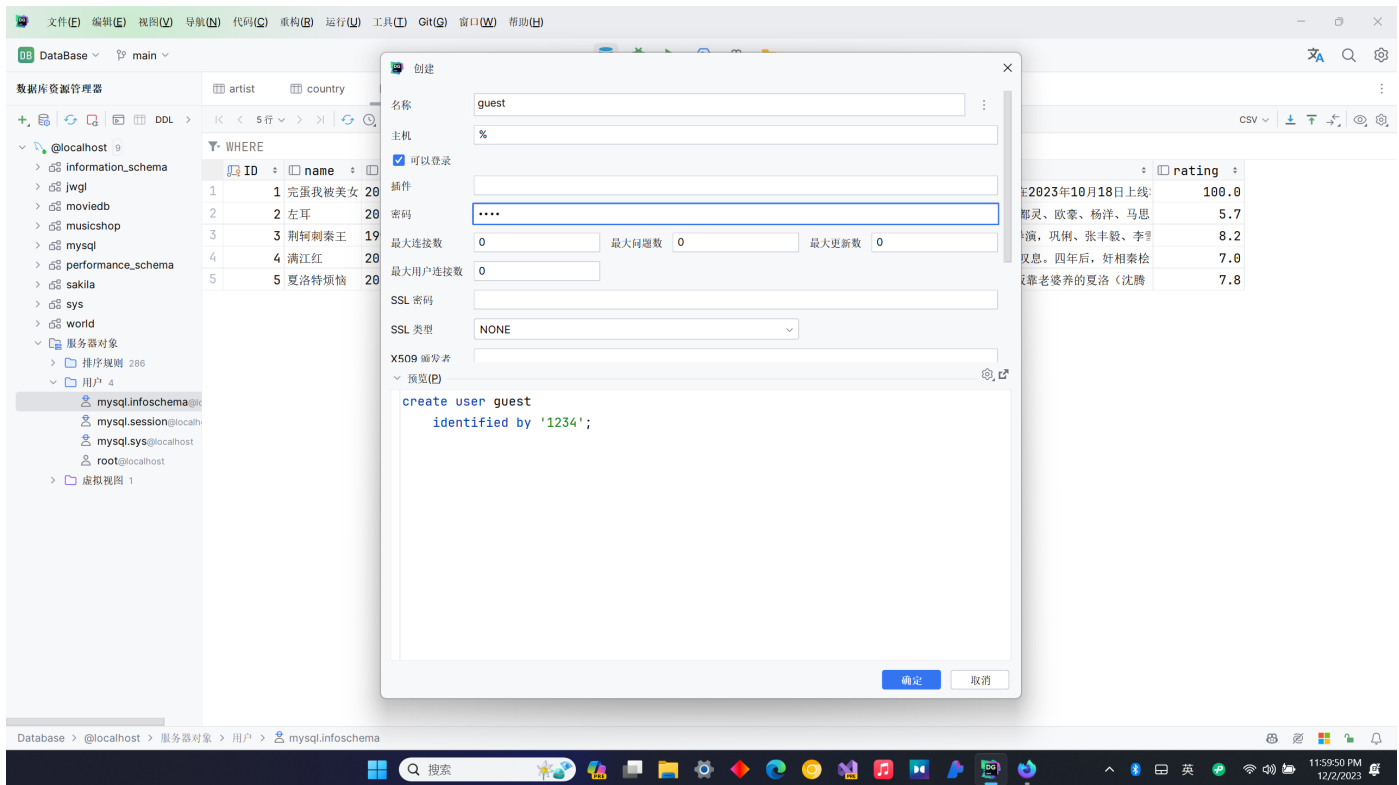


- Report
 - 过程
 - 1. 定义用户及授权
 - 尝试将NetMusicShop的Albums表的查询权限、插入、删除授予该用户
 - 查询该用户权限是否符合要求
 - 2. 配置审计功能
 - 授予guest用户插入audit表权限
 - 开启binlog
 - 配置init-connect
 - 使用guest登录后insert一条记录，delete一条记录到Albums
 - 使用root登录，查询audit表，查看是否有记录产生
 - 验证审计能力
 - 查阅binlog
 - 验证host的作用

