

---

Subject: [PATCH v6] posix timers: allocate timer id per process  
Posted by [Stanislav Kinsbursky](#) on Wed, 24 Oct 2012 11:45:26 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

This patch is required CRIU project ([www.criu.org](http://www.criu.org)).  
To migrate processes with posix timers we have to make sure, that we can restore posix timer with proper id.  
Currently, this is not true, because timer ids are allocated globally.  
So, this is precursor patch and it's purpose is make posix timer id to be allocated per process.

Patch replaces global idr with global hash table for posix timers and makes timer ids unique not globally, but per process. Next free timer id is type of integer and stored on signal struct (posix\_timer\_id). If free timer id reaches negative value on timer creation, it will be dropped to zero and -EAGAIN will be returned to user.

Hash table has 512 slots.  
Key is constructed as follows:  
`key = hash_32(hash_32(current->signal) ^ posix_timer_id);`

Note: with this patch, id, returned to user, is not the minimal free anymore. It means, that id, returned to user space in loop, listed below, will be increasing on each iteration till INT\_MAX and then dropped to zero:

```
while(1) {  
    id = timer_create(...);  
    timer_delete(id);  
}
```

Signed-off-by: Stanislav Kinsbursky <[skinsbursky@parallels.com](mailto:skinsbursky@parallels.com)>

---

v6:

- 1) include of "linux/idr.h" removed from "include/linux/sched.h"
- 2) include of "linux/idr.h" removed from "kernel/posix-timers.c"
- 3) per-process id overlap on timer add fixed

v5:

- 1) Patch changelog updated

v4:

- 1) a couple of coding style fixes (lines over 80 characters)

v3:

- 1) hash calculation simlified to improve perfomance.

v2:

1) Hash table become RCU-friendly. Hash table search now done under RCU lock protection.

I've tested scalability on KVM with 4 CPU. The testing environment was build of 10 processes, each had 512 posix timers running (SIGSEV\_NONE) and was calling timer\_gettime() in loop. With all this stuff being running, I was measuring time of calling of syscall timer\_gettime() 10000 times.

Without this patch: ~7ms

With this patch : ~7ms

---

```
include/linux/posix-timers.h | 1
include/linux/sched.h        | 3 +
kernel/posix-timers.c        | 114 ++++++-----
3 files changed, 78 insertions(+), 40 deletions(-)
```

diff --git a/include/linux/posix-timers.h b/include/linux/posix-timers.h

index 042058f..60bac69 100644

--- a/include/linux/posix-timers.h

+++ b/include/linux/posix-timers.h

@@ -55,6 +55,7 @@ struct cpu\_timer\_list {

/\* POSIX.1b interval timer structure. \*/

struct k\_itimer {

struct list\_head list; /\* free/ allocate list \*/

+ struct hlist\_node t\_hash;

spinlock\_t it\_lock;

clockid\_t it\_clock; /\* which timer type \*/

timer\_t it\_id; /\* timer id \*/

diff --git a/include/linux/sched.h b/include/linux/sched.h

index 0dd42a0..9f8e2ea 100644

--- a/include/linux/sched.h

+++ b/include/linux/sched.h

@@ -536,7 +536,8 @@ struct signal\_struct {

unsigned int has\_child\_subreaper:1;

/\* POSIX.1b Interval Timers \*/

- struct list\_head posix\_timers;

+ int posix\_timer\_id;

+ struct list\_head posix\_timers;

/\* ITIMER\_REAL timer for the process \*/

struct hrtimer real\_timer;

diff --git a/kernel/posix-timers.c b/kernel/posix-timers.c

index 69185ae..9cfb86a 100644

--- a/kernel/posix-timers.c

+++ b/kernel/posix-timers.c

@@ -40,7 +40,7 @@

#include <linux/list.h>

```

#include <linux/init.h>
#include <linux/compiler.h>
#include <linux/idr.h>
#include <linux/hash.h>
#include <linux/posix-clock.h>
#include <linux/posix-timers.h>
#include <linux/syscalls.h>
@@ -49,29 +49,25 @@
#include <linux/export.h>

/*
- * Management arrays for POSIX timers. Timers are kept in slab memory
- * Timer ids are allocated by an external routine that keeps track of the
- * id and the timer. The external interface is:
- *
- * void *idr_find(struct idr *idp, int id);      to find timer_id <id>
- * int idr_get_new(struct idr *idp, void *ptr);  to get a new id and
- *                                             related it to <ptr>
- * void idr_remove(struct idr *idp, int id);    to release <id>
- * void idr_init(struct idr *idp);              to initialize <idp>
- *                                             which we supply.
- * The idr_get_new *may* call slab for more memory so it must not be
- * called under a spin lock. Likewise idr_remove may release memory
- * (but it may be ok to do this under a lock...).
- * idr_find is just a memory look up and is quite fast. A -1 return
- * indicates that the requested id does not exist.
+ * Management arrays for POSIX timers. Timers are now kept in static hash table
+ * with 512 entries.
+ * Timer ids are allocated by local routine, which selects proper hash head by
+ * key, constructed from current->signal address and per signal struct counter.
+ * This keeps timer ids unique per process, but now they can intersect between
+ * processes.
 */

/*
 * Lets keep our timers in a slab cache :-)
 */
static struct kmem_cache *posix_timers_cache;
static struct idr posix_timers_idr;
static DEFINE_SPINLOCK(idr_lock);
+
+#define POSIX_TIMERS_HASH_BITS 9
+#define POSIX_TIMERS_HASH_SIZE (1 << POSIX_TIMERS_HASH_BITS)
+
+/* Hash table is size of PAGE currently */
+static struct hlist_head posix_timers_hashtable[POSIX_TIMERS_HASH_SIZE];
+static DEFINE_SPINLOCK(hash_lock);

