Seguridad y Auditoría Informática

Auditoría de MySQL
Basada en Benchmark CIS

Auditoría de MySQL

(CIS_Oracle_MySQL_Community_Server_5.6_Benchmark_v1.1.0.pdf)

¿Qué nos interesa controlar?

1. Configuración a Nivel del Sistema Operativo
2. Instalación y Planificación
3. Permisos en el Sistema de Archivos
4. Controles Generales
5. Permisos de MySQL
6. Auditoría y Registros
7. Autenticación
8. Red
9. Replicación

1. Configuración a Nivel del Sistema Operativo

1.1. La Base de Datos debe estar en una partición diferente a la del sistema

- Se descubre el directorio de datos ejecutando:

```
MariaDB [(none)]> show variables where variable_name = 'datadir';
+---------------+-----------------+
| Variable_name | Value           |
+---------------+-----------------+
| datadir       | /var/lib/mysql/ |
+---------------+-----------------+
```

1. Configuración a Nivel del Sistema Operativo

1.1. La Base de Datos debe estar en una partición diferente a la del sistema

- Luego en el sistema operativo, sobre el directorio de datos obtenido, se ejecuta:

```
[root /]$ df -h /var/lib/mysql/
Filesystem      Size  Used Avail Use% Mounted on
overlay         801G  121G  640G  16% /
```

- Se valida que la partición no sea una del sistema.

1. Configuración a Nivel del Sistema Operativo

1.2. Utilizar una Cuenta Dedicada con Mínimos Privilegios para el Servicio MySQL

- Ejecutar el siguiente comando para verificar:

```
[root /]$ ps -ef | egrep "^mysql.*$"
mysql        183      37  0 10:26 pts/0    00:00:01 /usr/sbin/mysqld --basedir=/usr
--datadir=/var/lib/mysql --plugin-dir=/usr/lib/x86_64-linux-gnu/mariadb18/plugin --u
ser=mysql --skip-log-error --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/m
ysqld/mysqld.sock --port=3306
```

- Si no se retorna ninguna línea, es un hallazgo.
- Se asume que el usuario corriendo MySQL es ***mysql***

1. Configuración a Nivel del Sistema Operativo

1.3. Deshabilitar el historial de comandos de MySQL

- Ejecutar el siguiente comando para verificar:

```
[root /]$ find /home -name ".mysql_history"
[root /]$ find /root -name ".mysql_history"
/root/.mysql_history
[root /]$ ls -las /root/.mysql_history
4 -rw------- 1 root root 48 Mar 30 10:37 /root/.mysql_history
[root /]$
```

- Para cada archivo retornado, determinar si el archivo está enlazado simbólicamente en ***/dev/null***

1. Configuración a Nivel del Sistema Operativo

1.5. Deshabilitar el inicio de sesión interactivo

- Ejecutar el siguiente comando para verificar:

```
[root /]$ getent passwd mysql | egrep "^.*[\/bin\/false|\/sbin\/nologin]$"
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

- No obtener ningún resultado implica un hallazgo

1. Configuración a Nivel del Sistema Operativo

1.6. Verificar que 'MYSQL_PWD' no está establecida en los perfiles de usuario

- Ejecutar los siguientes comandos para verificar:

```
[root /]$ grep MYSQL_PWD /home/*/.{bashrc,profile,bash_profile}
grep: /home/*/.bashrc: No such file or directory
grep: /home/*/.profile: No such file or directory
grep: /home/*/.bash_profile: No such file or directory
[root /]$ grep MYSQL_PWD /root/.{bashrc,profile,bash_profile}
grep: /root/.bash_profile: No such file or directory
```

- No se deberían obtener resultados de estos comandos

2. Instalación y Planificación

2.1. Copias de Seguridad y Recuperación ante Desastres

2.1.1. Política de Copia de Seguridad Establecida

- Verificar si existen copias programadas con:

```
[root /]$ crontab -l
no crontab for root
```

- Si no hay resultados, no hay tareas programadas de backup

3. Permisos en Sistema de Archivos

3.1. Asegurarse que ‘datadir’ tiene Permisos Apropiados

- Se descubre el directorio de datos ejecutando:

```
MariaDB [(none)]> show variables where variable_name = 'datadir';
+---------------+-----------------+
| Variable_name | Value           |
+---------------+-----------------+
| datadir       | /var/lib/mysql/ |
+---------------+-----------------+
1 row in set (0.01 sec)
```

- Luego en el sistema operativo, sobre el directorio de datos obtenido, se ejecu

