

Sécurité et gestion efficace des Bases De Données

La sécurité et la gestion efficace des bases jouent un rôle fondamental dans la protection des informations sensibles, la garantie de l'intégrité des données et le maintien de la confiance des utilisateurs.

Une base de données bien gérée et sécurisée permet non seulement de prévenir les accès non autorisés et les fuites de données, mais aussi d'assurer la disponibilité et la fiabilité des informations essentielles au fonctionnement des organisations.

Une approche proactive en matière de sécurité et de gestion des bases de données peut prévenir les pertes financières, protéger la réputation de l'entreprise et optimiser les performances des systèmes d'information, contribuant ainsi directement à la réussite et à la pérennité de l'organisation.

1. Sécurisation de la Base de Données

La sécurisation de ma base de données est une étape importante pour garantir l'intégrité et la confidentialité des données. J'ai mis en place plusieurs mesures de sécurité, en mettant l'accent sur la gestion des utilisateurs et des privilèges.

Cette approche démontre une méthodologie structurée applicable à divers contextes d'entreprise, en mettant l'accent sur la sécurité, les performances et l'adaptabilité aux besoins spécifiques du business.

1.1 Gestion des Utilisateurs et des Privilèges

La gestion des utilisateurs et des privilèges est un aspect fondamental de la sécurité des bases de données. Elle nous permet de contrôler précisément qui a accès à quelles données et quelles opérations peuvent être effectuées par chaque utilisateur. Cette approche suit le principe du moindre privilège, assurant que chaque utilisateur n'a accès qu'aux données et fonctionnalités nécessaires à son rôle. Pour s'assurer que seuls les utilisateurs autorisés ont accès à la fonction de déchiffrement dans MySQL, j'ai mis en place plusieurs mesures de sécurité :

1.2 Création d'Utilisateurs avec des Rôles Spécifiques

J'ai créé plusieurs types d'utilisateurs, chacun avec des niveaux d'accès différents adaptés à leurs responsabilités :

a) Administrateur de la Faculté :

```
mysql> CREATE USER IF NOT EXISTS 'admin_faculte'@'localhost' IDENTIFIED BY 'mot_de_passe_securise_admin';
Query OK, 0 rows affected, 1 warning (0.07 sec)

mysql>
```

```
mysql> GRANT ALL PRIVILEGES ON formation.* TO 'admin_faculte'@'localhost' WITH GRANT OPTION;
Query OK, 0 rows affected (0.01 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.06 sec)
```

b) Manager d'Inventaire :

```
mysql> CREATE USER 'manager_inventaire'@'localhost' IDENTIFIED BY 'mot_de_passe_securise_manager';
Query OK, 0 rows affected (0.06 sec)

mysql> GRANT SELECT, INSERT, UPDATE ON formation.UE TO 'manager_inventaire'@'localhost';
Query OK, 0 rows affected (0.01 sec)
```

Ce rôle a des privilèges limités, permettant uniquement la lecture, l'insertion et la mise à jour des données dans la table UE.

c) Analyste:

```
mysql> CREATE USER 'analyste'@'localhost' IDENTIFIED BY 'mot_de_passe_securise_analyste';
Query OK, 0 rows affected (0.06 sec)

mysql> GRANT SELECT ON formation.UE TO 'analyste'@'localhost';
```

L'analyste a un accès en lecture seule, lui permettant de consulter les données sans pouvoir les modifier.

1.3 Mesures de Sécurité Supplémentaires

En plus de la gestion des utilisateurs, je peux implémenter d'autres mesures de sécurité :

```
mysql> SHOW GRANTS FOR 'admin_ecommerce'@'localhost';
+-----+-----+
| Grants for admin_ecommerce@localhost |
+-----+-----+
| GRANT USAGE ON *.* TO 'admin_ecommerce'@'localhost' |
| GRANT EXECUTE ON PROCEDURE 'e_commerce'.'.dechiffrer_info_confidentielle' TO 'admin_ecommerce'@'localhost' |
+-----+-----+
2 rows in set (0.00 sec)

mysql> |
```

Chiffrement des données sensibles : Utilisation de fonctions de chiffrement pour protéger les informations confidentielles.

```
mysql> SELECT sku, nom,
-> AES_DECRYPT(info_confidentielles, 'clé_secrete') AS info_confidentielles_dechiffrees
-> FROM Produits
-> WHERE sku = 'LAP001';
+-----+-----+-----+
--+
| sku | nom | info_confidentielles_dechiffrees |
+-----+-----+-----+
--+
| LAP001 | Ordinateur portable XYZ | 0x496E666F726D61746966E20636F6E666964656E7469656C6C6520737572206C652070726F64756974 |
+-----+-----+-----+
1 row in set (0.00 sec)

mysql> |
```

Création de vues : Pour limiter l'accès à certaines données sans exposer la structure complète de la base.

Audits réguliers : Mise en place de logs pour suivre les accès et les modifications de la base de données.

