Registro de Eventos

Práctica 3 de Administración de Sistemas Gestores de Bases de Datos

13/10/2020

2º ASIR
Rafael Jiménez Cobos

Contenido

He realizado la práctica con dos máquinas virtuales debido a una serie de errores que no pude solucionar a tiempo.

1. Creamos el usuario y le damos permisos

He creado al usuario practica3-2, la base de datos practica3, y dentro de ella, las tablas "tablasi" y "tablano". A continuación, le permito el acceso al usuario practica3-2 desde otro host a la tabla "tablasi" de la base de datos practica3.

```
MariaDB [(none)]> grant all on practica3.tablasi to 'practica3-2'@'192.168.0.10' identified by 'usua
rio' with grant option;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> _
```

Como se puede apreciar, al mostrar las tablas solo tenemos acceso a "tablasi".

```
MariaDB [(none)]> use practica3;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [practica3]> show tables;
+---------------------+
| Tables_in_practica3 |
+---------------------+
| tablasi             |
+---------------------+
1 row in set (0.001 sec)

MariaDB [practica3]> _
```

Para el siguiente punto, intentamos acceder a una tabla a la que no podamos, lo que dará error.

2. Auditoría de la actividad realizada

Abrimos el fichero de configuración de MariaDB y habilitamos las siguientes entradas:

```
#
# * Logging and Replication
#
# Both location gets rotated by the cronjob.
# Be aware that this log type is a performance killer.
# As of 5.1 you can enable the log at runtime!
general_log_file        = /var/log/mysql/mysql.log
general_log             = 1
#
# Error log - should be very few entries.
#
log_error = /var/log/mysql/error.log
```

Esto activará el log general y el log de errores, ficheros a los que someteremos a una auditoría.

Si mostramos el contenido del fichero mysql.log, este será el resultado:

```
201013 18:09:01     37 Connect   practica3-2@192.168.0.10 as anonymous on
                    37 Query     select @@version_comment limit 1
201013 18:09:05     37 Query     SELECT DATABASE()
                    37 Init DB   practica3
                    37 Query     show databases
                    37 Query     show tables
                    37 Field List       tablasi
201013 18:09:13     37 Query     select * from tablano
201013 18:09:16     37 Query     select * from tablasi
201013 18:09:17     37 Quit
```

Como podemos comprobar, el usuario practica3-2 se ha conectado a través del host 192.168.0.10, ha seleccionado la base de datos practica3, ha mostrado las bases de datos y las tablas. Por último, ha realizado dos consultas: una a “tablasi”, que sí dio resultado, y otra a “tablano”, que dio error debido a que ese usuario no tiene permisos suficientes.

Sin embargo, si intentamos mostrar el fichero error.log, veremos que no tiene ningún error. Lo volveremos a comprobar más adelante.

3. Habilitamos el resto de logs

Abrimos el fichero de configuración de MariaDB y habilitamos las siguientes entradas:

```
#
# Enable the slow query log to see queries with especially long duration
slow_query_log_file     = /var/log/mysql/mariadb-slow.log
long_query_time         = 10
log_slow_rate_limit     = 1000
log_slow_verbosity      = query_plan
#log-queries-not-using-indexes
#
# The following can be used as easy to replay backup logs or for replication.
# note: if you are setting up a replication slave, see README.Debian about
#       other settings you may need to change.
#server-id              = 1
log_bin                 = /var/log/mysql/mysql-bin.log
expire_logs_days        = 10
#max_binlog_size         = 100M
#binlog_do_db            = include_database_name
#binlog_ignore_db        = exclude_database_name
```

Esto habilitará los ficheros log binarios y los ficheros log de búsquedas lentas.

4. Segunda auditoría de la actividad realizada

Tras habilitar todos los logs, vamos a volver a realizar actividades en la base de datos para luego poder realizar otra auditoría.

```
MariaDB [(none)]> use mysql;
ERROR 1044 (42000): Access denied for user 'practica3-2'@'192.168.0.10' to database 'mysql'
MariaDB [(none)]> use practica3;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [practica3]> show tables;
+---------------------+
| Tables_in_practica3 |
+---------------------+
| tablasi             |
+---------------------+
1 row in set (0.001 sec)

MariaDB [practica3]> select * from tablasi;
+----+----------------------+
| id | nombre               |
+----+----------------------+
|  1 | Hola, estoy probando |
+----+----------------------+
1 row in set (0.001 sec)

MariaDB [practica3]> insert into tablasi values (2,'De momento, funciona');
Query OK, 1 row affected (0.014 sec)

MariaDB [practica3]> insert into tablano values (2,'Esto es una prueba');
ERROR 1142 (42000): INSERT command denied to user 'practica3-2'@'192.168.0.10' for table 'tablano'
MariaDB [practica3]>
```

