Quintessence Labs

APPLICATION NOTE

qCrypt Key Management Server

Using qCrypt as a Key Manager for MySQL

Overview

This document shows how to configure the MySQL keyring_okv and qCrypt key manager to work together.

Intended audience: MySQL database managers and cyber security operations personnel.
Assumptions: Familiarity with MySQL database configuration.

Introduction

MySQL supports encryption of database content with keys managed by an external OASIS KMIP key management server. The qCrypt Key Manager conforms to the OASIS KMIP standard and supports the key management requirements of MySQL.

In order for MySQL to communicate with qCrypt using KMIP, a mutually authenticated TLS session must be established over a TCP connection. During the TLS handshake, both MySQL (the client) and qCrypt (the server) perform a number of public key cryptography (PKC) operations to authenticate each other. Additionally, the establishment of the secret key used to encrypt the communications between MySQL and qCrypt involves PKC operations.

MySQL must be configured with PKI credentials (private key, client certificate, and trusted root, or CA, certificate) in order to successfully establish a TLS session with qCrypt.

This document shows how to configure the MySQL keyring_okv and qCrypt to work together.

Configuring keyring_okv for the QuintessenceLabs qCrypt appliance

The QuintessenceLabs qCrypt appliance supports the KMIP protocol (versions 1.0, 1.1, 1.2, 1.3, and 1.4). As of MySQL 5.7.18, the keyring_okv keyring plugin (which supports KMIP 1.1) can use qCrypt as its KMIP back end for keyring storage.

Use the following procedure to configure keyring_okv and qCrypt to work together.

1. Create the configuration directory that will contain the qCrypt support files, and make sure that the keyring_okv_conf_dir system variable is set to name that directory (for details, see General keyring_okv Configuration in MySQL documentation).
2. In the configuration directory, create a subdirectory named ssl to use for storing the required SSL certificate and key files.
3. In the configuration directory, create a file named okvclient.ora. It should have following format:

   ```
   SERVER=host_ip:port_num
   STANDBY_SERVER=host_ip:port_num
   ```

   For example, if a qCrypt replication group is running behind a load balancer with VIP 192.168.1.20 and listening on port 5696, the okvclient.ora file looks like this:

   ```
   SERVER=192.168.1.20:5696
   STANDBY_SERVER=192.168.1.20:5696
   ```

   If members of a qCrypt replication group are accessible directly, and, for example using IP addresses 192.168.1.40, and 192.168.1.41, both on port 5696, the okvclient.ora file looks like this:

   ```
   SERVER=192.168.1.40:5696
   STANDBY_SERVER=192.168.1.41:5696
   ```

4. Connect to the qCrypt Administration Console as an administrator with permissions to generate client credentials, and register a KMIP client.
5. Navigate to PKI Management >> Credentials and generate client credentials.
6. Navigate to KMIP Clients >> Clients and create a KMIP client linked to the client credentials. In the Action Policy drop-down list, select Default All Allowed. Leave the Rate Limiting Policy value set to None. Download the client's connection pack (you may choose either zip or tar formats).

7. Extract the files from the client connection pack, and save them in the ssl directory. Rename the CA file to CA.pem. Rename the client certificate file to cert.pem. Rename the client private key file to key.pem.

After completing the above procedure, restart the MySQL server. It loads the keyring_okv plugin and keyring_okv uses the files in its configuration directory to communicate with qCrypt.

About QuintessenceLabs

QuintessenceLabs' portfolio of modular products addresses the most difficult security challenges, helping implement robust security strategies to protect data today and in the future. For more information on QuintessenceLabs' data protection solutions, please visit **www.quintessencelabs.com**

Quintessence Labs

AUSTRALIA
Unit 1, Lower Ground
15 Denison St
Deakin, ACT 2600
+61 2 6260 4922

UNITED STATES
175 Bernal Road
Suite 220
San Jose CA 95119
+1 650 870 9920

www.quintessencelabs.com

Document ID: 3508
AN-2018009-001