

Ruby - Bug #13284

IA64 ruby 2.4 miniruby segfault

03/05/2017 11:56 PM - ntfshard (Maksim Derbasov)

Status:	Closed	
Priority:	Normal	
Assignee:	takano32 (Mitsuhiro TAKANO)	
Target version:		
ruby -v:		Backport: 2.2: UNKNOWN, 2.3: DONE, 2.4: DONE
Description		
Hello, I faced with this degradation (2.0.0 work perfect) <pre>[ruby-2.4.0]\$ gdb ./miniruby GNU gdb Red Hat Linux (6.3.0.0-1.143.el4rh) Copyright 2004 Free Software Foundation, Inc. GDB is free software, covered by the GNU General Public License, and you are welcome to change it and/or distribute copies of it under certain conditions. Type "show copying" to see the conditions. There is absolutely no warranty for GDB. Type "show warranty" for details. This GDB was configured as "ia64-redhat-linux-gnu"...Using host libthread_db library "/lib/libthread_db.so.1". (gdb) run Starting program: /tmp/ruby-2.4.0/miniruby Reading symbols from shared object read from target memory...done. Loaded system supplied DSO at 0xa000000000000000 [Thread debugging using libthread_db enabled] [New Thread 16384 (LWP 28566)] Program received signal SIGSEGV, Segmentation fault. [Switching to Thread 16384 (LWP 28566)] reserve_stack (limit=0x60000ffc000010e0 <Address 0x60000ffc000010e0 out of bounds>, size=17179852800) at thread_pthread.c:722 722 limit[0] = 0; (gdb) print sz Variable "sz" is not available. (gdb) bt #0 reserve_stack (limit=0x60000ffc000010e0 <Address 0x60000ffc000010e0 out of bounds>, size=17179852800) at thread_pthread.c:722 #1 0x400000000038ee30 in ruby_init_stack (addr=0x60000fffffb4a0, bsp=0x60000ffbffffc080) at thread_pthread.c:751 #2 0x4000000000024460 in main (argc=1, argv=0x60000fffffb4b8) at main.c:34</pre> P.S. I did not get the main idea of a code but it looks a little bit dangerous (http://man7.org/linux/man-pages/man3/alloca.3.html http://stackoverflow.com/questions/1018853/why-is-the-use-of-alloca-not-considered-good-practice)		

Associated revisions

Revision 7aa74a0d0a22d74f1b3053280c56501aaf0b1e3c - 07/10/2017 06:57 AM - takano32 (Mitsuhiro TAKANO)

a64: fix crash on register stack mark/sweep pass

- thread_pthread.c: move 'register_stack_start' earlier.
[ruby-core:79928] [Bug #13284] [Fix GH-1625]

Author: Sergei Trofimovich slyfox@gentoo.org

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@59307 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7aa74a0d - 07/10/2017 06:57 AM - takano32 (Mitsuhiro TAKANO)

a64: fix crash on register stack mark/sweep pass

- thread_pthread.c: move 'register_stack_start' earlier.

[ruby-core:79928] [Bug #13284] [Fix GH-1625]

Author: Sergei Trofimovich slyfox@gentoo.org

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@59307 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 66163b7749fa4eb9e3e085dcfaac9df4715bc1f2 - 07/23/2017 08:05 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 59307: [Backport #13284]

```
a64: fix crash on register stack mark/sweep pass

* thread_pthread.c: move 'register_stack_start' earlier.
[ruby-core:79928] [Bug #13284] [Fix GH-1625]

Author:      Sergei Trofimovich <slyfox@gentoo.org>
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@59405 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 66163b77 - 07/23/2017 08:05 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 59307: [Backport #13284]

```
a64: fix crash on register stack mark/sweep pass

* thread_pthread.c: move 'register_stack_start' earlier.
[ruby-core:79928] [Bug #13284] [Fix GH-1625]

