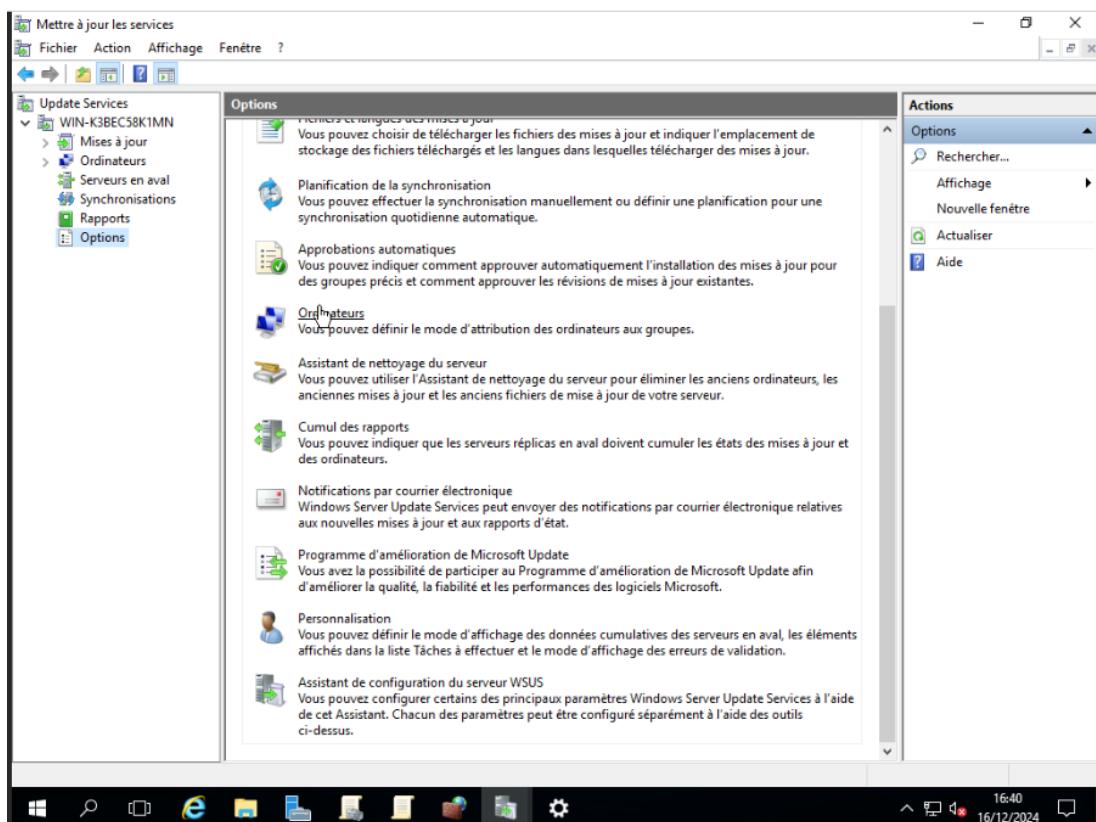
Pour cela il va falloir aller dans ordinateur \tous les ordinateurs puis clic droit « ajouter un nouveau groupe d'ordinateur »



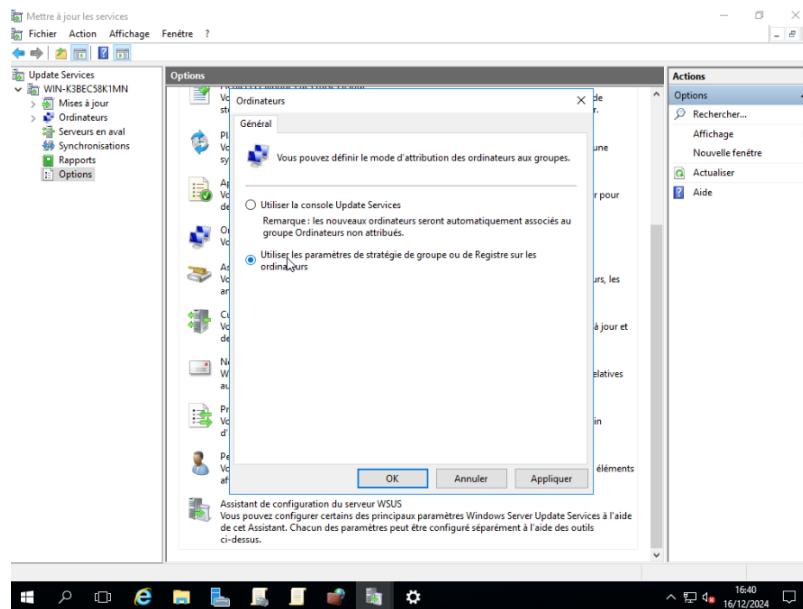
Une fois les trois groupes créer, votre console d'administrations devraient ressembler à ça



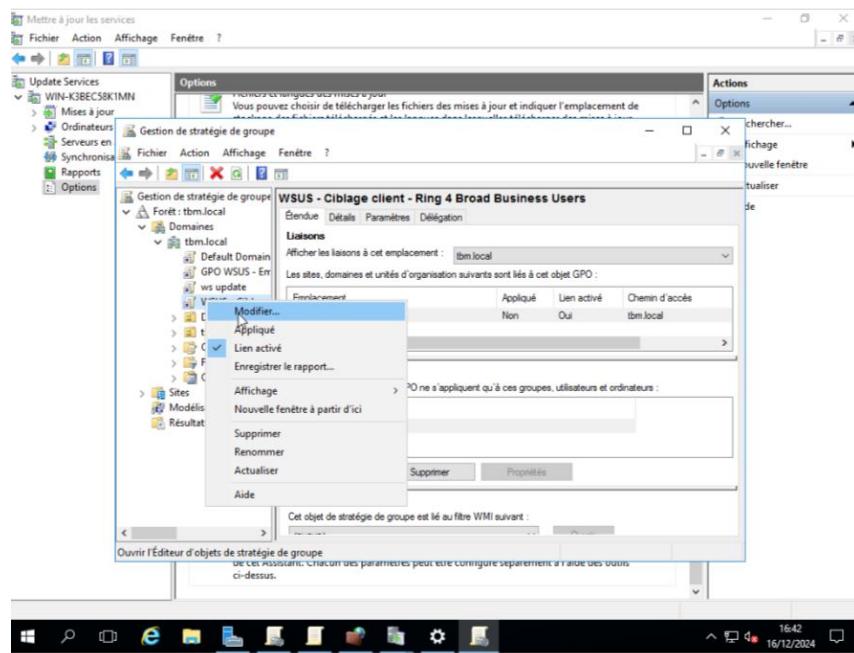
Ensuite dans les options de wsus il faudra sélectionner « ordinateurs »



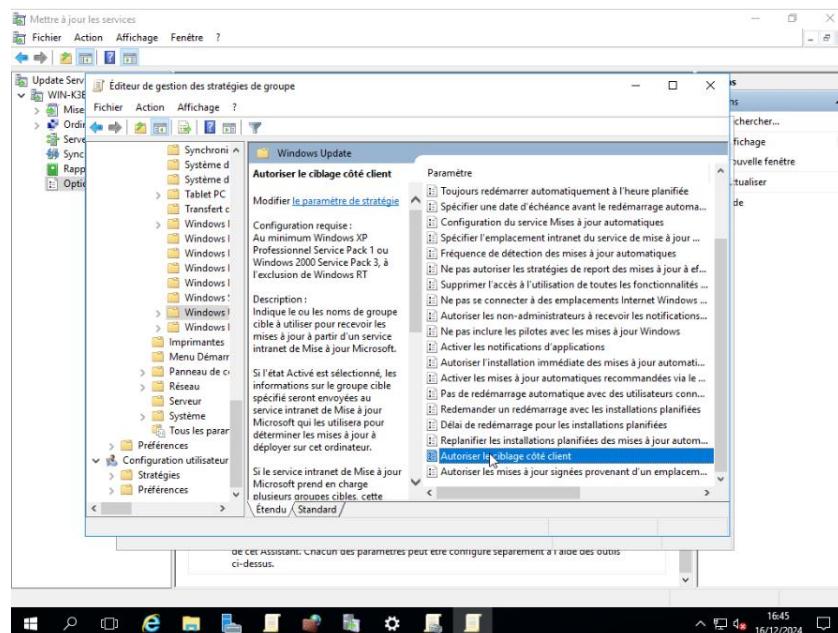
Une fois dans les paramètres, il faudra cocher la case « Utiliser la stratégie de groupe ou les paramètres de registre sur les ordinateurs » pour pouvoir utiliser les gpo pour WSUS



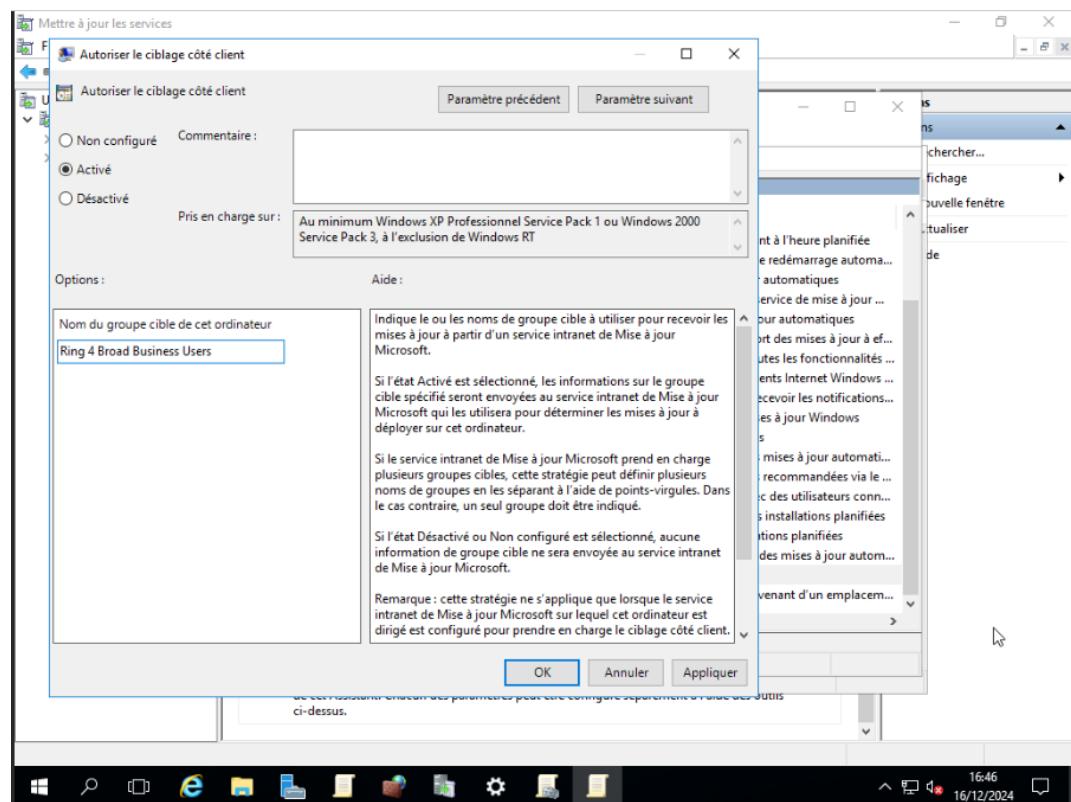
Une fois que cela est fait, il faudra retourner dans gestion de stratégie de groupe et créer une nouvelle gpo pour le groupe « Ring 4 Broad Business Users » et la modifier comme fait précédemment



Dans « Configuration ordinateur\Stratégies\Modèles d'administration\Composants Windows\Windows Update » on sélectionnera « autoriser le ciblage côté client »



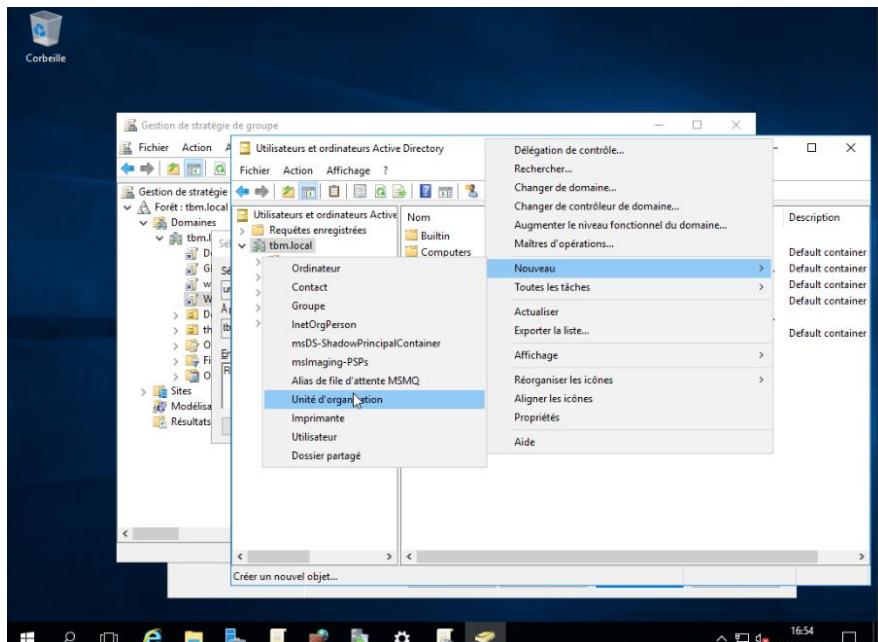
Il va falloir activer ce paramètre et entrer dans le nom de groupe « Ring 4 Broad Business Users ».



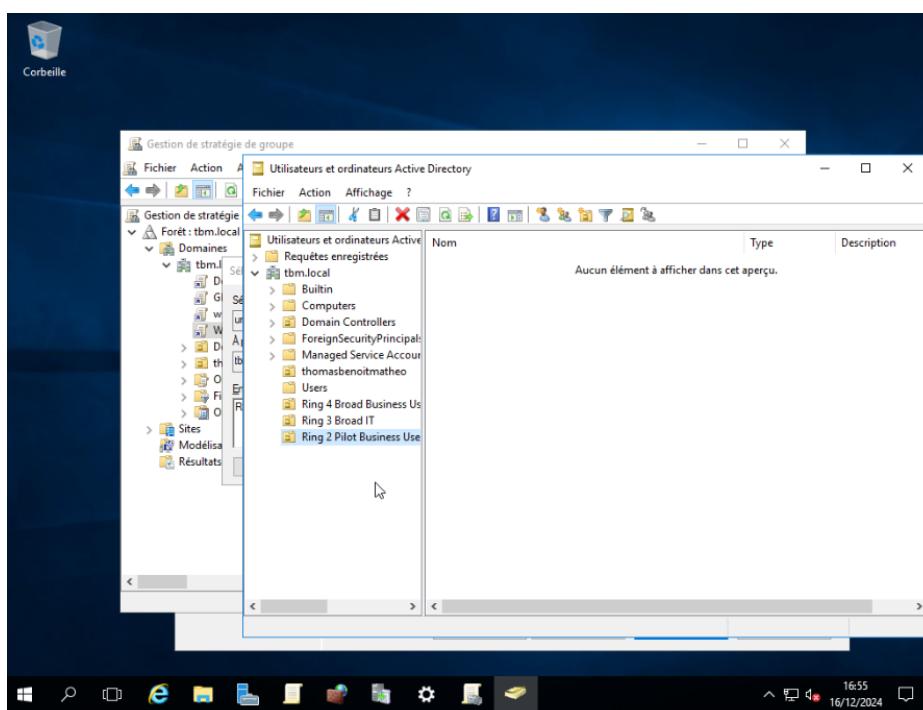
Une fois cela fait il va falloir crée 3 unités d'origination sur lequel appliquer les gpo.

