

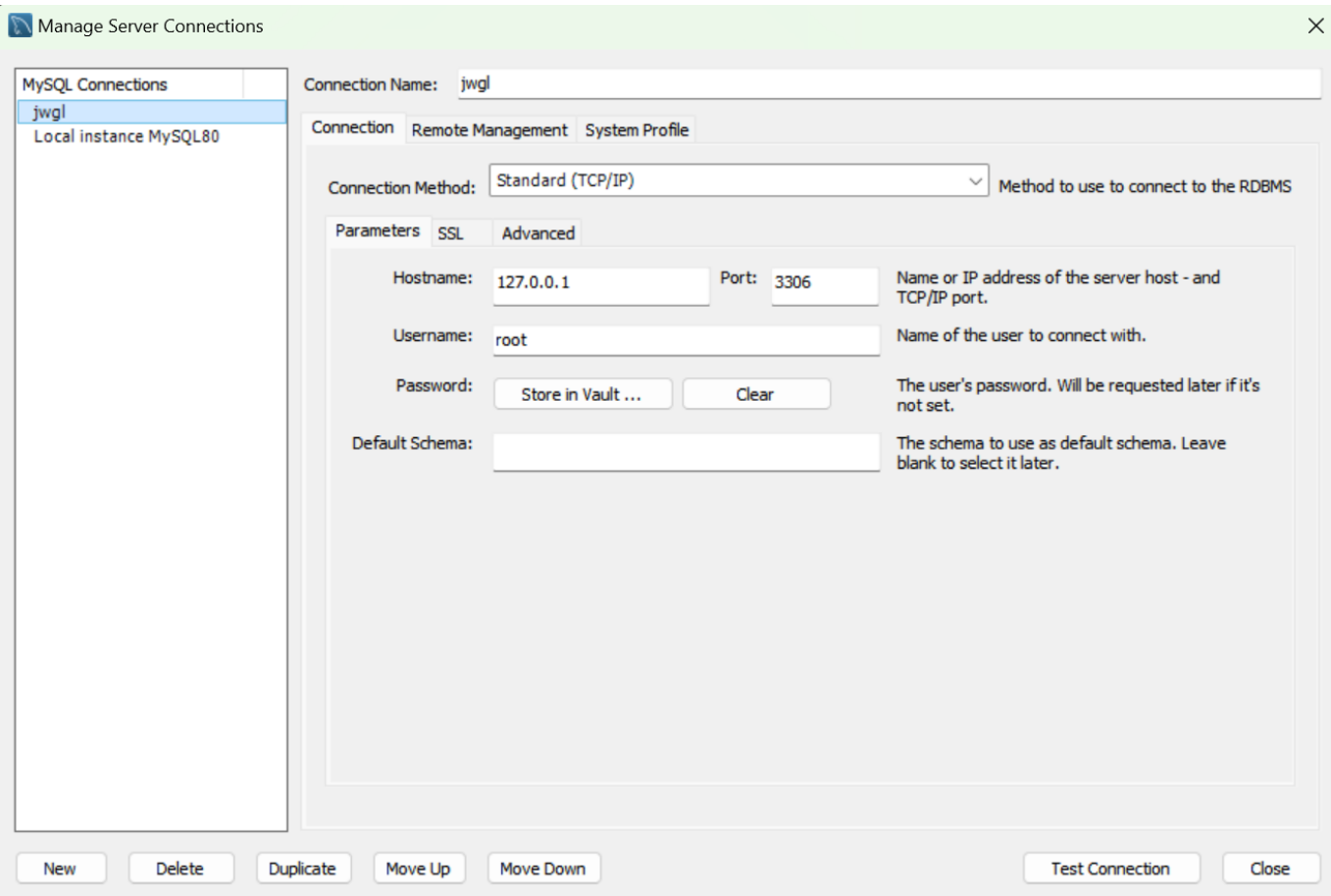
使用init-connect实现审计

一、实验目的

- 验证Mysql创建用户
- 验证Grant授权的作用
- 配置数据库审计，实现对Mysql进行审计
- 验证用户标识中host的作用

二、定义用户及授权

1.使用root登录mysql



2.创建新用户，查询用户

```
1      -- 创建新用户
2  ●    CREATE USER 'guest'@'%' IDENTIFIED BY '123456';
3      -- 查询用户
4  ●    SELECT HOST,USER,AUTHENTICATION_STRING FROM mysql.user;
```

