Ruby master - Bug #11596

Getting [BUG] rb_vm_get_cref: unreachable

10/14/2015 10:01 PM - tenderlovemaking (Aaron Patterson)

Status:	Closed		
Priority:	Normal		
Assignee:	ko1 (Koichi Sasada)		
Target version:			
ruby -v:	ruby 2.3.0dev (2015-10-15 trunk 52128) [x86_64-darwin15]	**Backport:**	2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN

Description

I'm getting a crash when running the Rails tests.

When I run this in the ActiveRecord tests:

```
$ ruby -v -I lib:test test/cases/scoping/default_scoping_test.rb -n test_default_scope_select_igno
red_by_grouped_aggregations
```

I get this:

```
[aaron@TC activerecord (4-2-stable)]$ ruby -v -I lib:test test/cases/scoping/default_scoping_test.
rb -n test_default_scope_select_ignored_by_grouped_aggregations
ruby 2.3.0dev (2015-10-15 trunk 52128) [x86_64-darwin15]
Using sqlite3
Run options: -n test_default_scope_select_ignored_by_grouped_aggregations --seed 13158

# Running:

test/cases/scoping/default_scoping_test.rb:375: [BUG] rb_vm_get_cref: unreachable
ruby 2.3.0dev (2015-10-15 trunk 52128) [x86_64-darwin15]

-- Crash Report log information --------------------------------------------
   See Crash Report log file under the one of following:
     * ~/Library/Logs/CrashReporter
     * /Library/Logs/CrashReporter
     * ~/Library/Logs/DiagnosticReports
     * /Library/Logs/DiagnosticReports
   for more details.
Don't forget to include the above Crash Report log file in bug reports.

-- Control frame information -----------------------------------------------
c:0023 p:0040 s:0101 E:0023c0 METHOD test/cases/scoping/default_scoping_test.rb:375
c:0022 p:0029 s:0096 e:000095 BLOCK  /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest/test.rb:106
c:0021 p:0008 s:0094 e:000093 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest/test.rb:204
c:0020 p:0009 s:0090 e:000089 BLOCK  /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest/test.rb:103
c:0019 p:0020 s:0088 e:000087 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest/test.rb:256
c:0018 p:0009 s:0084 e:000083 BLOCK  /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest/test.rb:102
c:0017 p:0040 s:0082 E:000200 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:317
c:0016 p:0041 s:0075 E:002058 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest/test.rb:276
c:0015 p:0009 s:0069 E:001bc0 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest/test.rb:101
c:0014 p:0014 s:0066 e:000065 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:759
c:0013 p:0020 s:0060 e:000058 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:293
```

```
c:0012 p:0014 s:0053 e:000052 BLOCK  /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:287 [FINISH]
c:0011 p:---- s:0050 e:000049 CFUNC  :each
c:0010 p:0010 s:0047 e:000046 BLOCK  /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:286
c:0009 p:0040 s:0045 E:000030 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:317
c:0008 p:0024 s:0038 E:000ae8 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:306
c:0007 p:0070 s:0032 E:000d50 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:285
c:0006 p:0013 s:0025 e:000024 BLOCK  /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:149 [FINISH]
c:0005 p:---- s:0022 e:000021 CFUNC  :map
c:0004 p:0039 s:0019 e:000018 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:149
c:0003 p:0135 s:0011 e:000010 METHOD /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:126
c:0002 p:0071 s:0005 E:0011e8 BLOCK  /Users/aaron/.rbenv/versions/ruby-trunk/lib/ruby/gems/2.3.0/g
ems/minitest-5.3.3/lib/minitest.rb:55 [FINISH]
c:0001 p:0000 s:0002 E:000d90 (none) [FINISH]
```

It seems that the problem was introduced with r52056. [This is the test case I am running](). I'll try to make the test case smaller, but for now if you check out the rails repository then do:

```
$ git checkout 4-2-stable
$ bundle
$ cd activerecord
$ ruby -v -I lib:test test/cases/scoping/default_scoping_test.rb -n test_default_scope_select_igno
red_by_grouped_aggregations
```

It will segv. Reverting r52056 fixes the problem for me.

