1. Présentation du contexte (GSB) : 2
2. Liste des besoins (sujet) : 3
3. Cahier des charges incluant une estimation financière des investissements 4
3.1 Introduction et Contexte du projet 4
3.2 Objectif du projet 4
3.3 informations sur les services 4
3.4 Estimation financière 6
4. Schémas des processus de l'entreprise modifiés par le projet 7
5. Diagramme de Gantt 8
5.1 Durée prévisionnelle du projet 8
5.2 Durée effective du projet 8
5.3 Diagramme des ressources montrant la répartition des taches 9
6. Description de la réalisation étape par étape 10
6.1 Mise en place d'un outil de gestion de parc informatique : GLPI 10
6.2 Mise en place d'un outil de sauvegarde : Rsync 12
6.3 Mise en place d'un outil de supervision : Prometheus et Grafana 13
6.4 Configuration des mises à jour automatisés avec windows server 15
6.5 Configuration Pfsense 19
6.6 Configuration Portail captif 20
6.7 Configuration d'un Active Directory 22
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 : Rsync 27
7.3 Ajout d'une machine à la solution de superviseur: Prometheus et Grafana 29
7.4 Automatisation de deux containers :Docker 31
8. Manuel technique 33
8 .1 Mise en place d'un outil de gestion de parc informatique : GLPI 33
8.2 Mise en place d'un outil de sauvegarde : Rsync 37
8.3 Mise en place d'un outil de supervision : Prometheus et grafana 38
8.4 Configuration des mises à jour automatisés avec windows server 43
8.5 Configuration Pfsense 66

8.6 Configuration Portail captif 68
8.7 Configuration d'un Active Directory 74
8.8 Déploiement automatisé avec Docker 75
9. Manuel utilisateur 77
9 .1 Mise en place d'un outil de gestion de parc informatique : GLPI 77
9.2 Mise en place d'un outil de sauvegarde : Rsync 86
9.3 Utilisation de Prometheus et Grafana 88
9.4 Utilisation du portail captif 93
9.5 Déploiement automatisé avec Docker 94
10. Références bibliographiques (liste des sources documentaires) 96
11. Conclusion sur le travail réalisé ou restant à faire 97

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 utilisateur 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 couché supérieur 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'automatiquer 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	Prometheus/Grafana	Service permettant de surveiller les appareils du par cet 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	Rsync	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 a 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, Prometheus/Grafana)	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 taches

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.
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.
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 : Rsync

ETAPE 1 : Installation de Rsync

1. **Mettre à jour la liste des paquets**
    - Utiliser la commande apt-get update.
2. **Installer Rsync**
    - Utiliser la commande apt-get install -y rsync.

ETAPE 2 : Préparation des Répertoires

1. **Créer les répertoires nécessaires**
    - Utiliser la commande mkdir pour créer les dossiers pour contenir les données à sauvegarder, à restaurer et pour stocker sur la machine distante :

ETAPE 3 : Téléchargement et Configuration des Scripts

1. **Télécharger les scripts** save.sh **et** backup.sh
    - Utiliser les commandes wget pour télécharger les scripts pour automatiser les sauvegardes et restaurations avec rsync.

6.3 Mise en place d’un outil de supervision : Prometheus et Grafana

Étape 1 : Installation et Configuration de Prometheus

1. Téléchargement et extraction de Prometheus

- Télécharger Prometheus depuis le dépôt officiel et extraire les fichiers téléchargés.
- Déplacer les fichiers extraits dans un répertoire standard du système pour une organisation optimale.

2. Création de l’environnement pour Prometheus

- Créer un utilisateur dédié pour Prometheus sans accès shell, pour des raisons de sécurité.
- Créer un répertoire destiné au stockage des données de Prometheus.
- Configurer les permissions sur le répertoire de stockage et les fichiers pour qu’ils appartiennent à l’utilisateur Prometheus.

3. Configuration du service Prometheus avec SystemD

- Créer un fichier de configuration SystemD pour que Prometheus puisse fonctionner comme un service système.
- Configurer le service pour qu’il démarre automatiquement au lancement de la machine et qu’il redémarre en cas d’échec.
- Démarrer le service Prometheus et s'assurer de son bon fonctionnement.