Pour cela il faut aller dans gestionnaire des serveurs puis « utilisateurs et outils active directory »

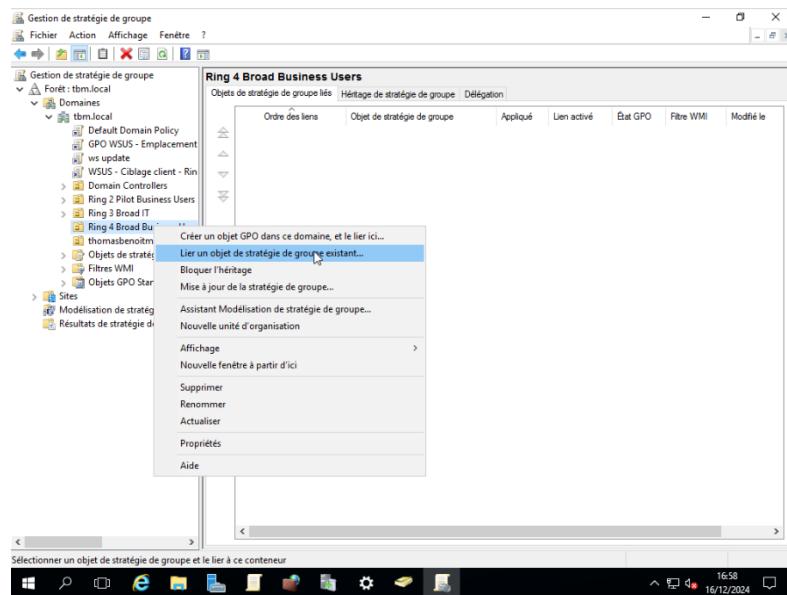
Puis dans foret\domaine puis faire clic droit et sélectionner nouveau puis « Unité d'organisation »



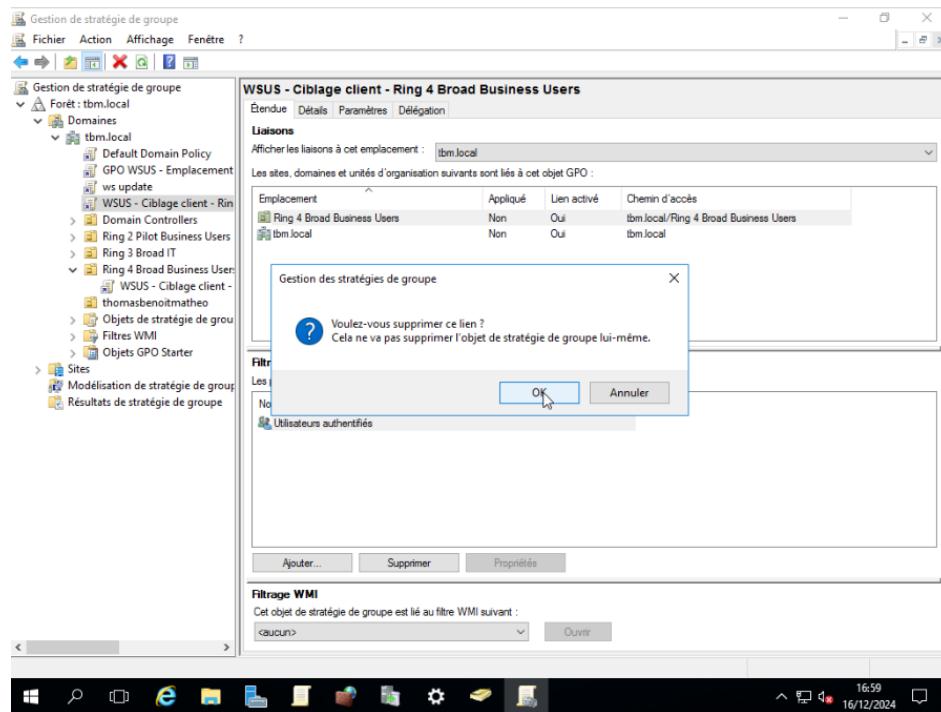
Une fois fini le résultat devrait ressembler à ça :



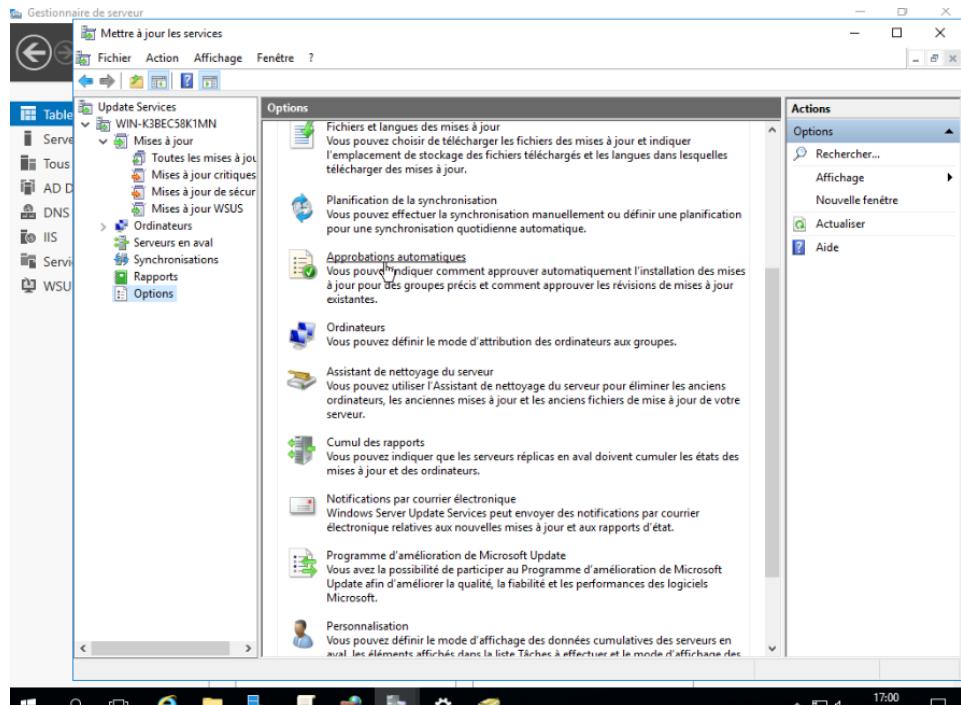
Vous pouvez maintenant appliquer la gpo précédemment créer au groupe « ring 4 Broad Business Users » avec clic droit puis « lier un objet de stratégie de groupe existant »



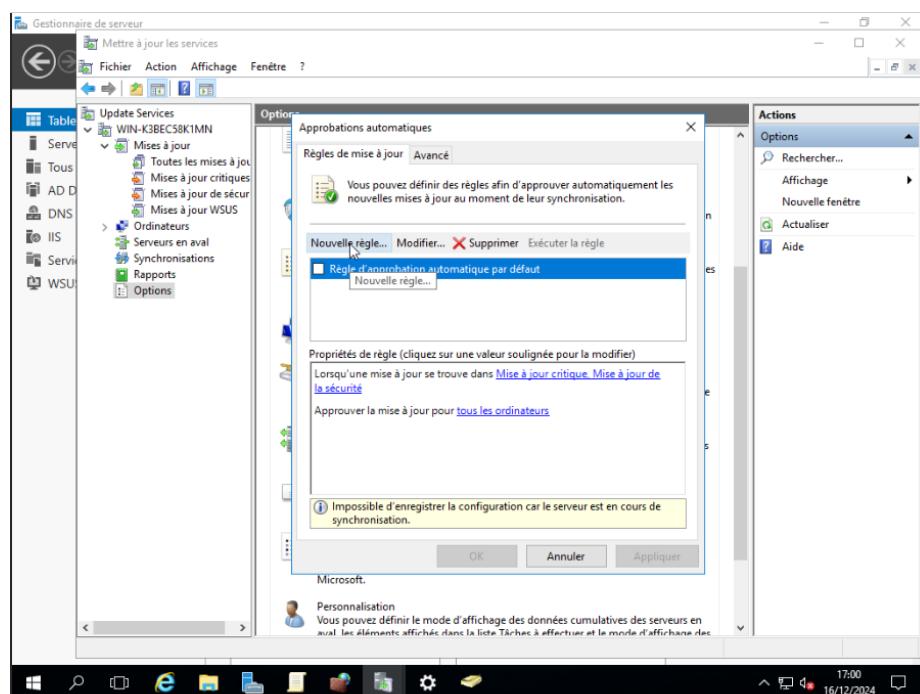
Vous pouvez également supprimer le lien du domaine pour que cette gpo s'applique uniquement à l'unité d'organisation précédemment créer.



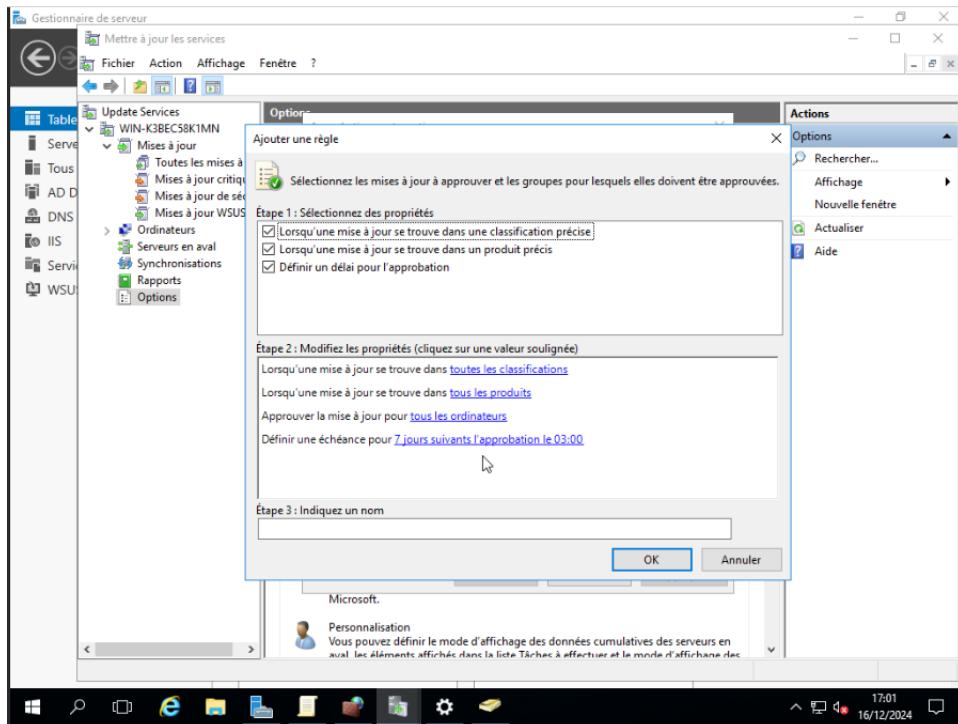
Ensuite il faudra retourner sur la console d'administration wsus puis aller dans les options afin de paramétrer les approbations automatiques



Il faudra sélectionner « nouvelle règle » afin de créer une nouvelle règle concernant les approbations automatiques.

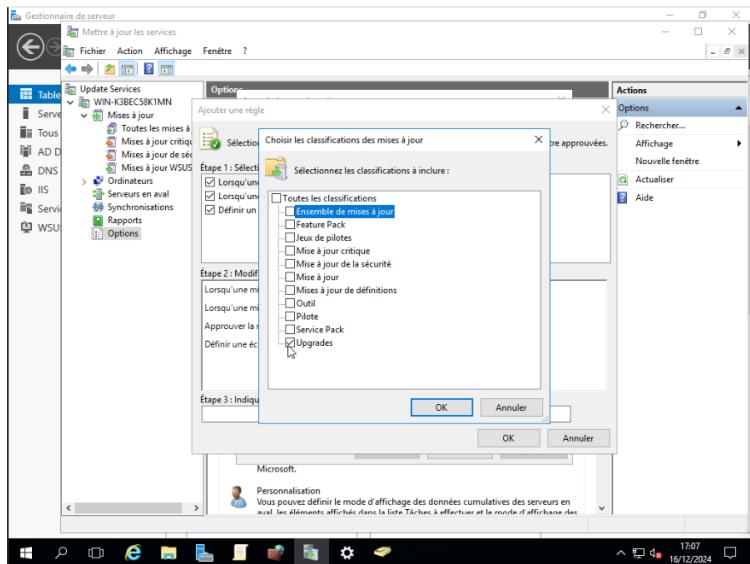


L'écran devrait ressembler à ça :

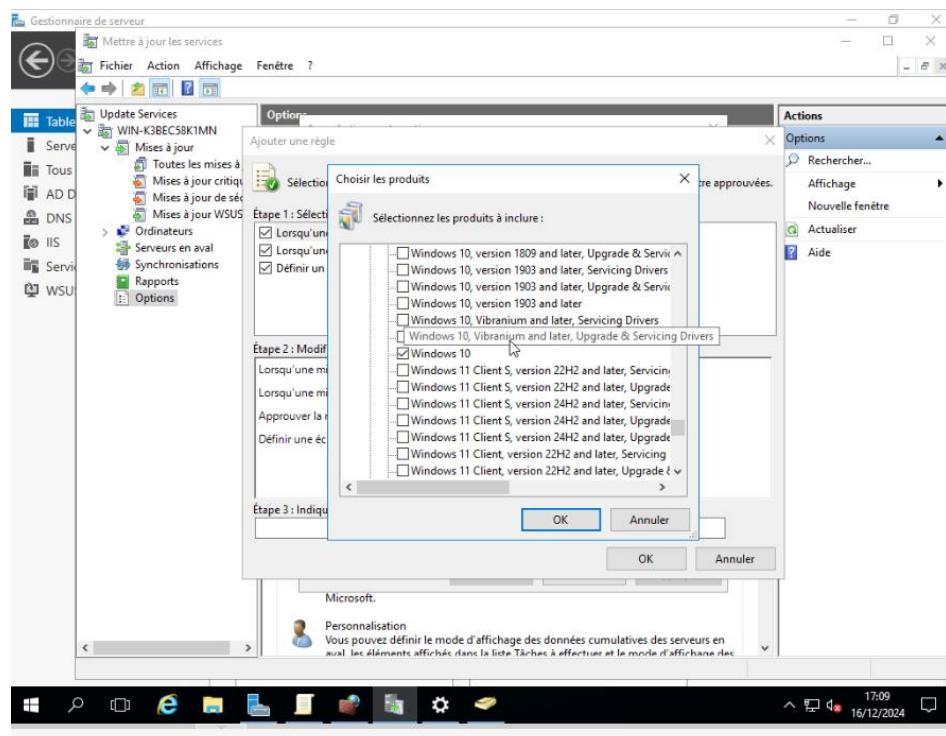


Parmi les 4 paramètres nous allons laissons par défaut uniquement l'échéance, nous allons modifier le reste

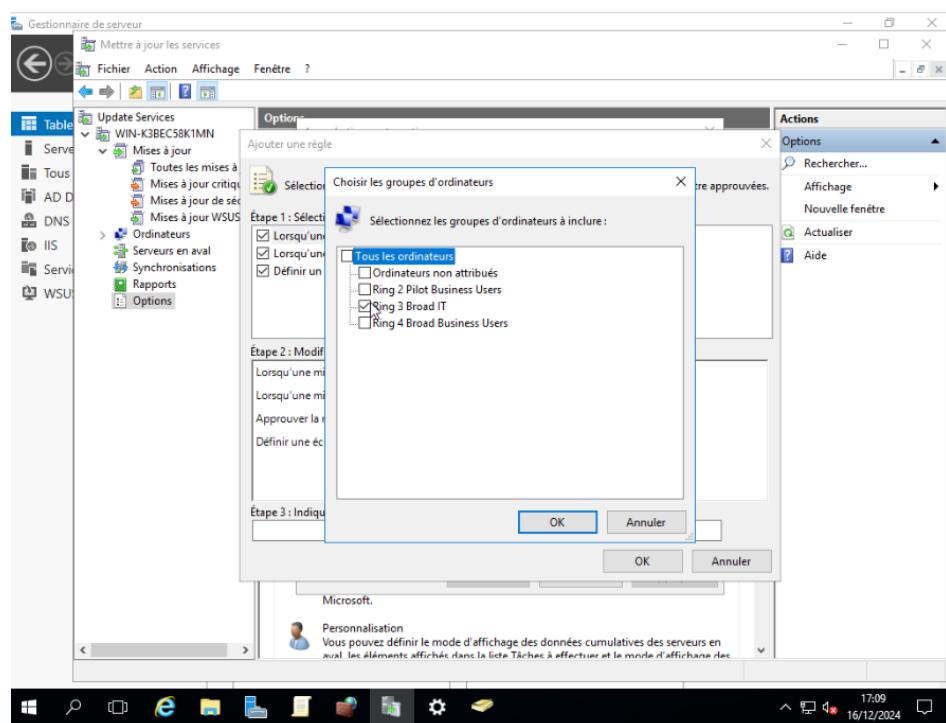
Concernant les classifications, seul « Upgrades » doit être cochée :



