Chapitre 4
Sécurité et gestion des utilisateurs

1. Introduction

La sécurité des données du système informatique de l'entreprise n'est pas seulement l'affaire du RSSI (Responsable de la sécurité des systèmes d'information). Les techniques et les bonnes pratiques nécessaires pour se protéger doivent être connues et appliquées, par tout un chacun. Les éléments de la chaîne applicative étant interdépendants, la robustesse de cette chaîne va dépendre de la solidité de son maillon le plus faible. Un test non effectué par l'application, un compte utilisateur qui a trop de droits sur la base de données, une mise à jour de sécurité non effectuée ou tout simplement une maladresse sur le serveur de production peuvent être à l'origine du vol ou de l'altération des numéros de cartes bancaires de vos clients par exemple. Les conséquences peuvent alors être désastreuses tant financièrement qu'en terme d'image pour la société. Certes la sécurité absolue n'existe pas, mais nous allons dans ce chapitre essayer de vous donner toutes les pratiques nécessaires pour minimiser les risques.

2. Sécurisation du serveur MariaDB

Les questions liées à la sécurité doivent être posées dès l'installation du serveur de base de données. MariaDB dérive étroitement de MySQL, or dans la philosophie de MySQL l'utilisateur doit pouvoir télécharger, installer et utiliser le SGBDR (Système de gestion de bases de données relationnelles) sans aucune difficulté. Cette simplicité est l'un des points forts de MySQL, car d'une part, cela a permis de démocratiser l'utilisation d'une base de données en rendant accessible cet univers (beaucoup de développeurs ont connu les bases de données grâce à MySQL) et d'autre part, cela donne la possibilité de tester très simplement son application. L'inconvénient majeur est que son installation par défaut est très permissive, notamment en matière de sécurité...

2.1 Sécurisation de l'installation

Le but de cette section n'est pas de revenir sur l'installation du serveur qui est détaillée au chapitre Installation du serveur, mais simplement de rappeler quelques points cruciaux concernant la sécurité. Vous devrez certainement les adapter en fonction de votre type d'installation et de votre système d'exploitation.

2.1.1 Contrôler les droits

Vous devez créer un groupe et un utilisateur dédié pour lancer l'instance `mysqld` :

```
$ groupadd mysql
$ useradd -g mysql mysql
```

Le répertoire de données contient les informations sensibles, il doit donc être préservé d'actes de malveillance ou de la visualisation par des personnes non autorisées :

```
$ cd /usr/local/mariadb/
$ chown -R root .
$ chown -R mysql data
$ chgrp -R mysql .
```

`mysqld` ne doit en aucun cas être exécuté avec l'administrateur système `root` sous UNIX (ou `administrateur` sous MS Windows). Un utilisateur avec par exemple le droit `FILE` pourrait créer des fichiers en tant que `root`.

2.1.2 Mettre un mot de passe au compte utilisateur root

C'est le super-utilisateur de MariaDB (à ne pas confondre avec l'administrateur système `root` sous UNIX) ; il a donc tous les droits sur le serveur MariaDB ; il doit être protégé par un mot de passe. Ceci est valable quel que soit le système d'exploitation.

```
$ mysql –u root # connexion au serveur avec l'utilisateur root sans
mot de passe
mysql> SET PASSWORD FOR root@localhost = password('m0T2p4ss3'); /*
la commande set password permet de mettre un mot de passe à un compte
utilisateur */
```

Comme vous allez le voir un peu plus loin, un utilisateur MariaDB est composé d'un nom « user » et du nom de la machine à partir de laquelle l'utilisateur se connecte « host ». Vous pouvez donc avoir un compte `'root'@'localhost'` qui permet de se connecter au serveur avec l'utilisateur `root` à condition que le client soit sur la même machine que le serveur MariaDB (en local) et par exemple un compte `'root'@'123.45.67.89'` qui, lui ne permet de se connecter en `root` qu'à partir de la machine qui a comme adresse IP 123.45.67.89. Ce sont bien deux comptes différents, qui peuvent avoir des droits et des mots de passe différents. Cette possibilité offerte par le serveur peut permettre une gestion des droits très fine. Cependant, par expérience, nous vous conseillons de n'avoir qu'une seule occurrence par utilisateur, par souci de simplification de la gestion des droits et donc pour diminuer les risques d'erreurs. En d'autres termes, ne gardez que l'utilisateur `'root'@'localhost'`. Si vous avez besoin d'administrer votre serveur à distance, au lieu d'avoir `'root'@'%'` (qui permet de se connecter avec l'utilisateur `root` depuis n'importe quelle machine), utilisez le protocole de communication sécurisée SSH ou un équivalent.

```
mysql> SELECT user, host, password FROM mysql.user WHERE user = 'root' \G
*************************** 1. row ***************************
user: root
host: localhost
password: *228F5395471FEFD9B0BB291954D2189384329691
*************************** 2. row ***************************
```

```
user: root
host: 123.456.78.9
password: *63D85DCA15EAFFC58C908FD2FAE50CCBC60C4EA2

mysql> DROP USER 'root'@'123.456.78.9' ;

mysql> SELECT user, host, password FROM mysql.user WHERE user = 'root' \G
*************************** 1. row ***************************
user: root
host: localhost
password: *228F5395471FEFD9B0BB291954D2189384329691
```

