

---

Subject: Re: Containers don't handle keys, but should they?

Posted by [David Howells](#) on Fri, 14 Mar 2008 15:49:20 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Serge E. Hallyn <serue@us.ibm.com> wrote:

> It looks like maybe just adding a struct user\_namespace \* to a struct key  
> should suffice.

That's not quite sufficient. The per-UID key\_user structs also need to be differentiated. Unfortunately, I can't just merge it into user\_struct as I then end up with a reference loop user\_struct -> uid\_keyring -> user\_struct.

Rooting the key\_user trees in user\_namespace will probably do the trick.

A couple of questions:

- (1) A process may inherit a session keyring over clone(). Should this be discarded if CLONE\_NEWUSER is set? Or would I need to copy it?
- (2) In a recent patch, I've given the root user its own quota limits. Is UID 0 always the root user in any container? Or would it make more sense just to scrap the per-root quota limits?

David

---

Containers mailing list

Containers@lists.linux-foundation.org

<https://lists.linux-foundation.org/mailman/listinfo/containers>

---