Report

过程

1. 定义用户及授权



```
select '%','guest',authentication_string from mysql.user;
```

	%	guest	authentication_string
1	%	guest	\$A\$005\$;IDC2PENQDC3y\QCAN=]:8SUB
2	%	guest	\$A\$005\$THISISACOMBINATIONOFINVA...
3	%	guest	\$A\$005\$THISISACOMBINATIONOFINVA...
4	%	guest	\$A\$005\$THISISACOMBINATIONOFINVA...
5	%	guest	\$A\$005\$DRSzItBS.63%h0VTpNAKESCqM

尝试将NetMusicShop的Albums表的查询权限、插入、删除授予该用户

```
GRANT SELECT, INSERT, DELETE ON MusicShop.Albums TO 'guest'@'%';  
FLUSH PRIVILEGES;
```

查询该用户权限是否符合要求

```
show grants for 'guest'@'%';
```

	Grants for guest@%
1	GRANT USAGE ON *.* TO `guest`@`%`
2	GRANT INSERT ON `auditlog`.`audit` TO `guest`@`%`

2.配置审计功能

授予guest用户插入audit表权限

```
grant insert
on auditlog.audit
to 'guest'@'%';
FLUSH PRIVILEGES;
```

开启binlog

```
Warning (code 1366): Incorrect string value: '\xD6\xD0\xB9\xFA\xB1\xEA...' for column 'VARIABLE_VALUE' at row 1
MySQL localhost:33060+ ssl SQL> show variables like 'log_%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| log_bin       | ON    |
| log_bin_basename | C:\ProgramData\MySQL\MySQL Server 8.0\Data\MARS-bin |
| log_bin_index  | C:\ProgramData\MySQL\MySQL Server 8.0\Data\MARS-bin.index |
| log_bin_trust_function_creators | OFF |
| log_bin_use_v1_row_events | OFF |
| log_error      | .\MARS.err |
| log_error_services | log_filter_internal; log_sink_internal |
| log_error_suppression_list |  |
| log_error_verbosity | 2 |
| log_output      | FILE |
| log_queries_not_using_indexes | OFF |
| log_raw         | OFF |
| log_replica_updates | ON |
| log_slave_updates | ON |
| log_slow_admin_statements | OFF |
| log_slow_extra  | OFF |
| log_slow_replica_statements | OFF |
| log_slow_slave_statements | OFF |
| log_statements_unsafe_for_binlog | ON |
| log_throttle_queries_not_using_indexes | 0 |
| log_timestamps  | UTC   |
+-----+-----+
21 rows in set, 1 warning (0.0018 sec)
Warning (code 1366): Incorrect string value: '\xD6\xD0\xB9\xFA\xB1\xEA...' for column 'VARIABLE_VALUE' at row 1
MySQL localhost:33060+ ssl SQL>
```

配置init-connect

```
MySQL Shell 8.0.34

Copyright (c) 2016, 2023, Oracle and/or its affiliates.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Type '\help' or '\?' for help; '\quit' to exit.
MySQL JS> \connect root@localhost
Creating a session to 'root@localhost'
Fetching schema names for auto-completion... Press ^C to stop.
Your MySQL connection id is 15 (X protocol)
Server version: 8.0.34 MySQL Community Server - GPL
No default schema selected; type \use <schema> to set one.
MySQL localhost:33060+ ssl JS> \sql
Switching to SQL mode... Commands end with ;
Fetching global names for auto-completion... Press ^C to stop.
MySQL localhost:33060+ ssl SQL> show variables like 'init_connect%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| init_connect  | insert into auditlog.audit(id,thread_id,login_time,localname,matchname) values(null,connection_id(),now(),user(),current_user()); |
+-----+-----+
1 row in set, 1 warning (0.0015 sec)
Warning (code 1366): Incorrect string value: '\xD6\xD0\xB9\xFA\xB1\xEA...' for column 'VARIABLE_VALUE' at row 1
MySQL localhost:33060+ ssl SQL>
```