```
[root /]$ ls -l /var/lib/mysql/.. | grep mysql
drwxr-xr-x 1 mysql mysql 4096 Mar 30 10:26 mysql
```

- Verificar que los permisos correspondan al usuario ***mysql***

3. Permisos en Sistema de Archivos

3.2. Asegurar que los archivos ‘log_bin_basename’ (archivos de log binarios) tienen Permisos Apropiados

- Se descubre el directorio de datos ejecutando:

```
MariaDB [(none)]> show variables like 'log_bin_basename';
+-------------------+-------+
| Variable_name     | Value |
+-------------------+-------+
| log_bin_basename  |       |
+-------------------+-------+
1 row in set (0.00 sec)
```

- De existir archivos, se debe verificar que los permisos de cada uno sean ***660*** (rw,rw,-) para ***mysql:mysql***

3. Permisos en Sistema de Archivos

3.3. Asegurar que los archivos ‘log_error’ (archivos de log de errores) tienen Permisos Apropiados

- Se descubre el directorio de datos ejecutando:

```
MariaDB [(none)]> show variables like 'log_error';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| log_error     |       |
+---------------+-------+
1 row in set (0.00 sec)
```

- De existir archivos, se debe verificar que los permisos de cada uno sean ***660*** (rw,rw,-) para ***mysql:mysql***

3. Permisos en Sistema de Archivos

3.4. Asegurar que los archivos ‘slow_query_log’ (queries que toman +10” para correr) tienen Permisos Apropiados

- Se descubre el directorio de datos ejecutando:

```
MariaDB [(none)]> show variables like 'slow_query_log_file';
+---------------------+-------------------------+
| Variable_name       | Value                   |
+---------------------+-------------------------+
| slow_query_log_file | 40034d206d78-slow.log |
+---------------------+-------------------------+
1 row in set (0.01 sec)
```

- De existir archivos, se debe verificar que los permisos de cada uno sean ***660*** (rw,rw,-) para ***mysql:mysql***

3. Permisos en Sistema de Archivos

3.5. Asegurar que los archivos ‘relay_log_basename’ (set de logs creados por un esclavo durante la replicación) tienen Permisos Apropiados

- Se descubre el directorio de datos ejecutando:

```
MariaDB [(none)]> show variables like 'relay_log_basename';
+----------------------+-------+
| Variable_name        | Value |
+----------------------+-------+
| relay_log_basename   |       |
+----------------------+-------+
1 row in set (0.00 sec)
```

- De existir archivos, se debe verificar que los permisos de cada uno sean ***660*** (rw,rw,-) para ***mysql:mysql***

3. Permisos en Sistema de Archivos

3.6. Asegurar que el archivo ‘general_log_file’ (log general de lo que es realizado por **mysqld**) tienen Permisos Apropiados

- Se descubre el directorio de datos ejecutando:

```
MariaDB [(none)]> show variables like 'general_log_file';
+------------------+------------------+
| Variable_name    | Value            |
+------------------+------------------+
| general_log_file | 40034d206d78.log |
+------------------+------------------+
1 row in set (0.00 sec)
```

- De existir archivos, se debe verificar que los permisos de cada uno sean ***660*** (rw,rw,-) para ***mysql:mysql***

4. General

4.1. Asegurar que las Últimas Actualizaciones de Seguridad fueron aplicadas

- Se descubre la versión ejecutando:

```
MariaDB [(none)]> show variables where variable_name like 'version';
+---------------+---------------------------+
| Variable_name | Value                     |
+---------------+---------------------------+
| version       | 10.1.26-MariaDB-0+deb9u1 |
+---------------+---------------------------+
1 row in set (0.00 sec)
```

- Comparar contra la última versión estable en: https://downloads.mariadb.org/mariadb/+releases/

4. General

4.2. Asegurar que la base de datos ‘test’ no está instalada

- Se descubre el directorio de datos ejecutando:

```
MariaDB [(none)]> show databases like 'test';
Empty set (0.02 sec)
```

- Si la base de datos existiera, deberá ser removida.

4. General

4.3. Asegurar que ‘allow-suspicious-udfs’ (adjuntar funciones de librería compartidas) está establecido en ‘FALSE’

- Se descubre ejecutando el comando:

```
[root /]$ ps -ef | grep mysqld
root          37       1  0 10:26 pts/0    00:00:00 /bin/bash /usr/bin/mysqld_safe
mysql        183      37  0 10:26 pts/0    00:00:32 /usr/sbin/mysqld --basedir=/usr --datadir
=/var/lib/mysql --plugin-dir=/usr/lib/x86_64-linux-gnu/mariadb18/plugin --user=mysql --skip-l
og-error --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock --port=33
06
```

- Asegurar que --allow-suspicious-udfs no está especificado en el comando de inicio **mysqld**.

4. General

4.4. Asegurar que ‘local_infile’ (determina si los archivos ubicados en el cliente MySQL se puede cargar o seleccionar a través de LOAD DATA INFILE o SELECT local_file) está Deshabilitado

- Se descubre ejecutando la consulta:

