

Ruby - Bug #9426

Segmentation fault with signal in test_tracks_objspace_count

01/18/2014 11:28 AM - akr (Akira Tanaka)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.2.0dev (2014-01-18 trunk 44636) [x86_64-linux]	Backport: 1.9.3: DONTNEED, 2.0.0: DONTNEED, 2.1: DONE

Description

test-all Control-C SEGV
test_tracks_objspace_count

Process.kill

% uname -mrsv
Linux 3.10-3-amd64 #1 SMP Debian 3.10.11-1 (2013-09-10) x86_64
% lsb_release -idrc
Distributor ID: Debian
Description: Debian GNU/Linux testing (jessie)
Release: testing
Codename: jessie
% svn diff
Index: test/-ext-/tracepoint/test_tracepoint.rb
=====

```
--- test/-ext-/tracepoint/test_tracepoint.rb (revision 44636)
+++ test/-ext-/tracepoint/test_tracepoint.rb (working copy)
@@ -34,6 +34,7 @@
     GC.disable
     GC.stat(stat1)
     result = Bug.tracepoint_track_objspace_events{
+       Process.kill(:TERM, $$)
       GC.enable
       1_000_000.times{''}
       GC.disable
% ./ruby -I.ext/x86_64-linux test/-ext-/tracepoint/test_tracepoint.rb -n test_tracks_objspace_count
Run options: -n test_tracks_objspace_count

# Running tests:

[1/1] TestTracepointObj#test_tracks_objspace_count/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:871:
[BUG] Segmentation fault at 0x0000000000000000
ruby 2.2.0dev (2014-01-18 trunk 44636) [x86_64-linux]
```

-- Control frame information -----

```
c:0022 p:0004 s:0100 e:000099 BLOCK /home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:871
c:0021 p:0062 s:0097 e:000095 METHOD /home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:872
c:0020 p:0069 s:0091 e:000090 METHOD /home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1265
c:0019 p:0019 s:0083 e:000082 METHOD /home/akr/tst3/lib/ruby/2.2.0/test/unit/testcase.rb:17
c:0018 p:0068 s:0079 e:000078 BLOCK /home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:940 [FINISH]
c:0017 p:---- s:0073 e:000072 CFUNC :map
c:0016 p:0103 s:0070 e:000069 METHOD /home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:933
c:0015 p:0015 s:0060 e:000058 BLOCK /home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:663 [FINISH]
c:0014 p:---- s:0055 e:000054 CFUNC :each
c:0013 p:0067 s:0052 e:000051 METHOD /home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:661
c:0012 p:0135 s:0046 e:000045 METHOD /home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:884
c:0011 p:0009 s:0036 e:000035 METHOD /home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1092
c:0010 p:0009 s:0033 e:000032 BLOCK /home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1079 [FINISH]
c:0009 p:---- s:0030 e:000029 CFUNC :each
c:0008 p:0048 s:0027 e:000026 METHOD /home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1078
```

```

c:0007 p:0017 s:0023 e:000022 METHOD /home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1066
c:0006 p:0019 s:0019 e:000018 METHOD /home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:27
c:0005 p:0010 s:0015 e:000014 METHOD /home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:780
c:0004 p:0027 s:0010 e:000008 BLOCK /home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:372
c:0003 p:0031 s:0007 e:000006 METHOD /home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:33
c:0002 p:0024 s:0004 e:000003 BLOCK /home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:371 [FINISH]
c:0001 p:0000 s:0002 E:0011b8 TOP [FINISH]

```

```

/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:371:in `block in autorun'
/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:33:in `run_once'
/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:372:in `block (2 levels) in autorun'
/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:780:in `run'
/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:27:in `run'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1066:in `run'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1078:in `_run'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1078:in `each'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1079:in `block in _run'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1092:in `run_tests'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:884:in `_run_anything'
/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:661:in `_run_suites'
/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:661:in `each'
/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:663:in `block in _run_suites'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:933:in `_run_suite'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:933:in `map'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:940:in `block in _run_suite'
/home/akr/tst3/lib/ruby/2.2.0/test/unit/testcase.rb:17:in `run'
/home/akr/tst3/lib/ruby/2.2.0/minitest/unit.rb:1265:in `run'
/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:872:in `run_test'
/home/akr/tst3/lib/ruby/2.2.0/test/unit.rb:871:in `ensure in run_test'

```

-- C level backtrace information -----

```

zsh: segmentation fault ./ruby -I.ext/x86_64-linux test/-ext-/tracepoint/test_tracepoint.rb -n
% gdb ruby

```

GNU gdb (GDB) 7.6.1 (Debian 7.6.1-1)

Copyright (C) 2013 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 "x86_64-linux-gnu".