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

使用root登录，查询audit表，查看是否有记录产生

```
MySQL Shell
Your MySQL connection id is 30 (X protocol)
Server version: 8.0.34 MySQL Community Server - GPL
No default schema selected; type \use <schema> to set one.
MySQL localhost:33060+ ssl SQL> show variables like 'init_connect%';
+-----+
| Variable_name | Value |
+-----+
| init_connect | insert into auditlog.audit(id,thread_id,login_time,localname,matchname) values(null,connection_id(),no
w(),user(),current_user()); |
+-----+
1 row in set, 1 warning (0.0017 sec)
Warning (code 1366): Incorrect string value: '\xD6\xD0\xB9\xFA\xB1\xEA...' for column 'VARIABLE_VALUE' at row 1
MySQL localhost:33060+ ssl SQL> select *
-> from auditlog.audit;
+-----+-----+-----+-----+-----+
| id | thread_id | login_time | localname | matchname |
+-----+-----+-----+-----+-----+
| 1 | 21 | 2023-12-03 01:10:13 | guest@localhost | guest% |
| 2 | 22 | 2023-12-03 01:10:22 | guest@localhost | guest% |
| 3 | 23 | 2023-12-03 01:10:22 | guest@localhost | guest% |
| 4 | 24 | 2023-12-03 01:10:25 | guest@localhost | guest% |
| 5 | 25 | 2023-12-03 01:10:58 | guest@localhost | guest% |
| 6 | 26 | 2023-12-03 01:11:09 | guest@localhost | guest% |
+-----+-----+-----+-----+-----+
6 rows in set (0.0011 sec)
MySQL localhost:33060+ ssl SQL>
```

验证审计能力

查阅binlog

```
(5) 第五步 验证审计能力
管理员: Windows PowerShell
# The proper term is pseudo_replica_mode, but we use this compatibility alias
# to make the statement usable on server versions 8.0.24 and older.
/*!50530 SET @@SESSION.PSEUDO_SLAVE_MODE=1*/;
/*!50003 SET @@OLD_COMPLETION_TYPE=@@COMPLETION_TYPE,COMPLETION_TYPE=0*/;
DELIMITER /*!*/;
# at 4
#231202 23:57:22 server id 1 end_log_pos 126 CRC32 0xffae65e2 Start: binlog v 4, server v 8.0.34 created 231202 23:57:
22 at startup
# Warning: this binlog is either in use or was not closed properly.
ROLLBACK/*!*/;
BINLOG '
41NrZQ8BAAAAGegAAAH4AAAAABAAQAOC4wLjM0AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAADiU2t1EwANAAGAAAAABAAEAAAAAYgAEGggAAAAICAgCAAAACgoKKioAEjQA
CigAAeJlrV8=
'/*!*/;
# at 126
#231202 23:57:22 server id 1 end_log_pos 157 CRC32 0xf6c714f1 Previous-GTIDs
# [empty]
# at 157
#231203 00:01:01 server id 1 end_log_pos 236 CRC32 0xdb94bf0c Anonymous_GTID last_committed=0 sequence_number=
1 rbr_only=no original_committed_timestamp=1701532861647234 immediate_commit_timestamp=1701532861647234
transaction_length=315
# original_commit_timestamp=1701532861647234 (2023-12-03 00:01:01.647234 中国标准时间)
# immediate_commit_timestamp=1701532861647234 (2023-12-03 00:01:01.647234 中国标准时间)
/*!80001 SET @@session.original_commit_timestamp=1701532861647234*//*!*/;
/*!80014 SET @@session.original_server_version=80034*//*!*/;
/*!80014 SET @@session.immediate_server_version=80034*//*!*/;
SET @@SESSION.GTID_NEXT= 'ANONYMOUS'/*!*/;
# at 236
-- More -- |
```

验证host的作用

```
UPDATE mysql.user
SET Host = '222.31.67.72'
WHERE User = 'guest';
FLUSH PRIVILEGES;
```



```
MySQL Shell 8.0.34

Copyright (c) 2016, 2023, Oracle and/or its affiliates.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Type '\help' or '? for help; '\quit' to exit.
MySQL JS > \sql
Switching to SQL mode... Commands end with ;
MySQL SQL > \connect guest@222.31.67.72
Creating a session to 'guest@222.31.67.72'
Please provide the password for 'guest@222.31.67.72': ****
MySQL Error 2003 (HY000): Can't connect to MySQL server on '222.31.67.72:3306' (10060)
MySQL SQL > |
```

尝试从本机（通常是localhost或127.0.0.1）进行连接。MySQL的用户权限系统是基于用户名和主机名的，所以如果你的host字段不匹配你尝试连接的主机，那么连接将不会成功。