MySQL数据库审计实验

一【实验目标】

- 掌握MySQL数据库的审计方式

二【实验环境】

- Ubuntu 操作系统
- MySQL 5.6

三【实验原理】

MySQL是一个关系型数据库管理系统，由瑞典MySQL AB 公司开发，目前属于Oracle 旗下产品。MySQL 是最流行的关系型数据库管理系统之一，在 WEB 应用方面，MySQL是最好的 RDBMS (Relational Database Management System，关系数据库管理系统) 应用软件。假设这么一个情况，你是某公司mysql-DBA，某日突然公司数据库中的所有被人为删了。尽管有数据备份，但是因服务停止而造成的损失上千万，现在公司需要查出那个做删除操作的人。但是拥有数据库操作权限的人很多，如何排查，证据又在哪？这些问题都可以通过MySQL的审计功能解决。

其实mysql本身已经提供了详细的sql执行记录－general log ，但是开启它有以下几个缺点：

（1）无论sql有无语法错误，只要执行了就会记录，导致记录大量无用信息，后期的筛选有难度。

（2）sql并发量很大时，log的记录会对输入输出造成一定的影响，使数据库效率降低。

（3）日志文件很容易快速膨胀，不妥善处理会对磁盘空间造成一定影响。

为了避免以上问题，可以使用init-connect + binlog的方法进行MySQL的操作审计。

由于mysql binlog记录了所有对数据库实际修改的sql语句，及其执行时间和connection_id，但是却没有记录connection_id对应的详细用户信息。