```

```

/*
 * we assume that the new SIGEV_THREAD_ID shares no bits with the other
 @@ -152,6 +148,57 @@ static struct k_itimer *__lock_timer(timer_t timer_id, unsigned long
 *flags);
 __timr;      \
 })

+static int hash(struct signal_struct *sig, unsigned int nr)
+{
+ return hash_32(hash32_ptr(sig) ^ nr, POSIX_TIMERS_HASH_BITS);
+}
+
+static struct k_itimer *__posix_timers_find(struct hlist_head *head,
+      struct signal_struct *sig,
+      timer_t id)
+{
+ struct hlist_node *node;
+ struct k_itimer *timer;
+
+ hlist_for_each_entry_rcu(timer, node, head, t_hash) {
+ if ((timer->it_signal == sig) && (timer->it_id == id))
+ return timer;
+ }
+ return NULL;
+}
+
+static struct k_itimer *posix_timer_by_id(timer_t id)
+{
+ struct signal_struct *sig = current->signal;
+ struct hlist_head *head = &posix_timers_hashtable[hash(sig, id)];
+
+ return __posix_timers_find(head, sig, id);
+}
+
+static int posix_timer_add(struct k_itimer *timer)
+{
+ struct signal_struct *sig = current->signal;
+ int first_free_id = sig->posix_timer_id;
+ struct hlist_head *head;
+ int ret = -ENOENT;
+
+ do {
+ spin_lock(&hash_lock);
+ head = &posix_timers_hashtable[hash(sig, sig->posix_timer_id)];
+ if (!__posix_timers_find(head, sig, sig->posix_timer_id)) {
+ hlist_add_head_rcu(&timer->t_hash, head);
+ ret = sig->posix_timer_id;
+ }

```

```

+ if (++sig->posix_timer_id < 0)
+   sig->posix_timer_id = 0;
+ if ((sig->posix_timer_id == first_free_id) && (ret == -ENOENT))
+   /* Loop over all possible ids completed */
+   ret = -EAGAIN;
+ spin_unlock(&hash_lock);
+ } while (ret == -ENOENT);
+ return ret;
+}
+
static inline void unlock_timer(struct k_itimer *timr, unsigned long flags)
{
    spin_unlock_irqrestore(&timr->it_lock, flags);
@@ -271,6 +318,7 @@ static __init int init_posix_timers(void)
    .timer_get = common_timer_get,
    .timer_del = common_timer_del,
};
+ int i;

    posix_timers_register_clock(CLOCK_REALTIME, &clock_realtime);
    posix_timers_register_clock(CLOCK_MONOTONIC, &clock_monotonic);
@@ -282,7 +330,8 @@ static __init int init_posix_timers(void)
    posix_timers_cache = kmem_cache_create("posix_timers_cache",
        sizeof (struct k_itimer), 0, SLAB_PANIC,
        NULL);
- idr_init(&posix_timers_id);
+ for (i = 0; i < POSIX_TIMERS_HASH_SIZE; i++)
+ INIT_HLIST_HEAD(&posix_timers_hashtable[i]);
    return 0;
}

@@ -504,9 +553,9 @@ static void release_posix_timer(struct k_itimer *tmr, int it_id_set)
{
    if (it_id_set) {
        unsigned long flags;
- spin_lock_irqsave(&idr_lock, flags);
- idr_remove(&posix_timers_id, tmr->it_id);
- spin_unlock_irqrestore(&idr_lock, flags);
+ spin_lock_irqsave(&hash_lock, flags);
+ hlist_del_rcu(&tmr->t_hash);
+ spin_unlock_irqrestore(&hash_lock, flags);
    }
    put_pid(tmr->it_pid);
    sigqueue_free(tmr->sigq);
@@ -552,22 +601,9 @@ SYSCALL_DEFINE3(timer_create, const clockid_t, which_clock,
    return -EAGAIN;

    spin_lock_init(&new_timer->it_lock);

```

```

- retry:
- if (unlikely(!idr_pre_get(&posix_timers_id, GFP_KERNEL))) {
- error = -EAGAIN;
- goto out;
- }
- spin_lock_irq(&idr_lock);
- error = idr_get_new(&posix_timers_id, new_timer, &new_timer_id);
- spin_unlock_irq(&idr_lock);
- if (error) {
- if (error == -EAGAIN)
- goto retry;
- /*
-  * Weird looking, but we return EAGAIN if the IDR is
-  * full (proper POSIX return value for this)
-  */
- error = -EAGAIN;
+ new_timer_id = posix_timer_add(new_timer);
+ if (new_timer_id < 0) {
+ error = new_timer_id;
+ goto out;
+ }

@@ -640,7 +676,7 @@ static struct k_itimer *__lock_timer(timer_t timer_id, unsigned long *flags)
struct k_itimer *timr;

rcu_read_lock();
- timr = idr_find(&posix_timers_id, (int)timer_id);
+ timr = posix_timer_by_id(timer_id);
if (timr) {
spin_lock_irqsave(&timr->it_lock, *flags);
if (timr->it_signal == current->signal) {

```

---