Subject: Re: [PATCH] NFS: init client before declaration Posted by Stanislav Kinsbursky on Tue, 22 May 2012 15:03:37 GMT View Forum Message <> Reply to Message

```
On 22.05.2012 18:29, Myklebust, Trond 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.
It looks like in this case we will have another races:
CPU#0
           CPU#1
nfs4 init client
nfs idmap new
nfs idmap register
rpc get sb net (fail - no pipefs)
    rpc_fill_super
    rpc_pipefs_event
    nfs_get_client_for_event
   (skip client - NFS_CS_READY is not set)
nfs_mark_client_ready(NFS_CS_READY)
```

And we are having client without idmap pipe	
> Cheers > Trond >	
 Best regards, Stanislav Kinsbursky	