Subject: Re: Containers don't handle keys, but should they?
Posted by serue on Fri, 14 Mar 2008 14:54:47 GMT
View Forum Message <> Reply to Message

Quoting David Howells (dhowells@redhat.com):
>
> Am I right in thinking that a UID in one container is not necessarily
> equivalent to the numerically equivalent UID in another container?
>
> If that's the case then the key management code will need changing as it
> assumes all keys belonging to one numeric UID eat out of the same quota and
> the numeric UIDs are used in security checks.
>
> Furthermore, processes in one container can access keys created by a process
> in another container by ID. Is this desirable or not?
>
> David

Yes, the confusion comes from using the word 'container' which doesn't really exist. The user namespaces (CLONE_NEWUSER) are what provide separate of uids. We want uid 5 in one user namespace to have completely separate set of keys from uid 5 in another user namespace.

This isn't yet a crucial thing to get right as the user namespaces are only partially implemented, but it's certainly a good thing to be looking at and fix when convenient to do so. It looks like maybe just adding a struct user_namespace * to a struct key should suffice.

-serge