Fondation Mérieux

LabBook

LabBook v3.6

Journal d'audit LabBook

V1

Janvier 2026

Fondation **Mérieux**
Lutte contre les maladies infectieuses depuis 1967
www.fondation-merieux.org

Table des matières

1. Présentation et intérêt du journal d'audit

Le journal d'audit est une fonctionnalité introduite dans la version 3.6 de LabBook visant à renforcer la traçabilité, la sécurité et la transparence des opérations réalisées dans le système.

Il permet d'enregistrer automatiquement toutes les actions sensibles effectuées par les utilisateurs, telles que :

- les connexions et déconnexions,
- les opérations sur les utilisateurs,
- les opérations sur les demandes d'analyse
- les accès aux ressources,
- les modifications de paramètres ou de données.

Le journal d'audit constitue un outil essentiel pour :

- le suivi des activités des utilisateurs ;
- l'analyse des incidents et des accès non autorisés ;
- le respect des exigences qualité et réglementaires (ISO, audits internes, inspections) ;
- la redevabilité des utilisateurs selon leur rôle.

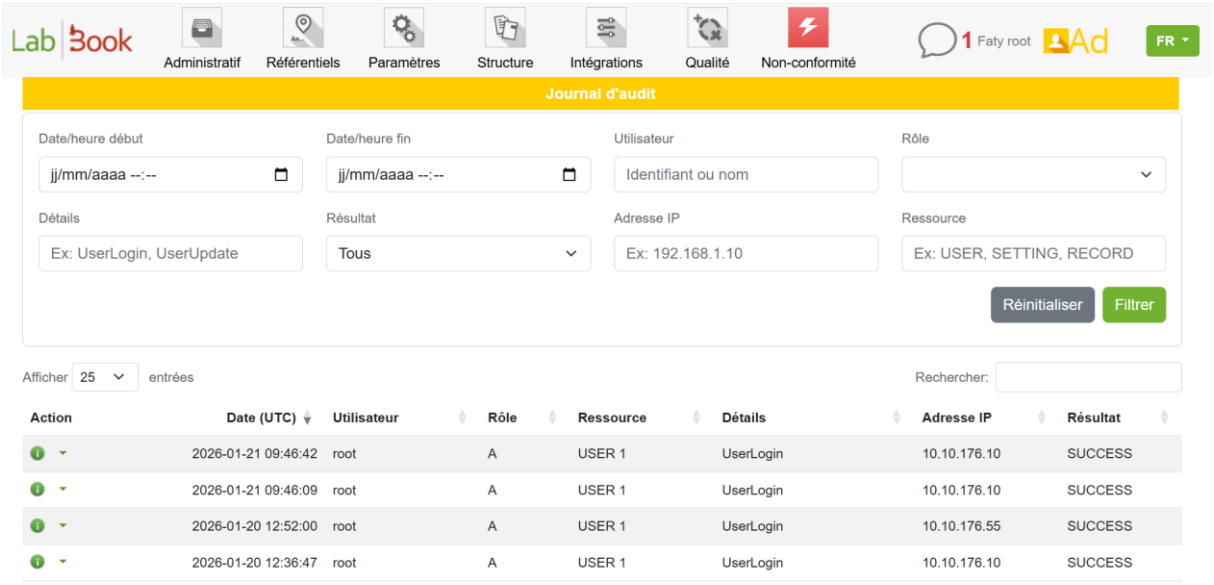
2. Contenu du journal d'audit

Chaque ligne du journal d'audit correspond à une action effectuée dans LabBook. Les informations suivantes sont affichées :

Colonne	Description
Date (UTC)	Date et heure exactes de l'action enregistrée, exprimées en temps universel (UTC).
Utilisateur	Identifiant de l'utilisateur ayant réalisé l'action (ex. root).
Rôle	Rôle attribué à l'utilisateur au moment de l'action (ex. Administrateur).
Ressource	Type de ressource concernée par l'action (ex. USER, RECORD, SETTING).
Détails	Nature de l'action réalisée (ex. UserLogin).
Adresse IP	Adresse IP de la machine depuis laquelle l'action a été effectuée.
Résultat	Statut de l'action (SUCCESS ou ECHEC).
Action	Bouton permettant de consulter le détail complet de l'événement.

3. Exemple d'une ligne du journal d'audit

La fonctionnalité Journal d'audit est accessible depuis le menu Qualité par l'utilisateur disposant du profil Administrateur (root). Pour les autres utilisateurs, l'accès à cette fonctionnalité est conditionné à l'attribution explicite des droits correspondants par l'administrateur. Une fois ces droits accordés, la fonctionnalité devient visible et accessible dans le menu Qualité de leur interface utilisateur.



Exemple :

- Date (UTC) : 2026-01-21 09:46:42
- Utilisateur : root
- Rôle : A (Administrateur)
- Ressource : USER 1
- Détails : UserLogin
- Adresse IP : 10.10.176.10
- Résultat : SUCCESS

Interprétation

Cette ligne indique qu'un utilisateur ayant le compte root, disposant du rôle Administrateur, s'est connecté avec succès au système LabBook depuis l'adresse IP 10.10.176.10 à la date et heure indiquées.