Result Grid | Filter Rows: | Export: | Wrap Cell Content:

	HOST	USER	AUTHENTICATION_STRING
▶	%	guest	*6BB4837EB74329105EE4568DDA7DC67ED2CA...
	localhost	mysql.infoschema	\$A\$005\$THISISACOMBINATIONOFINVALIDSAL...
	localhost	mysql.session	\$A\$005\$THISISACOMBINATIONOFINVALIDSAL...
	localhost	mysql.sys	\$A\$005\$THISISACOMBINATIONOFINVALIDSAL...
	localhost	root	*F285A6DC6AA0A3313F7FF0DFB150ACE0B09...

3.将NetMusicShop的Albums表的查询权限、插入、删除授予该用户，查询用户权限

```
6      -- 授予权限
7  ●    GRANT SELECT,INSERT,DELETE
8      ON netmusicshop.Albums
9      TO guest;
10     -- 刷新
11  ●    flush privileges;
12
13     -- 查询用户权限是否符合要求
14  ●    SHOW GRANTS FOR guest;
```

Result Grid | Filter Rows: | Export: | Wrap Cell

	Grants for guest@%
▶	GRANT USAGE ON *.* TO `guest`@`%`
	GRANT SELECT, INSERT, DELETE ON `netmusic...

三、配置审计功能

1.创建审计数据库和数据表

```
-- 创建审计数据库和审计日志表
CREATE DATABASE auditlog;
use auditlog;
create table audit(
    id int not null auto_increment,
    thread_id int not null,
    login_time timestamp,
    localname varchar(50) default null,
    matchname varchar(50) default null,
    primary key (id)
);
```

2.授予guest用户插入audit表权限

```
-- 授予guest用户插入audit表权限
GRANT INSERT
ON audit
TO guest;
```

3.开启binlog

查询是否开启

33 • SHOW VARIABLES LIKE 'log_%';

Result Grid | Filter Rows: | Export: | Wrap Cell Content:

	Variable_name	Value
▶	log_bin	ON
	log_bin_basename	D:\MySQLData\MySQL\MySQL Server 8.0\Data\...
	log_bin_index	D:\MySQLData\MySQL\MySQL Server 8.0\Data\...
	log_bin_trust_function_creators	OFF
	log_bin_use_v1_row_events	OFF
	log_error	.\KING-WIN.err
	log_error_services	log_filter_internal; log_sink_internal
	log_error_suppression_list	

