Subject: Re: [PATCH 20/25] sysfs: Rename Support multiple superblocks
Posted by ebiederm on Wed, 08 Aug 2007 16:55:10 GMT
View Forum Message <> Reply to Message

Tejun Heo <htejun@gmail.com> writes:

> Eric W. Biederman wrote:
>>> /* Find the first parent which has valid dentry.
>>>   */
>>> dentry = NULL;
>>> cur = sd;
>>> while (!(dentry = __sysfs_get_dentry(sb, cur))) {
>>>   if (cur->s_flags & SYSFS_FLAG_REMOVED) {
>>>   dentry = ERR_PTR(-ENOENT);
>>>   break;
>>>   }
>>>   cur = cur->s_parent;
>>> }
>>
>> Here we depend on the fact that sysfs_root is pointed to
>> by sb->s_root so we know it will always have a dentry.
>
> Hmmm... dentry could be ERR_PTR(-ENOENT) here if the REMOVED flag test
> succeeded, right?

Ugh right. Now that I don't have the locking it probably makes
sense to have that path just return or branch to the exit.

>
>>> /* from the found dentry, look up depth times */
>>> while (dentry->d_fsdata != sd) {
>
> And then dereferenced. The REMOVED test should never succeed there, so
> we're probably in the clear but still the code looks a bit scary.

Agreed. That is a bug. Either the removed test needs to
be removed because it can't happen or that case needs to be handled.

Thanks for spotting this one.

Mental blind spots are the worst.

Eric

_____
Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers