Cifrado de la conexión

Práctica 4 de Administración de Sistemas Gestores de Bases de Datos

19/10/2020
2ºASIR
Rafael Jiménez Cobos

Contenido

Creación de los certificados

Con OpenSSL vamos a generar una clave privada para la CA (Certificate Authority) y luego, la utilizaremos para generar el certificado x509 para la CA.

```
rajico@debian:~$ openssl genrsa 2048 > ca-key.pem
Generating RSA private key, 2048 bit long modulus (2 primes)
.............................................................+++++
.........................+++++
e is 65537 (0x010001)
rajico@debian:~$ openssl req -new -x509 -nodes -days 365000 -key ca-key.pem -out ca.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Cordoba
Locality Name (eg, city) []:Cordoba
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Rafael Jimenez
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:192.168.0.5 admin
Email Address []:
rajico@debian:~$ _
```

A continuación, generamos una clave privada y un certificado de peticiones para el servidor.

```
rajico@debian:~$ openssl req -newkey rsa:2048 -days 365000 -nodes -keyout server-key.pem -out server
-req.pem
Ignoring -days; not generating a certificate
Generating a RSA private key
........+++++
.......................+++++
writing new private key to 'server-key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Cordoba
Locality Name (eg, city) []:Cordoba
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Rafael Jimenez
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:192.168.0.5 server
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
rajico@debian:~$ _
```

Además, procesamos la llave para eliminar la contraseña. Por último, usamos la petición de certificado y la clave privada de la CA junto al certificado x509 para generar un certificado x509 firmado.

```
rajico@debian:~$ openssl rsa -in server-key.pem -out server-key.pem
writing RSA key
rajico@debian:~$ openssl x509 -req -in server-req.pem -days 365000 -CA ca.pem -CAkey ca-key.pem -set
_serial 01 -out server-cert.pem
Signature ok
subject=C = ES, ST = Cordoba, L = Cordoba, O = Rafael Jimenez, CN = 192.168.0.5 server
Getting CA Private Key
rajico@debian:~$
```

Verificamos el certificado del servidor con el certificado CA.

```
rajico@debian:~$ openssl verify -CAfile ca.pem server-cert.pem
server-cert.pem: OK
rajico@debian:~$
```

Configuración del servidor

He cambiado el usuario propietario a mysql y el grupo a root para la carpeta donde he guardado todos los ficheros.

```
rajico@debian:~$ sudo chown -Rv mysql:root /etc/mysql/certificates/
cambiado el propietario de '/etc/mysql/certificates/server-req.pem' de root:root a mysql:root
cambiado el propietario de '/etc/mysql/certificates/server-key.pem' de root:root a mysql:root
cambiado el propietario de '/etc/mysql/certificates/server-cert.pem' de root:root a mysql:root
cambiado el propietario de '/etc/mysql/certificates/ca.pem' de root:root a mysql:root
cambiado el propietario de '/etc/mysql/certificates/ca-key.pem' de root:root a mysql:root
cambiado el propietario de '/etc/mysql/certificates/' de root:root a mysql:root
rajico@debian:~$ _
```

En el fichero 50-server.conf he añadido las siguientes líneas:

```
# For generating SSL certificates you can use for example the GUI tool "tinyca".
#
#ssl-ca = /etc/mysql/cacert.pem
#ssl-cert = /etc/mysql/server-cert.pem
#ssl-key = /etc/mysql/server-key.pem

ssl-ca = /etc/mysql/certificates/ca.pem
ssl-key = /etc/mysql/certificates/server-key.pem
ssl-cert = /etc/mysql/certificates/server-cert.pem
```

Configuración del cliente

Editamos el fichero 50-mysql-clients.cnf y añadimos la línea “ssl=1”, lo que forzará al cliente a usar ssl.

```
  GNU nano 3.2              /etc/mysql/mariadb.conf.d/50-mysql-clients.cnf

#
# These groups are read by MariaDB command-line tools
# Use it for options that affect only one utility
#

[mysql]
# Default is Latin1, if you need UTF-8 set this (also in server section)
default-character-set = utf8mb4

ssl=1
```

Comprobación de la conexión

En la captura se puede apreciar que el cifrado SSL está en uso.

```
rajico@debian:~$ mysql -u rafa -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 37
Server version: 10.3.23-MariaDB-0+deb10u1-log Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> status
--------------
mysql  Ver 15.1 Distrib 10.3.23-MariaDB, for debian-linux-gnu (x86_64) using readline 5.2

Connection id:          37
Current database:
Current user:           rafa@localhost
SSL:                    Cipher in use is DHE-RSA-AES256-SHA
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server:                 MariaDB
Server version:         10.3.23-MariaDB-0+deb10u1-log Debian 10
Protocol version:       10
Connection:             Localhost via UNIX socket
Server characterset:    utf8mb4
Db     characterset:    utf8mb4
Client characterset:    utf8mb4
Conn.  characterset:    utf8mb4
UNIX socket:            /var/run/mysqld/mysqld.sock
Uptime:                 22 sec

Threads: 8  Questions: 61  Slow queries: 60  Opens: 32  Flush tables: 1  Open tables: 26  Queries pe
r second avg: 2.772
--------------

MariaDB [(none)]> _
```