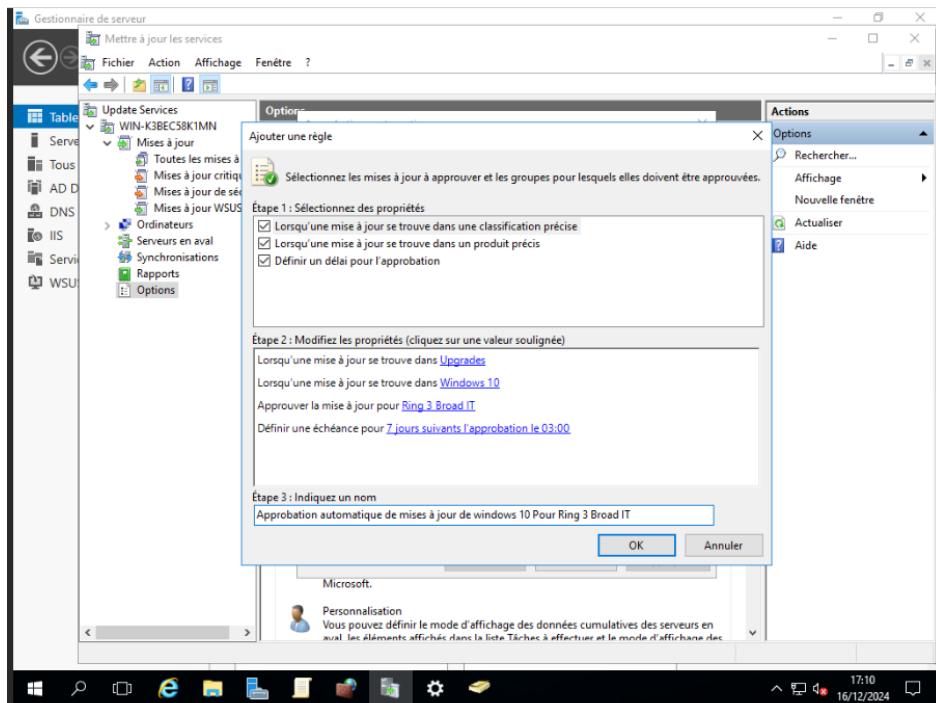
Concernant les produits, seuls windows 10 doit être cochée :



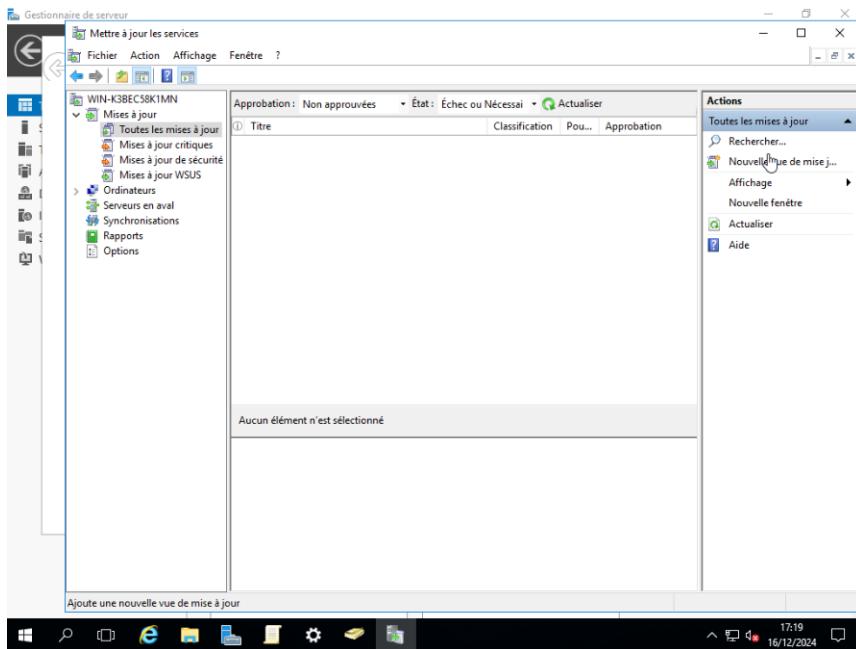
Concernant les groupes d'ordinateur, seul le groupe « Ring 3 Broad IT » doit être cochée :



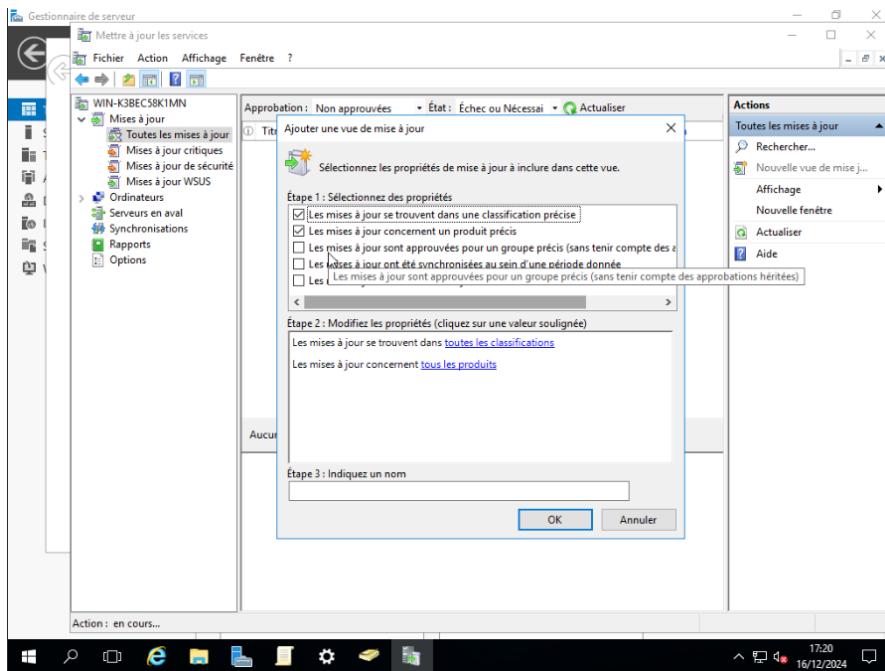
Ensuite pour finaliser la règle, il faudra la nommer



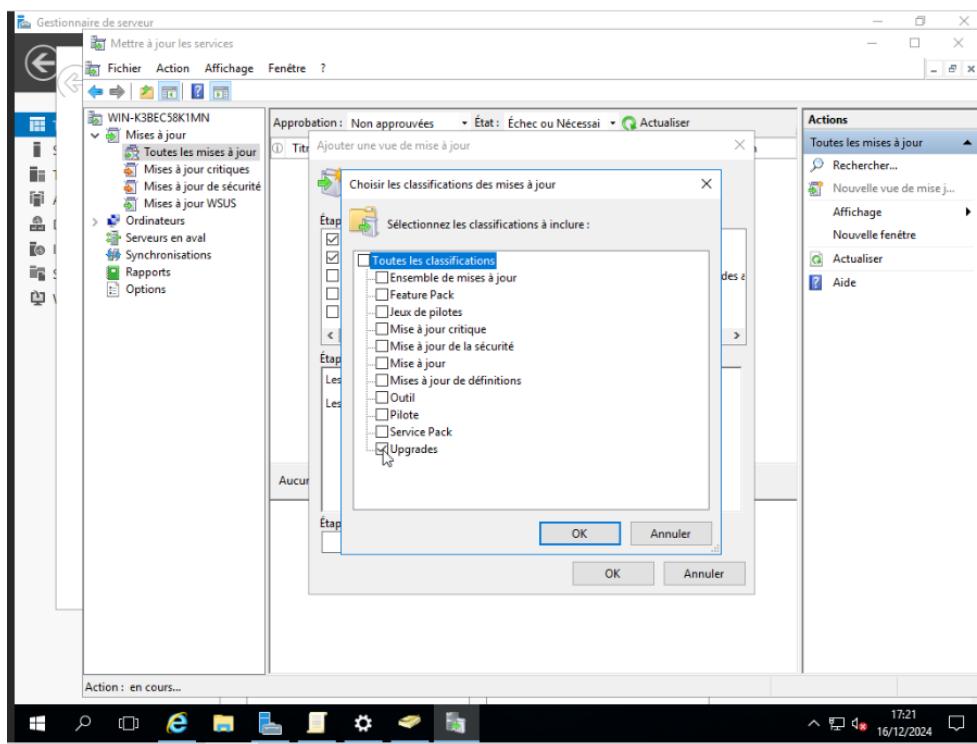
Après l'ajout de la règle il faudra se rendre vers Mises à jour/Toutes les mises à jour puis dans la barre « Actions » sélectionner « Nouvelle vue de mise à jour ».



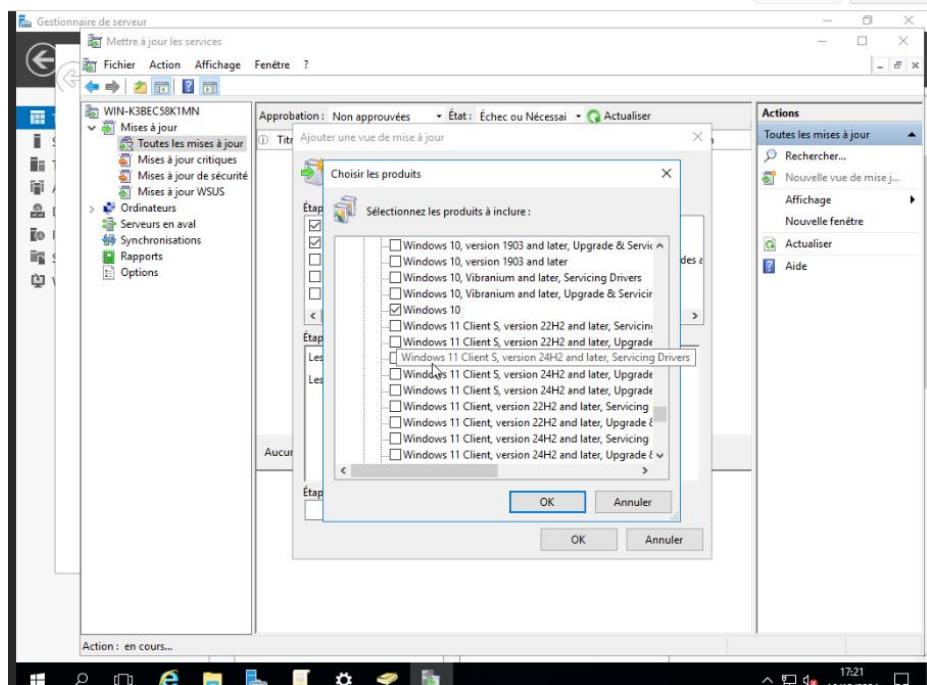
Il faudra laisser cocher uniquement « Les mises à jour se trouvent dans une classification précise » et « Les mises à jour concernent un produit précis »



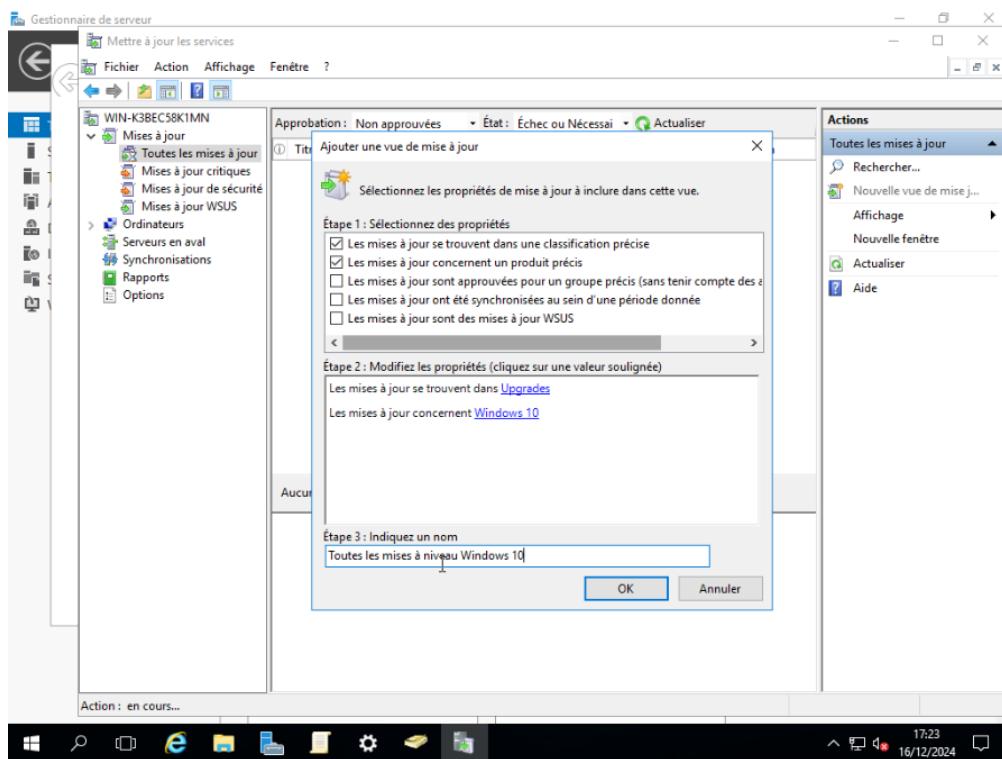
Comme pour la règle précédente dans les classifications on laisse cocher uniquement « Upgrades »

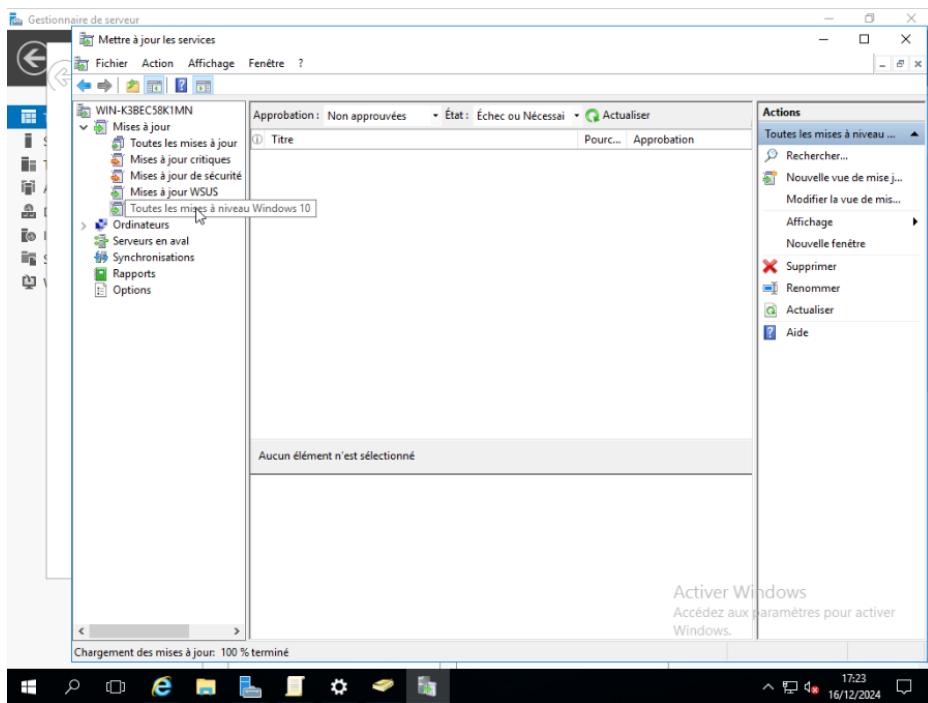


Et pour le produit on laisse uniquement « Windows 10 »



Pour finaliser la création de cette « vue », il faudra indiquer un nom





Une fois cela fait, la configuration de wsus pour l'automatisation des mises à jour sera finalisée.

