I was testing a project I have and qgis (master) froze. 
strace shows it hanging in: futex(0x45b791c, FUTEX_WAIT_PRIVATE, 1, NULL

gdb shows this backtrace:

(gdb) bt
#0  pthread_cond_wait@GLIBC_2.3.2 () at ../nptl/sysdeps/unix/sysv/linux/x86_64/pthread_cond_wait.S:185
#1  0x00007fc914e816 in QWaitCondition::wait(QMutex*, unsigned long) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#2  0x00007fc914b8e4 in QFutureInterfaceBase::waitForFinished() () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#3  0x00007fc914b60daf in QgsMapRendererParallelJob::cancel (this=0x522b360) at
    /usr/src/qgis/qgis/src/core/qgsmaprendererparalleljob.cpp:92
#4  0x00007fc914f2f9f in QgsMapCanvas::stopRendering (this=0x1f3c3c0) at
    /usr/src/qgis/qgis/src/gui/qgsmapcanvas.cpp:770
#5  0x00007fc914f2f9f in QgsMapCanvas::refreshMap (this=0x1f3c3c0) at /usr/src/qgis/qgis/src/gui/qgsmapcanvas.cpp:649
#6  0x00007fc914f2f9f in QgsMapCanvas::qt_static_metacall (_o=0x1f3c3c0, _c=QMetaObject::InvokeMetaMethod, _id=40,
    _a=0x7fff919dca60)
    at /usr/src/qgis/build/src/gui/moc_qgsmapcanvas.cxx:166
#7  0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#8  0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#9  0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#10 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#11 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#12 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#13 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#14 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#15 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#16 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#17 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#18 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#19 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#20 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#21 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#22 0x00007fc914f2f9f in QMetaObject::activate(QObject*, QMetaObject const*, int, void**) () from
    /usr/lib/x86_64-linux-gnu/libQtCore.so.4
All I did to trigger it was changing visibility of a couple of layers and navigate. I'm tagging it as "Causes crash or corruption" as you can't exit from a deadlock w/out killing the process.

---

**History**

**#1 - 2015-02-19 04:32 AM - Martin Dobias**

What about the worker threads - what were they waiting for?

**#2 - 2015-02-19 04:51 AM - Jürgen Fischer**

Martin Dobias wrote:

> What about the worker threads - what were they waiting for?

Good question :)

- **<strk> master branch**
- **<strk> Process 10380 attached**
- **<strk> futex(0x45b791c, FUTEX_WAIT_PRIVATE, 1, NULL**
- **<strk> ^^^ that's coming from strace, it's stuck there, deadlock !**
- **<jef> strk: where?**
- **<strk> jef: #12228**

---

**#3 - 2015-02-19 04:57 AM - Jürgen Fischer**

BTW thread apply all bt in gdb produces backtraces for all threads.

---

**#4 - 2015-02-19 04:59 AM - Jürgen Fischer**

- **Tag set to mtr**

---

**#5 - 2015-05-10 01:03 AM - Giovanni Manghi**

- **Target version changed from Version 2.8 to Version 2.8.2**

---

**#6 - 2015-05-14 03:02 AM - Giovanni Manghi**

- **Target version changed from Version 2.8.2 to Version 2.10**

---

**#7 - 2015-05-27 11:33 PM - Andreas Neumann**
Strk - what are the data sources? Postgis, perhaps?

I have similar issues with Postgis connections and MTR if my number of cores for rendering goes beyond 2-3. If I limit the nr of cores to 2, the problem disappears.

I would really like to see a fix for this. I have not created a bug report, because it was very hard to reproduce and apparently shows up on my Windows version more often than on Linux. But that is perhaps because on Linux my Postgis connections are local, whereas on Windows the connections are remote.