Étape 2 : Installation et Configuration de Grafana

1. Préparation de l’environnement

- Mettre à jour les paquets du système et installer les dépendances nécessaires.
- Ajouter la clé GPG et le dépôt officiel de Grafana pour garantir des mises à jour fiables et sécurisées.

2. Installation et configuration de Grafana

- Installer Grafana depuis le dépôt ajouté.
- Activer Grafana pour qu’il démarre automatiquement au démarrage du système.
- Démarrer le service Grafana et vérifier qu’il fonctionne correctement.

Étape 3 : Installation et Configuration de Node Exporter

1. Téléchargement et installation de Node Exporter

- Télécharger la version la plus récente de Node Exporter à partir de son dépôt officiel.
- Extraire les fichiers téléchargés et déplacer l'exécutable vers un répertoire standard du système.
- Configurer les permissions pour que l'exécutable appartienne à l'utilisateur Prometheus.

2. Configuration du service Node Exporter avec SystemD

- Créer un fichier de configuration SystemD pour que Node Exporter fonctionne comme un service système.
- Configurer le service pour qu'il démarre automatiquement au lancement du système.
- Démarrer le service Node Exporter et vérifier son fonctionnement.

Étape 4 : Configuration de Prometheus pour surveiller Node Exporter

1. Modification du fichier de configuration Prometheus

- Ajouter une section de configuration dans le fichier prometheus.yml pour permettre à Prometheus de collecter des métriques depuis Node Exporter.
- Redémarrer le service Prometheus pour appliquer les modifications et s'assurer que les cibles sont correctement surveillées.

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 Créer 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 créer 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, puis sélectionnez OK.

- Si cela n’est pas déjà fait rajouter une règle de pare feu entrant autorisant le port 8530

5. Créer 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 Créer 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.
- Créer 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.
- **(La règle ne peut pas être validée tant que la synchronisation n’a pas été terminé)**

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.

  (Ça ne marche pas tant que la synchronisation n'a pas été terminé)

- 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

1. Mettre en place pfsense dans l'infrastructure (j'ai donc installé un iso de pfsense vu qu'on travaille avec des VM)

2. Ensuite installation de pfsense puis configuration de l'interface WAN et LAN.

3. Une fois installer aller sur une machine windows du même réseau et taper l'ip du pfsense (ici 192.168.1.1) puis configurer les différentes règles NAT, pare-feu et les différent services disponnible et necessaire .

4. Mise en place du serveur DHCP et DNS.

5. Les règles mise en place sont : autorisation de ping dans le pare-feu. En règle NAT : connexion RDP au windows server et ssh pour la machine linux ubuntu.

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

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 »

Avant d'éxecuter 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 :

Si on se rend sur le site de la machine debian (192.168.1.45) au port 62354(le port utilisé par agent glpi nous tombons sur ça :

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 : Rsync

Pour ce jeu de test comme pour glpi nous utiliserons deux machines linux.

-1 ubuntu server 192.168.1.52 qui est la machine qui va sauvegarder, supprimer puis restaurer ces données

-1 debian 192.168.1.45 qui est le serveur rsync

Tout d'abord on va donner les droits pour l'accès aux dossiers desktop/backup/save que ce soit pour la debian comme pour ubuntu.

```
root@debian:/home# chmod -R 777  /home/mgrosmann/
root@debian:/home#
```

Tout d'abord nous allons nous rendre dans le répertoire « /home/mgrosmann/desktop » qui nous sert de « $SOURCE_DIR » et éditer un fichier « rsync.txt »

```
root@ubuntu:~# cd /home/mgrosmann/desktop
root@ubuntu:/home/mgrosmann/desktop# echo "coucou j'effectue un test pour rsync" > rsync.txt
```

Nous allons nous rendre dans le répertoire ou est contenu le script « save.sh » (ici /root)

Et l'exécuter.

```
root@ubuntu:/home/mgrosmann/desktop# cd /root
root@ubuntu:~# bash save.sh
```

Voici le résultat afficher :

```
root@ubuntu:~# bash save.sh
The authenticity of host '192.168.1.45 (192.168.1.45)' can't be established.
ED25519 key fingerprint is SHA256:VGJD0jhXMHq+9QMp7JZNOW0FckSoZwojjIFT8x5Zh0U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.45' (ED25519) to the list of known hosts.
mgrosmann@192.168.1.45's password:
sending incremental file list
desktop/
rsync: [generator] recv_generator: mkdir "/home/mgrosmann/save/desktop" failed: Permission denied (13)
*** Skipping any contents from this failed directory ***

sent 98 bytes  received 20 bytes  12,42 bytes/sec
total size is 37  speedup is 0,31
rsync error: some files/attrs were not transferred (see previous errors) (code 23) at main.c(1338) [sender=3.2.7]
root@ubuntu:~#
```

Tout porte à croire que la sauvegarde à réussi, mais pour vérifier nous allons vérifier l'existence du fichier sur la machine debian.

