AP "GSB - Gestion des remboursements de frais"
Tracer les accès afin de gérer les incidents

I. Contexte

Dans le cadre du RGPD, la CNIL demande de tracer les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).
Afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques.
Pour ce faire, un dispositif de gestion des traces et des incidents doit être mis en place : celui-ci doit enregistrer les évènements pertinents et garantir que ces enregistrements ne peuvent être altérés. Dans tous les cas, il ne faut pas conserver ces éléments pendant une durée excessive.
Vous allez donc prévoir un système de journalisation des activités des utilisateurs. Ces évènements ne pourront pas être conservés au-delà six mois (délai légal).

https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents

II. Présentation du travail à faire

1) Stockage des traces

Vous allez créer une table dans la base de données qui permettra d'enregistrer toutes les actions réalisées par les utilisateurs via l'application.

Tous les évènements réalisés seront enregistrés dans une table qui sera appelée LogEvenement.

Pour chaque évènement, les informations suivantes seront enregistrées dans la table LogEvenement :

- Le login et l'IP de l'utilisateur
- Le type d'action réalisé sur l'enregistrement d'une table : ajout, modification, suppression (les suppressions sont des suppressions logiques), consultation
- Le nom de la table concernée
- La date et l'heure de l'évènement
- Le numéro de l'enregistrement concerné par l'évènement

2) Evolution de l'application

Chaque fonctionnalité de l'application devra être adaptée pour qu'elle permette l'écriture de chaque évènement dans la table LogEvenement

Puis, vous développerez deux nouvelles fonctionnalités :

- La première fonctionnalité permettra à l'administrateur d'obtenir les caractéristiques de toutes les actions enregistrées pour un utilisateur et une table sélectionnés par l'administrateur.
- La deuxième fonctionnalité listera les actions les plus suspectes qui doivent être analysées : cette fonctionnalité permettra d'obtenir les adresses ip et l'identifiant des utilisateurs qui ont fait plus de 40 fois la même action sur une même table au cours de la journée.

3) Suppression des traces

D'après le RGPD, le délai de conservation de ces traces d'activités est de 6 mois sauf si des traitements justifiés nécessitent d'allonger le délai de conservation de ces données, mais ce n'est pas le cas de GSB.

Il est donc indispensable de supprimer ces traces régulièrement : chaque soir, un traitement sera chargé de supprimer les traces de plus de 6 mois.

Proposer deux solutions pour répondre à ce besoin.

Comment planifier une procédure stockée dans MySQL : https://www.it-swarm-fr.com/fr/mysql/comment-planifier-une-procedure-stockee-dans-mysql/972198383/