For bug reporting instructions, please see:

<<http://www.gnu.org/software/gdb/bugs/>>...

Reading symbols from /home/akr/tst3/ruby/ruby...done.

(gdb) handle SIGTERM noprint

Signal Stop Print Pass to program Description

SIGTERM No No Yes Terminated

```

(gdb) run -I.ext/x86_64-linux test/-ext-/tracepoint/test_tracepoint.rb -n test_tracks_objspace_cou
nt

```

```

Starting program: /home/akr/tst3/ruby/ruby -I.ext/x86_64-linux test/-ext-/tracepoint/test_tracepoi
nt.rb -n test_tracks_objspace_count

```

warning: Could not load shared library symbols for linux-vdso.so.1.

Do you need "set solib-search-path" or "set sysroot"?

[Thread debugging using libthread_db enabled]

Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

[New Thread 0x7ffff7ff7700 (LWP 21427)]

Run options: -n test_tracks_objspace_count

Running tests:

```

[1/1] TestTracepointObj#test_tracks_objspace_count

```

Program received signal SIGSEGV, Segmentation fault.

```

0x000055555556bd8c6 in vm_call0 (th=0x12, recv=17870283871161941922, id=3458764880324436804, argc=1
073741909,

```

```

    argv=0xa00000555555a347, me=0x8800000000000012, defined_class=17870283321406128128) at vm_eval
.c:51
51 }

```

(gdb) bt

```

#0  0x000055555556bd8c6 in vm_call0 (th=0x12, recv=17870283871161941922, id=3458764880324436804, ar
gc=1073741909,
    argv=0xa00000555555a347, me=0x8800000000000012, defined_class=17870283321406128128) at vm_eval
.c:51
#1  0x0100000000000000 in ?? ()
#2  0xf800000000000000 in ?? ()
#3  0x88000000000000012 in ?? ()
#4  0x300000555555a347 in ?? ()
#5  0xf800000001f7fd99 in ?? ()
#6  0x500000555555a246 in ?? ()
#7  0xa00000555555a798 in ?? ()
#8  0x400000555555a1e6 in ?? ()
#9  0xd300007fffffff3 in ?? ()
#10 0x0000005555556bed in ?? ()
#11 0x0100000000000000 in ?? ()
#12 0xf800000000000000 in ?? ()
#13 0x88000000000000012 in ?? ()
#14 0x180000555555a347 in ?? ()
#15 0xa000000000000053 in ?? ()
#16 0x600000555555a1e6 in ?? ()
#17 0x3500007fffffff3 in ?? ()
#18 0xd000005555556bf6 in ?? ()
#19 0x9000000000000052 in ?? ()
#20 0xf800000000560425 in ?? ()
#21 0x88000000000000012 in ?? ()
#22 0xb00000555555a347 in ?? ()
#23 0x0000007fffffff3 in ?? ()
#24 0xb000000000000000 in ?? ()
#25 0xf600007fffffff3 in ?? ()
#26 0xd000005555556b04 in ?? ()
#27 0x4000000000000052 in ?? ()
#28 0x300000555555ea0b in ?? ()
#29 0xa000007ffff7fd99 in ?? ()
#30 0xb00000555555a1e6 in ?? ()
#31 0xf800007fffffff3 in ?? ()
#32 0x50000000000000012 in ?? ()
#33 0x090000555555e678 in ?? ()
---Type <return> to continue, or q <return> to quit---
#34 0x3000007ffff7eda3 in ?? ()
#35 0xa000007ffff7fd99 in ?? ()
#36 0x200000555555a1e6 in ?? ()
#37 0x0100007fffffff3 in ?? ()
#38 0x3800005555000000 in ?? ()
#39 0x580000000055a35b in ?? ()
#40 0xd000007fffffff3 in ?? ()
#41 0x9000000000000052 in ?? ()
#42 0x90000055555560307 in ?? ()
#43 0x300000555555a277 in ?? ()
#44 0x70000055555560428 in ?? ()
#45 0x0e00007fffffff3 in ?? ()
#46 0xa000005555556bb6 in ?? ()
#47 0x300000555555a1e6 in ?? ()
#48 0x1000007ffff7fd99 in ?? ()
#49 0x7000007ffff7fda0 in ?? ()
#50 0x3700007fffffff3 in ?? ()
#51 0x09000055555557a0 in ?? ()
#52 0x8000007ffff7eda3 in ?? ()
#53 0x2800007fffffff3 in ?? ()
#54 0x800000555555575c in ?? ()
#55 0x8800007fffffff3 in ?? ()
#56 0xb00000555555a347 in ?? ()
#57 0x3000007fffffff3 in ?? ()
#58 0xd0000055555557a1 in ?? ()
#59 0xb000000000000052 in ?? ()
#60 0xd000000000000014 in ?? ()
#61 0x8800007fffffff3 in ?? ()
#62 0xe00000555555a347 in ?? ()

