Ruby trunk - Bug #15329

Native implementation of coroutines - segfault

11/21/2018 06:54 PM - ahorek (Pavel Rosický)

Status:	Closed		
Priority:	Normal		
Assignee:	ioquatix (Samuel Williams)		
Target version:	2.6		
ruby -v:		**Backport:**	

Description

Hi, after https://github.com/ruby/ruby/commit/07a324a0f6464f31765ee4bc5cfc23a99d426705 issue #14739 was merged I'm getting a segfault

uname -a (WSL)

```
Linux DESKTOP-2POPPQP 4.4.0-17134-Microsoft #345-Microsoft Wed Sep 19 17:47:00 PST 2018 x86_64 x86
_64 x86_64 GNU/Linux
```

gcc -v

```
Using built-in specs.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/lib/gcc/x86_64-linux-gnu/4.8/lto-wrapper
Target: x86_64-linux-gnu
Configured with: ../src/configure -v --with-pkgversion='Ubuntu 4.8.4-2ubuntu1~14.04.4' --with-bugu
rl=file:///usr/share/doc/gcc-4.8/README.Bugs --enable-languages=c,c++,java,go,d,fortran,objc,obj-c
++ --prefix=/usr --program-suffix=-4.8 --enable-shared --enable-linker-build-id --libexecdir=/usr/
lib --without-included-gettext --enable-threads=posix --with-gxx-include-dir=/usr/include/c++/4.8
--libdir=/usr/lib --enable-nls --with-sysroot=/ --enable-clocale=gnu --enable-libstdcxx-debug --en
able-libstdcxx-time=yes --enable-gnu-unique-object --disable-libmudflap --enable-plugin --with-sys
tem-zlib --disable-browser-plugin --enable-java-awt=gtk --enable-gtk-cairo --with-java-home=/usr/l
ib/jvm/java-1.5.0-gcj-4.8-amd64/jre --enable-java-home --with-jvm-root-dir=/usr/lib/jvm/java-1.5.0
-gcj-4.8-amd64 --with-jvm-jar-dir=/usr/lib/jvm-exports/java-1.5.0-gcj-4.8-amd64 --with-arch-direct
ory=amd64 --with-ecj-jar=/usr/share/java/eclipse-ecj.jar --enable-objc-gc --enable-multiarch --dis
able-werror --with-arch-32=i686 --with-abi=m64 --with-multilib-list=m32,m64,mx32 --with-tune=gener
ic --enable-checking=release --build=x86_64-linux-gnu --host=x86_64-linux-gnu --target=x86_64-linu
x-gnu
Thread model: posix
gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04.4)
```

previous ruby builds were fine

```
ruby-head - #autoreconf.
ruby-head - #configuring.....................................................................
ruby-head - #post-configuration..
ruby-head - #compiling.......................................................................
.....................................................
ruby-head - #installing.......................
Error running '__rvm_make install',
please read /home/ahorek/.rvm/log/1542824691_ruby-head/install.log
There has been an error while running make install. Halting the installation.

make[1]: Entering directory `/home/ahorek/.rvm/src/ruby-head'
make[1]: Nothing to be done for `enc'.
make[1]: Leaving directory `/home/ahorek/.rvm/src/ruby-head'
making trans
make[1]: Entering directory `/home/ahorek/.rvm/src/ruby-head'
make[1]: Nothing to be done for `./enc/trans'.
make[1]: Leaving directory `/home/ahorek/.rvm/src/ruby-head'
making encs
make[1]: Entering directory `/home/ahorek/.rvm/src/ruby-head'
make[1]: Nothing to be done for `encs'.
```

```
make[1]: Leaving directory `/home/ahorek/.rvm/src/ruby-head'
./miniruby -I./lib -I. -I.ext/common  ./tool/runruby.rb --extout=.ext  -- --disable-gems -r./x86_6
4-linux-fake ./tool/rbinstall.rb --make="make" --dest-dir="" --extout=".ext" --mflags="" --make-fl
ags="" --data-mode=0644 --prog-mode=0755 --installed-list .installed.list --mantype="doc"
./tool/runruby.rb:110: warning: Insecure world writable dir /home/ahorek/.rvm/gems/ruby-2.5.1/bin
in PATH, mode 040777
Segmentation fault (core dumped)
make: *** [do-install-nodoc] Error 139
++ return 2
```

ioquatix (Samuel Williams) any ideas what could went wrong?

History

#1 - 11/21/2018 07:12 PM - ahorek (Pavel Rosický)

- File make.log added

- File install.log added

- File configure.log added

#2 - 11/21/2018 08:43 PM - ioquatix (Samuel Williams)

- Target version set to 2.6

- Assignee set to ioquatix (Samuel Williams)

I need stack trace can you please try to get it for me?

#3 - 11/21/2018 08:57 PM - ahorek (Pavel Rosický)

Sure, could you give me a hint how to get it? Unfortunatelly it isn't present in any of standard build logs...