En mettant en œuvre ces mesures de sécurité, j'assure non seulement la protection des données, mais je crée également un environnement où chaque utilisateur peut effectuer ses tâches de manière efficace et sécurisée.

```
mysql> SELECT * FROM vue_produits_publics;
```

id	sku	nom	prix	categorie
1	LAP001	Ordinateur portable XYZ	999.99	Électronique
2	SMT002	Smartphone ABC	599.99	Électronique
3	BOK003	Guide du développeur SQL	39.99	Livres
4	DSK004	Bureau ergonomique	299.99	Mobilier
5	CAM005	Caméra HD WiFi	79.99	Électronique

```
5 rows in set (0.00 sec)

mysql>
```

L'utilisation de AES_ENCRYPT () m'a permis de stocker les notes confidentielles de manière sécurisée. Seuls les utilisateurs ayant accès à la clé de chiffrement pourront déchiffrer ces informations, ajoutant ainsi une couche de sécurité supplémentaire à mes données sensibles.

```
mysql> SELECT * FROM Produits;
```

id	sku	nom	description	prix	quantite_stock	categorie
1	LAP001	Ordinateur portable XYZ	Ordinateur portable haute performance	999.99	50	Électronique
2	SMT002	Smartphone ABC	Smartphone dernière génération	599.99	100	Électronique
3	BOK003	Guide du développeur SQL	Livre de référence pour SQL	39.99	200	Livres
4	DSK004	Bureau ergonomique	Bureau ajustable en hauteur	299.99	30	Mobilier
5	CAM005	Caméra HD WiFi	Caméra de surveillance intérieure	79.99	75	Électronique

```
5 rows in set (0.00 sec)

mysql>
```

2. Test et validation : j'ai inséré des données de test et vérifié les performances avec des volumes de données réalistes.

2.1. Utilisation de procédures stockées :

J'ai créé une procédure stockée qui encapsule la logique de déchiffrement :

```
mysql> DROP PROCEDURE IF EXISTS dechiffreur_info_confidentielle;
Query OK, 0 rows affected (0.06 sec)

mysql>
mysql> DELIMITER //
mysql> CREATE PROCEDURE dechiffreur_info_confidentielle(IN p_sku VARCHAR(20))
-> BEGIN
->     SELECT sku, nom,
->         AES_DECRYPT(info_confidentielles, 'clé_secrete') AS info_confidentielles_dechiffrees
->     FROM Produits
->     WHERE sku = p_sku;
-> END //
Query OK, 0 rows affected (0.01 sec)

mysql> DELIMITER ;
mysql> SHOW CREATE PROCEDURE dechiffreur_info_confidentielle;
+-----+-----+-----+-----+-----+-----+
| Procedure | sql_mode | character_set_client | collation_connection | Database Collation |
+-----+-----+-----+-----+-----+-----+
| dechiffreur_info_confidentielle | ONLY_FULL_GROUP_BY,STRICT_TRANS_TABLES,NO_ZERO_IN_DATE,NO_ZERO_DATE,ERROR_FOR_DIVISION_BY_ZERO,NO_ENGINE_SUBSTITUTION | CREATE DEFINER='root'@'localhost' PROCEDURE 'dechiffreur_info_confidentielle'(IN p_sku VARCHAR(20))
BEGIN
    SELECT sku, nom,
        AES_DECRYPT(info_confidentielles, 'clé_secrete') AS info_confidentielles_dechiffrees
    FROM Produits
    WHERE sku = p_sku;
END | cp850 | cp850_general_ci | utf8mb4_0900_ai_ci |
+-----+-----+-----+-----+-----+-----+
```

```
mysql> SHOW PROCEDURE STATUS WHERE Db = 'e_commerce' AND Name = 'dechiffreur_info_confidentielle';
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Db      | Name      | Type | Definer | Modified | Created | Security_type | Comment | character_set_client | collation_ |
| connection | Database Collation |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| e_commerce | dechiffreur_info_confidentielle | PROCEDURE | root@localhost | 2024-07-04 10:42:36 | 2024-07-04 10:42:36 | DEFINER |  | cp850 | cp850_gene |
| ral_ci | utf8mb4_0900_ai_ci |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.06 sec)
```

3. Mise en place de vues sécurisées :

```
mysql> SHOW CREATE VIEW e-commerce.vue_products_publics;
+-----+-----+
| View | Create View |
+-----+-----+
| collation_connection | | character_set_client |
+-----+-----+
| vue_products_publics | CREATE ALGORITHM=UNDEFINED DEFINER='root'@'localhost' SQL SECURITY DEFINER VIEW 'vue_products_publics' AS select 'produits'.id AS 'id','produits'.sku AS 'sku','produits'.nom AS 'nom','produits'.prix AS 'prix','produits'.categorie AS 'categorie' from 'produits' where ('produits'.quantite_stock > 0) | cp850
+-----+-----+
1 row in set (0.00 sec)
```

```
mysql> SELECT * FROM Produits;
```

id	sku	nom	description	prix	quantite_stock	categorie	date_ajout	info_confidentielles
1	LAP001	Ordinateur portable XYZ	Ordinateur portable haute performance	999.99	50	Électronique	2024-07-04 08:48:49	0xBC1FE1266148737A6CADE9D5093A74AF
4921	FC7B31B30DCC8976B54CE6A1016A150EB4A826437C83CB190F6764C181A							
2	SMT002	Smartphone ABC	Smartphone dernière génération	599.99	100	Électronique	2024-07-04 08:48:49	0xFE1AB614DAACC3EE218F977A7A7CF086
207120	9C568A51A5B084B04CCD39B38E354967C31F1EE35B1A51019533C1B05							
3	BOM003	Guide du développeur SQL	Livre de référence pour SQL	39.99	200	Livres	2024-07-04 08:48:49	NULL
4	DSK004	Bureau ergonomique	Bureau ajustable en hauteur	299.99	30	Mobilier	2024-07-04 08:48:49	NULL
5	CAM005	Caméra HD WiFi	Caméra de surveillance intérieure	79.99	75	Électronique	2024-07-04 08:48:49	NULL

```
5 rows in set (0.00 sec)
```