Author:      Sergei Trofimovich <slyfox@gentoo.org>
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_4@59405 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f6d9f6fd2a7ad2f20472f3704ae7d4e810627c54 - 08/09/2017 08:24 AM - U.Nakamura

merge revision(s) 59307: [Backport #13284]

```
a64: fix crash on register stack mark/sweep pass

* thread_pthread.c: move 'register_stack_start' earlier.
[ruby-core:79928] [Bug #13284] [Fix GH-1625]

Author:      Sergei Trofimovich <slyfox@gentoo.org>
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@59537 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision f6d9f6fd - 08/09/2017 08:24 AM - U.Nakamura

merge revision(s) 59307: [Backport #13284]

```
a64: fix crash on register stack mark/sweep pass

* thread_pthread.c: move 'register_stack_start' earlier.
[ruby-core:79928] [Bug #13284] [Fix GH-1625]

Author:      Sergei Trofimovich <slyfox@gentoo.org>
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@59537 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 03/13/2017 08:30 AM - naruse (Yui NARUSE)

- Status changed from Open to Assigned
- Assignee set to takano32 (Mitsuhiro TAKANO)

#2 - 07/10/2017 06:57 AM - takano32 (Mitsuhiro TAKANO)

- Status changed from Assigned to Closed

Applied in changeset trunk|r59307.

a64: fix crash on register stack mark/sweep pass

- thread_pthread.c: move 'register_stack_start' earlier.

Author: Sergei Trofimovich slyfox@gentoo.org

#3 - 07/10/2017 11:13 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.2: UNKNOWN, 2.3: UNKNOWN, 2.4: UNKNOWN to 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: REQUIRED

#4 - 07/23/2017 08:05 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: REQUIRED to 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: DONE

ruby_2_4 r59405 merged revision(s) 59307.

#5 - 08/09/2017 08:24 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.2: UNKNOWN, 2.3: REQUIRED, 2.4: DONE to 2.2: UNKNOWN, 2.3: DONE, 2.4: DONE

ruby_2_3 r59537 merged revision(s) 59307.

#6 - 10/09/2017 02:37 PM - ntfshard (Maksim Derbasov)

- Status changed from Closed to Open

Hello

Sorry for delay, but ruby-2.4.2 still has this issue. May be something wrong with size argument?

```
[ruby-2.4.2]$ gdb ./miniruby
GNU gdb Red Hat Linux (6.3.0.0-1.143.el4rh)
Copyright 2004 Free Software Foundation, Inc.
```

```
(gdb) run
Starting program: /tmp/ruby-2.4.2/miniruby
Reading symbols from shared object read from target memory...done.
Loaded system supplied DSO at 0xa000000000000000
[Thread debugging using libthread_db enabled]
[New Thread 16384 (LWP 22035)]
```

```
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread 16384 (LWP 22035)]
reserve_stack (limit=0x60000ffc000010e0 <Address 0x60000ffc000010e0 out of bounds>, size=17179852800) at thread_pthread.c:722
722      limit[0] = 0;
(gdb) bt
#0  reserve_stack (limit=0x60000ffc000010e0 <Address 0x60000ffc000010e0 out of bounds>, size=17179852800) at thread_pthread.c:722
#1  0x200000080042bef0 in ruby_init_stack (addr=0x60000ffffffb8f0, bsp=Variable "bsp" is not available.
) at thread_pthread.c:757
#2  0x20000008000870a0 in main (argc=1, argv=0x60000ffffffb908) at main.c:34
(gdb)
```

#7 - 11/10/2017 07:08 AM - hsbt (Hiroshi SHIBATA)

- Status changed from Open to Assigned

#8 - 06/14/2018 11:23 AM - knedlsepp (Josef Kemetmüller)

I tried a few suggestions, which did not work out for me:

- Configure with --with-setjmp-type=_setjmp
- Compile using -O0 -fno-omit-frame-pointer -fno-stack-protector

What finally worked for me was to run the build without stack limits: ulimit -s unlimited.

#9 - 06/24/2019 08:30 PM - jeremyevans0 (Jeremy Evans)

- Status changed from Assigned to Closed

Ruby has dropped support for IA64.