#8 - 2015-05-28 12:59 AM - Giovanni Manghi
- Target version changed from Version 2.10 to Future Release - High Priority

Hi Andreas,

I would really like to see a fix for this. I have not created a bug report, because it was very hard to reproduce and apparently shows up on my Windows version more often than on Linux. But that is perhaps because on Linux my Postgis connections are local, whereas on Windows the connections are remote.

it seems there are different tickets with issues apparently caused by mtr, them main seems to be this #11141

#9 - 2015-05-28 02:27 AM - Sandro Santilli

I don't remember what the datasource was. Yes, debugging threading issues is an hell (thus the name of the valgrind tool, I guess)

#10 - 2015-05-28 03:14 AM - Jürgen Fischer
- Status changed from Open to Feedback

not reproduceable

#11 - 2015-06-14 01:46 AM - Giovanni Manghi
- Status changed from Feedback to Closed
- Resolution set to not reproducible

closing for lack of feedback.

#12 - 2015-07-31 03:19 AM - Sandro Santilli
- Status changed from Closed to Reopened
- Resolution deleted (not reproducible)

I've just reproduced this, in 2.8.3 (lacking an entry in the "Affected version" pull-down menu).

What I did:
1) Load the POSTGIS_SRC/topology/test/invalid_topology.sql script into a topology-enabled PostgreSQL database
2) Load the "invalid_topology" schema in qgis via DBManager (select the schema, pick Topology Viewer from the "schema" menu)
What I got: a blocked GUI

The backtrace:

(gdb) bt

#0  pthread_cond_wait@@GLIBC_2.3.2 () at ../nptl/sysdeps/unix/sysv/linux/x86_64/pthread_cond_wait.S:185
#1  0x000078953cc816 in QWaitCondition::wait(QMutex*, unsigned long) () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#2  0x000078953bf88e4 in QFutureInterfaceBase::waitForFinished() () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#3  0x00007895686281 in QgsMapRendererParallelJob::cancel (this=0x57c2ba0) at /usr/src/qgis/qgis-2.8/src/core/qgsmaprendererparalleljob.cpp:92
#4  0x000078954d46219 in QgsMapCanvas::stopRendering (this=0x26c7680) at /usr/src/qgis/qgis-2.8/src/gui/qgsmapcanvas.cpp:778
#5  0x000078954d5012 in QgsMapCanvas::refreshMap (this=0x26c7680) at /usr/src/qgis/qgis-2.8/src/gui/qgsmapcanvas.cpp:657

#13 - 2015-07-31 03:23 AM - Sandro Santilli

wioth  thread apply all bt
, as suggested by Jurgen:

(gdb) thread apply all bt

Thread 13 (Thread 0x789394ee700 (LWP 24245)):
#0  0x000078950fd12d in poll () at ../sysdeps/unix/syscall-template.S:81
#1  0x00007894ed81f4 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#2  0x00007894ed8230a in g_main_loop_run () from /lib/x86_64-linux-gnu/libgio-2.0.so.0
#3  0x00007894ed8336 in ?? () from /lib/x86_64-linux-gnu/libgio-2.0.so.0
#4  0x00007894eda6f05 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#5  0x00007894e383182 in start_thread (arg=0x789394ee700) at pthread_create.c:312
#6  0x000078950fd47d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:111

Thread 12 (Thread 0x78938ced700 (LWP 24246)):
#0  0x000078950fd12d in poll () at ../sysdeps/unix/syscall-template.S:81
#1  0x00007894ed81f4 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#2  0x00007894ed820ec in g_main_context_iteration () from /lib/x86_64-linux-gnu/libgio-2.0.so.0
#3  0x00007894eda6f05 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#4  0x00007894eda6f05 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#5  0x00007894e383182 in start_thread (arg=0x78938ced700) at pthread_create.c:312
#6  0x000078950fd47d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:111

Thread 11 (Thread 0x78931333700 (LWP 24253)):
#0  0x000078950fd12d in poll () at ../sysdeps/unix/syscall-template.S:81
#1  0x00007894ed81f4 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#2  0x00007894ed820ec in g_main_context_iteration () from /lib/x86_64-linux-gnu/libgio-2.0.so.0
#3  0x00007894eda6f05 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#4  0x00007894eda6f05 in ?? () from /lib/x86_64-linux-gnu/libglib-2.0.so.0
#5  0x00007894e383182 in start_thread (arg=0x78931333700) at pthread_create.c:312
#6  0x000078950fd47d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:111