已开启

4.配置init-connect

(1) 配置init-connect参数

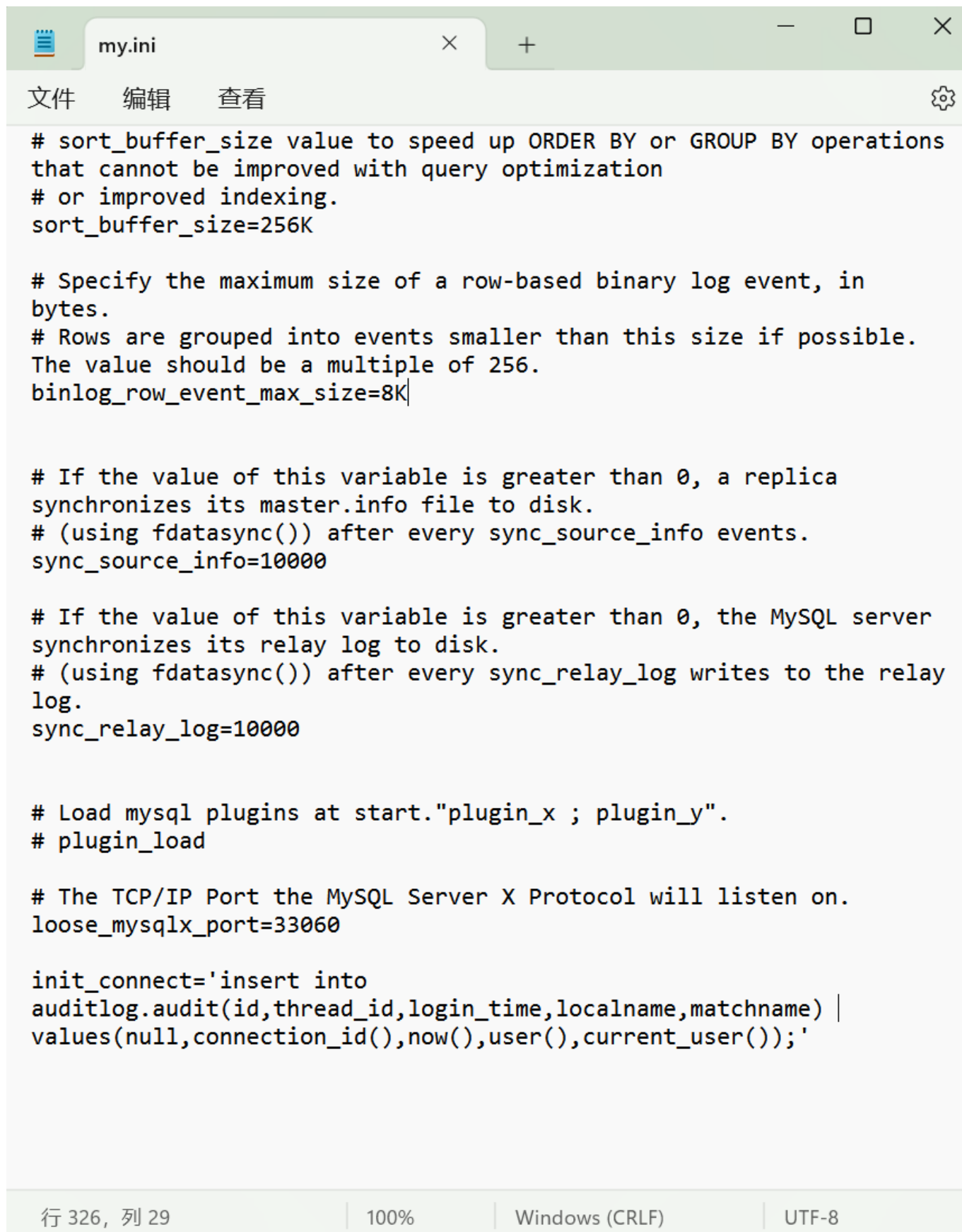
执行代码

```
set global init_connect='insert into
auditlog.audit(id,thread_id,login_time,localname,matchname)
values(null,connection_id(),now(),user(),current_user());'
```

重启mysql，查看配置是否还在，代码为

```
show variables like 'init_connect%';
```

发现重启后原先配置无效，解决方案：找到my.ini文件，在最后增加init-connect='insert into auditlog.audit(id,thread_id,login_time,localname,matchname) values(null,connection_id(),now(),user(),current_user());'即可