## 8.5 Configuration Pfsense

J'ai commencé par mettre en place un serveur DHCP pour ce faire j'ai donc installé un pfsense et voici sa configuration :

WAN (wan)	-> em0	-> v4: 192.168.182.213/24
LAN (lan)	-> em1	-> v4: 192.168.2.1/24
DMZ (opt1)	-> em2	-> v4: 192.168.10.1/24
SERVEURS (opt2)	-> em1.300	-> v4: 192.168.1.254/24

Interface List									
Name ↑	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
DMZ	Linux Bridge	Yes	Yes	Yes					
enp2s0f0	Network Device	Yes	No	No					
enp2s0f1	Network Device	No	No	No					
vmb0	Linux Bridge	Yes	Yes	No	enp2s0f0		192.168.182.1/24	192.168.182.254	
vmb1	Linux Bridge	Yes	Yes	Yes					
vmb1.300	Linux VLAN	Yes	Yes	No					

Ensuite j'ai donc configuré le serveur DHCP grâce au pfsense que j'ai installé pour permettre l'adressage ip automatique et simplifié la vie de l'entreprise. Il faut d'abord mettre en place le serveur DHCP pour ce faire il faut aller dans services > DHCP server. Ensuite choisissez la plage d'ip qui vous intéresse pour les appareils réseau de l'entreprise puis enregistré.

J'ai ensuite créé une carte réseau pour la DMZ et voici les règles pare-feu rentré dans pfsense :

Firewall Rules											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 TCP	DMZ net	*	WAN net	*	*	none		proxy1	
<input type="checkbox"/>	0/0 B	IPv4 *	DMZ net	*	LAN net	*	*	none		bloquer les flux vers LAN	
<input type="checkbox"/>	0/0 B	IPv4 *	DMZ net	*	SERVEURS net	*	*	none		bloquer les flux vers SERVEURS	
<input type="checkbox"/>	0/0 B	IPv4 TCP	DMZ net	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	DMZ net	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	0/393 KiB	IPv4 TCP/UDP	DMZ net	*	*	53 (DNS)	*	none			

Puis j'ai configuré mes règles pare-feu pour le réseau LAN :

Floating	WAN	LAN	DMZ	SERVEURS							
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2/443 KIB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	LAN net	*	DMZ net	*	*	none		bloquer les flux entre LAN et DMZ	
<input type="checkbox"/>	42/340.74 MIB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	*	*	*	*	*	none		Ping	

Et enfin j'ai créé mon VLAN300 dédié au serveur et voici les règles pare-feu misent :

Floating	WAN	LAN	DMZ	SERVEURS							
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	SERVEURS net	22 (SSH)	*	none			
<input type="checkbox"/>	0/420 KIB	IPv4 TCP	*	*	SERVEURS net	443 (HTTPS)	*	none			
<input type="checkbox"/>	0/398 KIB	IPv4 TCP	SERVEURS net	*	LAN net	*	*	none			
<input type="checkbox"/>	0/127 KIB	IPv4 *	SERVEURS net	*	DMZ net	*	*	none		bloquer les flux entre SERVEURS et DMZ	
<input type="checkbox"/>	8/782.52 MiB	IPv4 TCP	SERVEURS net	*	WAN net	*	*	none		proxy1	
<input type="checkbox"/>	0/2 KIB	IPv4 ICMP any	*	*	*	*	*	none		ping	
<input type="checkbox"/>	0/13.06 MiB	IPv4 UDP	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

J'ai ensuite ajouté mes serveurs au vlan comme ça :

### Edit: Network Device

Bridge:	vmbr1	Model:	Intel E1000
VLAN Tag:	300	MAC address:	BC:24:11:A5:2E:B6
Firewall:	<input checked="" type="checkbox"/>	<input type="button" value="Help"/> <input type="button" value="Advanced"/> <input type="button" value="OK"/>	

## 8.6 Configuration Portail captif

Pour le mettre en place il faut aller dans Status > Captive Portal dans l'outil pfSense.

Puis cliquer sur add (ou ajouter si vous avez pfSense en français)

The screenshot shows the 'Services / Captive Portal' section. Below it is a table titled 'Captive Portal Zones' with columns: Zone, Interfaces, Number of users, Description, and Actions. A green '+' button labeled 'Add' is located at the bottom right of the table area.

Suivez les différentes étapes :

Il faudra donner un nom pour « Zone name » et pour « Zone Description »

The screenshot shows the 'Services / Captive Portal / Add Zone' page. It contains two input fields: 'Zone name' with the value 'PORTAIL' and 'Zone description' with the value 'Portal Captif'. Below the fields is a blue 'Save & Continue' button.

Ensuite il faudra cocher la case « Enable Captive Portal », entrer un nom pour « Description » et sélectionner LAN pour « Interfaces »

The screenshot shows the 'Services / Captive Portal / PORTAIL / Configuration' page. Under the 'Captive Portal Configuration' section, the 'Enable' checkbox is checked. The 'Description' field contains 'Portal Captif'. The 'Interfaces' dropdown menu has 'WAN' and 'LAN' listed, with 'LAN' selected. Other configuration options include 'Maximum concurrent connections' set to 1 and 'Idle timeout (Minutes)' set to 5.

<b>Logout popup window</b>	<input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
<b>Pre-authentication redirect URL</b>	<input type="text" value="http://www.google.fr"/> Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRURL\$ variable in captiveportal's HTML pages.
<b>After authentication Redirection URL</b>	<input type="text" value="http://www.google.fr"/> Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.
<b>Blocked MAC address redirect URL</b>	<input type="text"/> Blocked MAC addresses will be redirected to this URL when attempting access.
<b>Concurrent user logins</b>	<input checked="" type="checkbox"/> Disable Concurrent user logins If enabled only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.
<b>MAC filtering</b>	<input checked="" type="checkbox"/> Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

### Authentication

<b>Authentication Method</b>	<input type="button" value="Use an Authentication backend"/>	<input type="text" value="Select an Authentication Method to use for this zone. One method must be selected."/> - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.
<b>Authentication Server</b>	<input type="button" value="Local Database"/>  You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.	
<b>Secondary authentication Server</b>	<input type="button" value="Local Database"/>  You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.	
<b>Reauthenticate Users</b>	<input type="checkbox"/> Reauthenticate connected users every minute If reauthentication is enabled, requests are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; the cached credentials are necessary for the portal to perform automatic reauthentication requests.	
<b>Local Authentication Privileges</b>	<input checked="" type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set	

### HTTPS Options

<b>Login</b>	<input type="checkbox"/> Enable HTTPS login When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.
--------------	---



Puis cliquer sur save est le portail captif est mis en place.  
Il faut maintenant mettre en place les autorisations utilisateurs. Pour ce faire, il faut aller dans System > User Manager > Groups. Puis cliquer sur Add (ou ajouter en français )

Groups			
Group name	Description	Member Count	Actions
all	All Users	1	
admins	System Administrators	1	

Puis créer un groupe (vous pouvez le nom que vous souhaitez )

System / User Manager / Groups / Edit

Group name	Agent
Scope	Local
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.	
Description	Delegation Creation Utilisateurs Portail
Group description, for administrative information only	
Group membership	<input type="text" value="admin"/> <div style="display: flex; justify-content: space-between;"> <div>Not members</div> <div>Members</div> </div> <div style="display: flex; justify-content: space-around;"> <span></span> <span></span> </div> <p>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</p>
<input type="button" value="Save"/>	

Nous venons donc de créer un groupe, il faut maintenant modifier les droits. Cliquer sur le stylo puis descendez et ajoutez des privilèges

Groups			
Group name	Description	Member Count	Actions
Agent	Delegation Creation Utilisateurs Portail	0	
admins	System Administrators	1	
all	All Users	1	

Sélectionner ces deux privilèges qui vont donner des accès administrateurs au portail captif pour les utilisateur inclus dans ce groupe, puis sauvegarder :

Assigned Privileges		
Name	Description	Action
WebCfg - System: User Manager	Allow access to the 'System: User Manager' page. (admin privilege)	
WebCfg - Status: Captive Portal	Allow access to the 'Status: Captive Portal' page.	
Security notice: Users in this group effectively have administrator-level access		
Save		

Il faut maintenant créer un utilisateur administrateur (pour que quelqu'un puisse gérer les différents comptes utilisateur lié au portail captif). Pour ce faire il faut aller dans System > User Manager > User

System / User Manager / Users				
Users	Groups	Settings	Authentication Servers	
<b>Users</b>				
Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	
Add		Delete		

puis add, vous pouvez lui donner le nom que vous souhaitez.

Users	Groups	Settings	Authentication Servers	
<b>User Properties</b>				
Defined by	USER			
Disabled	<input type="checkbox"/> This user cannot login			
Username	agent			
Password	*****	*****		
Full name	Agent autorisé à créer des utilisateurs du Portail Captif	User's full name, for administrative information only		
Expiration date		Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY		
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.			
Group membership	admins		Agent	
	Not member of		Member of	
Certificate	<input type="checkbox"/> Click to create a user certificate			

Maintenant que nous avons créé un groupe administrateur et un utilisateur administrateur, il faut créer un nouveau groupe pour les utilisateurs du portail.

Donc même procédure que précédemment, il faut aller dans System > User Manager > Groups :

System / User Manager / Groups			
Users	Groups	Settings	Authentication Servers
<b>Groups</b>			
Group name	Description	Member Count	Actions
Agent	Delegation Creation Utilisateurs Portail	1	
admins	System Administrators	1	
all	All Users	2	

Puis add :

Users	Groups	Settings	Authentication Servers
<b>Group Properties</b>			
Group name	Portail		
Scope	Local	<input type="button" value="▼"/> <small>Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.</small>	
Description	Utilisateurs du Portail		
Group membership	admin agent  Not members      Members  <small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small>		

Puis save, il faut ensuite modifier les privilèges lié au groupe :

Cliquez sur add puis sélectionner le bon privilège :

Assigned Privileges			
Name	Description	Action	
User - Services: Captive Portal login	Indicates whether the user is able to login on the captive portal.		

Puis save.

Il nous reste plus qu'à créer un utilisateur test pour vérifier que tout fonctionne. Pour ce faire, même chose que précédemment. Retourner dans System > User Manager > User

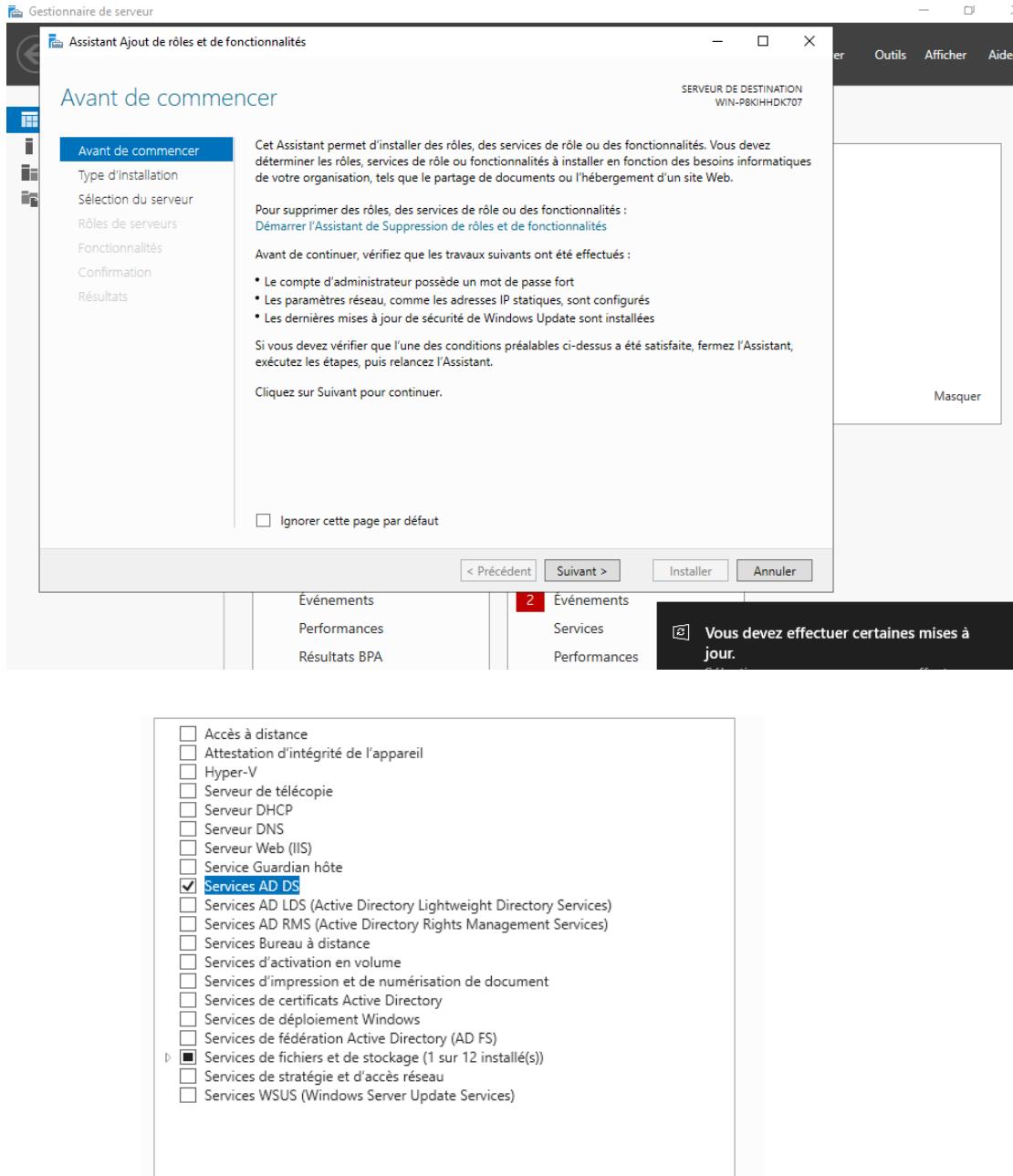
**User Properties**

Defined by	USER				
Disabled	<input type="checkbox"/> This user cannot login				
Username	test				
Password	****				
Full name	Un Utilisateur du Portail <small>User's full name, for administrative information only</small>				
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>				
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.				
Group membership	<table border="1"><tr><td>Agent</td><td>admins</td></tr><tr><td>Not member of</td><td>Portail</td></tr></table> <small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small>	Agent	admins	Not member of	Portail
Agent	admins				
Not member of	Portail				
Certificate	<input type="checkbox"/> Click to create a user certificate				

Une fois les étapes finies, notre portail Captif est mis en place !

## 8.7 Configuration d'un Active Directory

Pour mettre en place un Active Directory, je vais utiliser Windows server :  
On va cliquer sur Ajouter des rôles et des fonctionnalités



On coche le service AD DS qui installera le service Active Directory. Après cela on redémarre le windows server.

Après le redémarrage le service Active Directory est actif et nous pouvons commencer à créer des groupes, des utilisateurs, partages réseaux....

## 8.8 Déploiement automatisé avec LTSP

Déploiement automatisé avec LTSP :

Pour des choix économiques et efficaces, nous avons décidé de mettre en place un serveur LTSP, qui est un outil de déploiement d'images pxe sur des clients légers.

