Ruby master - Bug #18497

Fiber内でProcess.daemonをするとSegmentation faultが起こる

01/19/2022 08:11 AM - sevenc-nanashi (Nanashi. @sevenc-nanashi)

Status: Closed
Priority: Normal
Assignee:
Target version:
ruby -v: ruby 3.1.0p0 (2021-12-25 revision fb4df44d16) [aarch64-linux]
Backport: 2.6: REQUIRED, 2.7: REQUIRED, 3.0: REQUIRED, 3.1: DONE

Description
ruby -e 'Fiber.new { Process.daemon true, true }.resume'

OCIのUbuntu(ruby 3.1.0p0 (2021-12-25 revision fb4df44d16) [aarch64-linux])とWSL(ruby 3.1.0p0 (2021-12-25 revision fb4df44d16) [x86_64-linux])で確認できましたが、WSLでは確認できませんでした。

Associated revisions
Revision d650b176 - 01/19/2022 10:57 AM - nobu (Nobuyoshi Nakada)

rb_fiber_terminate must not return [Bug #18497]

In a forked process from a fiber, the fiber becomes the only fiber, fiber_switch does nothing as there is no other fibers, rb_fiber_terminate does not terminate the fiber. In that case, reaches the end of fiber_entry finally, which is declared as "COROUTINE" and should never return.

Revision 1c426ddb - 01/31/2022 10:22 AM - naruse (Yui NARUSE)

merge revision(s) 5c7af72304d0ad33cd3f12b24a44e8acd5b2c,d650b17686d49c2ce8e6a87039861154e93d4621: [Backport #18497]

---

Test ruby/test_fiber.rb | 6 ++----
1 file changed, 3 insertions(+), 3 deletions(-)

`rb_fiber_terminate` must not return [Bug #18497]

In a forked process from a fiber, the fiber becomes the only fiber, 'fiber_switch' does nothing as there is no other fibers, 'rb_fiber_terminate' does not terminate the fiber. In that case, reaches the end of 'fiber_entry' finally, which is declared as "COROUTINE" and should never return.

---

cont.c | 3 ++-
eval_intern.h | 2 +-{}
test/fiber/test_process.rb | 15 ++++++++++++++
test/ruby/test_fiber.rb | 5 +++++
4 files changed, 23 insertions(+), 2 deletions(-)

History
#1 - 01/19/2022 02:08 PM - nobu (Nobuyoshi Nakada)

- Backport changed from 2.6: UNKNOWN, 2.7: UNKNOWN, 3.0: UNKNOWN, 3.1: UNKNOWN to 2.6: REQUIRED, 2.7: REQUIRED, 3.0: REQUIRED, 3.1: REQUIRED

#2 - 01/19/2022 02:10 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset git|d650b17686d49c2ce8e6a87039861154e93d4621.

rb_fiber_terminate must not return [Bug #18497]
In a forked process from a fiber, the fiber becomes the only fiber, fiber_switch does nothing as there is no other fibers, rb_fiber_terminate does not terminate the fiber. In that case, reaches the end of fiber_entry finally, which is declared as "COROUTINE" and should never return.

#3 - 01/19/2022 02:34 PM - nobu (Nobuyoshi Nakada)

In 2.7 or earlier, bf3b2a43741e or the following patch is also needed.

diff --git a/cont.c b/cont.c
index 7f971a9e9d5..50403b8258d 100644
--- a/cont.c
+++ b/cont.c
@@ -1930,7 +1930,7 @@ fiber_current(void)
 )
 }
 static inline rb_fiber_t *
-rb_fiber_current(void)
+rb_fiber_current(bool terminate)
 {
     rb_fiber_t *fiber = fiber_current();
     rb_fiber_t *prev = fiber->prev;
@@ -1941,7 +1941,7 @@
     VM_ASSERT(root_fiber != NULL);
     return root_fiber;
@@ -2087,7 +2087,7 @@
     VM_ASSERT(root_fiber != NULL);
     if (root_fiber == fiber) {
         if (!terminate && root_fiber == fiber) {
+             rb_fiber_terminate(rb_fiber_t *fiber, int need_interrupt)
             rb_fiber_yield_kw(int argc, const VALUE *argv)
             rb_fiber_yield(int argc, const VALUE *argv)
         }
     }
     next_fiber = return_fiber(true);
     fiber->cont.machine.stack = NULL;
     fiber->cont.machine.stack_size = 0;
     next_fiber = return_fiber();
 }