The screenshot shows a text editor window with the title 'my.ini'. The editor has a menu bar with '文件' (File), '编辑' (Edit), and '查看' (View), and a settings icon on the right. The main text area contains the following MySQL configuration settings:

```
# sort_buffer_size value to speed up ORDER BY or GROUP BY operations
that cannot be improved with query optimization
# or improved indexing.
sort_buffer_size=256K

# Specify the maximum size of a row-based binary log event, in
bytes.
# Rows are grouped into events smaller than this size if possible.
The value should be a multiple of 256.
binlog_row_event_max_size=8K

# If the value of this variable is greater than 0, a replica
synchronizes its master.info file to disk.
# (using fdatsync()) after every sync_source_info events.
sync_source_info=10000

# If the value of this variable is greater than 0, the MySQL server
synchronizes its relay log to disk.
# (using fdatsync()) after every sync_relay_log writes to the relay
log.
sync_relay_log=10000

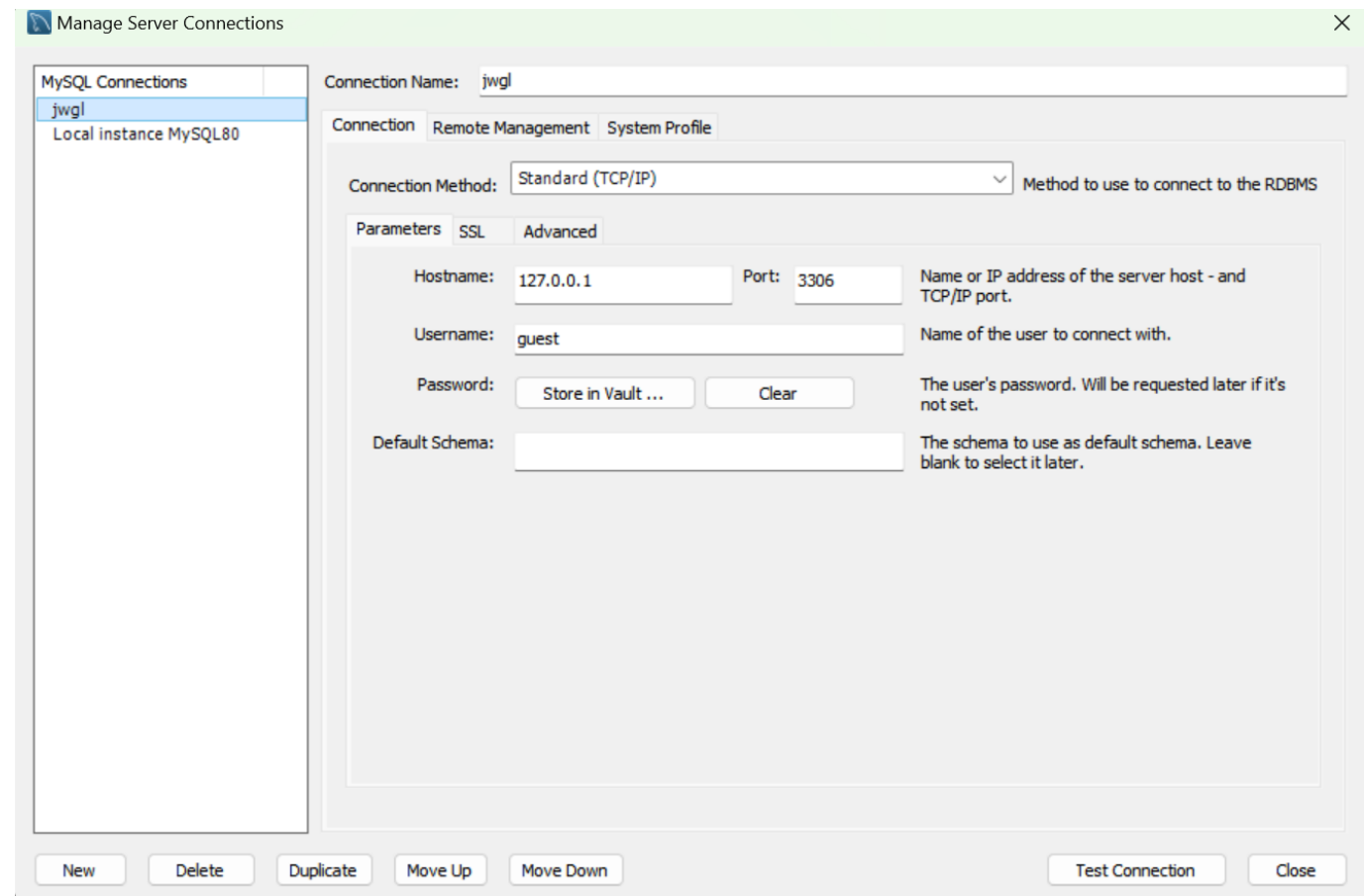
# Load mysql plugins at start."plugin_x ; plugin_y".
# plugin_load

# The TCP/IP Port the MySQL Server X Protocol will listen on.
loose_mysqlx_port=33060

init_connect='insert into
auditlog.audit(id,thread_id,login_time,localname,matchname) |
values(null,connection_id(),now(),user(),current_user());'
```

The status bar at the bottom of the editor shows '行 326, 列 29' (Line 326, Column 29), '100%' zoom, 'Windows (CRLF)' line endings, and 'UTF-8' encoding.