```
MariaDB [(none)]> show variables where variable_name = 'local_infile';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| local_infile  | ON    |
+---------------+-------+
1 row in set (0.00 sec)
```

- Si el resultado fuera “**ON**”, deberá cambiarse ***local-infile*** en el archivo de configuración de MySQL.

4. General

4.5. Asegurar que mysqld no se inicia con '--skip-grant-tables' (esta opción inicia mysql sin usar el sistema de privilegios)

- Se descubre editando el archivo de configuración de mysql y validando la configuracion:

  # vim /etc/mysql/my.cnf

```
#
[client-server]

# Import all .cnf files from configuration directory
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/
```

- Buscar "skip-grant-tables" y asegurarse que esté establecido en "FALSE".

5. Permisos de MySQL

5.1. Asegurar que solamente los Usuarios Administrativos tienen Acceso Completo a la Base de Datos

- Se descubre ejecutando las consultas:

```
MariaDB [(none)]> select user, host from mysql.user where (select_priv = 'y') or (insert_priv
 = 'y') or (update_priv = 'y') or (delete_priv = 'y') or (create_priv = 'y') or (drop_priv =
'y');
+------+-----------+
| user | host      |
+------+-----------+
| root | localhost |
+------+-----------+
1 row in set (0.00 sec)

MariaDB [(none)]> select user, host from mysql.db where db = 'mysql' and ((select_priv = 'y')
 or (insert_priv = 'y') or (update_priv = 'y') or (delete_priv = 'y') or (create_priv = 'y')
or (drop_priv = 'y'));
Empty set (0.00 sec)
```

- Todos los usuarios retornados deben ser usuarios administrativos.

5. Permisos de MySQL

5.2. Asegurar que ‘file_priv’ no está establecida en ‘Y’ para Usuarios No Administrativos

- Se descubre ejecutando la consulta:

```
MariaDB [(none)]> select user, host from mysql.user where file_priv = 'y';
+------+-----------+
| user | host      |
+------+-----------+
| root | localhost |
+------+-----------+
1 row in set (0.00 sec)
```

- Todos los usuarios retornados deben ser usuarios administrativos.

5. Permisos de MySQL

5.3. Asegurar que ‘process_priv’ no está establecida en ‘Y’ para Usuarios No Administrativos

- Se descubre ejecutando la consulta:

```
MariaDB [(none)]> select user, host from mysql.user where process_priv = 'y';
+------+-----------+
| user | host      |
+------+-----------+
| root | localhost |
+------+-----------+
1 row in set (0.01 sec)
```

- Todos los usuarios retornados deben ser usuarios administrativos.

5. Permisos de MySQL

5.4. Asegurar que ‘super_priv’ no está establecida en ‘Y’ para Usuarios No Administrativos

- Se descubre ejecutando la consulta:

```
MariaDB [(none)]> select user, host from mysql.user where super_priv = 'y';
+------+-----------+
| user | host      |
+------+-----------+
| root | localhost |
+------+-----------+
1 row in set (0.00 sec)
```

- Todos los usuarios retornados deben ser usuarios administrativos.

6. Auditoría y Registros

6.1. Asegurar que ‘log_error’ no está vacío

- Se descubre ejecutando la consulta:

```
MariaDB [(none)]> show variables like 'log_error';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| log_error     |       |
+---------------+-------+
1 row in set (0.00 sec)
```

- Asegurar que el valor retornado no está vacío.

6. Auditoría y Registros

6.2. Asegurar que los archivos de registro son almacenados en una partición diferente a la del sistema.

- Se descubre ejecutando la consulta:

```
MariaDB [(none)]> select @@global.log_bin_basename;
+-----------------------------+
| @@global.log_bin_basename |
+-----------------------------+
| NULL                        |
+-----------------------------+
1 row in set (0.00 sec)
```

- Asegurar que el valor retornado no indique root (“/”), /var o /usr.

6. Auditoría y Registros

6.3. Asegurar que ‘log_warnings’ está establecida en ‘2’.

- Se descubre ejecutando la consulta:

```
MariaDB [(none)]> show global variables like 'log_warnings';
+----------------+-------+
| Variable_name | Value |
+----------------+-------+
| log_warnings  | 1     |
+----------------+-------+
1 row in set (0.00 sec)
```

- Asegurar que el valor sea igual a 2.

6. Auditoría y Registros

6.4. Asegurar el Registro de Auditoría está Habilitado

- No está incluído en la Community Edition

7. Autenticación

7.1. Asegurar que ‘old_passwords’ está establecida en ‘1’ u ‘ON’.

- Se descubre ejecutando la consulta:

