Subject: Re: [PATCH] NFS: init client before declaration
Posted by Myklebust, Trond on Tue, 22 May 2012 14:29:44 GMT
View Forum Message <> Reply to Message

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.

Cheers
  Trond

--
Trond Myklebust
Linux NFS client maintainer

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