NAME

mysql_ssl_rsa_setup − create SSL/RSA files

SYNOPSIS

mysql_ssl_rsa_setup [*options*]

DESCRIPTION

This program creates the SSL certificate and key files and RSA key−pair files required to support secure connections using SSL and secure password exchange using RSA over unencrypted connections, if those files are missing. **mysql_ssl_rsa_setup** can also be used to create new SSL files if the existing ones have expired.

Note

mysql_ssl_rsa_setup uses the **openssl** command, so its use is contingent on having OpenSSL installed on your machine.

Another way to generate SSL and RSA files, for MySQL distributions compiled using OpenSSL, is to have the server generate them automatically. See Section 6.3.3.1, “Creating SSL and RSA Certificates and Keys using MySQL”.

Important

mysql_ssl_rsa_setup helps lower the barrier to using SSL by making it easier to generate the required files. However, certificates generated by **mysql_ssl_rsa_setup** are self−signed, which is not very secure. After you gain experience using the files created by **mysql_ssl_rsa_setup**, consider obtaining a CA certificate from a registered certificate authority.

Invoke **mysql_ssl_rsa_setup** like this:

```
shell> mysql_ssl_rsa_setup [options]
```

Typical options are **−−datadir** to specify where to create the files, and **−−verbose** to see the **openssl** commands that **mysql_ssl_rsa_setup** executes.

mysql_ssl_rsa_setup attempts to create SSL and RSA files using a default set of file names. It works as follows:

1. **mysql_ssl_rsa_setup** checks for the **openssl** binary at the locations specified by the PATH environment variable. If **openssl** is not found, **mysql_ssl_rsa_setup** does nothing. If **openssl** is present, **mysql_ssl_rsa_setup** looks for default SSL and RSA files in the MySQL data directory specified by the **−−datadir** option, or the compiled−in data directory if the **−−datadir** option is not given.

2. **mysql_ssl_rsa_setup** checks the data directory for SSL files with the following names:

```
ca.pem
server−cert.pem
server−key.pem
```

3. If any of those files are present, **mysql_ssl_rsa_setup** creates no SSL files. Otherwise, it invokes **openssl** to create them, plus some additional files:

ca.pem	Self−signed CA certificate
ca−key.pem	CA private key
server−cert.pem	Server certificate
server−key.pem	Server private key
client−cert.pem	Client certificate
client−key.pem	Client private key

These files enable secure client connections using SSL; see Section 6.3.1, “Configuring MySQL to Use Encrypted Connections”.

4. **mysql_ssl_rsa_setup** checks the data directory for RSA files with the following names:

private_key.pem	Private member of private/public key pair
public_key.pem	Public member of private/public key pair

5. If any of these files are present, **mysql_ssl_rsa_setup** creates no RSA files. Otherwise, it invokes **openssl** to create them. These files enable secure password exchange using RSA over unencrypted connections for accounts authenticated by the sha256_password or caching_sha2_password plugin; see Section 6.4.1.2, “SHA-256 Pluggable Authentication”, and Section 6.4.1.3, “Caching SHA-2 Pluggable Authentication”.

For information about the characteristics of files created by **mysql_ssl_rsa_setup**, see Section 6.3.3.1, “Creating SSL and RSA Certificates and Keys using MySQL”.

At startup, the MySQL server automatically uses the SSL files created by **mysql_ssl_rsa_setup** to enable SSL if no explicit SSL options are given other than **−−ssl** (possibly along with **−−ssl−cipher**). If you prefer to designate the files explicitly, invoke clients with the **−−ssl−ca**, **−−ssl−cert**, and **−−ssl−key** options at startup to name the ca.pem, server−cert.pem, and server−key.pem files, respectively.

The server also automatically uses the RSA files created by **mysql_ssl_rsa_setup** to enable RSA if no explicit RSA options are given.

If the server is SSL−enabled, clients use SSL by default for the connection. To specify certificate and key files explicitly, use the **−−ssl−ca**, **−−ssl−cert**, and **−−ssl−key** options to name the ca.pem, client−cert.pem, and client−key.pem files, respectively. However, some additional client setup may be required first because **mysql_ssl_rsa_setup** by default creates those files in the data directory. The permissions for the data directory normally enable access only to the system account that runs the MySQL server, so client programs cannot use files located there. To make the files available, copy them to a directory that is readable (but *not* writable) by clients:

- For local clients, the MySQL installation directory can be used. For example, if the data directory is a subdirectory of the installation directory and your current location is the data directory, you can copy the files like this:

  ```
  cp ca.pem client−cert.pem client−key.pem ..
  ```

- For remote clients, distribute the files using a secure channel to ensure they are not tampered with during transit.

If the SSL files used for a MySQL installation have expired, you can use **mysql_ssl_rsa_setup** to create new ones:

1. Stop the server.
2. Rename or remove the existing SSL files. You may wish to make a backup of them first. (The RSA files do not expire, so you need not remove them. **mysql_ssl_rsa_setup** will see that they exist and not overwrite them.)
3. Run **mysql_ssl_rsa_setup** with the **−−datadir** option to specify where to create the new files.
4. Restart the server.

mysql_ssl_rsa_setup supports the following command−line options, which can be specified on the command line or in the [mysql_ssl_rsa_setup] and [mysqld] groups of an option file. For information about option files used by MySQL programs, see Section 4.2.2.2, “Using Option Files”.

- **−−help**, **?**

  Display a help message and exit.

- **−−datadir=***dir_name*

  The path to the directory that **mysql_ssl_rsa_setup** should check for default SSL and RSA files and in which it should create files if they are missing. The default is the compiled–in data directory.

- **––suffix=***str*

  The suffix for the Common Name attribute in X.509 certificates. The suffix value is limited to 17 characters. The default is based on the MySQL version number.

- **––uid=name**, **–v**

  The name of the user who should be the owner of any created files. The value is a user name, not a numeric user ID. In the absence of this option, files created by **mysql_ssl_rsa_setup** are owned by the user who executes it. This option is valid only if you execute the program as root on a system that supports the chown() system call.

- **––verbose**, **–v**

  Verbose mode. Produce more output about what the program does. For example, the program shows the **openssl** commands it runs, and produces output to indicate whether it skips SSL or RSA file creation because some default file already exists.

- **––version**, **–V**

  Display version information and exit.

COPYRIGHT

SEE ALSO

For more information, please refer to the MySQL Reference Manual, which may already be installed locally and which is also available online at http://dev.mysql.com/doc/.

AUTHOR

Oracle Corporation (http://dev.mysql.com/).