Nous pouvons constater que le fichier a été parfaitement transféré à la machine debian.

```
root@debian:~# ls /home/mgrosmann/save
desktop
root@debian:~# ls /home/mgrosmann/save/desktop/
rsync.txt
root@debian:~# cat /home/mgrosmann/save/desktop/rsync.txt
coucou je fais un test
root@debian:~# _
```

Pour la suite du test nous allons donc supprimer le fichier « rsync.txt » sur la machine ubuntu :

```
root@ubuntu:~# cd /home/mgrosmann/desktop/
root@ubuntu:/home/mgrosmann/desktop# rm rsync.txt
root@ubuntu:/home/mgrosmann/desktop# _
```

Puis nous allons exécuter backup.sh :

```
root@ubuntu:/home/mgrosmann/desktop# cd /root
root@ubuntu:~# bash backup.sh
```

Le résultat affiché est le suivant :

```
root@ubuntu:~# bash backup.sh
mgrosmann@192.168.1.45's password:
receiving incremental file list
save/
save/desktop/
save/desktop/rsync.txt

sent 55 bytes  received 227 bytes  62,67 bytes/sec
total size is 23  speedup is 0,08
```

Ça a l'air d'avoir marché, mais une vérification ne fait pas de mal.

On constate que la restauration a été effectué avec succès.

```
root@ubuntu:~# ls /home/mgrosmann/backup/
save
root@ubuntu:~# ls /home/mgrosmann/backup/save
desktop
root@ubuntu:~# cat /home/mgrosmann/backup/save/desktop/rsync.txt
coucou je fais un test
root@ubuntu:~#
```

La sauvegarde et restauration avec rsync est un franc succès.

7.3 Ajout d'une machine à la solution de superviseur: Prometheus et Grafana

Pour ce jeu de test on va ajouter une machine debian(192.168.1.57) sur prometheus, on devrait pouvoir avoir accès a des statistiques sur cette machine depuis grafana.

Tout d'abord nous allons utiliser le script que nous avons utilisé pour configurer la supervision bien que nous allons le réduire en laissant que la partie qui installe le service « node_exporter » permettant la collecte des données.On laissera également la ligne permettant la création de l'utilisateur « prometheus » qui devra avoir accès au dossier « node_exporter »

```
#!/bin/bash
useradd --no-create-home --shell /bin/false prometheus
curl -s https://api.github.com/repos/prometheus/node_exporter/releases/latest | grep browser_download_url | grep linux-amd64 | cut -d '"' -f 4 | wget -qi -
tar -xvf node_exporter*.tar.gz
cd node_exporter*/
cp node_exporter /usr/local/bin
chown prometheus:prometheus /usr/local/bin/node_exporter
cat <<EOF > /etc/systemd/system/node_exporter.service
[Unit]
Description=Node Exporter
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
ExecStart=/usr/local/bin/node_exporter

[Install]
WantedBy=multi-user.target
EOF
systemctl daemon-reload
systemctl enable node_exporter
systemctl start node_exporter
```

Une fois ce script exécute l'utilisateur « prometheus » est créer et le service « node_exporter » est opérationnel sur la machine debian. Nous allons nous rendre sur le serveur prometheus (192.168.1.45) puis ajouter cette nouvelle machine.

Dans le fichier « /usr/share/prometheus/prometheus.yml » dans la section « static_configs » on ajoute la machine debian avec le port utilisé par node_exporter (9100).

```
    static_configs:
      - targets: ["localhost:9090"]
      - targets: ["localhost:9100"]
      - targets: ["192.168.1.57:9100"]
```

Ensuite il faut rédemarrer le serveur prometheus.

```
root@debian:~# systemctl daemon-reload
root@debian:~# systemctl restart prometheus.service
```

Si on se rend sur grafana on peut constater que le test fonctionne puisque nous avons désormais accès à la machine debian(192.168.1.57) récemment ajouté en plus de celle qui est utilisé pour le serveur prometheus.

