Configure ssh jump server to use SSL for MySQL

737 Manu Chacko September 26, 2024 Tweaks & Configuration 273

How to configure Ezeelogin to use SSL for MySQL version 8 on Ubuntu?

Overview: This article provides step-by-step instructions to configure Ezeelogin to use SSL for MySQL version 8 on Ubuntu, ensuring secure communication between the Ezeelogin ss jump server and the MySQL server.

Mysql - SSL setup on Ubuntu Mysql server

Step 1. Check the Current SSL/TLS Status

Log into MySQL session

```
:~# mysql -u root -p
```

Show the state of the SSL/TLS variables by typing:

```
mysql> show variables like '%ssl%';
```

```
+---------------------------------------+------------------+
| Variable_name  |  Value |
+---------------------------------------+------------------+
| admin_ssl_ca  |  |
| admin_ssl_capath  |  |
| admin_ssl_cert  |  |
| admin_ssl_cipher  |  |
| admin_ssl_crl  |  |
| admin_ssl_crlpath  |  |
| admin_ssl_key  |  |
| have_openssl  | YES  |
| have_ssl  | YES  |
| mysqlx_ssl_ca  |  |
| mysqlx_ssl_capath  |  |
| mysqlx_ssl_cert  |  |
| mysqlx_ssl_cipher  |  |
| mysqlx_ssl_crl  |  |
| mysqlx_ssl_crlpath  |  |
| mysqlx_ssl_key  |  |
| performance_schema_show_processlist |OFF  |
| ssl_ca  | ca.pem  |
| ssl_capath  |  |
| ssl_cert  | server-cert.pem |
| ssl_cipher  |  |
| ssl_crl  |  |
| ssl_crlpath  |  |
| ssl_fips_mode  | OFF  |
```

```
| ssl_key  | server-key.pem  |
| ssl_session_cache_mode  | ON  |
| ssl_session_cache_timeout  | 300  |
+-------------------------------------+-----------------+
27 rows in set (0.02 sec)
```

The **have_ssl** variable is marked as YES. This means that SSL functionality is enabled on the server.

Step 2: Now you can login to Mysql server with following command and grant Ezeelogin user to access the Ezeelogin database. you can refer the article to retrieve Ezeelogin database credentials.

Replace **ezlogin_databasename,ezlogin_db_username** and **ez_db_password** with your Ezeelogin database username.

```
:~# mysql -u root -p

[Enter password]

mysql> create user 'ezlogin_db_username'@'127.0.0.1' identified by 'ez_db_password';

mysql> grant all on ezlogin_databasename.* to 'ezlogin_db_username'@'127.0.0.1' with grant option;
```

```
mysql> flush privileges;


mysql> exit
```

Check the connection details by the following command :

```
 ~]# mysql -u ezlogin_db_username -p -h 127.0.0.1  --ssl-ca=/var/lib/mysql/ca.pem --ssl-cert=/var/lib/mysql/client-cert.pem --ssl-key=/var/lib/mysql/client-key.pem



example :




 ~]# mysql -u ezlogin_xxxx -p -h 127.0.0.1 -ssl-ca=/var/lib/mysql/ca.pem --ssl-cert=/var/lib/mysql/client-cert.pem --ssl-key=/var/lib/mysql/client-key.pem
```

In Case the certificate verification has been failed, refer SSL certificate failed with MYSQL SSL

```
mysql> s

--------------

. . .

SSL: Cipher in use is DHE-RSA-AES256-SHA

. . .

Connection: 127.0.0.1 via TCP/IP

. . .

----------------
```

SSL cipher is displayed, indicating that SSL is being used to secure our connection.

Step 3. Change the bind address & allow the Ezeelogin jump server user to access the database.

Edit the /etc/mysql/mysql.conf.d/mysqld.cnf & change bind-address

```
:~# vi /etc/mysql/mysql.conf.d/mysqld.cnf
```

```
Change bind-address to host ip or 0.0.0.0


bind-address 0.0.0.0
```

Restart the Mysql service

```
:~# systemctl restart mysql
```

Step 4. Check and correct the permission of /etc/certs directory and client-key.pem

```
:~# chmod 755 /var/lib/mysql


:~# ls -ld /var/lib/mysql
drwxr-xr-x 2 root root 4096 Sep 20 15:51 /var/lib/mysql


:~# chmod 644 /var/lib/mysql/client-key.pem


:~# ls -ld /var/lib/mysql/client-key.pem
-rw-r--r-- 1 mysql mysql 1705 Mar 29 2023 /var/lib/mysql/client-key.pem
```

Step 5. Configure Ezeelogin jump server to use SSL for Mysql

Add **mysql_ssl_key, mysql_ssl_cert, mysql_ssl_ca** and change **db_host,db_port** to **/usr/local/etc/ezlogin/ez.conf** as follows

Edit the **/usr/local/etc/ezlogin/ez.conf** file add the following

```
:~# vi /usr/local/etc/ezlogin/ez.conf

#Add the following



system_folder /var/www/ezlogin/
force_https no
uri_path /ezlogin/
db_host 127.0.0.1
db_port 3306
db_name ezlogin_qzms
db_user ezlogin_edcjwz
db_pass dsH)$s5xAE[QgFms
db_prefix aqvo_
cookie_encryption_key ASvs8^pnu^^X9
cookie_name lcrrfs
cookie_path /ezlogin/
```

```
www_folder /var/www/html/ezlogin/
admin_user admin
mysql_encrypt yes
mysql_ssl_key /var/lib/mysql/client-key.pem
mysql_ssl_cert /var/lib/mysql/client-cert.pem
mysql_ssl_ca /var/lib/mysql/ca.pem
mysql_ssl_capath /var/lib/mysql
mysql_ssl_verify no
```

Note: Make sure that you have changed **db_port** to ***3306*** & **db_host** to the ***127.0.0.1***

You have successfully configured SSL for Mysql 8 on the Ezeelogin SSH jump server, enhancing the security of your database connections and ensuring that sensitive data is encrypted during transmission.

Note: Make sure to grant the secondary IP to access primary node and the primary IP to the secondary node when configuring the cluster. Replace the secondary IP and primary IP with the appropriate IPs. Also, use same certificate and keys for both primary and secondary node.

```
:~# mysql -u root -p

[Enter password]

mysql> create user 'ezlogin_db_username'@'secondary IP or primary IP' identified by 'ez_db_password';

mysql> grant all on ezlogin_databasename.* to 'ezlogin_db_username'@'secondary IP or primary IP' with grant option;

mysql> flush privileges;

mysql> exit
```

Note: If you have any difficulties please contact support

Related Articles:

Configure ssh jump server to use SSL for Mariadb

Install Master/Slave Ezeelogin with MySQL SSL

Unable to access GUI while using MySQL SSL

failed to connect to database: Error: TLS/SSL error: Permission denied