RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

BASES DE DONNÉES RELATIONNELLES

Retrouvez, en une dizaine de bonnes pratiques, les ressources essentielles de l'ANSSI pour la mise en œuvre sécurisée de bases de données (BDD) relationnelles.

→ **Maintenir à jour le logiciel de gestion de la BDD (SGBD)** via les dépôts officiels et installer les mises à jour de sécurité – pour aller plus loin, consulter le guide Recommandations de configuration d'un système GNU/Linux et plus spécifiquement les mesures R58, R59, R60 et R61.

→ **Sécuriser l'administration des serveurs hébergeant la BDD** tel que décrit dans le guide Recommandations relatives à l'administration sécurisée des systèmes d'information, et **minimiser les extensions et outils d'administration utilisés.**

→ **Journaliser les évènements et les accès administrateurs** – se référer à l'annexe A du guide Recommandations d'architecture pour la sécurité d'un système de journalisation, et plus particulièrement aux recommandations R3, R9, R26 et R27.

→ **Sécuriser les accès :**

> utiliser des comptes d'accès distincts (pour les utilisateurs humains et les applications) avec une définition claire de leur usage ;

> authentifier systématiquement les accès (attention aux comptes par défaut et aux accès directs) et utiliser des mécanismes cryptographiques à l'état de l'art ;

> analyser régulièrement le compte administrateur natif, qui ne doit être utilisé qu'en dernier recours ;

> mettre en place une authentification multifacteur pour les administrateurs – voir les Recommandations relatives à l'authentification multifacteur et aux mots de passe.

→ **Appliquer le principe de moindre privilège :**

> limiter les droits des utilisateurs au strict nécessaire ;

> définir des rôles et les affecter aux utilisateurs.

→ **Durcir la configuration :**

> isoler les données des fichiers de configuration en les stockant sur des partitions ou dans des répertoires distincts ;

> désactiver les fonctionnalités avancées des BDD qui permettent de lire/écrire/exécuter des fichiers du système d'exploitation ;

> imposer un typage des données.

→ **Paramétrer la sauvegarde** – pour aller plus loin, consulter les publications « Les Fondamentaux » et « Les Essentiels » de l'ANSSI sur la sauvegarde des systèmes d'information.

V1.0 (12/24)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

→ **Protéger les données sensibles :**

> éviter les fuites de données en s'assurant de ne pas utiliser les données de production dans des environnements de développement ou autres environnements similaires ;

> porter une attention particulière vis-à-vis des BDD proposées en format SaaS (risque de mutualisation entre clients) ;

> chiffrer les données lors de leur transmission (*on-transit*) et lors de leur stockage (*at-rest*) ;

> dédier un serveur de BDD par niveau de sensibilité des données ;

> utiliser des mécanismes internes de la BDD pour limiter l'accès aux données (ex. : des vues).

→ **Prendre en compte les bonnes pratiques de développement pour l'accès aux BDD** (ex. : utiliser des requêtes préparées pour se protéger d'injections).

→ **Mettre en place une supervision de la BDD** sur les ressources physiques et/ou virtuelles du serveur (stockage, CPU, RAM) et auditer les événements potentiellement suspicieux.