```

```
#63 0xc100007fffffffffa4 in ?? ()
#64 0x080000555555568a2 in ?? ()
#65 0xa0000055555560308 in ?? ()
#66 0x3000005555555a842 in ?? ()
#67 0xc000007ffff7fd99 in ?? ()
#68 0x900000555555a842 in ?? ()
---Type <return> to continue, or q <return> to quit---
#69 0x6600007fffffffffaf in ?? ()
#70 0x60000055555556b30 in ?? ()
#71 0x5800007ffff7eda2 in ?? ()
#72 0x4000007ffff7eda2 in ?? ()
#73 0x4800007fffffffffa5 in ?? ()
#74 0x08000055555556acc in ?? ()
#75 0x0100000000000000 in ?? ()
#76 0x0000000000000000 in ?? ()
(gdb) l
46     ci->defined_class = defined_class;
47     ci->argc = argc;
48     ci->me = me;
49
50     return vm_call0_body(th, ci, argv);
51 }
52
53 #if OPT_CALL_CFUNC_WITHOUT_FRAME
54 static VALUE
55 vm_call0_cfunc(rb_thread_t* th, rb_call_info_t *ci, const VALUE *argv)
(gdb)

##### Debian GNU/Linux testing (jessie) #####
boron (### Debian GNU/Linux 6.0.8 (squeeze)) #####

##### configure - optflags=-O0 #####
(##### -O3 #####)
```

Associated revisions

Revision 41bdefd56f628781a19f5d5d5f6a9a05cb4f3e9e - 01/19/2014 08:56 AM - nobu (Nobuyoshi Nakada)

tracepoint.c: disable tracepoint

- ext/-test-/tracepoint/tracepoint.c (tracepoint_track_objspace_events): ensure tracepoint disabled. [ruby-dev:47901] [Bug #9426]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@44654 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 41bdefd5 - 01/19/2014 08:56 AM - nobu (Nobuyoshi Nakada)

tracepoint.c: disable tracepoint

- ext/-test-/tracepoint/tracepoint.c (tracepoint_track_objspace_events): ensure tracepoint disabled. [ruby-dev:47901] [Bug #9426]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@44654 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 575ff86a4b01d91fef49484de70caf7c5212bb22 - 02/20/2014 07:30 AM - naruse (Yui NARUSE)

merge revision(s) 44654: [Backport #9426]

```
tracepoint.c: disable tracepoint
```

```
* ext/-test-/tracepoint/tracepoint.c (tracepoint_track_objspace_events):
```

ensure tracepoint disabled. [ruby-dev:47901] [Bug #9426]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@45062 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 575ff86a - 02/20/2014 07:30 AM - naruse (Yui NARUSE)

merge revision(s) 44654: [Backport #9426]

```
tracepoint.c: disable tracepoint
```

```
* ext/-test-/tracepoint/tracepoint.c (tracepoint_track_objspace_events) :
```

ensure tracepoint disabled. [ruby-dev:47901] [Bug #9426]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@45062 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 01/18/2014 12:09 PM - hsbt (Hiroshi SHIBATA)

- Description updated

#2 - 01/19/2014 08:57 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

Applied in changeset r44654.

tracepoint.c: disable tracepoint

- ext/-test-/tracepoint/tracepoint.c (tracepoint_track_objspace_events):
ensure tracepoint disabled. [\[ruby-dev:47901\]](#) [Bug #9426]

#3 - 01/27/2014 03:54 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 1.9.3: UNKNOWN, 2.0.0: UNKNOWN, 2.1: UNKNOWN to 1.9.3: DONTNEED, 2.0.0: DONTNEED, 2.1: REQUIRED

#4 - 02/21/2014 04:33 AM - naruse (Yui NARUSE)

- Backport changed from 1.9.3: DONTNEED, 2.0.0: DONTNEED, 2.1: REQUIRED to 1.9.3: DONTNEED, 2.0.0: DONTNEED, 2.1: DONE