在后期审计进行行为追踪时，根据binlog记录的行为及对应的connection-id结合之前连接日志记录进行分析，得出最后的结论。

四【实验步骤】

1、输入用户名‘anma’，密码‘123456’登录ubuntu。如图1所示

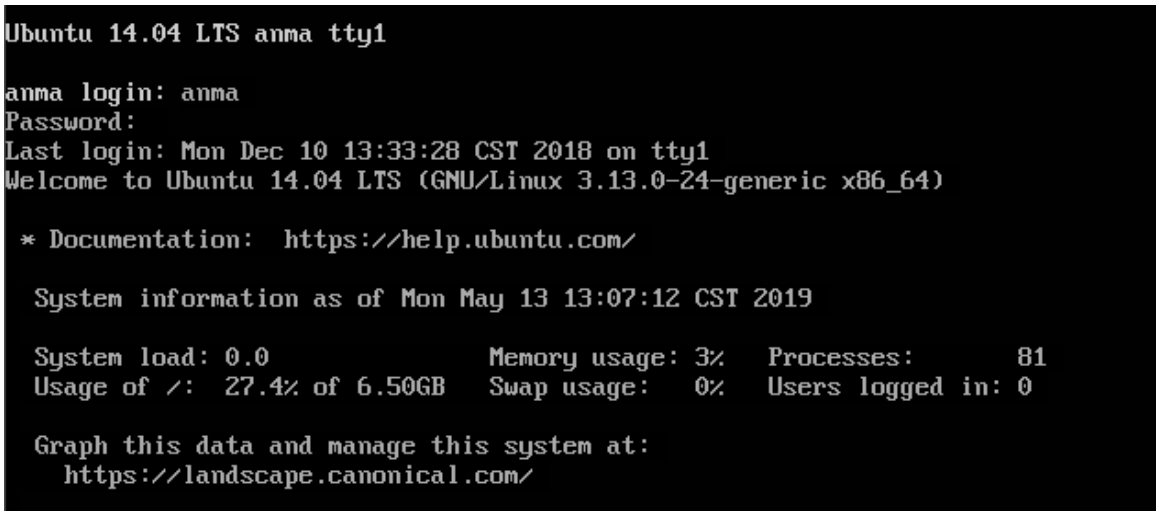

图1

2、打开终端，先输入命令“service mysqld status”查看MySQL数据库启动状态，若MySQL数据库已启动，直接进行步骤4。如图2所示

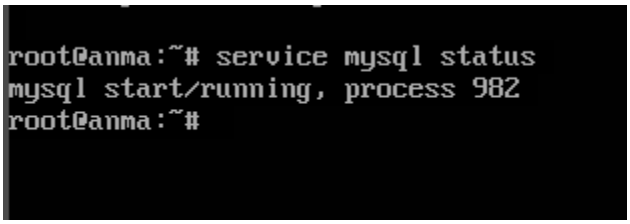

图2

3、若需要开启MySQL服务，输入命令“service mysql start”启动MySQL数据库，如图3所示

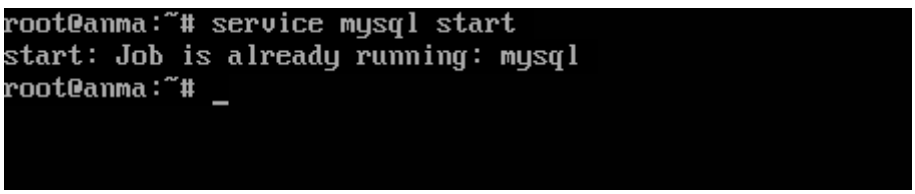

图3

4、输入“mysql -u root -p”，输入密码‘123456’启动MySQL数据库交互的命令行界面，如图4所示

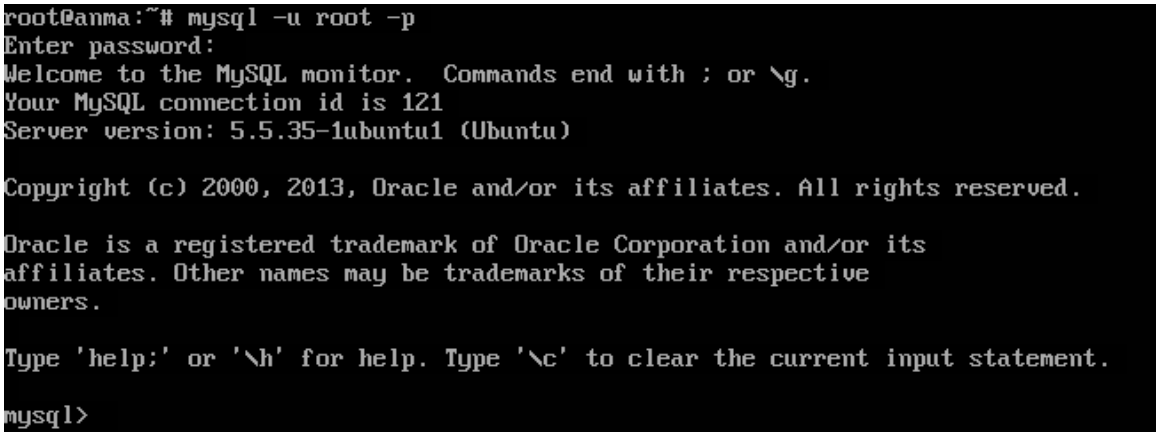

图4

5、输入“show global variables like '%general%';” 查看审计功能相关配置，可以看到包含两个变量，“general_log”为功能开启状态，当前值为“OFF”表示功能未开启。“general_log_file”变量的值为日志存储目录，当前日志存储在“/var/lib/mysql/anma.log”路径下，如图 5 所示。

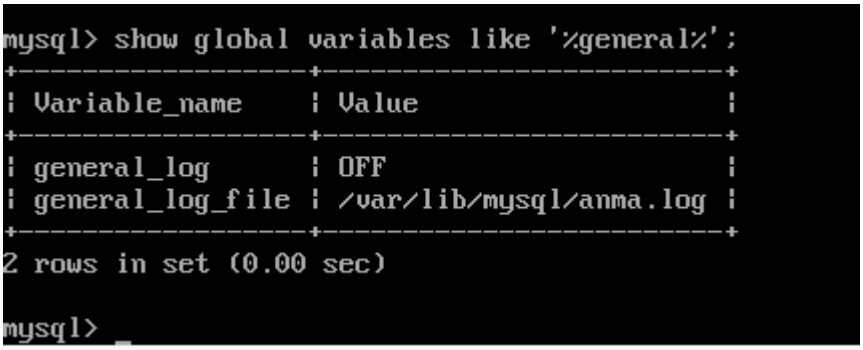

图 5

6、开启审计功能有两种方式，第一种是永久开启审计。输入“sudo vim /etc/mysql/my.cnf”编辑 MySQL 的配置文件，如图 6 所示。

图 5

7、在/etc/my.cnf 中添加下述配置

[mysqld]

general_log = on

general_log_file = /var/lib/mysql/anma.log

保存文件后重新启动 MySQL 即可开启审计功能，如图 7 所示。

```
[mysqld]
#
# * Basic Settings
#
user            = mysql
pid-file        = /var/run/mysqld/mysqld.pid
socket          = /var/run/mysqld/mysqld.sock
port            = 3306
basedir         = /usr
datadir         = /var/lib/mysql
tmpdir          = /tmp
lc-messages-dir = /usr/share/mysql
skip-external-locking
general_log     = on
general_log_file= /var/lib/mysql/anma.log_
#skip-grant-tables
# Instead of skip-networking the default is now to listen only on
-- INSERT --
```

图 7

7、另一种方式为临时开启审计功能，在 MySQL 交互式界面中输入“set global general_log = on;”开启审计功能，也可以通过更改“genral_log_file”变量的值更改日志保存路径。如图 7 所示。

```
mysql> set global general_log=on;
Query OK, 0 rows affected (0.00 sec)

mysql> show global variables like '%general%';
+------------------+--------------------------+
| Variable_name    | Value                    |
+------------------+--------------------------+
| general_log      | ON                       |
| general_log_file | /var/lib/mysql/anma.log  |
+------------------+--------------------------+
2 rows in set (0.00 sec)
```

图 7

8、查看“general_log_file”变量指定的日志文件内容，可以看到详细的 sql 执行历史记录，说明通过这种方式可以达到数据库审计的目的，如图 8 所示。

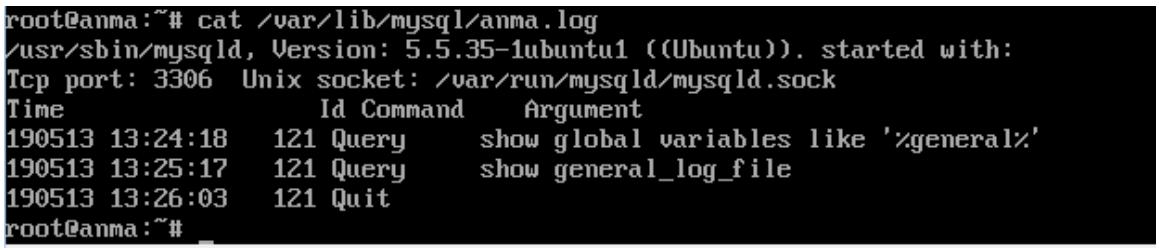

图 8

五【实验思考】

● 如何解决genral_log记录无用信息，占用io与磁盘空间过大导致数据库效率降低的问题？