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
    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 co
nfusion
[+] Running 7/7
 ✔ Network auto_default           Created                                    0.1s
 ✔ Volume "auto_glpi-data"        Created                                    0.0s
 ✔ Volume "auto_prometheus-data"  Created                                    0.0s
 ✔ Volume "auto_mariadb-data"     Created                                    0.0s
 ✔ Container mariadb              Started                                    0.9s
 ✔ Container glpi                 Started                                    0.9s
 ✔ Container prometheus           Started                                    0.8s
```

Les containers se lancent

```
ubuntu@ubuntu:~/auto$ sudo docker container ls -a
[sudo] password for ubuntu:
CONTAINER ID   IMAGE                  COMMAND                  CREATED          STATUS                    PORTS
        NAMES
803ce833f8c3   containrrr/watchtower  "/watchtower glpi pr…"   39 minutes ago   Up 39 minutes (healthy)   8080/tcp
        watchtower
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
35b1141fe5f3   prom/prometheus        "/bin/prometheus --c…"   55 minutes ago   Up 55 minutes             0.0.0.0:9090->9090/tcp, :::9090->9090
/tcp    prometheus
6a085613320e   mariadb                "docker-entrypoint.s…"   55 minutes ago   Up 55 minutes             3306/tcp
        mariadb
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

8. Manuel technique

Tous les scripts shell sont disponibles sur
https://github.com/mgrosmann/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.

```
#!/bin/bash
apt update
apt install mariadb-server -y
mysql_secure_installation <<EOF
y
n
y
y
y
y
EOF
mysql  <<EOF
ALTER USER 'root'@'localhost' IDENTIFIED BY 'root';
CREATE USER 'mgrosmann'@'localhost' IDENTIFIED BY 'password';
CREATE DATABASE test;
GRANT ALL PRIVILEGES ON test.* TO 'root'@'localhost';
FLUSH PRIVILEGES;
EOF
```

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

Voici le script utilisé :

```
#!/bin/bash
apt update
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
mysql   <<EOF
CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'glpi';
CREATE DATABASE glpi;
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost';
GRANT SELECT ON \`mysql\`.\`time_zone_name\` TO 'glpi'@'localhost';
FLUSH PRIVILEGES;
EOF
cd /var/www/html
wget https://github.com/glpi-project/glpi/releases/download/10.0.17/glpi-10.0.17.tgz
tar -xvzf glpi-10.0.17.tgz
chown root:root /var/www/html/glpi/ -R
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.

```
apt update
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
```

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 »

```
mysql  <<EOF
CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'glpi';
CREATE DATABASE glpi;
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost';
GRANT SELECT ON \`mysql\`.\`time_zone_name\` TO 'glpi'@'localhost';
FLUSH PRIVILEGES;
EOF
```

On se rend dans le repertoire « /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.

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

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

```
chown root:root /var/www/html/glpi/ -R
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

```
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 :

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

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

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

Si c'est la 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.

```
apt install perl
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.

```
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

```
systemctl enable glpi-agent
```

8.2 Mise en place d’un outil de sauvegarde : Rsync

Pour l’installation de Rsync, on mettra d’abord la liste des paquets à jour avec

```
sudo apt update
```

Puis on installera le paquet rsync avec

```
sudo apt install -y rsync
```

Rsync est désormais installé.

8.3 Mise en place d’un outil de supervision : Prometheus et grafana

Pour l’installation de promotheus et grafana le script suivant sera utilisé :

```
#!/bin/bash
wget https://github.com/prometheus/prometheus/releases/download/v2.41.0/prometheus-2.41.0.linux-amd64.tar.gz
tar xzf prometheus-2.41.0.linux-amd64.tar.gz
mv prometheus-2.41.0.linux-amd64/ /usr/share/prometheus
useradd --no-create-home --shell /bin/false prometheus
mkdir -p /var/lib/prometheus/data
chown prometheus:prometheus /var/lib/prometheus/data
chown -R prometheus:prometheus /usr/share/prometheus
cat <<EOF > /etc/systemd/system/prometheus.service
[Unit]
Description=Prometheus Server
Documentation=https://prometheus.io/docs/introduction/overview/
After=network-online.target

