Subject: Re: [PATCH] NFS: init client before declaration
Posted by Myklebust, Trond on Tue, 22 May 2012 15:00:17 GMT
View Forum Message <> Reply to Message

On Tue, 2012-05-22 at 10:29 -0400, Trond Myklebust wrote:
> On Tue, 2012-05-22 at 16:40 +0400, Stanislav Kinsbursky wrote:
> > Client have to be initialized prior to adding it to per-net clients list,
> > because otherwise there are races, shown below:
> >
> > CPU#0 CPU#1
> > _____ _____
> >
> > nfs_get_client
> > nfs_alloc_client
> > list_add(..., nfs_client_list)
> > rpc_fill_super
> > rpc_pipefs_event
> > nfs_get_client_for_event
> > __rpc_pipefs_event
> > (clp->cl_rpcclient is uninitialized)
> > BUG()
> > init_client
> > clp->cl_rpcclient = ...
> >
>
> Why not simply change nfs_get_client_for_event() so that it doesn't
> touch nfs_clients that have clp->cl_cons_state!=NFS_CS_READY?
>
> That should ensure that it doesn't touch nfs_clients that failed to
> initialise and/or are still in the process of being initialised.

...actually, come to think of it. Why not just add a helper function
"bool nfs_client_active(const struct nfs_client *clp)" to
fs/nfs/client.c that does a call to
 wait_event_killable(nfs_client_active_wq, clp->cl_cons_state < NFS_CS_INITING);
and checks the resulting value of clp->cl_cons_state?

--
Trond Myklebust
Linux NFS client maintainer

NetApp
Trond.Myklebust@netapp.com
www.netapp.com