Troubleshooting Mysql SSL in Secondary node

517 admin January 29, 2025 Common Errors & Troubleshooting 1840

How to troubleshoot and verify Mysql SSL In Secondary node

Overview: This article describes the troubleshooting steps to verify MYSQL SSL in slave/secondar node of Jumpserver.

During the MySQL SSL slave installation, if prompted about using a secure MySQL connection ("Do you want to use a secure MySQL connection?"), the following steps should be verified:

Step 1: If opting to **use a secure connection**, ensure the certificate paths for connecting to the master node are specified, which can be verified by manually connecting to the master node using SSL.

You can use the below command.

```
root@secondary:~# mysql -u ezlogin_database_username -p -h hostname or ip --ssl-ca=/var/lib/mysql/ca.pem --ssl-cert=/var/lib/mysql/client-cert.pem --ssl-key=/var/lib/mysql/client-key.pem
```

For example:

```
root@secondary:~# mysql -u ezlogin_xxxx -p -h 10.11.1.11 --ssl-ca=/var/lib/mysql/ca.pem --ssl-cert=/var/lib/mysql/client-cert.pem --ssl-key=/var/lib/mysql/client-key.pem
```

Make sure that you are able to log in to MySQL of the slave as root user and also from slave to master with Ezeelogin database username and password with SSL.

Step 1(A): If opting **not to use a secure connection**, proceed with the installation, and MySQL SSL can be configured later. Refer below articles.

For MySQL 5.5

For MySQL 5.7

Step 2: Connect MySQL with the database name and SSL in the below cases so that the master and slave are secure. A successful connection to MySQL SSL will take place if all cases are met.

2(a):From master to master itself with the below command:

```
root@gateway :~# mysql -u ezlogin_database_username -p -h master_ip
--ssl-ca=/etc/certs/ca.pem --ssl-cert=/etc/certs/client-cert.pem
--ssl-key=/etc/certs/client-key.pem
```

2(b): From master to slave with the below command:

```
root@gateway:~# mysql -u ezlogin_database_username -p -h slave_ip
--ssl-ca=/etc/certs/ca.pem --ssl-cert=/etc/certs/client-cert.pem
--ssl-key=/etc/certs/client-key.pem
```

2(c): From slave to slave itself with the below command

```
root@secondary :~# mysql -u ezlogin_database_username -p -h slave_ip
--ssl-ca=/etc/certs/ca.pem --ssl-cert=/etc/certs/client-cert.pem
--ssl-key=/etc/certs/client-key.pem
```

2(d): From slave to master with the below command.

```
root@secondary :~# mysql -u ezlogin_database_username -p -h maste_ip
--ssl-ca=/etc/certs/ca.pem --ssl-cert=/etc/certs/client-cert.pem
--ssl-key=/etc/certs/client-key.pem
```

Step 3: If the above cases apply, you should add the following lines to the ez.conf file on both the master and slave nodes.

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

```
system_folder /var/www/ezlogin/
force_https no
uri_path /ezlogin/
db_host 10.10.1.11
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 /etc/certs/client-key.pem
mysql_ssl_cert /etc/certs/client-cert.pem
mysql_ssl_ca /etc/certs/ca.pem
mysql_ssl_capath /etc/certs/
mysql_ssl_verify no
```

After adding the above lines in ez. conf, master and slave node connection will be secure.

Related Articles:

Error log file and configuration file to troubleshoot

unable to access gui while accessing with mysql ssl