[Service]
User=prometheus
Restart=on-failure
WorkingDirectory=/usr/share/prometheus
ExecStart=/usr/share/prometheus/prometheus --config.file=/usr/share/prometheus/prometheus.yml --storage.tsdb.path=/var/lib/prome

[Install]
WantedBy=multi-user.target
EOF
systemctl daemon-reload
systemctl enable prometheus
systemctl start prometheus
apt update
apt install -y gnupg2 curl software-properties-common dirmngr apt-transport-https lsb-release ca-certificates
curl https://packages.grafana.com/gpg.key | apt-key add -
add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
apt update
apt -y install grafana
```

```
systemctl daemon-reload
systemctl enable grafana-server
systemctl start grafana-server
curl -s https://api.github.com/repos/prometheus/node_exporter/releases/latest | grep browser_download_url | grep linux-amd64 | cut -d '"' -f 4 | wget -qi -
tar -xvf node_exporter*.tar.gz
cd node_exporter*/
cp node_exporter /usr/local/bin
chown prometheus:prometheus /usr/local/bin/node_exporter
cat <<EOF > /etc/systemd/system/node_exporter.service
[Unit]
Description=Node Exporter
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
ExecStart=/usr/local/bin/node_exporter

[Install]
WantedBy=multi-user.target
EOF
systemctl daemon-reload
systemctl enable node_exporter
systemctl start node_exporter
echo "Veuillez éditer le fichier '/usr/share/prometheus/prometheus.yml' et ajouter les configurations suivantes :"
echo "    scarpe_configs:"
echo "  - job_name: 'node_exporter'"
echo "    static_configs:"
echo "      - targets: ['localhost:9100']"
echo "Ensuite, redémarrez Prometheus avec : systemctl restart prometheus"
```

Tout d'abord on télécharge l'archive de prometheus, on la décompresse puis on déplace le dossier decompréssé dans le repertoire « /usr/share/prometheus »

```
#!/bin/bash
wget https://github.com/prometheus/prometheus/releases/download/v2.41.0/prometheus-2.41.0.linux-amd64.tar.gz
tar xzf prometheus-2.41.0.linux-amd64.tar.gz
mv prometheus-2.41.0.linux-amd64/ /usr/share/prometheus
```

Ensuite on crée l'utilisateur prometheus, on crée un repertoire « /var/lib/prometheus/data » puis on donne les droits à l'utilisateur prometheus à ce repertoire mais aussi au repertoire « /usr/share/prometheus »

```
useradd --no-create-home --shell /bin/false prometheus
mkdir -p /var/lib/prometheus/data
chown prometheus:prometheus /var/lib/prometheus/data
chown -R prometheus:prometheus /usr/share/prometheus
```

Ensuite nous allons éditer le fichier « /etc/systemd/system/prometheus.service » comme ci-dessous afin de faire de prometheus un service.

```
cat <<EOF > /etc/systemd/system/prometheus.service
[Unit]
Description=Prometheus Server
Documentation=https://prometheus.io/docs/introduction/overview/
After=network-online.target

[Service]
User=prometheus
Restart=on-failure
WorkingDirectory=/usr/share/prometheus
ExecStart=/usr/share/prometheus/prometheus --config.file=/usr/share/prometheus/prometheus.yml --storage.tsdb.path=/var/lib/pro

[Install]
WantedBy=multi-user.target
EOF
```

Pour finaliser l'installation de prometheus il va falloir activer le service prometheus et le démarrer

```
systemctl daemon-reload
systemctl enable prometheus
systemctl start prometheus
```

Ensuite passons à l'installation de grafana

Tout d'abord on va mettre à jour la liste des paquets puis installer toutes les dépendances à grafana et teléchrger la clé.

```
apt update
apt install -y gnupg2 curl software-properties-common dirmngr apt-transport-https lsb-release ca-certificates
curl https://packages.grafana.com/gpg.key | apt-key add -
add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"
```

Maintenant que les dépendances sont installées, on peut procéder à l'installation de grafana.