Al mostrar el contenido del fichero binario, podemos apreciar algunos datos, como por ejemplo la base de datos utilizada y el insert que he realizado en la tabla “tablasi”:

```
BEGIN
/*!*/;
# at 370
#201013 18:27:07 server id 1  end_log_pos 495 CRC32 0x8fa0937f  Query   thread_id=37    exec_time=0e
rror_code=0
use `practica3`/*!*/;
SET TIMESTAMP=1602606427/*!*/;
SET @@session.pseudo_thread_id=37/*!*/;
SET @@session.foreign_key_checks=1, @@session.sql_auto_is_null=0, @@session.unique_checks=1, @@sessi
on.autocommit=1, @@session.check_constraint_checks=1/*!*/;
SET @@session.sql_mode=1411383296/*!*/;
SET @@session.auto_increment_increment=1, @@session.auto_increment_offset=1/*!*/;
/*!\C utf8mb4 *//*!*/;
SET @@session.character_set_client=45,@@session.collation_connection=45,@@session.collation_server=4
5/*!*/;
SET @@session.lc_time_names=0/*!*/;
SET @@session.collation_database=DEFAULT/*!*/;
insert into tablasi values (2,'De momento, funciona')
/*!*/;
# at 495
#201013 18:27:07 server id 1  end_log_pos 526 CRC32 0x2bfd3e16  Xid = 69
COMMIT/*!*/;
DELIMITER ;
# End of log file
ROLLBACK /* added by mysqlbinlog */;
/*!50003 SET COMPLETION_TYPE=@OLD_COMPLETION_TYPE*/;
/*!50530 SET @@SESSION.PSEUDO_SLAVE_MODE=0*/;
```

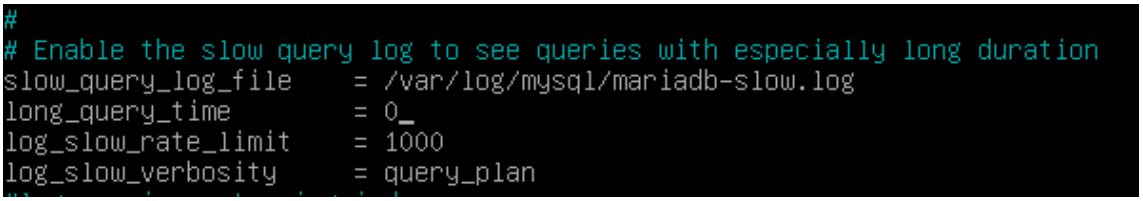
Al mostrar el contenido del fichero general, sin embargo, podemos apreciar que he obtenido más información:

```
201013 18:26:17     37 Connect  practica3-2@192.168.0.10 as anonymous on
                    37 Query    select @@version_comment limit 1
201013 18:26:22     37 Query    show databases
201013 18:26:29     37 Query    SELECT DATABASE()
                    37 Init DB  Access denied for user 'practica3-2'@'192.168.0.10' to database 'mys
ql'
201013 18:26:35     37 Query    SELECT DATABASE()
                    37 Init DB  practica3
                    37 Query    show databases
                    37 Query    show tables
                    37 Field List       tablasi
201013 18:26:41     37 Query    show tables
201013 18:26:48     37 Query    select * from tablasi
201013 18:27:07     37 Query    insert into tablasi values (2,'De momento, funciona')
201013 18:27:20     37 Query    insert into tablano values (2,'Esto es una prueba')
201013 18:28:04     37 Quit
```

De nuevo, he comprobado el contenido del fichero error.log y sigue estando vacío, a pesar de los errores cometidos.

5. Consultas lentas

Abrimos el fichero de configuración de MariaDB y bajamos el tiempo de consultas largas a 0:



Debido al tiempo tan minúsculo en el que se resuelven las consultas (por ejemplo, 0,0010 segundos), no he podido demostrar que la configuración es correcta y genera el fichero mariadb-slow.log.