Here is a trace from lldb:

```
Process 14459 stopped
* thread #1: tid = 0x51f083, 0x00007fff913b90ae libsystem_kernel.dylib`__pthread_kill + 10, queue
= 'com.apple.main-thread', stop reason = signal SIGABRT
    frame #0: 0x00007fff913b90ae libsystem_kernel.dylib`__pthread_kill + 10
libsystem_kernel.dylib`__pthread_kill:
->  0x7fff913b90ae <+10>: jae    0x7fff913b90b8            ; <+20>
    0x7fff913b90b0 <+12>: movq   %rax, %rdi
    0x7fff913b90b3 <+15>: jmp    0x7fff913b43ef            ; cerror_nocancel
    0x7fff913b90b8 <+20>: retq
(lldb) bt
* thread #1: tid = 0x51f083, 0x00007fff913b90ae libsystem_kernel.dylib`__pthread_kill + 10, queue
= 'com.apple.main-thread', stop reason = signal SIGABRT
  * frame #0: 0x00007fff913b90ae libsystem_kernel.dylib`__pthread_kill + 10
    frame #1: 0x00007fff87d04500 libsystem_pthread.dylib`pthread_kill + 90
    frame #2: 0x00007fff8a31137b libsystem_c.dylib`abort + 129
    frame #3: 0x0000000010005de99 ruby`die + 9 at error.c:392
    frame #4: 0x0000000010005dbc4 ruby`rb_bug(fmt="rb_vm_get_cref: unreachable") + 484 at error.c:4
08
    frame #5: 0x0000000100244415 ruby`rb_vm_get_cref(ep=0x0000000104d8be80) + 53 at vm_insnhelper.
c:492
    frame #6: 0x00000001002510b9 ruby`vm_get_ev_const(th=0x0000000101800000, orig_klass=8, id=4505
1, is_defined=0) + 57 at vm_insnhelper.c:604
    frame #7: 0x0000000010022fb0f ruby`vm_exec_core(th=0x0000000101800000, initial=0) + 1583 at ins
ns.def:197
    frame #8: 0x0000000100244e3b ruby`vm_exec(th=0x0000000101800000) + 187 at vm.c:1505
    frame #9: 0x0000000100257cbd ruby`invoke_block(th=0x0000000101800000, iseq=0x00000001044423e8,
 self=4319073000, block=0x00000001019ffda0, cref=0x0000000000000000, type=33, opt_pc=0) + 205 at v
m.c:817
    frame #10: 0x0000000100257b1f ruby`invoke_block_from_c_0(th=0x0000000101800000, block=0x000000
01019ffda0, self=4319073000, argc=1, argv=0x00007fff5fbfc058, blockptr=0x0000000000000000, cref=0x
0000000000000000, splattable=1) + 1215 at vm.c:867
    frame #11: 0x000000010025764d ruby`invoke_block_from_c_splattable(th=0x0000000101800000, block
```

```
=0x00000001019ffda0, self=4319073000, argc=1, argv=0x00007fff5fbfc058, blockptr=0x0000000000000000
, cref=0x0000000000000000) + 93 at vm.c:884
    frame #12: 0x0000000100257578 ruby`vm_yield(th=0x0000000101800000, argc=1, argv=0x00007fff5fbf
c058) + 72 at vm.c:919
    frame #13: 0x0000000100240102 ruby`rb_yield_0(argc=1, argv=0x00007fff5fbfc058) + 34 at vm_eval
.c:999
    frame #14: 0x00000001002400cc ruby`rb_yield_1(val=4306342800) + 28 at vm_eval.c:1005
    frame #15: 0x0000000100240147 ruby`rb_yield(val=4306342800) + 55 at vm_eval.c:1015
    frame #16: 0x00000001000055ea ruby`rb_ary_each(ary=4306342240) + 154 at array.c:1820
    frame #17: 0x00000001002500c3 ruby`call_cfunc_0(func=(ruby`rb_ary_each at array.c:1815), recv=
4306342240, argc=0, argv=0x0000000101900180) + 35 at vm_insnhelper.c:1466
    frame #18: 0x000000010024e465 ruby`vm_call_cfunc_with_frame(th=0x0000000101800000, reg_cfp=0x0
0000001019ffd80, calling=0x00007fff5fbfcf28, ci=0x0000000103c2a3a0, cc=0x0000000103c565c0) + 1541
 at vm_insnhelper.c:1632
    frame #19: 0x000000010024a58a ruby`vm_call_cfunc(th=0x0000000101800000, reg_cfp=0x00000001019f
fd80, calling=0x00007fff5fbfcf28, ci=0x0000000103c2a3a0, cc=0x0000000103c565c0) + 186 at vm_insnhe
lper.c:1727
    frame #20: 0x00000001002335be ruby`vm_exec_core(th=0x0000000101800000, initial=0) + 16606 at i
nsns.def:947
    frame #21: 0x0000000100244e3b ruby`vm_exec(th=0x0000000101800000) + 187 at vm.c:1505
    frame #22: 0x0000000100257cbd ruby`invoke_block(th=0x0000000101800000, iseq=0x0000000104443978
, self=4366645200, block=0x00000001019fff20, cref=0x0000000000000000, type=33, opt_pc=0) + 205 at
 vm.c:817
    frame #23: 0x0000000100257b1f ruby`invoke_block_from_c_0(th=0x0000000101800000, block=0x000000
01019fff20, self=4366645200, argc=1, argv=0x00007fff5fbfd918, blockptr=0x0000000000000000, cref=0x
0000000000000000, splattable=1) + 1215 at vm.c:867
    frame #24: 0x000000010025764d ruby`invoke_block_from_c_splattable(th=0x0000000101800000, block
