group_replication_recovery channel could then be inadvertently started with the stored credentials, on either the original member or members that were cloned from it. An automatic start of Group Replication on server boot (including after a remote cloning operation) would use the stored user credentials, and they would also be used if an operator did not specify the distributed recovery credentials on a START GROUP_REPLICATION command.

18.6.3.2 Secure Socket Layer (SSL) Connections for Distributed Recovery

Whether the distributed recovery connection is made using the standard SQL client connection or a distributed recovery endpoint, to configure the connection securely, you can use Group Replication's dedicated distributed recovery SSL options. These options correspond to the server SSL options that are used for group communication connections, but they are only applied for distributed recovery connections. By default, distributed recovery connections do not use SSL, even if you activated SSL for group communication connections, and the server SSL options are not applied for distributed recovery connections. You must configure these connections separately.

If a remote cloning operation is used as part of distributed recovery, Group Replication automatically configures the clone plugin's SSL options to match your settings for the distributed recovery SSL options. (For details of how the clone plugin uses SSL, see Configuring an Encrypted Connection for Cloning.)

The distributed recovery SSL options are as follows:

- group_replication_recovery_use_ssl: Set to ON to make Group Replication use SSL for distributed recovery connections, including remote cloning operations and state transfer from a donor's binary log. You can just set this option and none of the other distributed recovery SSL options, in which case the server automatically generates certificates to use for the connection, and uses the default cipher suites. If you want to configure the certificates and cipher suites for the connection, use the other distributed recovery SSL options to do this.

- group_replication_recovery_ssl_ca: The path name of the Certificate Authority (CA) file to use for distributed recovery connections. Group Replication automatically configures the clone SSL option clone_ssl_ca to match this.

  group_replication_recovery_ssl_capath: The path name of a directory that contains trusted SSL certificate authority (CA) certificate files.

- group_replication_recovery_ssl_cert: The path name of the SSL public key certificate file to use for distributed recovery connections. Group Replication automatically configures the clone SSL option clone_ssl_cert to match this.

- group_replication_recovery_ssl_key: The path name of the SSL private key file to use for distributed recovery connections. Group Replication automatically configures the clone SSL option clone_ssl_cert to match this.

- group_replication_recovery_ssl_verify_server_cert: Makes the distributed recovery connection check the server's Common Name value in the donor sent certificate. Setting this option to ON is the equivalent for distributed recovery connections of setting VERIFY_IDENTITY for the group_replication_ssl_mode option for group communication connections.

- group_replication_recovery_ssl_crl: The path name of a file containing certificate revocation lists.

- group_replication_recovery_ssl_crlpath: The path name of a directory containing certificate revocation lists.

- group_replication_recovery_ssl_cipher: A list of permissible ciphers for connection encryption for the distributed recovery connection. Specify a list of one or more cipher names, separated by