Pour installer LTSP :

```
wget https://ltsp.org/misc/ltsp-ubuntu-ppa-focal.list -O /etc/apt/sources.list.d/ltsp-ubuntu-ppa-focal.list
```

```
wget https://ltsp.org/misc/ltsp_ubuntu_ppa.gpg -O  
/etc/apt/trusted.gpg.d/ltsp_ubuntu_ppa.gpg
```

```
apt update
```

On télécharge ce qui est nécessaire pour installer le paquet LTSP.

```
apt install --install-recommends ltsp ltsp-binaries dnsmasq nfs-kernel-server openssh-server squashfs-tools ethtool net-tools eopentes
```

On installe tous les paquets nécessaires

```
gpasswd -a debian eopentes
```

Puis ajouter notre utilisateur Debian au groupe LTSP

```
root@debian:/etc# ltsp dnsmasq  
Installed /usr/share/ltsp/server/dnsmasq/ltsp-dnsmasq.conf in /etc/dnsmasq.d/ltsp-dnsmasq.conf  
Restarted dnsmasq
```

On lance le service dnsmasq

```
root@debian:/etc# dnsmasq -i ltsp_image
Using x86_64 as the base name of image /
Running: mount -t tmpfs -o mode=0755 tmpfs /tmp/tmp.Qiye45Yz6k/tmpfs
Running: mount -t overlay -o upperdir=/tmp/tmp.Qiye45Yz6k/tmpfs/0/up,lowerdir=/,
workdir=/tmp/tmp.Qiye45Yz6k/tmpfs/0/work /tmp/tmp.Qiye45Yz6k/tmpfs /tmp/tmp.Qiye
```

On lance l'image LTSP

On lance le service IPXE

```
root@debian:/etc# ltsp ipxe
Installed /usr/share/ltsp/server/ipxe/ltsp.ipxe in /srv/tftp/ltsp/ltsp.ipxe
Installed /usr/share/ltsp/binaries/memtest.0 in /srv/tftp/ltsp/memtest.0
Installed /usr/share/ltsp/binaries/memtest.efi in /srv/tftp/ltsp/memtest.efi
```

le service NFS

```
root@debian:/etc# ltsp nfs
Installed /usr/share/ltsp/server/nfs/ltsp-nfs.exports in /etc/exports.d/ltsp-nfs
.exports
Restarted nfs-kernel-server
```

et pour finir initrd

```
root@debian:/etc# ltsp initrd  
315 blocs  
Generated ltsp.img:  
-rw-r--r-- 1 root root 161280 28 avril 19:18 /srv/tftp/ltsp/ltsp.img
```

Le serveur LTSP est maintenant opérationnel

## 8.9 Mise en place d'un proxy : Squid

Afin de modérer les accès aux sites web dans l'infrastructure réseau, nous avons mis en place un proxy bloquant l'accès à certains sites internet. Pour cela nous allons utiliser squid, un outil permettant la mise en place d'un proxy sur le réseau.

Pour installer et configurer Squid :

```
sudo apt update
```

```
sudo apt install squid -y
```

Cela va installer le paquet squid

Ensuite dans le fichier de configuration de Squid

```
sudo nano /etc/squid/squid.conf
```

```
GNU nano 7.2                                     squid.conf
http://squid.gnu.org/ GNU/Linux system are free software;
on terms for each program are described in the
/usr/share/doc/*/*copyright.

# Réseau local autorisé
acl reseau_local src 192.168.2.0/24
http_access allow reseau_local
acl sites_bloques dstdomain "/etc/squid/blacklist.txt"
http_access deny sites_bloques
# Bloquer tout le reste
http_access deny all

T,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
:27:2650:a00:27ff:feec:461c/64 scope global dynamic enp0s3
    linklayer enp0s3 brd ff:ff:ff:ff:ff:ff
    38sec preferred_lft 86398sec
    27ff:feec:461c/64 scope link
    ever preferred_lft forever
T,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
:27:e0:d4:0b brd ff:ff:ff:ff:ff:ff
    linklayer enp0s8 brd 192.168.2.255 scope global enp0s8
```

Il faudra redémarrer le service squid

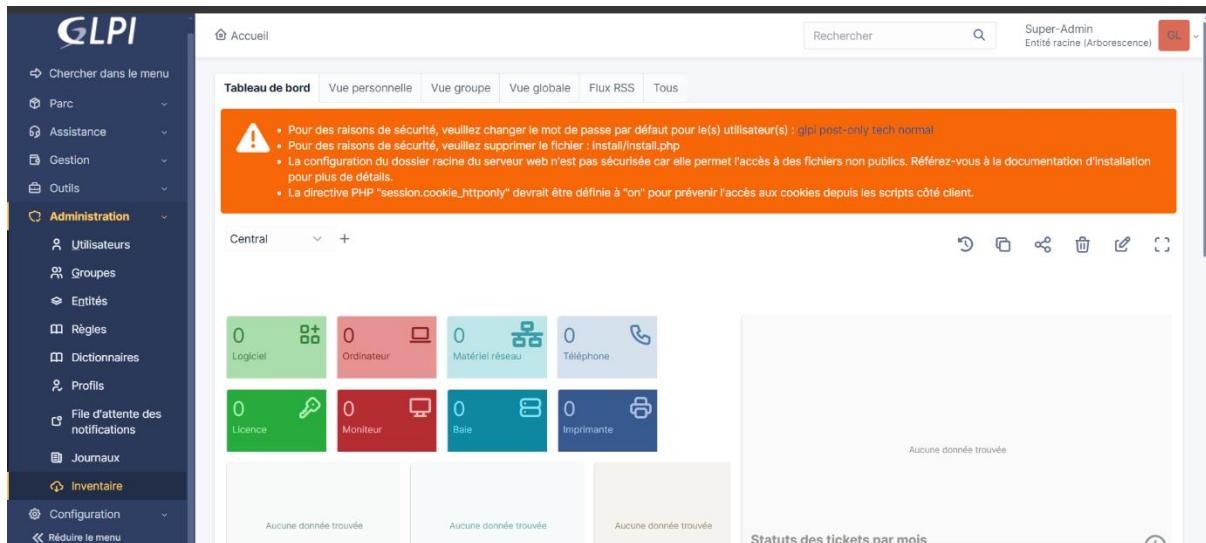
```
root@debian:/etc# systemctl restart squid
```

Cette configuration permettra le blocage de sites internet

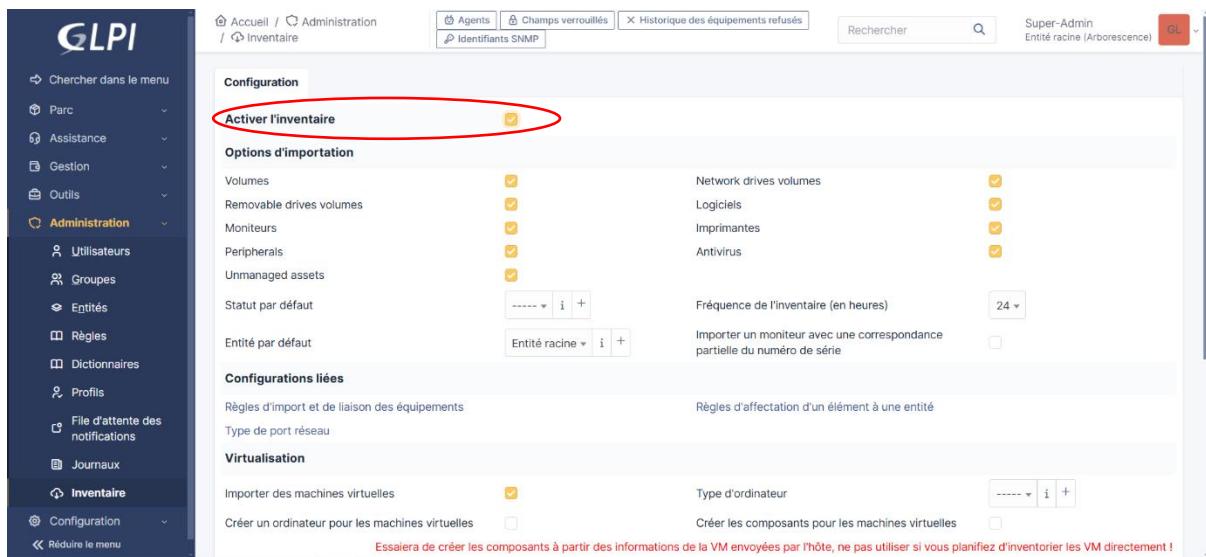
## 9. Manuel utilisateur

### 9 .1 Mise en place d'un outil de gestion de parc informatique : GLPI

Tout d'abord nous allons activer l'inventaire qui est par défaut désactivé, il faut se rendre dans Administration->inventaire



Il faudra cocher la case « Activer l'inventaire » qui est par défaut décocher.

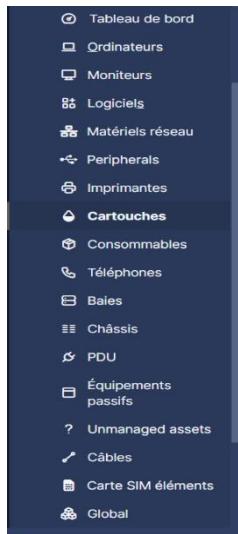


Concernant l'utilisation de glpi il y a plusieurs onglets.

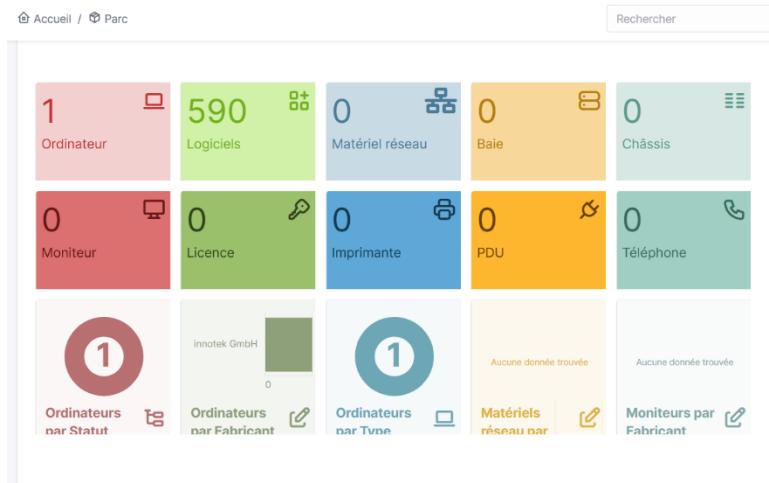
### I) L'onglet « Parc »

Cet onglet permet de gérer les équipements du parc informatique, tels que les ordinateurs, imprimantes, téléphones, etc. Il comprend un tableau de bord, une gestion des appareils, ainsi qu'une liste des logiciels installés sur ces appareils.

Les sous-onglets de cet onglet :



## Le tableau de bord :



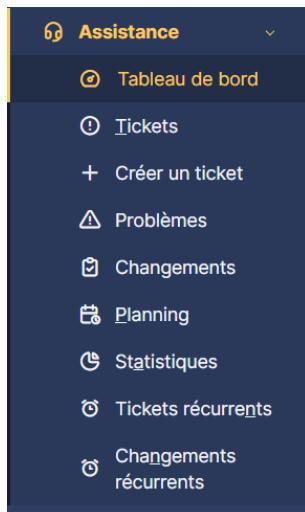
## La liste des logiciels :

Il y a aussi une partie « global » rassemblant tous les appareils.

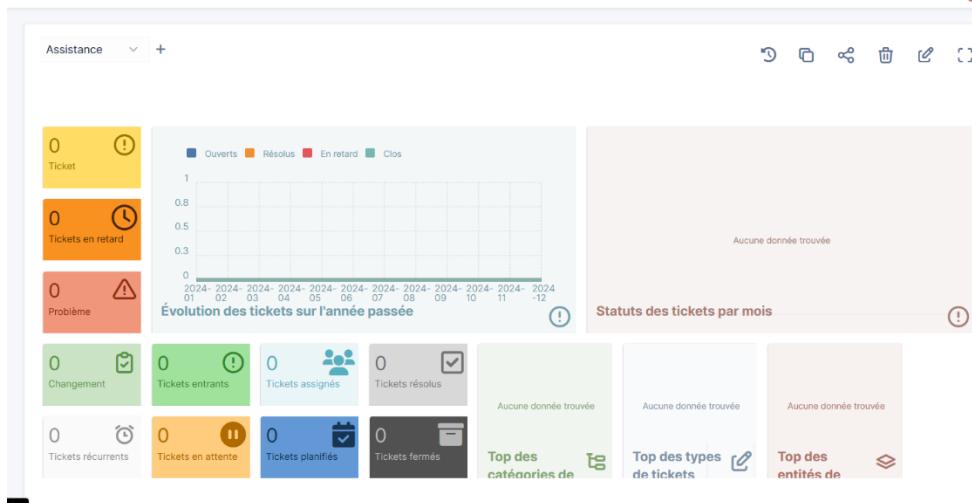
## II) L'onglet « Assistance »

Cet onglet permet de gérer les tickets d'incidents ou de demandes, créés par les utilisateurs ou les techniciens. C'est ici que vous pouvez ouvrir, suivre et clôturer les tickets.

Les options de cet onglet :



Le tableau de bord :

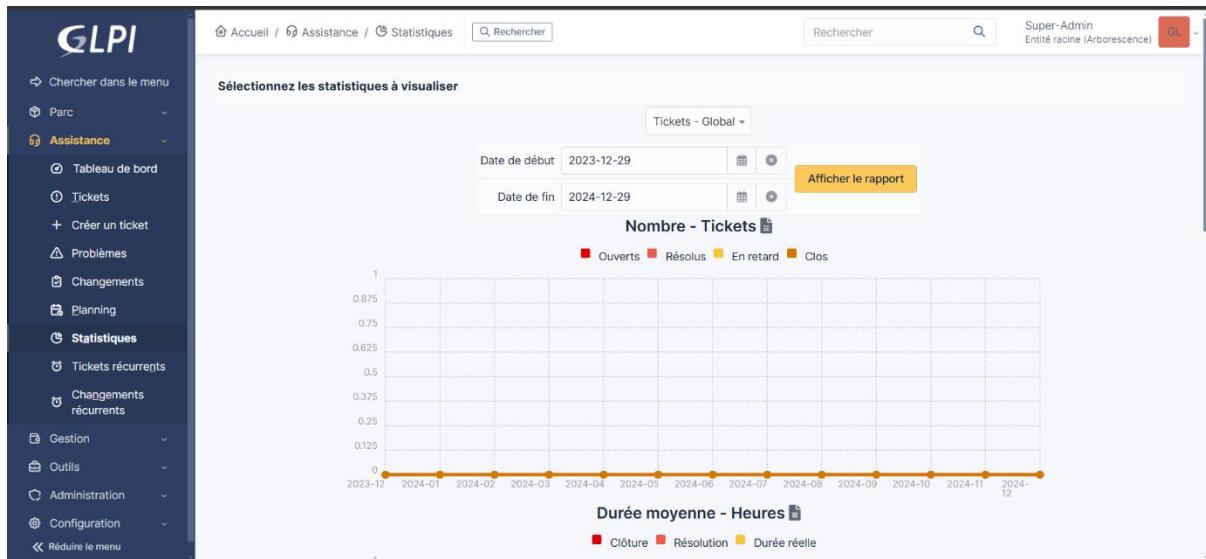


Le sous onglet « créer un ticket » :

The ticket creation form includes the following fields:

- Title:** Input field.
- Description:** Rich text editor with toolbar.
- File Upload:** Area for dragging files with placeholder text "Glissez et déposez votre fichier ici, ou Sélect. fichiers Aucun fichier choisi".
- Right-hand panel (Ticket details):**
  - Date d'ouverture: [ ]
  - Type: Incident
  - Catégorie: [ ]
  - Statut: Nouveau
  - Source de la demande: Helpdesk
  - Urgence: Moyenne
  - Impact: Moyen
  - Priorité: Moyenne
  - Durée totale: [ ]
  - Demande de: [ ]
- Buttons:** Back, Forward, and "Ajouter" (Add).

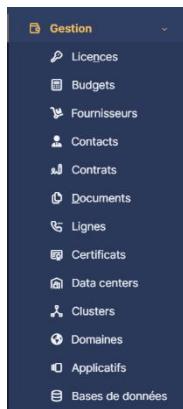
Les statistiques :



### III) L'onglet « Gestion »

L'onglet "Gestion" permet de configurer et de gérer les aspects administratifs et techniques de GLPI, y compris les licences, budgets, bases de données, et d'autres configurations essentielles pour gérer le parc informatique.

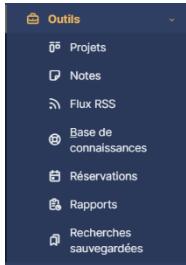
Les sous-onglets de l'onglet Gestion :



### IV) L'onglet « Outils »

L'onglet Outils permet d'accéder à diverses fonctionnalités administratives avancées. Cela comprend des outils comme les Flux RSS, les Notes, et les Rapports, qui vous aident à personnaliser et suivre plus efficacement l'activité dans GLPI.

Les sous-onglets de l'onglet Outils :



## V) L'onglet « Administration »

Nous l'avons vu précédemment afin d'activer l'inventaire. Cet onglet permet de gérer l'administration du parc informatique. Parmi les principales fonctionnalités, on retrouve notamment la gestion des utilisateurs, des profils, des entités.