=0x00000001019fff20, self=4366645200, argc=1, argv=0x00007fff5fbfd918, blockptr=0x0000000000000000
, cref=0x0000000000000000) + 93 at vm.c:884
    frame #25: 0x0000000100257578 ruby`vm_yield(th=0x0000000101800000, argc=1, argv=0x00007fff5fbf
d918) + 72 at vm.c:919
    frame #26: 0x0000000100240102 ruby`rb_yield_0(argc=1, argv=0x00007fff5fbfd918) + 34 at vm_eval
.c:999
    frame #27: 0x00000001002400cc ruby`rb_yield_1(val=4319073000) + 28 at vm_eval.c:1005
    frame #28: 0x0000000100240147 ruby`rb_yield(val=4319073000) + 55 at vm_eval.c:1015
    frame #29: 0x000000010000cfea ruby`rb_ary_collect(ary=4306416000) + 186 at array.c:2738
    frame #30: 0x00000001002500c3 ruby`call_cfunc_0(func=(ruby`rb_ary_collect at array.c:2731), re
cv=4306416000, argc=0, argv=0x00000001019000a0) + 35 at vm_insnhelper.c:1466
    frame #31: 0x000000010024e465 ruby`vm_call_cfunc_with_frame(th=0x0000000101800000, reg_cfp=0x0
0000001019fff00, calling=0x00007fff5fbfe958, ci=0x0000000103c4d520, cc=0x0000000103c4ee50) + 1541
 at vm_insnhelper.c:1632
    frame #32: 0x000000010024a58a ruby`vm_call_cfunc(th=0x0000000101800000, reg_cfp=0x00000001019f
ff00, calling=0x00007fff5fbfe958, ci=0x0000000103c4d520, cc=0x0000000103c4ee50) + 186 at vm_insnhe
lper.c:1727
    frame #33: 0x0000000100249aa7 ruby`vm_call_method_each_type(th=0x0000000101800000, cfp=0x00000
001019fff00, calling=0x00007fff5fbfe958, ci=0x0000000103c4d520, cc=0x0000000103c4ee50) + 183 at vm
_insnhelper.c:2014
    frame #34: 0x000000010024982f ruby`vm_call_method(th=0x0000000101800000, cfp=0x00000001019fff0
0, calling=0x00007fff5fbfe958, ci=0x0000000103c4d520, cc=0x0000000103c4ee50) + 159 at vm_insnhelpe
r.c:2138
    frame #35: 0x0000000100249785 ruby`vm_call_general(th=0x0000000101800000, reg_cfp=0x0000000101
9fff00, calling=0x00007fff5fbfe958, ci=0x0000000103c4d520, cc=0x0000000103c4ee50) + 53 at vm_insnh
elper.c:2181
    frame #36: 0x00000001002335be ruby`vm_exec_core(th=0x0000000101800000, initial=0) + 16606 at i
nsns.def:947
    frame #37: 0x0000000100244e3b ruby`vm_exec(th=0x0000000101800000) + 187 at vm.c:1505
    frame #38: 0x0000000100257cbd ruby`invoke_block(th=0x0000000101800000, iseq=0x0000000104438118
, self=4366645200, block=0x0000000103abed80, cref=0x0000000000000000, type=33, opt_pc=0) + 205 at
 vm.c:817
    frame #39: 0x0000000100257b1f ruby`invoke_block_from_c_0(th=0x0000000101800000, block=0x000000
0103abed80, self=4366645200, argc=0, argv=0x00000001016ef838, blockptr=0x0000000000000000, cref=0x
0000000000000000, splattable=0) + 1215 at vm.c:867
    frame #40: 0x000000010025a76a ruby`invoke_block_from_c_unsplattable(th=0x0000000101800000, blo
ck=0x0000000103abed80, self=4366645200, argc=0, argv=0x00000001016ef838, blockptr=0x00000000000000
00, cref=0x0000000000000000) + 90 at vm.c:892
    frame #41: 0x0000000100244218 ruby`vm_invoke_proc(th=0x0000000101800000, proc=0x0000000103abed
80, self=4366645200, argc=0, argv=0x00000001016ef838, blockptr=0x0000000000000000) + 248 at vm.c:9
```

```
40
    frame #42: 0x00000001002440a5 ruby`rb_vm_invoke_proc(th=0x0000000101800000, proc=0x0000000103a
bed80, argc=0, argv=0x00000001016ef838, blockptr=0x0000000000000000) + 117 at vm.c:968
    frame #43: 0x0000000100007058a ruby`rb_proc_call(self=4366959240, args=4319017000) + 106 at pro
c.c:784
    frame #44: 0x0000000100066015 ruby`rb_call_end_proc(data=4366959240) + 37 at eval_jump.c:13
    frame #45: 0x0000000100066360 ruby`exec_end_procs_chain(procs=0x0000000100301e30) + 128 at eva
l_jump.c:107
    frame #46: 0x0000000100066221 ruby`rb_exec_end_proc + 209 at eval_jump.c:123
    frame #47: 0x000000010006694b ruby`ruby_finalize_0 + 171 at eval.c:121
    frame #48: 0x0000000100066b8b ruby`ruby_cleanup(ex=0) + 507 at eval.c:180
    frame #49: 0x00000001000672c9 ruby`ruby_run_node(n=0x0000000101294620) + 73 at eval.c:301
    frame #50: 0x0000000100000aef ruby`main(argc=6, argv=0x00007fff5fbffa38) + 95 at main.c:36
    frame #51: 0x00007fff86fd45ad libdyld.dylib`start + 1
    frame #52: 0x00007fff86fd45ad libdyld.dylib`start + 1
```

