Subject: [IA64] unwind did not work for processes born with CLONE_STOPPED
Posted by dev on Mon, 19 Mar 2007 10:50:21 GMT
View Forum Message <> Reply to Message

[IA64] unwind did not work for processes born with CLONE_STOPPED

Minor problem for mainstream. Big problem for CPT, because all the
stopped/traced processes are born in this state, hence they cannot
be checkpointed again due to failing unwind.

The problem was identified as assumption in kernel unwind library
that top level frame is different of syscall frame. It is the case
unless process was born with CLONE_STOPPED.

Author: Alexey Kuznetsov <kuznet@ms2.inr.ac.ru>
Signed-Off-By: Alexey Kuznetsov <kuznet@ms2.inr.ac.ru>
Signed-Off-By: Kirill Korotaev <dev@sw.ru>

```
--- a/arch/ia64/kernel/unwind.c
+++ b/arch/ia64/kernel/unwind.c
@@ -60,6 +60,7 @@ #ifdef UNW_DEBUG
 #  define UNW_DEBUG_ON(n) unw_debug_level >= n
    /* Do not code a printk level, not all debug lines end in newline */
 #  define UNW_DPRINT(n, ...)  if (UNW_DEBUG_ON(n)) printk(__VA_ARGS__)
+#  undef inline
 #  define inline
 #else /* !UNW_DEBUG */
 #  define UNW_DEBUG_ON(n)  0
@@ -1943,9 +1944,9 @@ EXPORT_SYMBOL(unw_unwind);
 int
 unw_unwind_to_user (struct unw_frame_info *info)
 {
- unsigned long ip, sp, pr = 0;
+ unsigned long ip, sp, pr = info->pr;

- while (unw_unwind(info) >= 0) {
+ do {
    unw_get_sp(info, &sp);
    if ((long)((unsigned long)info->task + IA64_STK_OFFSET - sp)
        < IA64_PT_REGS_SIZE) {
@@ -1963,7 +1964,7 @@ unw_unwind_to_user (struct unw_frame_inf
      __FUNCTION__, ip);
    return -1;
   }
- }
+ } while (unw_unwind(info) >= 0);
  unw_get_ip(info, &ip);
  UNW_DPRINT(0, "unwind.%s: failed to unwind to user-level (ip=0x%lx)\n",
```

__FUNCTION__, ip);