

Affected version: mysql-5.7.24

We are observing a situation where all 1024 of MySQL's client threads are waiting on a lock, resulting in MySQL rejecting further clients. A strack trace of such a thread is below:

```
Thread 539 (Thread 0x7f00347e0700 (LWP 19419)):  
#0 0x00007f005ce814ed in __lll_lock_wait () from /lib64/  
libpthread.so.0  
#1 0x00007f005ce7ce01 in _L_lock_1093 () from /lib64/  
libpthread.so.0  
#2 0x00007f005ce7cda2 in pthread_mutex_lock () from /lib64/  
libpthread.so.0  
#3 0x0000000000ca6490 in native_mutex_lock (mutex=<optimized  
out>) at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/include/thr_mutex.h:84  
#4 my_mutex_lock (mp=<optimized out>) at /export/home/pb2/  
build/sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/include/thr_mutex.h:182  
#5 inline_mysql_mutex_lock (src_file=0x16731c0 "/export/home/  
pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/sql/sql_class.cc", src_line=1792,  
that=<optimized out>) at /export/home/pb2/build/  
sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/include/mysql/psi/mysql_thread.h:730  
#6 THD::release_resources (this=this@entry=0x104fc000) at /  
export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/  
mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_class.cc:1792  
#7 0x0000000000db07de in handle_connection  
(arg=arg@entry=0xfb2fae0) at /export/home/pb2/build/  
sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/sql/conn_handler/  
connection_handler_per_thread.cc:308  
#8 0x0000000001296ec4 in pfs_spawn_thread (arg=0xffb9880) at /  
export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/  
mysqlcom-5.7.24/mysqlcom-5.7.24/storage/perfschema/pfs.cc:2190  
#9 0x00007f005ce7add5 in start_thread () from /lib64/  
libpthread.so.0  
#10 0x00007f005b933ead in clone () from /lib64/libc.so.6
```

