Compte rendu – Projet 1 Partie 2

Clinique Pasteur – Centralisation des études

Introduction

Dans le cadre du projet de centralisation des études, il a été demandé d'étudier et de proposer des solutions techniques concernant trois volets essentiels :

1. La mise en place de mesures de **sécurité** conformes au RGPD,
2. La **sauvegarde des données** liées aux études et protocoles,
3. Le **déploiement automatisé** et sécurisé de l'application développée.

Le présent document détaille les propositions retenues pour répondre aux attentes du DSI.

1. Exigences de Sécurité (RGPD)

Solutions techniques proposées :

- Mise en place de Vlan séparés pour :(les Postes Administratifs, les services médicaux, les serveurs applicatifs et bases de données, un pare-feu, faire de l'inter-vlan pour assurer le filtrage qui n'autorisera que les flux nécessaires (ex : HTTPS entre postes et serveurs applicatifs).

- Chiffrement des communications : on utilisera du **TLS** (HTTPS) pour l'application qui lui utilise un certificat et du **SSH** pour l'administration, l'accès à la base de données uniquement depuis l'application (interdiction d'accès direct depuis les postes utilisateurs)

- Authentification et gestion des droits : on doit mettre en place un ADDS/LDAP pour les comptes nominatifs pour centraliser l'authentification, la gestion des rôles (Assistantes->saisie/gestion des inclusion, Médecin /chirurgiens->consultation et suivi, Administrateurs DSI->maintenance technique).

- Journalisation et traçabilité : mise en place de logs centralisés (SIEM/ELK) afin de tracer tous les accès aux données sensible et analyse, affiche sous forme de tableaux de bord personnalisables, mais permet aussi des recherches interactives enfin conservation des journaux selon les règles RGPD (durée limitée, accès restreint)

2. SAUVEGARDE DES DONNEES

La conservation et la protection des données étant essentielles, une politique de sauvegarde adaptée doit être définie.

2.1 Méthodes

- **Sauvegarde incrémentale quotidienne** pour réduire l'espace disque.
- **Sauvegarde complète hebdomadaire** pour assurer une copie intégrale du système.

2.2 Stockage

- Conservation locale sur un serveur de sauvegarde dédié ou un NAS.
- Réplication vers un **site secondaire** (hors site) avec chiffrement.
- Supports chiffrés pour tout stockage externe.

2.3 Plan de reprise d'activité (PRA)

- Mise en place d'un **serveur de secours** prêt à être activé en cas d'incident.
- Tests semestriels du PRA afin de garantir la fiabilité de la restauration.

2.4 Outils possibles

- Solutions natives Debian/Linux.

3.Déploiement de l’application

Pour déployer l’application de manière rapide et sécurisée, nous proposons d’utiliser les **stratégies de groupe (GPO)** dans Active Directory.
Cette méthode permet d’installer ou de mettre à jour automatiquement l’application sur les postes concernés, sans intervention manuelle.

Mise en œuvre :

1. Préparer le package d’installation (.msi ou .exe).
2. Mettre ce fichier sur un dossier partagé du serveur.
3. Créer une GPO dans Active Directory et lier l’installation de l’application.
4. Appliquer la GPO aux utilisateurs ou aux machines ciblées.
5. Lors du redémarrage, l’application se déploie automatiquement.

Avantages :

- Déploiement automatique et centralisé.
- Gain de temps (pas besoin d’aller sur chaque poste).
- Tous les postes disposent de la même version de l’application.