Procédures

- Accès base de données

Accès base de données

Modalités d'accès

> Aucun accès web à la base de données n'est possible (type PhpMyAdmin/Adminer/Forest, ...)

- La base de données est stockée sur un serveur homologué HDS ISO 27001
- Une fois sur le serveur, elle est accessible par nom d'utilisateur et mot de passe fort
- Le serveur est accessible uniquement via une connexion SSH protégée par une clé SSH forte (ed25519)
- Toutes les connexions SSH doivent passer par un serveur tiers de type bastion Wallix, autrement, la connexion ssh directe au serveur est impossib;e
- Ce bastion est whitelisté par IP, la whitelist est maintenue par l'infogérant Céleste

> La base de données est ainsi accessible uniquement aux développeurs·euses habilité·es

Les étapes pour qu'un·e développeur·euse puisse avoir à la base de données sont les suivantes

1. Demande de création de compte bastion auprès de l'infogérant. L'infogérant fournira un username et un mot de passe via un lien sécurisé visible une seule fois
2. Demande de whitelist de l'IP du lieu de travail auprès de l'infogérant
3. Connexion à l'interface wallix https://bastion.groupeot.com/, réinitialisation du MDP ajout d'une clé SSH au compte
4. Première connexion au serveur en SSH via le bastion via username et MDP
5. Ajout de la clé SSH dans le fichier .ssh/authorized_keys de l'utilisateur web
6. Obtention du mot de passe de la base de données auprès d'un·e membre de l'équipe de développement

> Les modalités et étapes d'accès à la base de données anonymisée de la plateforme de préproduction sont strictement identiques

Motifs légitimes d'accès

La base de données de production **ne doit jamais être consultée hors des motifs** suivants.

> En aucun cas, les situations suivantes ne doivent déclencher automatiquement un accès à la base de données de production

> - Toutes les autres solutions doivent avoir été envisagés, notamment des vérifications en préproduction

- Bug en production **irreproductible en préproduction** impactant les utilisateur·ices en causant une dégradation de service
  - Demande émanant des utilisateur·ices
  - Contrainte technique

Personnes habilitées

- Nils Lapotre Lead dev
- Antoine Aresu Développeur
- Cliven Colleemallay Développeur

Traçabilité

- Toutes les connexions sont tracées et horodatées dans le serveur de bastion prévu à cet effet dans le cadre du référentiel ISO 27001 HDS
- Les opérations effectuées sur la base de données, elles, ne sont pas tracées