Les sous-onglets de l'onglet « Administration »



Le sous-onglet Utilisateurs :

IDENTIFIANT	NOM DE FAMILLE	COURRIELS	TÉLÉPHONE	LIEU	ACTIF
glpi	Support			Oui	Oui
glpi-system	Support			Oui	Oui
normal	Support			Oui	Oui
post-only	Support			Oui	Oui
tech	Support			Oui	Oui

Le sous-onglet Profils :

Nom	ID	PROFIL PAR DÉFAUT	DERNIÈRE MODIFICATION
Admin	3	Non	
Hotliner	5	Non	
Observer	2	Non	
Read-Only	8	Non	
Self-Service	1	Oui	
Super-Admin	4	Non	
Supervisor	7	Non	
Technician	6	Non	

20 lignes / page De 1 à 8 sur 8 lignes

Le sous-onglet Entité :

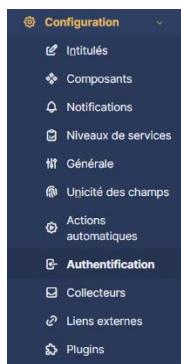
NOM COMPLET	Type
Entité racine	

20 lignes / page De 1 à 1 sur 1 lignes

## VI) L'onglet « Configuration »

Cet onglet permet de gérer la configuration de GLPI. Parmi les options disponibles, on retrouve notamment "Composants", qui contient les composants des appareils du parc, "Générale", qui contient les paramètres généraux de GLPI, "Authentification", afin de définir les authentifications externes, ainsi que "Plugins", qui permet d'ajouter des fonctionnalités supplémentaires pour étendre les capacités de GLPI.

Les sous-onglets de l'onglet Configuration :



Le sous-onglet Authentification :

The screenshot shows the 'Authentifications externes' (External Authentication) section of the GLPI configuration interface. The sidebar on the left lists several external authentication methods:

- Configuration
- Annuaire LDAP
- Serveur de messagerie
- Autres méthodes d'authentification

Le sous-onglet composant :

The screenshot shows the 'Composants' (Components) configuration page. The sidebar on the left lists various component categories:

- Alimentations
- Batteries
- Boîtiers
- Caméras
- Capteurs
- Cartes SIM
- Cartes graphiques
- Cartes mères

Le sous-onglet générale :

The screenshot shows the 'Générale' (General) configuration page. The sidebar on the left lists general configuration categories:

- Parc
- Assistance
- Gestion
- Purge de l'historique
- Système
- Sécurité
- Performance
- API
- Analyse d'impact
- GLPI Network
- Historique (15)
- Tous

The main configuration area includes:

- URL de l'application: http://192.168.1.45/gipi
- Texte sur la page de connexion (Rich Text Editor):
  - Format: Paragraph
  - Toolbar: B I A
  - Buttons: H1, H2, H3, H4, H5, H6, ...
- Lien d'aide dans l'interface simplifiée
- Lien d'aide dans l'interface standard
- Nombre de décimales par défaut: 2
- Autoriser l'accès anonyme à la FAQ:
- Traductions (Translations):
  - Traduction des intitulés:
  - Traduction de la base de connaissances:
  - Traduction des notes:

## Le sous-onglet plugin :

The screenshot shows the 'Installé' tab of a plugin management interface. The page has a header with 'Installé' and 'Découvrir' tabs, and a search bar labeled 'Filtrer la liste des plugins'. Below is a grid of installed plugins:

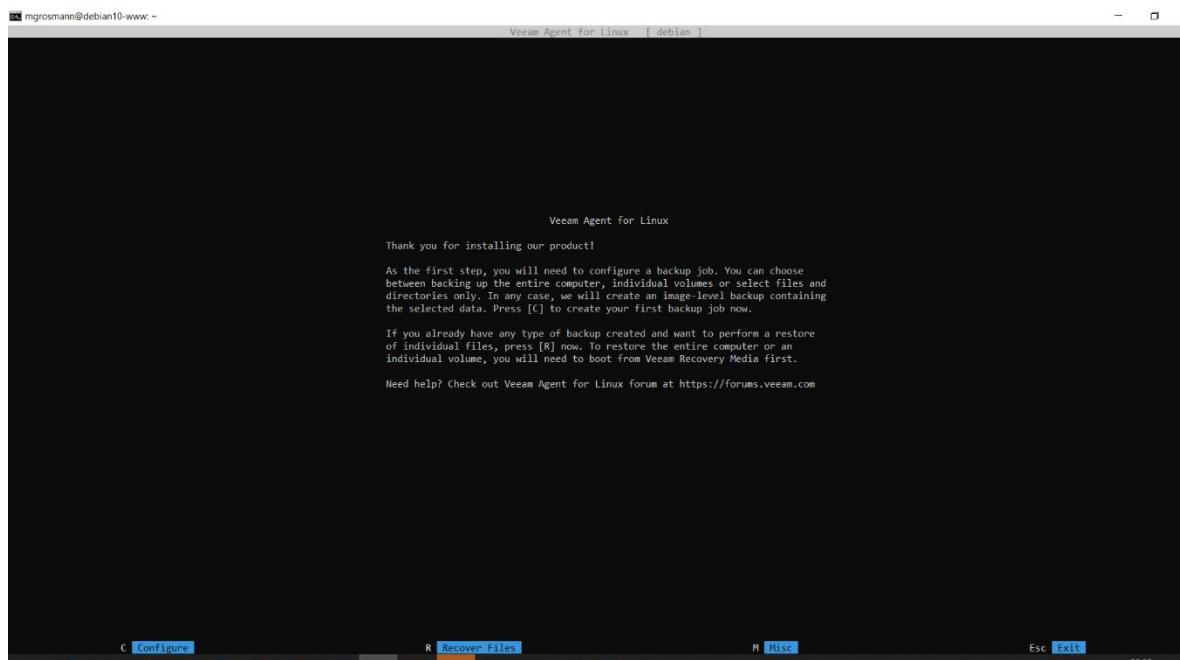
Plugin	Description	Version
Activités quotidiennes	GPL V2+ Xavier Caillaud, Infotel 3.1.5	
ActualTime	AGPL v3+ TICgal 3.0.0	
advancedplanning	GPL V3+ TECLIB' 1.1.0	
Comptes	GPL v2+ Xavier Caillaud, Infotel 3.0.4	
Dashboard applicatif	GPL V2+ Xavier Caillaud, Infotel 5.0.2	
Export des éléments utilisés	GPLV3 TECLIB' 2.5.2	
Web Resources	GPL V2+ Curtis Conard 2.0.4	

At the bottom, a message says 'Votre plugin ici ? Contactez-nous.' with an email icon.

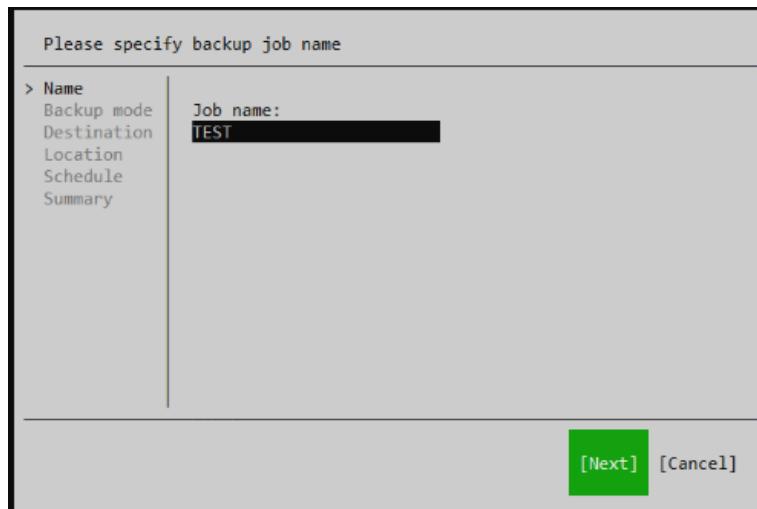
## 9.2 Mise en place d'un outil de sauvegarde : Veeam Backup

Pour lancer l'interface veeam il faut lancer la commande « veeam » et ensuite appuyer sur R pour recuper une backup déjà faite ou C pour configurer une nouvelle backup.

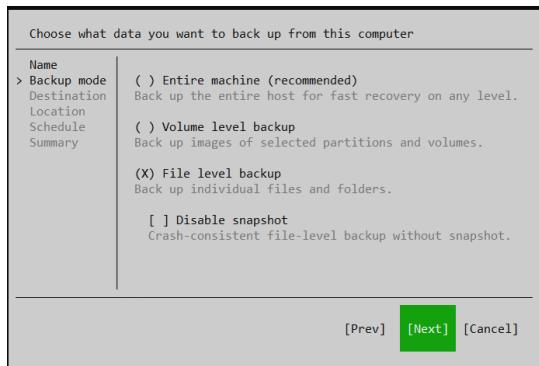
Dans cet exemple on va créer une backup du répertoire « /important »



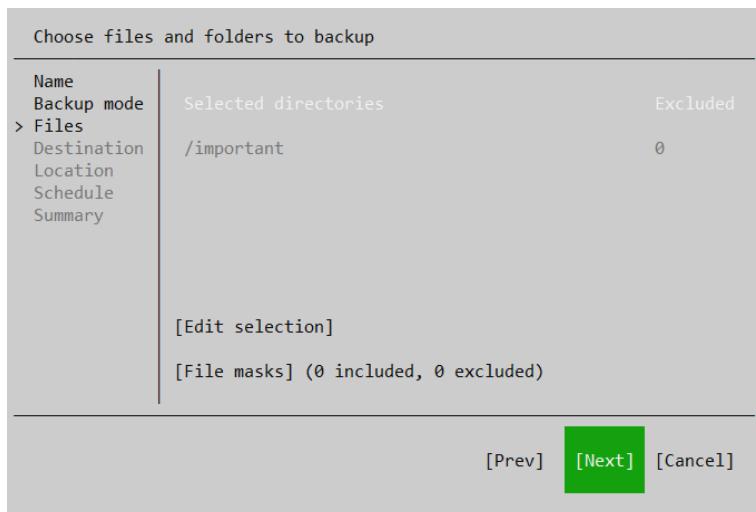
Tout d'abord il faut donner un nom à notre « job »



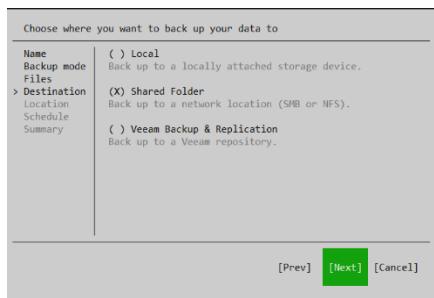
On peut sélectionner plusieurs niveau de backup comme l'entièreté de la machine ou un ou plusieurs dossiers.



On sélectionne le ou les éléments à sauvegarder



On peut sélectionner l'emplacement de destination de la backup



Dans le cas où on sauvegarde sur un serveur distant, on entre les informations correspondant au serveur

Specify a network location to backup to

Name	<input type="checkbox"/> NFS
Backup mode	<input checked="" type="checkbox"/> SMB
Files	
Destination	Server: 192.168.1.10
> Network	Folder: partage
Schedule	Domain: [REDACTED] Username: Administrateur
Summary	Password: *****

Restore points: 7 [Advanced]

[Prev] [Next] [Cancel]

On peut choisir d'exécuter le « job » automatiquement ou non

Choose when you want backup job to be started automatically

Name	<input type="checkbox"/> Run the job automatically
Backup mode	
Files	
Destination	
Network	
> Schedule	
Summary	

[Prev] [Next] [Cancel]

Après cela on peut exécuter le job juste après

Summary

Name	Job name: TEST
Backup mode	
Files	
Destination	Destination: //192.168.1.10/partage
Network	Backup: Directories: /important,
Schedule	To start the job out of schedule execute: veeamconfig job start --name "TEST"
> Summary	<input checked="" type="checkbox"/> Start job now

[Prev] [Finish] [Cancel]

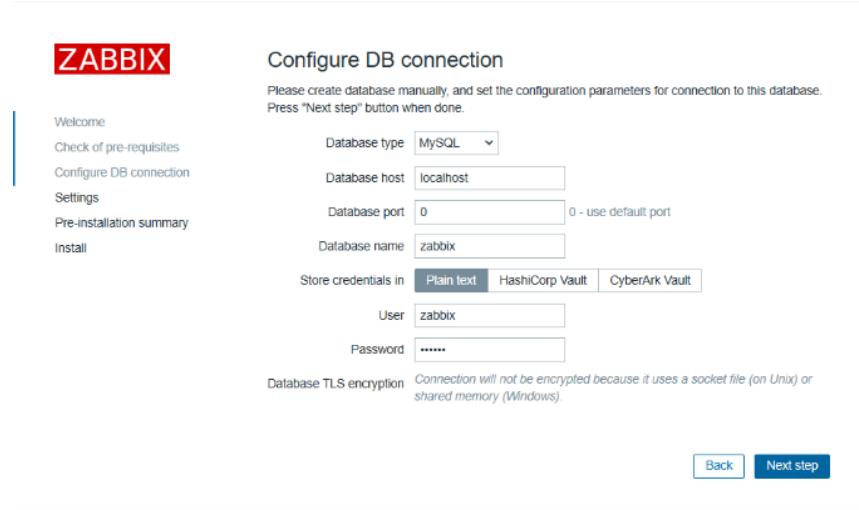
Le job commencera alors



### 9.3 Utilisation de Zabbix

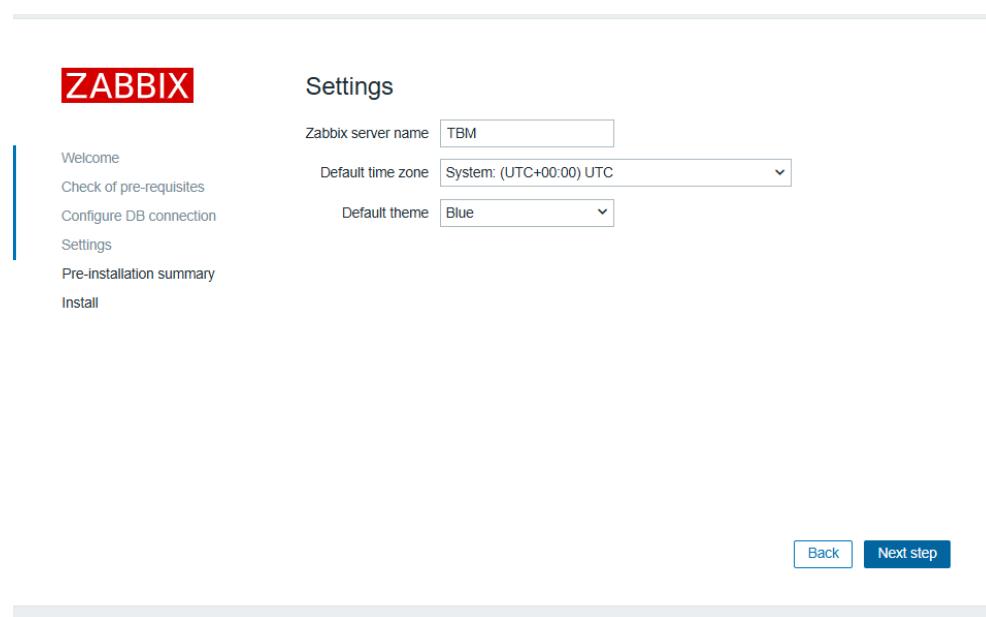
Tout d'abord on se rend sur l'interface web de zabbix

Il faudra renseigner la base de données à utiliser et aussi l'utilisateur à utiliser pour se connecter



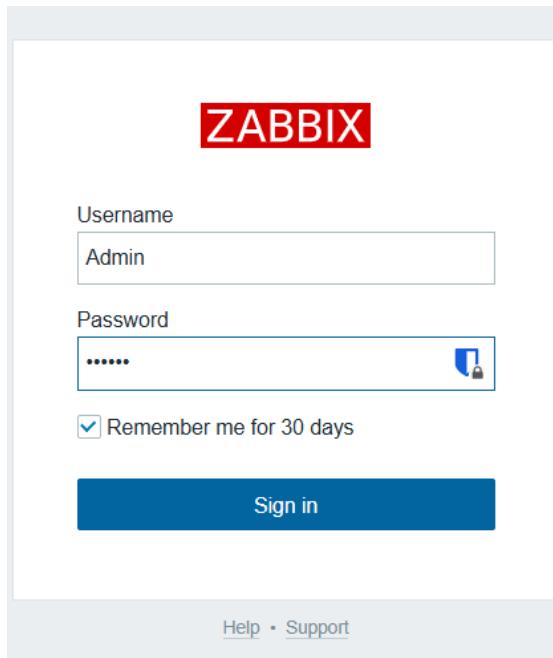
The screenshot shows the 'Configure DB connection' step of the Zabbix installation wizard. The title bar says 'ZABBIX'. The main content area is titled 'Configure DB connection' with the sub-instruction 'Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.' A sidebar on the left lists steps: Welcome, Check of pre-requisites, Configure DB connection (which is selected), Settings, Pre-installation summary, and Install. The configuration form includes fields for Database type (MySQL), Database host (localhost), Database port (0), Database name (zabbix), and options for storing credentials (Plain text, HashiCorp Vault, CyberArk Vault). Below these are fields for User (zabbix) and Password (\*\*\*\*\*). A note at the bottom states: 'Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).' At the bottom right are 'Back' and 'Next step' buttons.

