Using Encrypted Connections with ClustrixDB 1

ClustrixDB supports SSL and authentication with the sha256_password plugin.

Some security regulations require stronger protection of user passwords stored in the database. The sha256_password plugin provides a more secure method of storing user password credentials in ClustrixDB as compared to the default mysql_native_password plugin. When a user account is configured to use the sha256_password plugin, that user must then always connect using an SSL protected connection.

The instructions below provide steps for configuring ClustrixDB for SSL encrypted connections, and also configure ClustrixDB user accounts to use SHA256 password security along with SSL encrypted connections. To use this feature, use the instructions below to generate certificates and keys, copy them to all nodes, configure the database and users to use SSL when applicable (requires a mysql client 5.6.38 or higher).

ClustrixDB Configuration for SSL Encrypted Connections

To configure Xpand to use encrypted connections:

Create keys and certificates (using your choice of method) and copy them as the root user to every node:

```
shell> scp server-cert.pem root@hostname:/data/clustrix
shell> scp server-key.pem root@hostname:/data/clustrix
```

On each node, transfer ownership of those files to the xpand user:

```
shell> sudo chown xpand server-*.pem
```

Certificates and keys must be in the same location on every node.

Configure Xpand to use these certificates, keys, and SSL:

```
sql> SET GLOBAL ssl_cert = '/data/clustrix/server-cert.pem';
sql> SET GLOBAL ssl_key = '/data/clustrix/server-key.pem';
sql> ALTER CLUSTER RELOAD SSL;
sql> SET GLOBAL ssl_enabled = TRUE;
```

ALTER CLUSTER RELOAD SSL validates the location of the certificates and keys. If this command fails, the clustrix.log may include more detail.

Connecting from a client using an encrypted connections

The MySQL client version must be 5.6.38, 5.7 or higher client.

If you are using the mysql 5.6.38 client, you must specify the cipher type:

```
shell> mysql --ssl-cipher=AES256-SHA -u
username -h hostname -p
```

If you are using the mysql 5.7 client, there are no special options required:

```
shell> mysql
username -h h
ostname  -
p
```

The output of \s will show whether TLS is enabled:

```
sql> \s
```

and show as part of the output the type of encryption in use:

```
Cipher in use is AES256-SHA
```

This query will show the type of encryption used for all sessions:

```
sql> select * from system.sessions;
```

Setting Up Users

By default, passwords use mysql_native_password. To change an existing users' password to use sha256 encryption:

```
sql> ALTER USER 'seymour@'%' IDENTIFIED WITH
sha256_password BY 'foo';
```

To set it back to use mysql_native_password:

```
sql> ALTER USER 'seymour'@'%' IDENTIFIED WITH mysql_native_password by 'foo';
```

Create a new user using sha256_password authentication:

```
sql> CREATE USER 'seymour2'@'%' IDENTIFIED WITH
sha256_password BY 'foo';
```

Users with a password encrypted with SHA256 must use encrypted connections to connect to ClustrixDB. If a secure connection is not available, the user will encounter an error and be unable to connect.

Caveats for SHA2 usage

- Certificates and keys must exist on all nodes and be owned by the clxd user
- ClustrixDB does not support configuration a default authentication plugin other than mysql_native_password
- ClustrixDB does not support RSA password encryption
- Using encrypted connections have a performance overhead