GALERA SECURITY

Ask

Securing Communications in Galera Cluster

By default, Galera Cluster replicates data between each node without encrypting it. This is generally acceptable when the cluster nodes runs on the same host or in networks where security is guaranteed through other means. However, in cases where the cluster nodes exist on separate networks or they are in a high-risk network, the lack of encryption does introduce security concerns as a malicious actor could potentially eavesdrop on the traffic or get a complete copy of the data by triggering an SST.

To mitigate this concern, Galera Cluster allows you to encrypt data in transit as it is replicated between each cluster node using the Transport Layer Security (TLS) protocol. TLS was formerly known as Secure Socket Layer (SSL), but strictly speaking the SSL protocol is a predecessor to TLS and, that version of the protocol is now considered insecure. The documentation still uses the term SSL often and for compatibility reasons TLS-related server system and status variables still use the prefix `ssl_`, but internally, MariaDB only supports its secure successors.

In order to secure connections between the cluster nodes, you need to ensure that all servers were compiled with TLS support. See Secure Connections Overview to determine how to check whether a server was compiled with TLS support.

For each cluster node, you also need a certificate, private key, and the Certificate Authority (CA) chain to verify the certificate. If you want to use self-signed certificates that are created with OpenSSL, then see Certificate Creation with OpenSSL for information on how to create those.

Securing Galera Cluster Replication Traffic

In order to enable TLS for Galera Cluster's replication traffic, there are a number of wsrep_provider_options that you need to set, such as:

- You need to set the path to the server's certificate by setting the socket.ssl_cert wsrep_provider_option.
- You need to set the path to the server's private key by setting the socket.ssl_key wsrep_provider_option.
- You need to set the path to the certificate authority (CA) chain that can verify the server's certificate by setting the socket.ssl_ca wsrep_provider_option.
- If you want to restrict the server to certain ciphers, then you also need to set the socket.ssl_cipher wsrep_provider_option.

It is also a good idea to set MariaDB Server's regular TLS-related system variables, so that TLS will be enabled for regular client connections as well. See Securing Connections for Client and Server for information on how to do that.

For example, to set these variables for the server, add the system variables to a relevant server option group in an option file:

```
[mariadb]
...
ssl_cert = /etc/my.cnf.d/certificates/server-cert.pem
ssl_key = /etc/my.cnf.d/certificates/server-key.pem
ssl_ca = /etc/my.cnf.d/certificates/ca.pem
wsrep_provider_options="socket.ssl_cert=/etc/my.cnf.d/
certificates/server-cert.pem;socket.ssl_key=/etc/my.cnf.d/
certificates/server-key.pem;socket.ssl_ca=/etc/my.cnf.d/
certificates/ca.pem"
```

And then restart the server to make the changes persistent.

By setting both MariaDB Server's TLS-related system variables and Galera Cluster's TLS-related wsrep_provider_options, the server can secure both external client connections and Galera Cluster's replication traffic.

Securing State Snapshot Transfers

The method that you would use to enable TLS for State Snapshot Transfers (SSTs) would depend on the value of wsrep_sst_method.

mariadb-backup

See mariadb-backup SST Method: TLS for more information.

xtrabackup-v2

See xtrabackup-v2 SST Method: TLS for more information.

mysqldump

This SST method simply uses the mariadb-dump (previously mysqldump) utility, so TLS would be enabled by following the guide at Securing Connections for Client and Server: Enabling TLS for MariaDB Clients

rsync

This SST method supports encryption in transit via stunnel. See Introduction to State Snapshot Transfers (SSTs): rsync for more information.

Previous
Galera Security

Next
MariaDB Enterprise Cluster Security

Last updated 27 days ago

Was this helpful?