Remarque

Renommer le compte administrateur : vous pouvez renommer votre compte administrateur pour qu'il soit plus difficile à trouver par une personne malveillante : `RENAME USER 'root'@'localhost' TO 'leader'@'localhost';`

2.1.3 Supprimer les comptes anonymes

Dans le but de faciliter la prise en main du logiciel, un compte anonyme, c'est-à-dire un compte qui a le champ `user` à vide, peut être présent lors de l'installation de votre serveur. Il permet de se connecter au serveur avec n'importe quel utilisateur, en local et sans mot de passe. Il n'est guère besoin d'argumenter plus pour comprendre que, sur un serveur de production, un tel utilisateur n'est pas à sa place, il faut donc le supprimer. Ce principe doit être étendu à tous les comptes inutilisés, car c'est autant de problèmes potentiels en moins.

```
mysql> SELECT user, host, password FROM mysql.user WHERE user = '' \G
*************************** 1. row ***************************
user:
host: localhost
password:

mysql> DROP USER ''@localhost;

mysql> SELECT user, host, password FROM mysql.user WHERE user = '' \G
```

2.1.4 Supprimer le schéma test

Le schéma `test` est créé par MariaDB lors de l'installation pour toutes les versions antérieures à 10.0 et tous les utilisateurs ont le droit d'y accéder en lecture comme en écriture sans qu'il soit nécessaire de spécifier explicitement les droits adéquats. Un utilisateur mal intentionné pourrait alors remplir de données votre disque dur et ainsi empêcher le bon fonctionnement de votre application.

```
mysql> SHOW SCHEMAS;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| test               |
+--------------------+

mysql> DROP SCHEMA test;

mysql> SHOW SCHEMAS;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
+--------------------+
```

À noter que cette recommandation s'applique également à tout schéma `test` qui serait créé par la suite, mais également à tout schéma qui commencerait par le mot `test` suivi d'un underscore (_).

2.1.5 Sécuriser votre installation avec l'outil mysql_secure_installation

La mise en œuvre de ces différentes recommandations peut être effectuée avec l'outil `mysql_secure_installation`. Cet outil n'est pas disponible sous MS Windows, cependant l'installeur graphique propose également de sécuriser l'installation.

```
$ mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL
MySQL SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
```

```
In order to log into MySQL to secure it, we'll need the current
password for the root user. If you've just installed MySQL, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
```

2.2 Utilisation de SSL

Les données circulent en clair entre le client et le serveur MariaDB. Il est possible de les crypter en utilisant le protocole SSL (*Secure Sockets Layer*), qui permet d'assurer la sécurité, l'intégrité et la confidentialité des données échangées. Cependant, les traitements supplémentaires induits ont un impact non négligeable sur les performances, en les réduisant d'environ 30 %.

2.2.1 Les options

SSL propose une liste d'options. Plus d'informations sont disponibles sur le site de MariaDB : https://mariadb.com/kb/en/mariadb/secure-connections/. en voici une brève description :

- L'option `ssl` permet au serveur d'autoriser les connexions SSL et au client de se connecter en utilisant ce protocole.
- L'option `ssl-ca` permet de spécifier le fichier qui contient le certificat d'autorité (CA).
- L'option `ssl-capath` est le répertoire des fichiers contenant les certificats d'autorité SSL.
- L'option `ssl-cert` est le nom du certificat SSL à utiliser pour établir une connexion sécurisée.
- L'option `ssl-key` est le nom du fichier de la clé SSL à utiliser pour établir une connexion sécurisée.
- L'option `ssl-cipher` est la liste des chiffrements (*cipher*) autorisés à utiliser avec SSL.