MySQL5.7.16审计功能

作者:Fander

MySQL5.7企业版自带审计功能，但我们没有钱，用的是社区版。为了解决审计这个业务需求，我们可以去github上下载使用第三方审计插件

下载:

<https://bintray.com/mcafee/mysql-audit-plugin/release>

源码

<https://github.com/mcafee/mysql-audit>

教程

https://github.com/mcafee/mysql-audit/wiki

# 一、安装

1.首先看看你的mysql插件目录在哪里

root@localhost [(none)]>show variables like '%plugin\_dir%';

+---------------+------------------------------+

| Variable\_name | Value |

+---------------+------------------------------+

| plugin\_dir | /usr/local/mysql/lib/plugin/ |

+---------------+------------------------------+

1 row in set (0.01 sec)

2.解压审计插件(就用到一个so文件)，复制到插件目录

[root@vw010001135010 lib]# cp libaudit\_plugin.so /usr/local/mysql/lib/plugin/

[root@vw010001135010 lib]# cd /usr/local/mysql/lib/plugin/

[root@vw010001135010 plugin]# ll

3.不清楚要不要授权，反正我是授权了

chmod 777 libaudit\_plugin.so

4.编辑my.cnf文件

vi /etc/my.cnf

[mysqld]

plugin-load=AUDIT=libaudit\_plugin.so

audit\_validate\_checksum=OFF

audit\_offsets=7800, 7848, 3624, 4776, 456, 360, 0, 32, 64, 160, 536, 7964 #需要计算获取

audit\_json\_file=ON

audit\_json\_log\_file=/data2/shenji.json

audit\_record\_cmds=drop,alert,update,delete,insert,create

5.重启数据库，让my.cnf生效

6.登录数据库，安装插件

mysql -uroot –proot

root@localhost [(none)]>INSTALL PLUGIN AUDIT SONAME 'libaudit\_plugin.so';

审计的日志文件默认会放在数据data目录，叫mysql-audit.json

[root@vw010001135010 data]# cat mysql-audit.json

{"msg-type":"header","date":"1478084299887","audit-version":"1.0.9-585","audit-protocol-version":"1.0","hostname":"vw010001135010","mysql-version":"5.7.16-log","mysql-program":"/usr/local/mysql/bin/mysqld","mysql-socket":"/tmp/mysql3306.sock","mysql-port":"3306"}

{"msg-type":"activity","date":"1478084310786","thread-id":"2","query-id":"0","user":"","priv\_user":"","host":"localhost","ip":"","cmd":"Connect","query":"Connect"}

{"msg-type":"activity","date":"1478084310786","thread-id":"2","query-id":"0","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"Connect","query":"Connect"}

{"msg-type":"activity","date":"1478084310787","thread-id":"2","query-id":"2","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"show\_variables","objects":[{"db":"","name":"\*","obj\_type":"TABLE"},{"db":"performance\_schema","name":"session\_variables","obj\_type":"TABLE"}],"query":"show variables like '%audit%'"}

{"msg-type":"activity","date":"1478084445329","thread-id":"2","query-id":"3","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"show\_databases","objects":[{"db":"information\_schema","name":"/data/mysql/mysql3306/tmp/#sql\_4d79\_0","obj\_type":"TABLE"}],"query":"show databases"}

{"msg-type":"activity","date":"1478084478304","thread-id":"2","query-id":"4","user":"root","priv\_user":"root","host":"localhost","ip":"","cmd":"grant","query":"grant ALL on \*.\* to 'root'@'%' identified by '\*\*\*'"}

# 二、其他:

#查看审计相关的参数

root@localhost [(none)]>show variables like '%audit%';

# 三、Troubleshoot

其实可以去github上看他的wiki，里面就有讲troubleshoot

我这次安装只遇到一个问题，就是安装插件时:

root@localhost [(none)]>INSTALL PLUGIN AUDIT SONAME 'libaudit\_plugin.so';

ERROR 1123 (HY000): Can't initialize function 'AUDIT'; Plugin initialization function failed.

这个是因为这个编译好的so插件文件，不是最新的，测试好像MySQL5.7.9是没有问题，但MySQL5.7.16用这个so文件，会有问题，可以按照

<https://github.com/mcafee/mysql-audit/wiki/Troubleshooting>上Offset Extraction一节的方法获取offset值，设置到my.cnf 的audit\_offsets参数里

2016-11-03T08:58:40.169657Z 0 [ERROR] Audit Plugin: unable to open file /data2/shenji.json: Permission denied. audit file handler disabled!!