Investigation determined that this is a deadlock that originates from 3 threads that are engaged in a 3-way deadlock. Below is a table that describes the deadlock:



```
mysqlcom-5.7.24/include/thr_cond.h:140  
#5 my_cond_wait (mp=0x8206528, cond=0x82065f0) at /export/home/  
pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/include/thr_cond.h:195  
#6 inline_mysql_cond_wait (src_file=0x17079c0 "/export/home/  
pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/sql/rpl_slave.cc", src_line=1940,  
mutex=0x8206528, that=0x82065f0)  
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/include/mysql/psi/  
mysql_thread.h:1199  
#7 start_slave_thread (thread_key=<optimized out>,  
h_func=h_func@entry=0xee2f90 <handle_slave_sql(void*)>,  
start_lock=0x0, cond_lock=cond_lock@entry=0x8206528,  
start_cond=0x82065f0,  
    slave_running=<optimized out>, slave_run_id=0x82066e8,  
mi=mi@entry=0x813c000) at /export/home/pb2/build/  
sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/sql/rpl_slave.cc:1940  
#8 0x00000000ed90fb in start_slave_threads  
(need_lock_slave=need_lock_slave@entry=false,  
wait_for_start=wait_for_start@entry=true, mi=mi@entry=0x813c000,  
thread_mask=<optimized out>)  
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/rpl_slave.cc:2047  
#9 0x00000000ede705 in start_slave (thd=<optimized out>,  
connection_param=<optimized out>, master_param=<optimized out>,  
thread_mask_input=<optimized out>, mi=0x813c000,  
set_mts_settings=<optimized out>)  
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/rpl_slave.cc:10123  
#10 0x00000000edf02f in start_slave (thd=thd@entry=0x978c000)  
at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/  
mysqlcom-5.7.24/mysqlcom-5.7.24/sql/rpl_slave.cc:534  
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>  
#11 0x00000000edflca in start_slave_cmd  
(thd=thd@entry=0x978c000) at /export/home/pb2/build/  
sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/sql/rpl_slave.cc:685  
#12 0x00000000ce7e01 in mysql_execute_command  
(thd=thd@entry=0x978c000, first_level=first_level@entry=true)  
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_parse.cc:3442  
#13 0x00000000cebfd5 in mysql_parse (thd=thd@entry=0x978c000,  
parser_state=parser_state@entry=0x7f003be35480)  
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_parse.cc:5570  
#14 0x00000000cecb3d in dispatch command
```





```
[Switching thread 984 (Thread 0x7f003afc6700 (LWP 14000))]  
#0  0x00007f005ce7e0b4 in pthread_rwlock_rdlock () from /lib64/  
libpthread.so.0  
(gdb) bt  
#0  0x00007f005ce7e0b4 in pthread_rwlock_rdlock () from /lib64/  
libpthread.so.0  
#1  0x000000000007be5b2 in native_rw_rdlock (rwp=0x31a4058) at /  
export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/  
mysqlcom-5.7.24/mysqlcom-5.7.24/include/thr_rwlock.h:79  
#2  inline_mysql_rwlock_rdlock (src_line=471, src_file=0x14526e0  
"/export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/  
mysqlcom-5.7.24/mysqlcom-5.7.24/sql/rpl_gtid.h", that=0x31a4058)  
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/include/mysql/psi/  
mysql_thread.h:906  
#3  rdlock (this=0x31a4050) at /export/home/pb2/build/  
sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/sql/rpl_gtid.h:471  
#4  rdlock (this=<optimized out>) at /export/home/pb2/build/  
sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/sql/rpl_msr.h:374  
#5  show_heartbeat_period (thd=<optimized out>,  
var=0x7f003afc3440, buff=0x7f003afc3490 "439") at /export/home/  
pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/sql/mysqld.cc:6313  
#6  0x0000000000d3ae5f in show_status_array  
(thd=thd@entry=0xcf22000, wild=wild@entry=0x0,  
variables=0x32f6ac8, value_type=value_type@entry=OPT_GLOBAL,  
status_var=status_var@entry=0x7f003afc3980,  
    prefix=prefix@entry=0xl673770 "", tl=tl@entry=0x8593e98,  
ucase_names=false, cond=cond@entry=0x0)  
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_show.cc:3042  
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>  
#7  0x0000000000d42480 in fill_status  
(thd=0xcf22000, tables=0x8593e98, cond=0x0) at /export/home/pb2/  
build/sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/  
mysqlcom-5.7.24/sql/sql_show.cc:7442  
#8  0x0000000000d2f9ac in do_fill_table  
(thd=thd@entry=0xcf22000, table_list=table_list@entry=0x8593e98,  
qep_tab=qep_tab@entry=0xa30c7b0)  
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_show.cc:8149  
#9  0x0000000000d412cc in get_schema_tables_result  
(join=join@entry=0xa30c0d0,  
executed_place=executed_place@entry=PROCESSED_BY_JOIN_EXEC)  
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/  
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_show.cc:8279
```

```

#10 0x0000000000d2552d in JOIN::prepare_result
(this=this@entry=0xa30c0d0) at /export/home/pb2/build/
sb_0-30854123-1538633017.52/rpm/BUILD/mysqlcom-5.7.24/
mysqlcom-5.7.24/sql/sql_select.cc:909
#11 0x0000000000cb6cbf in JOIN::exec (this=0xa30c0d0) at /
export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/
mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_executor.cc:124
#12 0x0000000000d25e7d in handle_query (thd=thd@entry=0xcf22000,
lex=lex@entry=0xcf24168, result=result@entry=0x8594808,
added_options=added_options@entry=0,
removed_options=removed_options@entry=0)
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_select.cc:184
#13 0x000000000078f3d4 in execute_sqlcom_select
(thd=thd@entry=0xcf22000, all_tables=<optimized out>)
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_parse.cc:5144
#14 0x0000000000ce8f5b in mysql_execute_command
(thd=thd@entry=0xcf22000, first_level=first_level@entry=true)
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_parse.cc:2769
#15 0x0000000000cebfdd in mysql_parse (thd=thd@entry=0xcf22000,
parser_state=parser_state@entry=0x7f003afc5480)
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_parse.cc:5570
#16 0x0000000000cecb3d in dispatch_command
(thd=thd@entry=0xcf22000,
com_data=com_data@entry=0x7f003afc5d20, command=COM_QUERY)
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_parse.cc:1484
#17 0x0000000000cee53f in do_command (thd=thd@entry=0xcf22000)
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/
mysqlcom-5.7.24/mysqlcom-5.7.24/sql/sql_parse.cc:1025
#18 0x0000000000db09c8 in handle_connection
(arg=arg@entry=0xceb04e0)
    at /export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/
BUILD/mysqlcom-5.7.24/mysqlcom-5.7.24/sql/conn_handler/
connection_handler_per_thread.cc:300
#19 0x0000000001296ec4 in pfs_spawn_thread (arg=0xa6235b0) at /
export/home/pb2/build/sb_0-30854123-1538633017.52/rpm/BUILD/
mysqlcom-5.7.24/mysqlcom-5.7.24/storage/perfschema/pfs.cc:2190
#20 0x00007f005ce7add5 in start_thread () from /lib64/
libpthread.so.0
#21 0x00007f005b933ead in clone () from /lib64/libc.so.6

```

Required mutex is locked by thread 9775:

```
(gdb) print *(pthread_rwlock_t*)0x31a4058
```

```
$3 = {__data = {__lock = 0, __nr_readers = 0, __readers_wakeup = 0, __writer_wakeup = 0, __nr_readers_queued = 2, __nr_writers_queued = 0, __writer = 9775, __shared = 0, __pad1 = 0, __pad2 = 0, __flags = 0},  
      __size = '\000' <repeats 16 times>,  
      "\002\000\000\000\000\000\000\000/&", '\000' <repeats 29 times>,  
      __align = 0}  
(gdb)
```

## CONCLUSION:

```
THREAD 9775  
MUTEX 0x31a4060 GRANTED AT: sql/rpl_slave.cc: 664  
channel_map.wrlock();  
  
MUTEX 0x8206528 ATTEMPTED AT: sql/rpl_slave.cc: 1940  
mysql_cond_wait(start_cond, cond_lock);  
  
-----  
--  
  
THREAD 16089  
LOCK 0x8206528 GRANTED AT: sql/rpl_slave.cc: 7557  
mysql_mutex_lock(&rli->run_lock);  
  
LOCK 0x1fdff90 ATTEMPTED AT: sql/sql_class.cc: 1792  
mysql_mutex_lock(&LOCK_status);  
  
-----  
--  
  
THREAD 9775  
LOCK 0x1fdff90 GRANTED AT sql/sql_show.cc: 7434  
mysql_mutex_lock(&LOCK_status);  
  
LOCK 0x31a4060 ATTEMPTED AT sql/mysqld.cc: 6313  
channel_map.rdlock();
```

This appears to be a rare race condition and as such cannot be reproduced with ease, but the above analysis demonstrates that three threads can run in a sequence that will cause this deadlock, due to the out-of-order acquisition of the locks.