Subject: [PATCH 4/6] SUNRPC: remove RPC client pipefs dentries after unregister
Posted by Stanislav Kinsbursky on Wed, 23 Nov 2011 11:05:00 GMT
View Forum Message <> Reply to Message

Without this patch we have races:

```
rpc_fill_super    rpc_free_client
rpc_pipefs_event(MOUNT)   rpc_remove_pipedir
spin_lock(&rpc_client_lock);
rpc_setup_pipedir_sb
spin_unlock(&rpc_client_lock);
    spin_lock(&rpc_client_lock);
    (remove from list)
    spin_unlock(&rpc_client_lock);
    MEAMORY LEAKED
```

Signed-off-by: Stanislav Kinsbursky <skinsbursky@parallels.com>

---
 net/sunrpc/clnt.c | 2 +-
 1 files changed, 1 insertions(+), 1 deletions(-)

```
diff --git a/net/sunrpc/clnt.c b/net/sunrpc/clnt.c
index 61c76ae..23776a4 100644
--- a/net/sunrpc/clnt.c
+++ b/net/sunrpc/clnt.c
@@ -572,7 +572,6 @@ rpc_free_client(struct rpc_clnt *clnt)
 {
  dprintk("RPC:       destroying %s client for %s\n",
    clnt->cl_protname, clnt->cl_server);
- rpc_clnt_remove_pipedir(clnt);
  if (clnt->cl_parent != clnt) {
   rpc_release_client(clnt->cl_parent);
   goto out_free;
@@ -581,6 +580,7 @@ rpc_free_client(struct rpc_clnt *clnt)
   kfree(clnt->cl_server);
 out_free:
  rpc_unregister_client(clnt);
+ rpc_clnt_remove_pipedir(clnt);
  rpc_free_iostats(clnt->cl_metrics);
  kfree(clnt->cl_principal);
  clnt->cl_metrics = NULL;
```