```
apt update
apt -y install grafana
```

Comme pour prometheus, on va activer le service grafana et le démarrer

```
systemctl daemon-reload
systemctl enable grafana-server
systemctl start grafana-server
```

Passons maintenant à l'installation de node_exporter.

Nous allons télécharger l'archive la plus recente de node_exporter puis la decompresser.

```
curl -s https://api.github.com/repos/prometheus/node_exporter/releases/latest | grep browser_download_url | grep linux-amd64 | cut -d '"' -f 4 | wget -qi -
tar -xvf node_exporter*.tar.gz
```

Une fois decompressé, accéder au dossier puis, une fois a l'intérieur, copier le dossier « node_exporter » dans le repertoire « /usr/local/bin » puis donner les droits à l'utilisateur prometheus.

```
cd node_exporter*/
cp node_exporter /usr/local/bin
chown prometheus:prometheus /usr/local/bin/node_exporter
```

Ensuite nous allons éditer le fichier «/etc/systemd/system/node_exporter.service » tel que :

```
cat <<EOF > /etc/systemd/system/node_exporter.service
[Unit]
Description=Node Exporter
Wants=network-online.target
After=network-online.target

[Service]
User=prometheus
ExecStart=/usr/local/bin/node_exporter

[Install]
WantedBy=multi-user.target
EOF
```

Puis on active et démarre le service

```
systemctl daemon-reload
systemctl enable node_exporter
systemctl start node_exporter
```

Pour finaliser la configuration il faut éditer manuellement le fichier « /usr/share/prometheus/prometheus.yml » puisqu'il faut rajouter des lignes à des endroits trop spécifiques pour être fait depuis un script :

Dans la partie "scarpe_configs:" rajouter « - job_name: 'node_exporter' »

Dans la partie " static_configs:" rajouter « - targets: ['localhost:9100']"

Tel que :

```
# my global config
global:
  scrape_interval: 15s # Set the scrape interval to every 15 seconds. Default is every 1 minute.
  evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every 1 minute.
  # scrape_timeout is set to the global default (10s).

# Alertmanager configuration
alerting:
  alertmanagers:
    - static_configs:
        - targets:
          # - alertmanager:9093

# Load rules once and periodically evaluate them according to the global 'evaluation_interval'.
rule_files:
  # - "first_rules.yml"
  # - "second_rules.yml"

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  # The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
  - job_name: "prometheus"
  - job_name: 'node_exporter'

    # metrics_path defaults to '/metrics'
    # scheme defaults to 'http'.

    static_configs:
      - targets: ["localhost:9090"]
      - targets: ["localhost:9100"]
```

Les services assurant la supervision sont désormais opérationnel.

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 active 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 regle 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 ou un autre windows server fera partie du domaine.

Vous pourez 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'originations sur lequel appliqué 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

Il faut cependant noter que tant que la synchronisation des mises à jour n'a pas été finalisé on ne pourra pas sauvegarder la règle

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

Par suite de cela dans la partie « Mises à jour », la vue nouvellement crée apparaitra, bien qu'étant donné que la synchronisation n'a pas été achevé, les mises à jour ne s'affichent pas encore.

Une fois la synchronisation terminé, la configuration de wsus pour l'automisation des mises à jour sera finalisée.

8.5 Configuration Pfsense

J’ai commencé par mettre en place un serveurs DHCP et DNS pour ce faire j'ai donc installer un pfsense et voici sa configuration :

```
The IPv4 WAN address has been set to 192.168.182.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.182.254/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 8d9122ce1fc0585e5cc0

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

 WAN (wan)       -> em0        -> v4: 192.168.182.254/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

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

Ensuite j'ai donc configuré le serveur DHCP puis le serveur DNS 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 appareil réseau de l’entreprise puis enregistré.

Pour le serveur DNS il faut aller dans services > DNS Resolver. Il vous suffit d’activer

puis activer les autres paramètres pour lier le serveur DNS au serveur DHCP (si ce n’est pas déjà fait). Une fois tous cochés, sauvegarder les modifications et le tour est joué.

DHCP Registration	☑ Register DHCP leases in the DNS Resolver If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.
Static DHCP	☑ Register DHCP static mappings in the DNS Resolver If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.