```
MariaDB [(none)]> show variables where variable_name = 'old_passwords';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| old_passwords | OFF   |
+---------------+-------+
1 row in set (0.00 sec)
```

- Asegurar que el valor no sea igual a 1 u “ON”.

7. Autenticación

7.2. Asegurar que ‘secure_auth’ está establecida en ‘ON’.

- Se descubre ejecutando la consulta:

```
MariaDB [(none)]> show variables where variable_name = 'secure_auth';
+----------------+-------+
| Variable_name | Value |
+----------------+-------+
| secure_auth   | ON    |
+----------------+-------+
1 row in set (0.00 sec)
```

- Asegurar que el valor sea igual a “ON”.

7. Autenticación

7.3. Asegurar que las contraseñas no se almacenan en la Configuración Global

- Se descubre abriendo el archivo de configuración my.cnf, yendo a la sección [client] y asegurándose que no se está especificando ***password***

```
#
[client-server]

# Import all .cnf files from configuration directory
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/
```

7. Autenticación

7.4. Asegurar que ‘sql_mode’ contiene ‘NO_AUTO_CREATE_USER’

- Se descubre ejecutando las siguientes consultas:

```
MariaDB [(none)]> select @@global.sql_mode;
+--------------------------------------------+
| @@global.sql_mode                          |
+--------------------------------------------+
| NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION |
+--------------------------------------------+
1 row in set (0.00 sec)

MariaDB [(none)]> select @@session.sql_mode;
+--------------------------------------------+
| @@session.sql_mode                         |
+--------------------------------------------+
| NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION |
+--------------------------------------------+
1 row in set (0.00 sec)
```

- Asegurar que cada resultado contiene ‘NO_AUTO_CREATE_USER’.

7. Autenticación

7.5. Asegurar todas las cuentas MySQL tienen contraseña especificada.

- Se descubre ejecutando la siguiente consulta:

```
MariaDB [(none)]> select user, host from mysql.user where (plugin in('mysql_native_password',
 'mysql_old_password','') and (length(password) = 0 or password is null)) or (plugin='sha256_
password' and length(authentication_string) = 0);
Empty set (0.00 sec)
```

- No debería ser retornada ninguna cuenta si todas las cuentas tienen una contraseña especificada.

7. Autenticación

7.6. Asegurar que la Política de Contraseñas está especificada.

- Se descubre ejecutando la siguiente consulta:

```
MariaDB [(none)]> show variables like 'validate_password%';
Empty set (0.01 sec)
```

- El conjunto de resultados debería mostrar:
  - validate_password_length (14+)
  - validate_password_mixed_case_count (1+)
  - validate_password_number_count (1+)
  - validate_password_special_char_count (1+)
  - validate_password_policy (MEDIUM/STRONG)

7. Autenticación

7.6. Asegurar que la Política de Contraseñas está especificada (2).

- Las siguientes líneas deberían estar presentes en la configuración global:

  plugin-load=validate_password.so

  validate-password=FORCE_PLUS_PERMANENT

```
#
[client-server]

# Import all .cnf files from configuration directory
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/
```

8. Red

8.1. Asegurar que ‘have_ssl’ está establecida en ‘YES’

- Se descubre ejecutando las siguientes consultas

```
MariaDB [(none)]> show variables where variable_name = 'have_ssl';
+---------------+----------+
| Variable_name | Value    |
+---------------+----------+
| have_ssl      | DISABLED |
+---------------+----------+
1 row in set (0.00 sec)
```

- Asegurar que el valor retornado es “YES”

8. Red

8.2. Asegurar que ‘ssl_type’ está establecido en ‘ANY’, ‘X509’ o ‘SPECIFIED’ para todos los Usuarios Remotos

- Se descubre ejecutando la siguiente consulta:

```
MariaDB [(none)]> select user, host, ssl_type from mysql.user where not host in ('::1', '127.
0.0.1', 'localhost');
Empty set (0.01 sec)
```

- Asegurar que el valor retornado de ssl_type para cada usuario es ‘ANY’, ‘X509’ o ‘SPECIFIED’

9. Replicación

Involucra Controles para instancias con Alta Disponibilidad como:

1. Asegurar que el tráfico de replicación se realiza por medios seguros (VPN. SSL/TLS, SSH)
2. Donde se almacenan los registros maestros y esclavos.
3. Forzar que en el contexto Esclavo se verifique el certificado SSL Maestro.
4. Asegurar que los Usuarios de Replicación no tienen Privilegios Excesivos.
5. Asegurar que los Usuarios de Replicación no usan comodines para los nombres de equipo ('<user>'@'%')

¿Preguntas?

¡Muchas Gracias!