Il faudra ensuite donner un nom au serveur Zabbix



The screenshot shows the 'Settings' step of the Zabbix installation wizard. The title bar says 'ZABBIX'. The main content area is titled 'Settings' with the sub-instruction 'Zabbix server name TBM'. A sidebar on the left lists steps: Welcome, Check of pre-requisites, Configure DB connection, Settings (which is selected), Pre-installation summary, and Install. The configuration form includes fields for Zabbix server name (TBM), Default time zone (System: (UTC+00:00) UTC), and Default theme (Blue). At the bottom right are 'Back' and 'Next step' buttons.

Les identifiants sont Admin zabbix

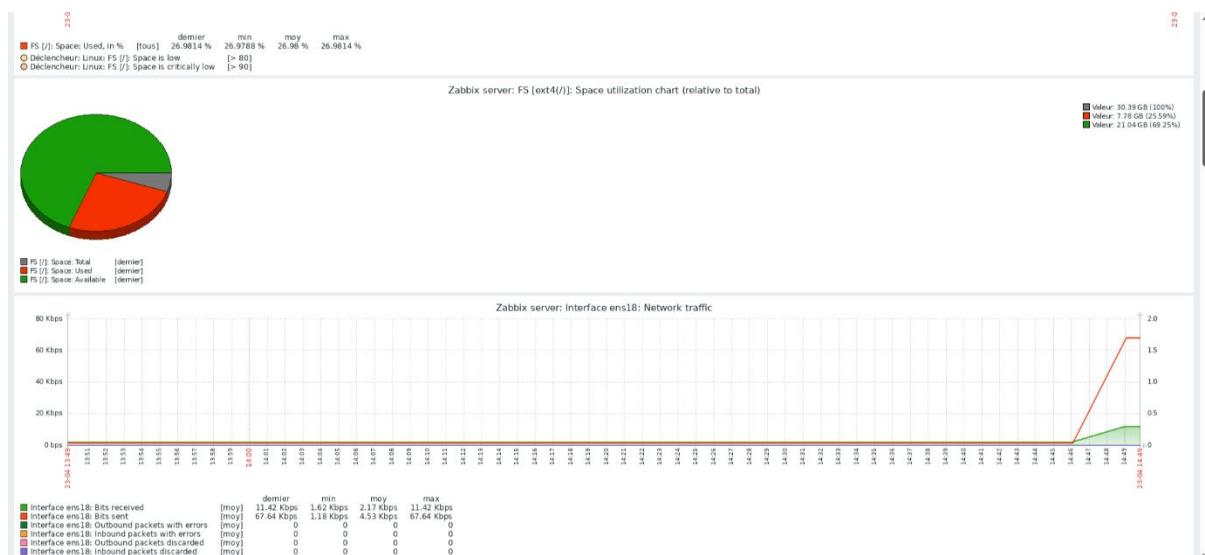


On tombe sur ça

The image shows the Zabbix Global view dashboard. On the left is a dark sidebar with navigation links like Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Users, Administration, Support, Integrations, Help, User settings, and Sign out. The main area has several sections: "Top hosts by CPU utilization" showing "Zabbix server" with 2.43% utilization; a central box with a green arrow pointing up and the value "1.53"; a "System information" table with various metrics; a "Host availability" chart with 1 Available host; a "Problems by severity" chart with 0 Disaster, 0 High, 0 Average, 0 Warning, 0 Information, and 0 Not classified problems; a "Current problems" table with no data found; and a "Geomap" section showing a map of Riga, Latvia.

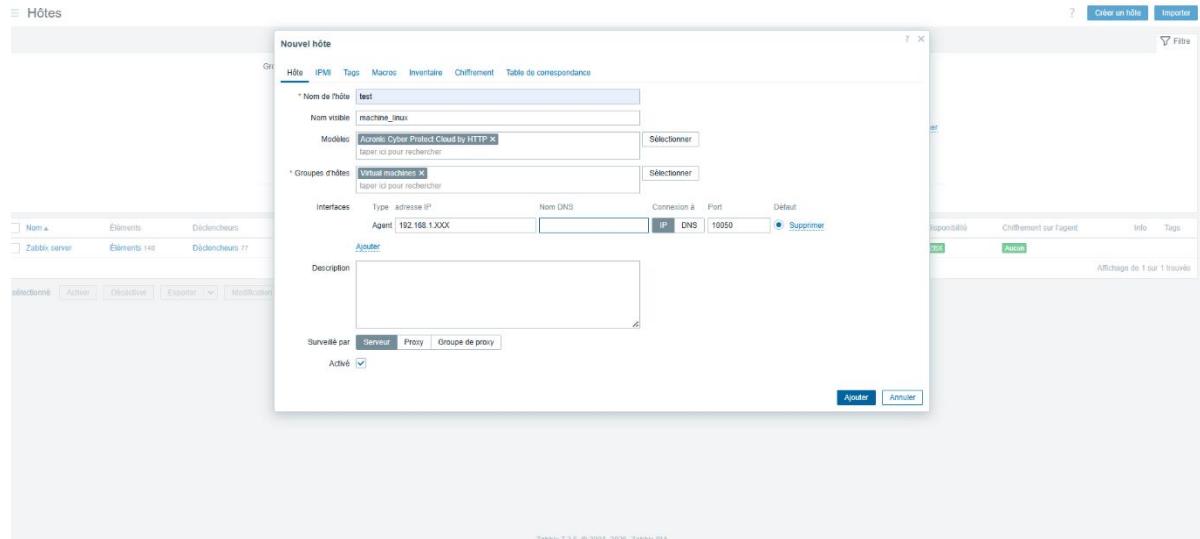
Si on se rend dans collecte de données -> Hôtes on peut accéder à la liste des machines sur le serveur zabbix

Si on clique sur « Graphiques » on a accès a des graphiques sur les données des machines ajoutés au serveur zabbix



De retour sur collecte de données -> hôtes, si on sélectionne « crée un hôte » on peut ajouter un nouvel hôte sur le serveur Zabbix.

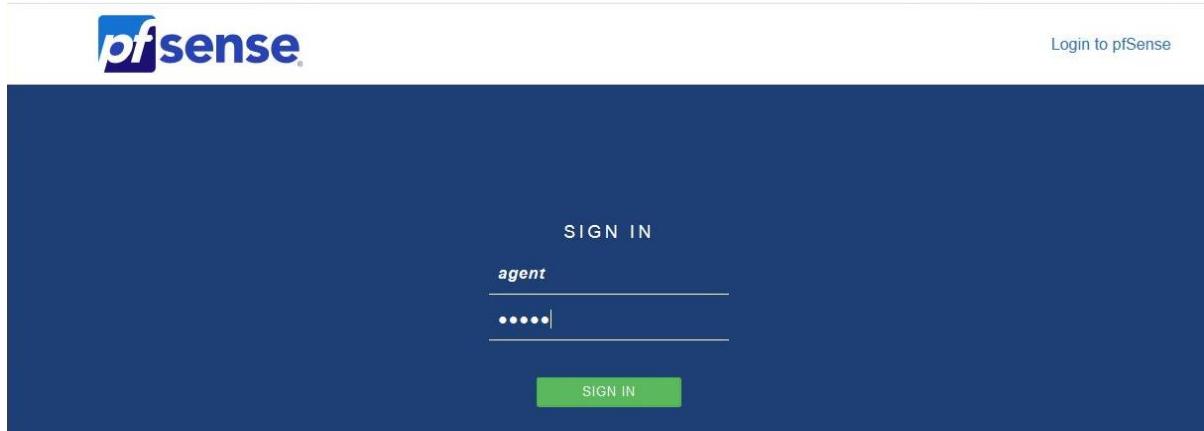
A noter qu'en modèle/template il faut mettre windows ou linux by agent Zabbix ou agent Zabbix active ou snmp en fonction de votre machine et de la façon donc les données sont récoltées. A noter que pour FreeBSD seul agent Zabbix est pris en compte



## 9.4 Utilisation du portail captif

Administrateur portail captif :

Pour gérer les utilisateurs du portail captif il faut mettre l'ip du portail captif dans un navigateur web, puis vous devez vous authentifier avec le compte administrateur que vous avez créé précédemment :



Puis vous avez accès à cette page :

A screenshot of the pfSense User Manager interface. The top navigation bar includes the pfSense logo, 'COMMUNITY EDITION', and links for 'System', 'Status', and 'Help'. Below the navigation is a breadcrumb trail: 'System / User Manager / Users'. A sub-navigation bar shows 'Users' is selected. The main content area displays a table titled 'Users'. The table has columns: 'Username', 'Full name', 'Status', 'Groups', and 'Actions'. Three users are listed: 'admin' (System Administrator), 'agent' (Agent autorisé à créer des utilisateurs du Portail Captif), and 'test' (Un Utilisateur du Portail). Each user row includes edit and delete icons in the 'Actions' column. At the bottom right of the table are 'Add' and 'Delete' buttons.

Depuis cette page vous pouvez créer et supprimer les utilisateurs lié au portail captif :

**Users**

<b>User Properties</b>	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	bubu
Password	****
Full name	2eme Utilisateur du Portail User's full name, for administrative information only
Expiration date	
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY	
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	<div style="display: flex; align-items: center;"> <div style="flex: 1;"> <p>Agent admins</p> </div> <div style="flex: 1; border: 1px solid #ccc; padding: 2px; margin-left: 10px;"> <p>Portal</p> </div> </div>
Not member of	
<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p></p> <p>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</p> </div> <div style="text-align: center;"> <p></p> </div> </div>	
Certificate	<input type="checkbox"/> Click to create a user certificate

Utilisateur portail captif :

Quand vous êtes un utilisateur vous devez juste ouvrir un navigateur web puis vous allez être redirigée automatiquement sur cette page :



Il vous suffira de mettre votre identifiant et mot de passe puis le tour est joué vous avez accès à internet !

## 9.5 Déploiement automatisé avec Docker

Comme dit dans le titre le service est automatique, pour vérifier s'il est toujours actif ou pour ajouter un conteneur de plus à automatiser, cette commande est nécessaire :

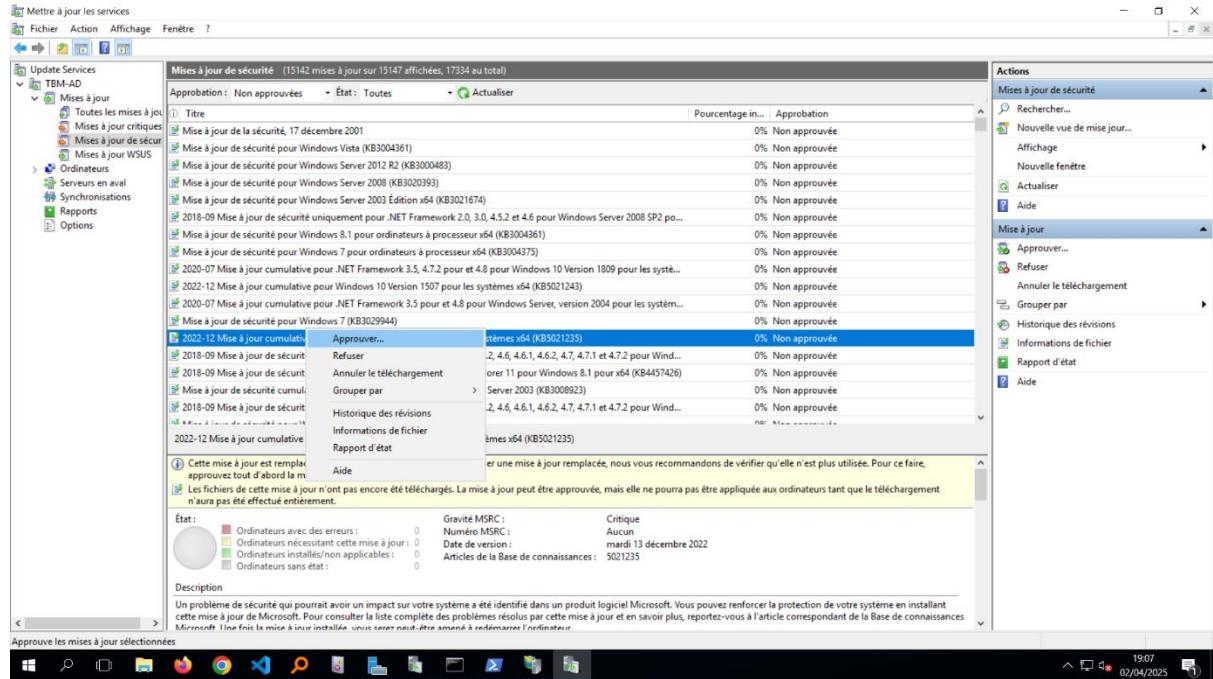
```
sudo docker run -d \ --name watchtower \ -v  
/var/run/docker.sock:/var/run/docker.sock \ containrrr/watchtower  
glpi prometheus mariadb      /pourajouterconteneur
```

Pour vérifier s'il est toujours actif :

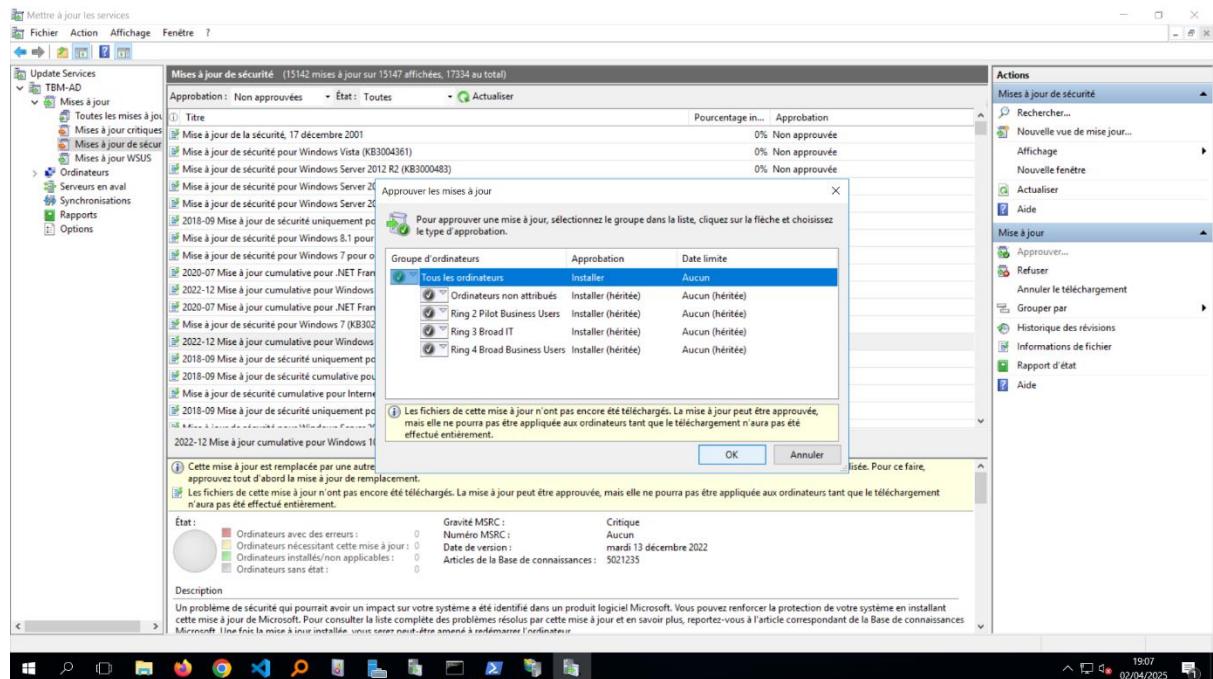
```
time="2024-12-28T14:49:42Z" level=info msg="Waiting for the notification goroutine to finish" notify=no  
ubuntu@ubuntu:~/auto$ sudo docker logs watchtower  
time="2024-12-28T14:33:12Z" level=info msg="Watchtower 1.7.1"  
time="2024-12-28T14:33:12Z" level=info msg="Using no notifications"  
time="2024-12-28T14:33:12Z" level=info msg="Only checking containers which name matches \"glpi\" or \"prometheus\" or \"mariadb\""  
time="2024-12-28T14:33:12Z" level=info msg="Scheduling first run: 2024-12-29 14:33:12 +0000 UTC"  
time="2024-12-28T14:33:12Z" level=info msg="Note that the first check will be performed in 23 hours, 59 minutes, 59 seconds"
```