(2) 使用guest登录后insert一条记录，delete一条记录到Albums



(3) 使用root登录，查询audit表，查看是否有记录产生

Result Grid

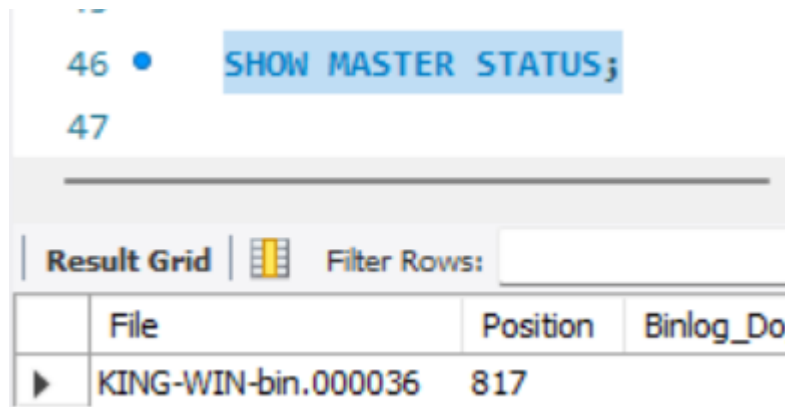
Filter Rows:

Edit:

Export/Import:

	id	thread_id	login_time	localname	matchname
▶	1	12	2023-12-05 23:56:21	guest@localhost	guest@%
	2	16	2023-12-06 00:23:06	guest@localhost	guest@%
	3	17	2023-12-06 00:23:12	guest@localhost	guest@%
	4	18	2023-12-06 00:23:12	guest@localhost	guest@%
	5	19	2023-12-06 00:25:29	guest@localhost	guest@%
	6	20	2023-12-06 00:25:29	guest@localhost	guest@%
	7	26	2023-12-06 00:31:27	guest@localhost	guest@%
	8	28	2023-12-06 00:32:54	guest@localhost	guest@%
	9	29	2023-12-06 00:32:54	guest@localhost	guest@%
✱	NULL	NULL	NULL	NULL	NULL

(4)查看正在使用的binlog日志文件



(5)验证审计能力

退出mysql · 查阅binlog

```
PS D:\MySQL\MySQL Server 8.0\bin> mysqlbinlog.exe "D:\MySQLData\MySQL\MySQL Server 8.0\Data\KING-WIN-b
in.000036" | more
# The proper term is pseudo-rolling mode, but we use this compatibility alias
# The proper term is pseudo-rolling mode, but we use this compatibility alias
# The proper term is pseudo-rolling mode, but we use this compatibility alias
# The proper term is pseudo-rolling mode, but we use this compatibility alias
# The proper term is pseudo-rolling mode, but we use this compatibility alias
#231206 17:01:49 server id 1  end_log_pos 315 CRC32 0x3331abda  Query   thread_id=11  exec_time=0
error_code=0
SET TIMESTAMP=1701853309/*!*/;
SET @@session.pseudo_thread_id=11/*!*/;
```

5.验证host的作用

update修改guest的host

```
UPDATE mysql.user
SET mysql.user.host="222.31.67.72"
WHERE mysql.user.user="guest";
flush privileges;
```

从本机再次使用guest登录 · 失败

```
PS D:\MySQL\MySQL Server 8.0\bin> mysql -u guest -p
Enter password: *****
ERROR 1045 (28000): Access denied for user 'guest'@'localhost' (using password: YES)
PS D:\MySQL\MySQL Server 8.0\bin> |
```

原因可能为：原本的host为%，表示所有IP都有连接权限，而改成其他IP之后，本机无法连接。