

Installation de SSL avec MariaDB sous Debian

Modifiez le fichier `/etc/mysql/mariadb.conf.d/50-server.cnf` (ou `/etc/mysql/mariadb.cnf`) comme suit : La valeur du nom commun utilisée pour les certificats/clés du serveur et du client doit être différente de la valeur du nom commun utilisée pour le certificat CA. Pour éviter tout problème, je les règle comme suit. Sinon, vous obtiendrez une erreur d'échec de la vérification de la certification. Par conséquent, définissez-le comme suit :

Nom commun de l'AC : administrateur MariaDB

Nom commun du serveur : serveur MariaDB

Nom commun du client : client MariaDB

Créez un répertoire nommé `ssl` dans le répertoire `/etc/mysql/`

```
$ cd /etc/mysql
$ sudo mkdir ssl
$ cd ssl
```

Tapez la commande suivante pour créer une nouvelle clé CA :

```
sudo openssl genrsa 4096 > ca-key.pem
```

Tapez la commande suivante pour générer le certificat à l'aide de cette clé :

```
$ sudo openssl req -new -x509 -nodes -days 365000 -key ca-key.pem -out ca-cert.pem
```

Maintenant, vous devez avoir deux fichiers comme suit :

- `/etc/mysql/ssl/ca-cert.pem` – Fichier de certificat pour l'autorité de certification (CA).
- `/etc/mysql/ssl/ca-key.pem` – Fichier clé pour l'autorité de certification (CA).

Créer le certificat SSL du serveur

Pour créer la clé du serveur, exécutez :

```
sudo openssl req -newkey rsa:2048 -days 365000 -nodes -keyout server-key.pem -out server-req.pem
```

Ensuite, créer la clé RSA du serveur, saisissez :

```
openssl rsa -in server-key.pem -out server-key.pem
```

Enfin, signez le certificat du serveur, exécutez :

```
openssl x509 -req -in server-req.pem -days 365000 -CA ca-cert.pem -CAkey ca-key.pem -  
set_serial 01 -out server-cert.pem
```

Maintenant, vous devez avoir des fichiers supplémentaires :

- /etc/mysql/ssl/server-cert.pem – Fichier de certificat du serveur MariaDB.
- /etc/mysql/ssl/server-key.pem – Fichier de clé du serveur MariaDB.

Vous devez utiliser les deux fichiers ci-dessus sur le serveur MariaDB lui-même et sur tout autre nœud que vous allez utiliser pour le trafic de cluster/réplication. Ces deux fichiers sécuriseront la communication côté serveur.

Configurer le serveur MariaDB pour utiliser SSL

Modifiez le fichier /etc/mysql/mariadb.conf.d/50-server.cnf comme suit :

```
### MySQL Server ###  
## Securing the Database with ssl option and certificates ##  
## There is no control over the protocol level used. ##  
## mariadb will use TLSv1.0 or better. ##  
#ssl  
ssl-ca=/etc/mysql/ssl/ca-cert.pem  
ssl-cert=/etc/mysql/ssl/server-cert.pem  
ssl-key=/etc/mysql/ssl/server-key.pem  
## Set up TLS version here. For example TLS version 1.2 and 1.3 ##  
tls_version = TLSv1.2, TLSv1.3
```

Enregistrez et fermez le fichier. Sécurisez les clés à l'aide de la commande chmod/commande chown :

```
sudo chown -Rv mysql:root /etc/mysql/ssl/
```

Revision #2

Created 10 November 2021 06:31:26 by ggpilou2

Updated 10 November 2021 06:40:33 by ggpilou2