## 9.6 Ajoute de mises à jour approuvés avec WSUS

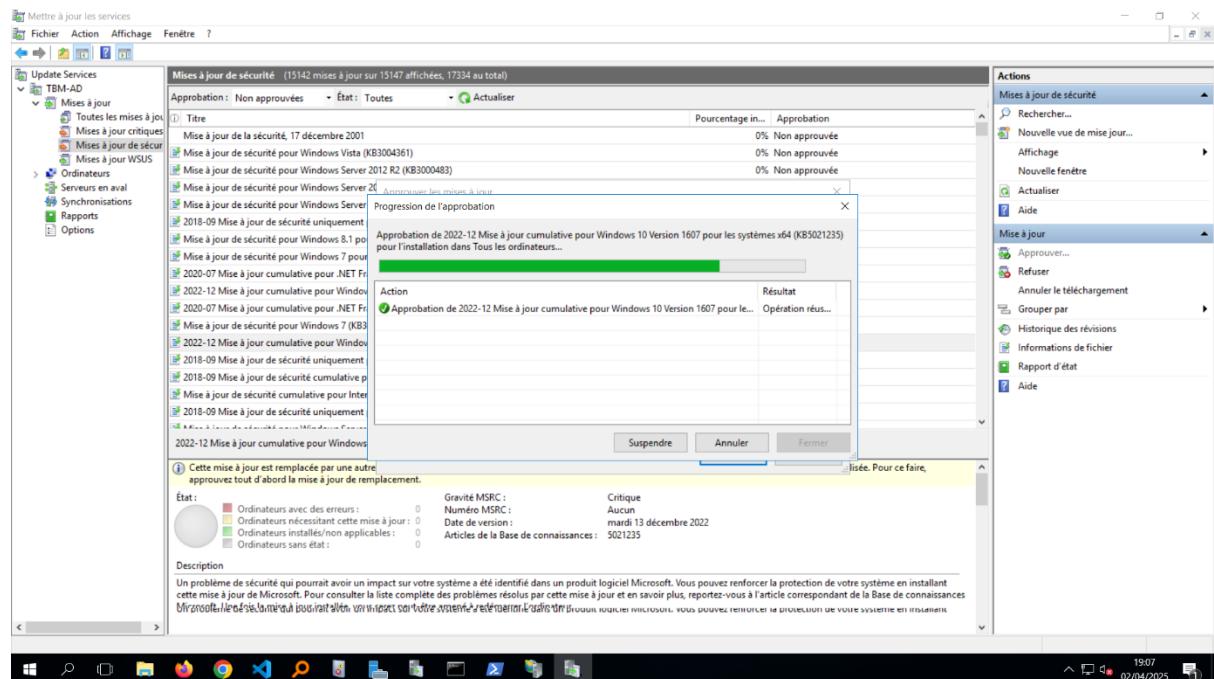
Pour approuver des mises à jour sur wsus il suffit de faire un clic droit puis « approuver »



On peut ensuite choisir sur quel ordinateur on affecte ce changement



Une fois fait un chargement se lancera.



Vous savez maintenant comment manier wsus.

## 9.7 Utilisation du proxy squid

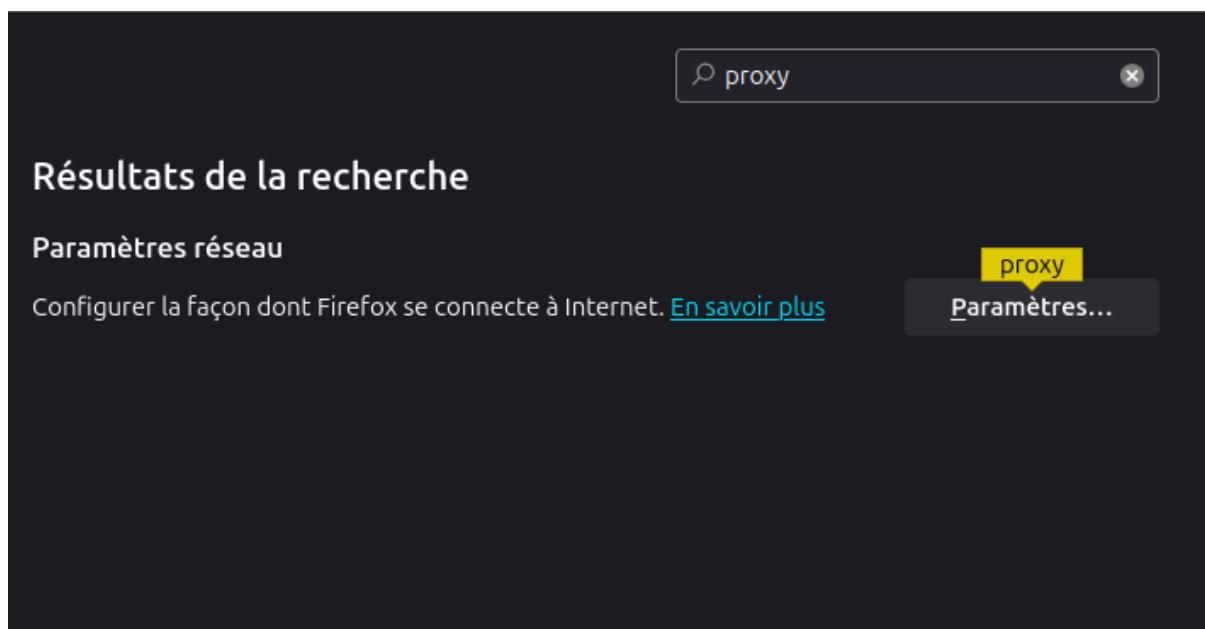
Pour modifier les sites indésirables dans le réseau il faudra modifier le fichier correspondant :

```
GNU nano 7.2                         blacklist.txt
twitter.com
facebook.com

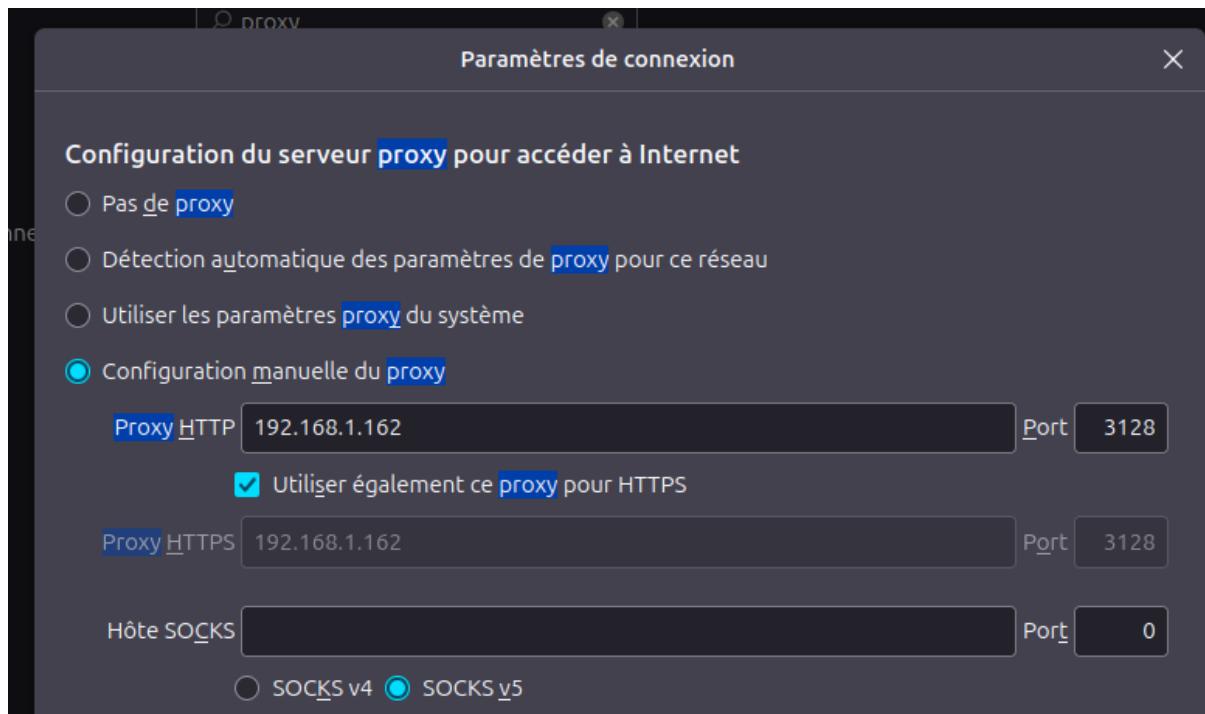
es with ABSOLUTELY NO WARRANTY, to the extent
ole law.
21 00:54:14 CEST 2025 from 192.168.1.4 on pts/0
a
LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
:00:00:00:00:00 brd 00:00:00:00:00:00
: scope host lo
ever preferred_lft forever
ope host noprefixroute
ever preferred_lft forever
T,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
:27:ec:46:1c brd ff:ff:ff:ff:ff:ff
52/24 brd 192.168.1.255 scope global dynamic enp0s3
98sec preferred_lft 43198sec
47:2650:a00:27ff:feec:461c/64 scope global dynamic mngrtmpaddr
98sec preferred_lft 66398sec
27ff:feec:461c/64 scope link
ever preferred_lft forever
T,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
:27:e0:d4:0b brd ff:ff:ff:ff:ff:ff
724 brd 192.168.2.255 scope global enp0s8
```

C'est grâce à ce fichier que le proxy sait quel site doit être bloqué.

Pour rentrer le proxy dans le navigateur :



Ensuite rentrer l'adresse et le proxy s'appliquera :



## 9.8 Utilisation de LSTP

Pour régénérer une image LTSP, il suffit seulement de lancer la commande

```
ltstp image /
```

Si une modification est faite, comme l'installation d'un logiciel, la création d'une nouvelle image mettra donc à jour le serveur.

## 10. Références bibliographiques (liste des sources documentaires)

GLPI	<p>Le script pour glpi est basé sur le site suivant :  <a href="https://faq.teclib.com/03_knowledgebase/procedures/install_glpi">https://faq.teclib.com/03_knowledgebase/procedures/install_glpi</a></p> <p>Le script pour agent-glpi est basé sur le site suivant : <a href="https://colinfo.fr/configuration-et-installation-de-lagent-glpi-sous-windows-et-linux/">https://colinfo.fr/configuration-et-installation-de-lagent-glpi-sous-windows-et-linux/</a></p>
Veeam	<p>Script basé sur le site suivant :</p> <p><a href="https://helpcenter.veeam.com/docs/agentforlinux/userguide/installation_process.html?ver=60">https://helpcenter.veeam.com/docs/agentforlinux/userguide/installation_process.html?ver=60</a></p>
Zabbix	<p>Script basé sur le site suivant :</p> <p><a href="https://www.zabbix.com/fr/download?zabbix=7.2&amp;os_distribution=alma_linux&amp;os_version=9&amp;components=server_frontend_agent&amp;db=mysql&amp;ws=apache">https://www.zabbix.com/fr/download?zabbix=7.2&amp;os_distribution=alma_linux&amp;os_version=9&amp;components=server_frontend_agent&amp;db=mysql&amp;ws=apache</a></p>
Gestion centralisée des mises à jour	<p>Pour les actions à entreprendre pour configurer wsus</p> <p><a href="https://learn.microsoft.com/fr-fr/windows/deployment/update/waas-manage-updates-wsus">https://learn.microsoft.com/fr-fr/windows/deployment/update/waas-manage-updates-wsus</a></p>
Portail captif	<p><a href="https://www.pc2s.fr/pfsense-portail-captif-avec-authentification-utilisateur/">https://www.pc2s.fr/pfsense-portail-captif-avec-authentification-utilisateur/</a></p>
Configutation pfsense	<p><a href="https://prouya.net/?d=2014/08/24/12/09/58-pfsense-configurer-son-serveur-dhcp">https://prouya.net/?d=2014/08/24/12/09/58-pfsense-configurer-son-serveur-dhcp</a></p> <p><a href="https://www.arsouyes.org/blog/2019/23_DNS_Personnel/">https://www.arsouyes.org/blog/2019/23_DNS_Personnel/</a></p>
Configuration d'un Active Directory	<p><a href="https://www.it-connect.fr/creer-un-domaine-ad-avec-windows-server-2016/">https://www.it-connect.fr/creer-un-domaine-ad-avec-windows-server-2016/</a></p>
Déploiement automatisé avec LSTP	<p><a href="https://ltsp.org/docs/installation/">https://ltsp.org/docs/installation/</a></p>
Mise en place d'un serveur proxy avec squid	<p><a href="https://fr.linux-console.net/?p=21028">https://fr.linux-console.net/?p=21028</a></p>

## 11. Conclusion sur le travail réalisé ou restant à faire

Nous pouvons conclure que les services mis en place représentent une avancée significative pour l'infrastructure de la société GSB, notamment d'un point de vue cyber-sécurité. Ces services sont essentiels pour toute entreprise, quelle que soit sa taille, ses objectifs ou sa capacité financière.

Parmi ces services, nous avons la mise en place de routeurs et de pare-feux logiciels pour renforcer la sécurité du réseau avec le logiciel PfSense. Un portail captif a également été installé pour authentifier les utilisateurs avant d'accéder au réseau internet. PfSense permet également d'assurer les services DNS et DHCP, automatisant ainsi l'attribution des adresses IP et la résolution des noms de domaine, simplifiant la gestion du réseau.

Un contrôleur de domaine avec Windows Server 2016 a également été configuré pour centraliser la gestion des utilisateurs et des ressources de l'entreprise. La gestion centralisée des mises à jour Windows grâce au service WSUS (Windows Server Update Service) permet de maintenir tous les systèmes à jour et sécurisés, tout en filtrant les mises à jour selon les préférences.

Nous avons également mis en place un outil de gestion de parc et de tickets pour suivre les incidents et les demandes avec GLPI, ainsi qu'un outil de supervision pour surveiller les performances et la disponibilité des systèmes grâce à la solution Zabbix pour une meilleure visualisation des données et statistiques. Le déploiement automatisé avec l'outil Docker facilite l'installation et la configuration des nouveaux systèmes, tandis qu'une solution de sauvegarde et de restauration avec Veeam Backup assure la protection et la récupération des données importantes de l'entreprise.

Dans le contexte actuel, où les cyber-attaques, notamment les ransomwares, sont de plus en plus fréquentes, il est crucial de sauvegarder les ressources de l'entreprise. Les solutions de sauvegarde et de restauration mises en place offrent un stockage sécurisé des ressources et garantissent une récupération rapide en cas de sinistre.

Ainsi, en modernisant leur infrastructure, GSB pourra améliorer son efficacité opérationnelle, la qualité de ses services, et renforcer sa productivité tout en assurant une cybersécurité robuste pour protéger les données et les ressources de l'entreprise.