4. Signification de l'action UserLogin

Le journal d'audit LabBook enregistre différents types d'actions en fonction des opérations réalisées par les utilisateurs dans le système.

Exemple « Action UserLogin »

L'action **UserLogin** correspond à une tentative de connexion d'un utilisateur au système LabBook. Elle est enregistrée systématiquement, que la connexion soit réussie ou échouée, ce qui permet :

- de suivre les accès au système ;
- d'identifier les connexions suspectes ;
- d'analyser les problèmes d'authentification.

Autres types d'actions enregistrées

En fonction des droits de l'utilisateur et des fonctionnalités utilisées, le journal d'audit peut également enregistrer d'autres actions. Parmi elles nous pouvons citer :

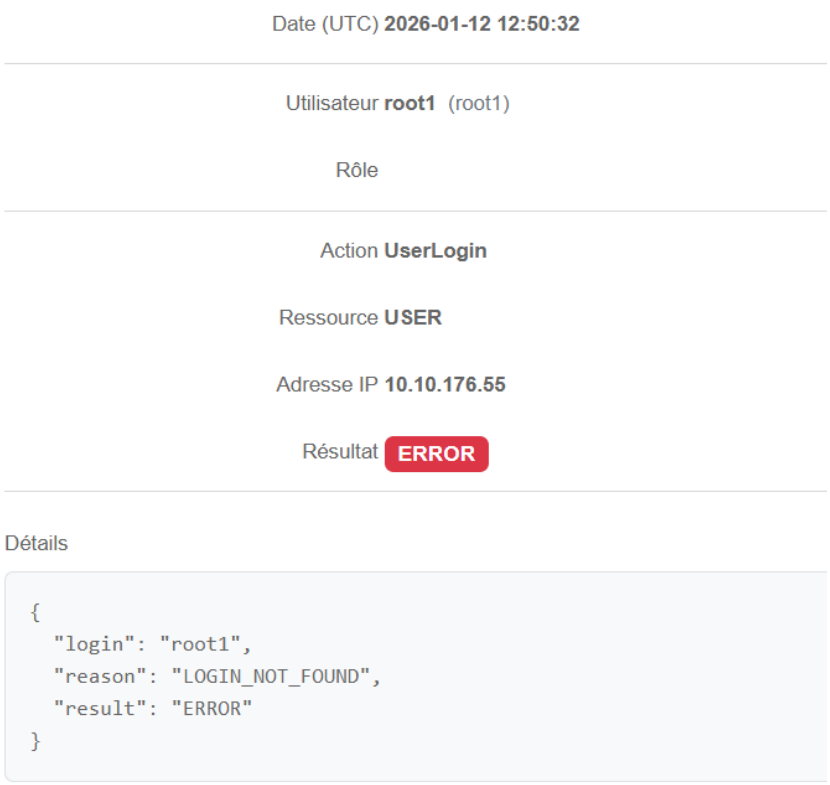
- UserPasswordUpdate : modification du mot de passe d'un utilisateur ;
- UserCreate : création d'un nouveau compte utilisateur ;
- UserUpdate : modification des informations d'un utilisateur ;
- SettingSendReport : envoi d'un rapport depuis les paramètres du système ;
- SettingUpdate : modification des paramètres de configuration ;
- RecordCreate / RecordUpdate : création ou mise à jour d'un dossier ou d'un enregistrement.

Ces actions permettent d'assurer une traçabilité complète des opérations sensibles, de renforcer la sécurité du système et de disposer d'éléments fiables lors des audits, des contrôles qualité ou des investigations en cas d'incident.

5. Consultation des détails d'une action

Dans la colonne Action, un bouton Consulter est disponible pour chaque ligne du journal.

En cliquant sur Consulter, l'utilisateur accède à l'écran Détail du journal d'audit.



Cet écran affiche des informations complémentaires, notamment :

- la date et l'heure exactes,
- l'utilisateur et son rôle,
- la ressource concernée,
- l'adresse IP,
- le résultat de l'action,
- ainsi que les détails techniques au format structuré (JSON).

Exemple de détails affichés :

```
{
  "login": "root",
  "result": "SUCCESS",
  "id_user": 1
}
```

6. Archivage et purge des audits

Les événements d'audit sont enregistrés en continu dans la base de données LabBook.

Un traitement automatique s'exécute le 1er jour de chaque mois à 02h00 (UTC). En cas d'indisponibilité du serveur, il est relancé automatiquement dès que celui-ci redevient accessible.

Lorsque la durée de conservation configurée est dépassée, les audits antérieurs à la période définie sont exportés dans le répertoire /storage/resource/audit, puis supprimés de la table d'audit. Ce mécanisme est appliqué automatiquement chaque mois.

Par défaut, la durée de conservation est fixée à 12 mois. Dans ce cas, la base de données contient en permanence uniquement les audits des 12 derniers mois, les audits plus anciens étant archivés hors base afin de préserver les performances du système.

L'ancienneté peut être régler de 1 à 60 mois maximum.

La durée de conservation est configurable via le champ
« Ancienneté de conservation des audits avant archivage et purge (en mois) », accessible depuis l'interface Administrateur : Paramètres → Préférences

Fondation **Mérieux**

Lutte contre les maladies infectieuses depuis 1967

www.fondation-merieux.org