Thread 10 (Thread 0x78925296700 (LWP 24254)):
#0  0x000078950fd12d in poll () at ../sysdeps/unix/syscall-template.S:81
#1  0x000078948707220d in ?? () from /lib/x86_64-linux-gnu/libQtWebKit.so.4
#2  0x0000789487060f66 in ?? () from /lib/x86_64-linux-gnu/libQtWebKit.so.4
#3  0x00007894e383182 in start_thread (arg=0x78925296700) at pthread_create.c:312
#4  0x000078950fd47d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:111

Thread 9 (Thread 0x78933ff700 (LWP 24256)):
#0  0x000078950fd12d in poll () at ../sysdeps/unix/syscall-template.S:81

2021-08-01 4/11
Thread 2 (Thread 0x7f88af7f7e00 (LWP 24296)):

#0 0x00000000005805bf in __libc_wait (stat_loc=0x7f88af7fc460) at ../sysdeps/unix/sysv/linux/wait.c:35
#1 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#2 0x0000000000987e61 in QDebug::~QDebug() ()
#3 0x0000000000580193 in dumpBacktrace (depth=20) at /usr/src/qgis/qgis-2.8/src/app/main.cpp:236
#4 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#5 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#6 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#7 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#8 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#9 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#10 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#11 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#12 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#13 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#14 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#15 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#16 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#17 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#18 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#19 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#20 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#21 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
#22 0x00000000005802c8 in myMessageOutput (type=QtWarningMsg, msg=0x7f88a402a718 ""GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements"") at /usr/src/qgis/qgis-2.8/src/app/main.cpp:349
Thread 1 (Thread 0x7f6595000800 (LWP 242444)):
#0  pthread_cond_wait@Glibc_2.3.2 () at ../nptl/sysdeps/unix/sysv/linux/x86_64/pthread_cond_wait.S:185
#1  0x0000000000000000 in start_thread (arg=0x7f88af7fe700) at pthread_create.c:312
#2  0x0000000000000000 in QFutureInterfaceBase::waitForFinished() () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#3  0x0000000000000000 in QMutex::QMutex() () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#4  0x0000000000000000 in QMutex::QMutex() () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#5  0x0000000000000000 in QFutureInterfaceBase::waitForFinished() () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4
#6  0x0000000000000000 in QMutex::QMutex() () from /usr/lib/x86_64-linux-gnu/libQtCore.so.4

Could it be the lack of exception handling in Thread 2?

msg=0x7f88a402a718 "\"GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements\n\" %*

- Target version deleted (Future Release - High Priority)
- Affected QGIS version changed from 2.6.0 to 2.8.2

Could it be the lack of exception handling in Thread 2?

msg=0x7f88a402a718 "\"GEOS exception: IllegalArgumentException: point array must contain 0 or >1 elements\n\" %*

- File invalid_topo.sql.gz added
I'm attaching a dump to reproduce this. I could reproduce it just fine with 2.8. Master doesn't seem to have the problem.

#17 - 2015-07-31 06:23 AM - Giovanni Manghi
- Affected QGIS version changed from 2.8.2 to 2.8.3

#18 - 2015-10-05 03:26 AM - Jürgen Fischer
- Category set to Symbology

#19 - 2016-06-09 03:17 AM - Sandro Santilli
- Status changed from Reopened to In Progress

I cannot reproduce with current master either (2.15 -- d1cac84). Given 2.14 is the new LTR I'll test that one and if fixed would close this bug.

#20 - 2016-06-09 03:47 AM - Sandro Santilli
- Target version set to Version 2.14
- Status changed from In Progress to Closed
- Resolution set to fixed/implemented

2.14.3 is not affected either, while I confirm 2.8.9 is. Given 2.14 is the new LTR, I'm closing this as fixed.

Files

invalid_topo.sql.gz  83.6 KB  2015-07-31  Sandro Santilli