Related issues:

Related to Ruby master - Bug #11594: A Proc call may corrupt a local variable	**Closed**

History

#1 - 10/17/2015 12:30 AM - wanabe (_ wanabe)

Reproduced.

```
$ ruby -v -I lib:test test/cases/scoping/default_scoping_test.rb -n test_default_scope_select_ignored_by_group
ed_aggregations
ruby 2.3.0dev (2015-10-15 trunk 52128) [x86_64-linux]
Using sqlite3
Run options: -n test_default_scope_select_ignored_by_grouped_aggregations --seed 60909

# Running:

test/cases/scoping/default_scoping_test.rb:375: [BUG] rb_vm_get_cref: unreachable
ruby 2.3.0dev (2015-10-15 trunk 52128) [x86_64-linux]

... (snip) ...

[NOTE]
You may have encountered a bug in the Ruby interpreter or extension libraries.
Bug reports are welcome.
For details: http://www.ruby-lang.org/bugreport.html

Aborted (core dumped)
```

And it looks r52129 works fine for me.

```
$ ruby -v -I lib:test test/cases/scoping/default_scoping_test.rb -n test_default_scope_select_ignored_by_group
ed_aggregations
ruby 2.3.0dev (2015-10-15 trunk 52129) [x86_64-linux]
Using sqlite3
Run options: -n test_default_scope_select_ignored_by_grouped_aggregations --seed 45527

# Running:

.

Finished in 0.199474s, 5.0132 runs/s, 5.0132 assertions/s.

1 runs, 1 assertions, 0 failures, 0 errors, 0 skips
```

#2 - 10/17/2015 12:32 AM - wanabe (_ wanabe)

- Related to Bug #11594: A Proc call may corrupt a local variable added

#3 - 10/23/2015 08:26 AM - ko1 (Koichi Sasada)

- Assignee set to ko1 (Koichi Sasada)

#4 - 10/23/2015 10:12 AM - ko1 (Koichi Sasada)

- Status changed from Open to Closed

sorry i missed #1 comment written by wanabe-san.

if it can be reproduced yet, please reopen this ticket.

Files

ruby_2015-10-14-150003_TC.crash	22.9 KB	10/14/2015	tenderlovemaking (Aaron Patterson)