#4 - 11/21/2018 10:30 PM - ioquatix (Samuel Williams)

Interesting, I did some research about WSL, apparently it can run unmodified binaries from Linux.

I checked the configure log and it says

```
checking native coroutine implementation for x86_64-linux... amd64
```

Do you mind trying the latest branch here?

https://github.com/ioquatix/ruby/tree/native-fiber

#5 - 11/22/2018 01:28 AM - ahorek (Pavel Rosický)

hmm, it has something to do with rvm...

I've tried to build trunk manually and it works

I double checked a few commits before
https://github.com/ruby/ruby/commit/07a324a0f6464f31765ee4bc5cfc23a99d426705
and there's no segfault if I build it via rvm.

commits after that including the lastest trunk and your native-fiber branch always fails. What's rvm doing differently?

WSL should be able to run Linux binaries, but there're still some bugs and unimplemented features like this one
https://github.com/Microsoft/WSL/issues/1262
so obtaining a stack trace is quite difficult. I'm not sure what to do next...

at least I'll share some numbers
ruby 2.6.0dev (2018-11-22 trunk 65908) [x86_64-linux]
WSL with native fiber
setup time for 1000 fibers: 0.027490
execution time for 10000 messages: 3.558456
setup time for 1000 fibers: 0.042641
execution time for 10000 messages: 4.034067
setup time for 1000 fibers: 0.042021
execution time for 10000 messages: 4.071040
setup time for 1000 fibers: 0.029907
execution time for 10000 messages: 4.000733
setup time for 1000 fibers: 0.033170
execution time for 10000 messages: 4.031574

ruby 2.6.0dev (2018-11-20 trunk_test 65833) [x86_64-linux]
WSL without native fiber
setup time for 1000 fibers: 0.032594
execution time for 10000 messages: 92.511626
setup time for 1000 fibers: 0.031483
execution time for 10000 messages: 92.130597
setup time for 1000 fibers: 0.023076
execution time for 10000 messages: 92.837384
setup time for 1000 fibers: 0.023592
execution time for 10000 messages: 91.769230
setup time for 1000 fibers: 0.042044
execution time for 10000 messages: 93.895609

ruby 2.5.1p57 (2018-03-29 revision 63029) [x64-mingw32]
Windows 10 without native fiber
setup time for 1000 fibers: 0.021157
execution time for 10000 messages: 5.506048
setup time for 1000 fibers: 0.035167
execution time for 10000 messages: 5.419805
setup time for 1000 fibers: 0.056107
execution time for 10000 messages: 5.718922
setup time for 1000 fibers: 0.034599
execution time for 10000 messages: 5.400970
setup time for 1000 fibers: 0.031754
execution time for 10000 messages: 5.065231

it looks like the original version is very slow on WSL, but your implementation is 23 times faster

#6 - 11/22/2018 01:55 AM - ioquatix (Samuel Williams)

Native fiber implementation is all about speed and consistent interface across all supported platforms. It's good to hear there is speed improvement on WSL with native fiber. It also looks like it's a little bit faster than CreateFiber Win32 API.

> commits after that including the lastest trunk and your native-fiber branch always fails. What's rvm doing differently?

Can you show me the report of failure?

#7 - 11/22/2018 02:09 AM - ahorek (Pavel Rosický)

the same error

```
./miniruby -I./lib -I. -I.ext/common  ./tool/runruby.rb --extout=.ext  -- --disable-gems -r./x86_64-linux-fake
 ./tool/rbinstall.rb --make="make" --dest-dir="" --extout=".ext" --mflags="" --make-flags="" --data-mode=0644
--prog-mode=0755 --installed-list .installed.list --mantype="doc"
./tool/runruby.rb:110: warning: Insecure world writable dir /home/ahorek/.rvm/gems/ruby-2.5.1/bin in PATH, mod
e 040777
Segmentation fault (core dumped)
make: *** [do-install-nodoc] Error 139
++ return 2
```

but without a stack trace it isn't very useful.

could Valgrind be used somehow to get the trace?

#8 - 11/22/2018 02:21 AM - ioquatix (Samuel Williams)

You need to use debugger to get stack trace.

