
Subject: Re: [RFC][PATCH 1/2] add user namespace [try #2]
Posted by [Dave Hansen](#) on Mon, 28 Aug 2006 15:06:25 GMT
[View Forum Message](#) <> [Reply to Message](#)

On Mon, 2006-08-28 at 16:56 +0200, Cedric Le Goater wrote:

```
>
> + * Clone a new ns copying an original user ns, setting refcount to 1
> + * @old_ns: namespace to clone
> + * Return NULL on error (failure to kmalloc), new ns otherwise
> + */
> +static struct user_namespace *clone_user_ns(struct user_namespace
> +*old_ns)
> +{
> +    struct user_namespace *ns;
> +
> +    ns = kmalloc(sizeof(struct user_namespace), GFP_KERNEL);
> +    if (ns) {
> +        int n;
> +        struct user_struct *new_user;
> +
> +        kref_init(&ns->kref);
> +
> +        for(n = 0; n < UIDHASH_SZ; ++n)
> +            INIT_LIST_HEAD(ns->uidhash_table + n);
> +
> +        /* Insert new root user. */
> +        ns->root_user = alloc_uid(ns, 0);
> +        if (!ns->root_user) {
> +            kfree(ns);
> +            return NULL;
> +        }
> +
> +        /* Reset current->user with a new one */
> +        new_user = alloc_uid(ns, current->uid);
> +        if (!new_user) {
> +            kfree(ns);
> +            return NULL;
> +        }
> +    }
```

Does this leak the ns->root_user?

```
> +
> +        switch_uid(new_user);
> +    }
> +    return ns;
> +}
```

-- Dave

Subject: Re: [RFC][PATCH 1/2] add user namespace [try #2]
Posted by [Cedric Le Goater](#) on Mon, 28 Aug 2006 15:14:58 GMT
[View Forum Message](#) <> [Reply to Message](#)

Dave Hansen wrote:

```
> On Mon, 2006-08-28 at 16:56 +0200, Cedric Le Goater wrote:
>> + * Clone a new ns copying an original user ns, setting refcount to 1
>> + * @old_ns: namespace to clone
>> + * Return NULL on error (failure to kmalloc), new ns otherwise
>> + */
>> +static struct user_namespace *clone_user_ns(struct user_namespace
>> +*old_ns)
>> +{
>> +    struct user_namespace *ns;
>> +
>> +    ns = kmalloc(sizeof(struct user_namespace), GFP_KERNEL);
>> +    if (ns) {
>> +        int n;
>> +        struct user_struct *new_user;
>> +
>> +        kref_init(&ns->kref);
>> +
>> +        for(n = 0; n < UIDHASH_SZ; ++n)
>> +            INIT_LIST_HEAD(ns->uidhash_table + n);
>> +
>> +        /* Insert new root user. */
>> +        ns->root_user = alloc_uid(ns, 0);
>> +        if (!ns->root_user) {
>> +            kfree(ns);
>> +            return NULL;
>> +        }
>> +
>> +        /* Reset current->user with a new one */
>> +        new_user = alloc_uid(ns, current->uid);
>> +        if (!new_user) {
>> +            kfree(ns);
>> +            return NULL;
>> +        }
>> +
>
> Does this leak the ns->root_user?
```

arg !

thanks,

C.

Containers mailing list
Containers@lists.osdl.org
<https://lists.osdl.org/mailman/listinfo/containers>

Subject: Re: [RFC][PATCH 1/2] add user namespace [try #2]
Posted by [Cedric Le Goater](#) on Thu, 31 Aug 2006 12:36:15 GMT
[View Forum Message](#) <> [Reply to Message](#)

Cedric Le Goater wrote:

> Dave Hansen wrote:

>> On Mon, 2006-08-28 at 16:56 +0200, Cedric Le Goater wrote:

>>> + * Clone a new ns copying an original user ns, setting refcount to 1

>>> + * @old_ns: namespace to clone

>>> + * Return NULL on error (failure to kmalloc), new ns otherwise

>>> + */

>>> +static struct user_namespace *clone_user_ns(struct user_namespace
>>> *old_ns)

>>> +{

>>> + struct user_namespace *ns;

>>> +

>>> + ns = kmalloc(sizeof(struct user_namespace), GFP_KERNEL);

>>> + if (ns) {

>>> + int n;

>>> + struct user_struct *new_user;

>>> +

>>> + kref_init(&ns->kref);

>>> +

>>> + for(n = 0; n < UIDHASH_SZ; ++n)

>>> + INIT_LIST_HEAD(ns->uidhash_table + n);

>>> +

>>> + /* Insert new root user. */

>>> + ns->root_user = alloc_uid(ns, 0);

>>> + if (!ns->root_user) {

>>> + kfree(ns);

>>> + return NULL;

>>> + }

>>> +

>>> + /* Reset current->user with a new one */

>>> + new_user = alloc_uid(ns, current->uid);

>>> + if (!new_user) {

>>> + kfree(ns);

```
>>> +          return NULL;
>>> +      }
>> Does this leak the ns->root_user?
>
> arg !
>
> thanks,
```

Sorry, I forgot to include the fix.

C.

Signed-off-by: Cedric Le Goater <clg@fr.ibm.com>

kernel/user.c | 1 +
1 file changed, 1 insertion(+)

Index: 2.6.18-rc4-mm3/kernel/user.c

=====

--- 2.6.18-rc4-mm3.orig/kernel/user.c

+++ 2.6.18-rc4-mm3/kernel/user.c

```
@@ -125,6 +125,7 @@ static struct user_namespace *clone_user
/* Reset current->user with a new one */
new_user = alloc_uid(ns, current->uid);
if (!new_user) {
+ free_uid(ns->root_user);
  kfree(ns);
  return NULL;
}
```

Containers mailing list
Containers@lists.osdl.org
<https://lists.osdl.org/mailman/listinfo/containers>
