Subject: Re: [PATCH v2] SUNRPC: skip dead but not buried clients on PipeFS events
Posted by Stanislav Kinsbursky on Thu, 26 Apr 2012 06:31:45 GMT
View Forum Message <> Reply to Message

> On Fri, Apr 20, 2012 at 06:11:02PM +0400, Stanislav Kinsbursky wrote:
>> v2: atomic_inc_return() was replaced by atomic_inc_not_zero().
>>
>> These clients can't be safely dereferenced if their counter in 0.
> I'm pretty confused by how these notifiers work....
>
> rpc_release_client decrements cl_count to zero temporarily, to have it
> immediately re-incremented by rpc_free_auth.
>
> So if we're called concurrently with rpc_release_client then it's sort
> of random whether someone gets this callback.
>
> Is that a problem?
>
> Also, is this an existing bug? (In which case Trond should take it
> now.)

Sorry, I was mistaken in previous letter.
Yes, this is an existent bug.
I.e. without this patch notifier can dereference a client, which is
actually dead already, but haven't deleted itself from the client's list.
And then notifier will try to work with this client and even release it
at the end.