Here is an example of running it in GDB to get stack trace:

```
(gdb) run --disable-gems -I. -I../lib -I../test/lib ../test/ruby/test_enumerator.rb
Starting program: C:\msys64\home\samuel\ruby\build\ruby.exe --disable-gems -I. -I../lib -I../test/lib ../test/
ruby/test_enumerator.rb
[New Thread 29384.0x73bc]
[New Thread 29384.0x7b88]
[New Thread 29384.0x710c]
[New Thread 29384.0x6958]
[New Thread 29384.0x2c64]
Run options:
# Running tests:
Thread 1 received signal SIGSEGV, Segmentation fault.
0x000000006a635a83 in rb_vm_bh_to_procval ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
(gdb) bt
```

```
#0  0x000000006a635a83 in rb_vm_bh_to_procval ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#1  0x000000006a635afc in vm_yield_with_cfunc.isra ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#2  0x000000006a63782e in vm_invoke_block ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#3  0x000000006a6427bf in vm_exec_core ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#4  0x000000006a6396a8 in rb_vm_exec ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#5  0x000000006a63be53 in vm_call0_body.constprop ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#6  0x000000006a63cbbb in rb_call0 ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#7  0x000000006a63d24c in iterate_method ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#8  0x000000006a634fb3 in rb_iterate0 ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#9  0x000000006a635241 in rb_block_call ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#10 0x000000006a4bd88b in enumerator_block_call ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#11 0x000000006a63bf0e in vm_call0_body.constprop ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#12 0x000000006a63cbbb in rb_call0 ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#13 0x000000006a63d24c in iterate_method ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#14 0x000000006a634fb3 in rb_iterate0 ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#15 0x000000006a635241 in rb_block_call ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#16 0x000000006a4bda13 in next_i ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#17 0x000000006a635b95 in vm_yield_with_cfunc.isra ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#18 0x000000006a63b592 in rb_vm_invoke_proc ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#19 0x000000006a49ed1e in rb_fiber_start ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#20 0x000000006a49f429 in fiber_entry ()
   from C:\msys64\home\samuel\ruby\build\x64-msvcrt-ruby260.dll
#21 0x0000000000000000 in ?? ()
Backtrace stopped: previous frame inner to this frame (corrupt stack?)
(gdb)
```

I just merged windows stack allocation into trunk. It shouldn't affect you thought.

#9 - 11/22/2018 06:30 AM - ioquatix (Samuel Williams)

Based on all the evidence, I think it's compiler bug.

Do you mind testing with clang? It will help to support this hypothesis if it doesn't crash and give me a better idea of what to check next.

#10 - 11/22/2018 06:32 AM - ioquatix (Samuel Williams)

Also, on gcc, can you please try:

```
./configure optflags="-O0" debugflags="-ggdb3" && mingw32-make
```

See if that still has crash when running tests.

#11 - 11/22/2018 10:16 AM - ahorek (Pavel Rosický)

- File clang_ruby_trunk.zip added

- File clang_ruby_2.5.2.zip added

```
rvm install ruby-head --disable-binary -- --enable-shared CC=clang
```

also tested with gcc-8 (Ubuntu 8.1.0-5ubuntu1~14.04) 8.1.0 - exactly the same error
passing -O0 debugflags=-ggdb3" makes no change

for comparsion

```
rvm install ruby-2.5.2 --disable-binary -- --enable-shared CC=clang
```

and https://github.com/ruby/ruby/commit/27665e5134582bf58fb196268d659cc19df39f61 (the previous commit before #14739) was successful

interesting is that building trunk without rvm works

```
git clone https://github.com/ruby/ruby.git
autoconf
./configure
make
make install
```

according to the log it fails on segfault at this step

```
./miniruby -I./lib -I. -I.ext/common  ./tool/runruby.rb --extout=.ext  -- --disable-gems -r./x86_64-linux-fake
 ./tool/rbinstall.rb --make="make" --dest-dir="" --extout=".ext" --mflags="" --make-flags="" --data-mode=0644
--prog-mode=0755 --installed-list .installed.list --mantype="doc"
```

I tried to run the command directly in the rvm's build directory and it also works... something really weird is happening

#12 - 11/22/2018 11:48 AM - ioquatix (Samuel Williams)

I only experience crash with -O3, I think it's an alignment issue. I am going to look into it more tomorrow, right now I wouldn't spend too much time on this until I investigate alignment issues. Thanks for your continued reports and help.

#13 - 11/22/2018 12:59 PM - ahorek (Pavel Rosický)

I'll let you know if I find something useful. Thanks

#14 - 11/24/2018 05:48 AM - ioquatix (Samuel Williams)

Can you please try trunk now? This issue might be fixed.

#15 - 11/24/2018 05:59 PM - ahorek (Pavel Rosický)

good news! I can confirm it's fixed by https://github.com/ruby/ruby/commit/f33adbc11e0fa0a2bd73b96ee3a3529481eb111d . Thanks!

#16 - 11/24/2018 08:51 PM - ioquatix (Samuel Williams)

- Status changed from Open to Closed

Great, thanks for the report. Let me know if you have any other issues.

#17 - 12/12/2018 01:59 AM - ioquatix (Samuel Williams)

- Backport deleted (2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN)

Files

configure.log	29.1 KB	11/21/2018	ahorek (Pavel Rosický)
install.log	18.6 KB	11/21/2018	ahorek (Pavel Rosický)
make.log	53.3 KB	11/21/2018	ahorek (Pavel Rosický)
clang_ruby_2.5.2.zip	84.5 KB	11/22/2018	ahorek (Pavel Rosický)
clang_ruby_trunk.zip	72.9 KB	11/22/2018	ahorek (Pavel Rosický)