I'm running mdrun without arguments on 32-bit Ubuntu 14.04 machine. CMake configuration log from that machine is attached.

Upon running mdrun segfaults with:

$ mdrun
GROMACS: gmx mdrun, VERSION 5.0-rc1-dev-20140624-4347a4c-unknown
Segmentacijska greška (core dumped)

Running with gdb I get:

$ gdb mdrun
GNU gdb (Ubuntu 7.7-0ubuntu3.1) 7.7
Copyright (C) 2014 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
Find the GDB manual and other documentation resources online at:
For help, type "help".

03/19/2020
Type "apropos word" to search for commands related to "word"...
Reading symbols from mdrun...done.
(gdb) run
Starting program: /home/vedranm/software/gromacs/bin/mdrun
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/i386-linux-gnu/libthread_db.so.1".
GROMACS: gmx mdrun, VERSION 5.0-rc1-dev-20140624-4347a4c-unknown

GROMACS is written by:
Emile Apol             Rossen Apostolov          Herman J.C. Berendsen Par Bjelkmar
Aldert van Buuren     Rudi van Drunen         Anton Feenstra      Sebastian Fritsch
Gerrit Groenhof       Christoph Junghans      Peter Kasson         Carsten Kutzner
Per Larsson           Justin A. Lemkul        Magnus Lundborg     Pieter Meulenhoff
Erik Marklund         Teemu Murtola           Szilard Pall          Sander Pronk
Roland Schulz         Alexey Shvetsov         Michael Shirts       Alfons Sijbers
Peter Tieleman        Christian Wennberg      Maarten Wolf
and the project leaders:
Mark Abraham, Berk Hess, Erik Lindahl, and David van der Spoel

Copyright (c) 1991-2000, University of Groningen, The Netherlands.
Copyright (c) 2001-2014, The GROMACS development team at
Uppsala University, Stockholm University and
the Royal Institute of Technology, Sweden.
check out http://www.gromacs.org for more information.

GROMACS is free software; you can redistribute it and/or modify it
under the terms of the GNU Lesser General Public License
as published by the Free Software Foundation; either version 2.1
of the License, or (at your option) any later version.

GROMACS: gmx mdrun, VERSION 5.0-rc1-dev-20140624-4347a4c-unknown

Program received signal SIGSEGV, Segmentation fault.
__GI___pthread_mutex_lock (mutex=0x6a647275) at ../nptl/pthread_mutex_lock.c:66
66 ../nptl/pthread_mutex_lock.c: Nema takve datoteke ili direktorija.
(gdb) backtrace
#0 __GI___pthread_mutex_lock (mutex=0x6a647275) at ../nptl/pthread_mutex_lock.c:66
#1 0xb64c4af4 in pthread_mutex_lock (mutex=0x6a647275) at forward.c:192
#2 0xb7d723ae in tMPI_Thread_mutex_lock (mutex=0x80862fc)
at /home/vedranm/workspace/gromacs/src/external/thread_mpi/src/threads.c:478
#3 0xb690c481 in tMPI::mutex::lock (this=0x80862fc)
at /home/vedranm/workspace/gromacs/src/external/thread_mpi/src/threads.h:131
#4 0xb690c9c7 in tMPI::lock_guard<tMPI::mutex>::lock_guard (this=0xbfffed8c, m=...)
at /home/vedranm/workspace/gromacs/src/external/thread_mpi/src/threads.h:84
#5 0xb690bf39 in gmx::CommandLineProgramContext::fullBinaryPath (this=0x8086280)
at /home/vedranm/workspace/gromacs/src/gromacs/commandline/cmdlineprogramcontext.cpp:407
#6 0xb6b66d69e in gmx::printBinaryInformation (fp=0xb6576960 <_IO_2_1_stderr_), programContext=...,
    settings=...) at /home/vedranm/workspace/gromacs/src/gromacs/gmxlib/copyrite.cpp:804
#7 0xb690e0c1 in gmx::CommandLineModuleManager::run (this=0xbfffee5c, argc=1, argv=0xbfffe34)
at /home/vedranm/workspace/gromacs/src/gromacs/commandline/cmdlinemodulemanager.cpp:536
#8 0x08056307 in main (argc=1, argv=0xbfffe34) at /home/vedranm/workspace/gromacs/src/programs/gmx.cpp:58

Commenting out calls to pthread_mutex_* "fixes" the problem (diff is attached).

Associated revisions
Revision 5886961e - 06/29/2014 09:26 AM - Roland Schulz
Fix detection of i386 in tmpi

The i386 without underscore is not recommended for new code and is not
defined if -std=... (other than gnu...) is passed on the command line.
i386 is already present for GCC 3.2 so there is no need for the old
name. Also we use i386 in other places in the code already.
We dont pass such a flag by default for 4.6, but the user could.
In 5.0 this fixes tmpi if the compiler supports c++11 and we pass
std=c++11.
Fixes #1533
Change-Id: i615cb91d3e3196a90fa4ba03fa183bf47af5d444

History
#1 - 06/25/2014 09:14 PM - Rossen Apostolov
  could it be related to https://gerrit.gromacs.org/#/c/3668/?

#2 - 06/26/2014 10:23 PM - Erik Lindahl
  - Assignee set to Erik Lindahl

  No idea what it is, but I'll try to fit it friday morning.

  @Rossen: Based on the version string, it does not include the X32 commit (and that shouldn't have anything to do with pure 32-bit linux anyway).

  Vedran, very short on time before 5.0, but I would love to have this working, so if you have a few minutes to spare you could help:
  1) Can you reproduce it by doing a 32-bit build on a 64-bit machine? If nothing else, that would mean I can run it on my own machines to debug.
  2) Does it work fine if you
     (a) disable MPI completely, or
     (b) enable native MPI support (e.g. with open-MPI) instead of our built-in thread-MPI?

... and, finally, if you set the build type to "Debug" that should add the -g flag so we get much more explicit output about the culprit code from gdb!

Erik

#3 - 06/28/2014 07:29 AM - Mark Abraham
  Vedran, can you please attach src/config.h from the build tree? In particular, is TMPI_ATOMICS set?

  Also, what is the value of ret in line 478 (ie tMPI_Thread_mutex_lock in ../../threads.c) before the segfault?

#4 - 06/28/2014 07:37 AM - Roland Schulz
  I can reproduce this on my system. 64-bit OpenSuse. Compiled with -m32. I don't understand the error yet. TMPI_ATOMICS is set. ASAN claims that there is a heap-buffer-overflow

    #2 0xf64d07d3 in tMPI_Thread_mutex_init (mtx=0xf3d00fec) at ../../external/thread_mpi/src/threads.c:388
    #3 0xf4f4a8b8f in mutex (this=0xf3d00fec) at ../../external/thread_mpi/include/thread_mpi/mutex.h:113
    #4 gmx::CommandLineProgramContext::Impl::Impl (this=0xf3d00fd0, argc=1, argv=0xffffcbb4, env=...) at ../../src/gromacs/commandline/cmdlineprogramcontext.cpp:324

    Which then causes a segfault on the next lock. But I don't get how the "mtx->mutex = ..." (the address with the problem is &mtx->mutex) can be a problem.

#5 - 06/28/2014 08:45 AM - Teemu Murtola
  What's the full error message from ASAN (and/or valgrind)? How does the overflow cause the segfault? (i.e., what address is incorrect there?)

#6 - 06/28/2014 10:49 AM - Mark Abraham
  388 is broken because the cast between differently-sized structs is invalid. Alignment might make the problem silent on 64bit targets.

#7 - 06/28/2014 11:10 AM - Mark Abraham
  - Status changed from New to Fix uploaded
  - Affected version - extra info set to likely 4.5 and 4.6 also

  Fix (on release-4-6 branch) at https://gerrit.gromacs.org/#/c/3716/. Please test, I don't (know if I) have ready access to a test machine.

#8 - 06/28/2014 11:10 AM - Mark Abraham
  - Assignee changed from Erik Lindahl to Mark Abraham

#9 - 06/28/2014 11:21 AM - Mark Abraham
Oops, that's not the problem. I missed that the LHS was mtx->mutex not mtx.

#10 - 06/28/2014 05:10 PM - Vedran Miletic
Will test today or tomorrow, and provide the requested info. At the moment I have no 32-bit OS installations around me.

#11 - 06/28/2014 10:27 PM - Roland Schulz
- Affected version - extra info deleted (likely 4.5 and 4.6 also)

If I compile the latest 4.6 in 32bit, it passes all regression tests. Thus I don't think 4.5 or 4.6 are affected.
The unit tests crash too. Thus it isn't just the CommandLineProgramContext usage of the mutex.

#12 - 06/29/2014 12:09 AM - Roland Schulz
The first revision for which the unit tests fail is:

commit 1adde8a13dbbea812ed3ee825548fc87baed2c3c
Author: Teemu Murtola <teemu.murtola@gmail.com>
Date:   Sun May 5 12:55:31 2013 +0300

Better concurrency support for analysis nbsearch.

But I don't think it is caused by that commit. Rather it adds one of these mutexes which cause the problem.

#13 - 06/29/2014 07:06 AM - Roland Schulz
I found the problem. tmpi was using i386 to check for architecture but for newer GCC versions we pass -std=c++11 which causes gcc not to define the deprecated name outside of the reserved namespace. This caused the tMPI_Atomic to be a different size in the C and C++ code.

#14 - 06/29/2014 07:25 AM - Gerrit Code Review Bot
Gerrit received a related patchset '1' for Issue #1533.
Uploader: Roland Schulz (roland@rschulz.eu)
Change-id: I615cb91d3e3196a90fa4ba03fa183bf47af5d444
Gerrit URL: https://gerrit.gromacs.org/3722

#15 - 06/29/2014 10:00 AM - Erik Lindahl
- Status changed from Accepted to Fix uploaded

#16 - 06/29/2014 10:00 AM - Erik Lindahl
- Status changed from Fix uploaded to Resolved

#17 - 06/29/2014 10:00 AM - Erik Lindahl
- Status changed from Resolved to Closed

#18 - 06/29/2014 01:52 PM - Vedran Miletic
Works now. Thanks!

Files
offending-calls.patch  947 Bytes  06/25/2014  Vedran Miletic
gmx-cmake.log          9.61 KB   06/25/2014  Vedran Miletic