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)

Suivez les différentes étapes :

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

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

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)

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

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

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

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

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

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 :

Puis add :

Puis save, il faut ensuite modifier les privilèges lié au groupe :
Cliquez sur add puis sélectionner le bon privilège :

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

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 Docker

Le déploiement automatisé avec Docker sert à faciliter la gestion, la mise à jour et le déploiement de vos applications comme **GLPI** (pour la gestion des ressources informatiques) et **Prometheus.** Dans Docker, les conteneurs sont basés sur des images. Lorsque de nouvelles versions de ces images sont publiées (par exemple, avec des correctifs de sécurité ou des fonctionnalités améliorées).

Pour ce faire il faut déjà installer Docker sur le serveur :

On met à jour le serveur

```
ubuntu@ubuntu:~$ sudo apt update && sudo apt upgrade -y
```

Installer les dépendances nécessaires

```
ubuntu@ubuntu:~$ sudo apt install -y apt-transport-https ca-certificates curl software-properties-common
```

Ajouter la clé GPG de Docker

```
ubuntu@ubuntu:~$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
```

Ajouter le dépôt Docker

```
ubuntu@ubuntu:~$ echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu
 $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

On remet à jour

```
ubuntu@ubuntu:~$ sudo apt update
```

On peut installer docker

```
ubuntu@ubuntu:~$ sudo apt install -y docker-ce
```

Pour vérifier s'il est installé :

```
ubuntu@ubuntu:~$ docker --version
Docker version 27.4.1, build b9d17ea
ubuntu@ubuntu:~$ _
```

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 désactiver, 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 » :

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 :

Le sous-onglet Profils :

Actions

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 :

Actions

NOM COMPLET
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 :

Le sous-onglet composant :

Le sous-onglet générale :

Le sous-onglet plugin :

9.2 Mise en place d'un outil de sauvegarde : Rsync

Rsync permet de sauvegarder les données en les envoyant vers une autre machine Linux. Pour cela, nous utiliserons une machine Linux cliente et une autre machine Linux dédiée aux sauvegardes et restaurations des données.

Nous allons créer trois dossiers dans le répertoire personnel de l'utilisateur :

- **Desktop** : contiendra les fichiers à sauvegarder.
- **Save** : répertoire destiné à recevoir les sauvegardes, principalement utilisé par la machine qui stocke les back-ups à restaurer.
- **Backup** : utilisé comme répertoire où envoyer les données à restaurer.

```
mkdir -p /home/mgrosmann/backup
mkdir -p /home/mgrosmann/desktop
mkdir -p /home/mgrosmann/save
```

Maintenant que ces fichiers sont créés nous allons télécharges des scripts pour automatiser la sauvegarde et la restauration avec rsync.

On leur donnera les droits avec la commande « chmod +x »

```
wget https://mgrosmann.onrender.com/script/save.sh
wget https://mgrosmann.onrender.com/script/backup.sh
chmod +x save.sh
chmod +x backup.sh
```

Le fichiers save.sh et backup.sh ressemble à ça :

```
#!/bin/bash
SOURCE_DIR="/home/mgrosmann/desktop"
BACKUP_DIR="/home/mgrosmann/backup"
REMOTE_USER="mgrosmann"
REMOTE_HOST="192.168.1.45"
REMOTE_DIR="/home/mgrosmann/save"
rsync -avz $SOURCE_DIR $REMOTE_USER@$REMOTE_HOST:$REMOTE_DIR
```

Le fichier save.sh

```
#!/bin/bash
SOURCE_DIR="/home/mgrosmann/desktop"
BACKUP_DIR="/home/mgrosmann/backup"
REMOTE_USER="mgrosmann"
REMOTE_HOST="192.168.1.45"
REMOTE_DIR="/home/mgrosmann/save"
rsync -avz $REMOTE_USER@$REMOTE_HOST:$REMOTE_DIR $BACKUP_DIR
```

Le fichier backup.sh

On peut également modifier le script en incluant davantage la commande « read -p » pour pouvoir entrer des variables et pouvoir choisir un dossier a chaque exécution sans avoir a changé a chaque fois le contenu du script tel que :

Pour save.sh :

```
#!/bin/bash
read -p "Entrez le répertoire à sauvegarder  : " SOURCE_DIR
read -p "Entrez le répertoire qui contiendra les backup : " BACKUP_DIR
read -p "Entrez le nom de l'utilisateur distant : " REMOTE_USER
read -p "Entrez l'adresse IP ou le nom d'hôte de la machine distante  : " REMOTE_HOST
read -p "Entrez le répertoire de sauvegarde sur la machine distante : " REMOTE_DIR
rsync -avz $SOURCE_DIR $REMOTE_USER@$REMOTE_HOST:$REMOTE_DIR
```

Pour backup.sh :

```
#!/bin/bash
read -p "Entrez le répertoire à sauvegarder  : " SOURCE_DIR
read -p "Entrez le répertoire qui contiendra les backup : " BACKUP_DIR
read -p "Entrez le nom de l'utilisateur distant : " REMOTE_USER
read -p "Entrez l'adresse IP ou le nom d'hôte de la machine distante  : " REMOTE_HOST
read -p "Entrez le répertoire de sauvegarde sur la machine distante : " REMOTE_DIR
rsync -avz $REMOTE_USER@$REMOTE_HOST:$REMOTE_DIR $BACKUP_DIR
```

Ou encore taper la commande à la main tel que :

Pour sauvegarder :

```
rsync -avz nom_dossier_a_sauvegarder utilisateur@adresse_ip_duserveur:dossier_distant
```

Pour restaurer :

```
rsync -avz utilisateur@adresse_ip_duserveur:dossier_distant dossier_backup_local
```

9.3 Utilisation de Prometheus et Grafana

Tout d'abord nous allons nous rendre sur l'interface web de Grafana en entrant les identifiants et mot de passe par défaut (admin pour les 2)

Pour des raisons de sécurité nous allons ensuite changer le mot de passe :

Dans l'écran d'acceuil on va sélectionner « add your first data source »

Puis on sélectionne prometheus

On entrera un nom (ici « my-prometheus-server »)

Puis on indiquera l'adresse du serveur prometheus (ici « 192.168.1.45)

Concernant tous les paramètres, on laisse leur valeur par défaut puis on sélectionne « save and test » pour sauvegarder et tester la liaison grafana-prometheus.

Si la liaison réussi vous devriez avoir ce message :

Ensuite il faudra aller dans le menu dashboard puis sur new->import

On entrera en valeur « 1860 » dans la zone pour les dashboards disponible sur grafana.com/dashboard

Puis vous sélectionnerez le serveur prometheus avec le nom précédemment entrée (ici « my-prometheus-server »)

Voici le résultat dans le menu dashboard :

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 :

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

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"
```

10. Références bibliographiques (liste des sources documentaires)

GLPI	Le script pour glpi est basé sur le site suivant : https://faq.teclib.com/03_knowledgebase/procedures/install_glpi Le script pour agent-glpi est basé sur le site suivant : https://colinfo.fr/configuration-et-installation-de-lagent-glpi-sous-windows-et-linux/
Rsync	Installation de rsync : https://operavps.com/docs/install-rsync-command-in-linux/ Save.sh et backup.sh inspire du site : https://www.digitalocean.com/community/tutorials/how-to-use-rsync-to-sync-local-and-remote-directories
Prometheus	Script basé sur le site suivant : https://tutos-info.fr/wp-content/uploads/2023/01/TUTORIEL-INSTALLER-PROMETHEUS-ET-GRAFANA.pdf
Gestion centralisée des mises à jour	Pour les actions à entreprendre pour configurer wsus https://learn.microsoft.com/fr-fr/windows/deployment/update/waas-manage-updates-wsus
Portail captif	https://www.pc2s.fr/pfsense-portail-captif-avec-authentification-utilisateur/
Configutation pfsense	https://provya.net/?d=2014/08/24/12/09/58-pfsense-configurer-son-serveur-dhcp https://www.arsouyes.org/blog/2019/23_DNS_Personnel/
Configuration d'un Active Directory	https://www.it-connect.fr/creer-un-domaine-ad-avec-windows-server-2016/
Déploiement automatisé avec Docker	https://www.hostinger.fr/tutoriels/installer-docker-sur-ubuntu https://github.com/containrrr/watchtower https://github.com/DiouxX/docker-glpi https://github.com/prometheus/prometheus

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 Prometheus combinée à Grafana 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 Rsync 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.

Parmi le travail restant à faire, nous devons encore configurer l’isolement du réseau avec la mise en place des VLAN et des DMZ pour sécuriser davantage le réseau et limiter l’impact d’une cyber-attaque ayant pénétré dans le réseau.

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.