Subject: [patch 17/22] elevate write count over calls to vfs_rename()
Posted by Cedric Le Goater on Thu, 07 Jun 2007 15:25:44 GMT
View Forum Message <> Reply to Message

From: Dave Hansen <hansendc@us.ibm.com>

This also creates a little helper in the NFS code to
make an if() a little bit less ugly.

Signed-off-by: Dave Hansen <hansendc@us.ibm.com>

---
 fs/namei.c | 4 ++++
 fs/nfsd/vfs.c | 23 +++++++++++++++++++----
 2 files changed, 23 insertions(+), 4 deletions(-)

Index: 2.6.22-rc4-mm2-robindmount/fs/namei.c
===
--- 2.6.22-rc4-mm2-robindmount.orig/fs/namei.c
+++ 2.6.22-rc4-mm2-robindmount/fs/namei.c
@@ -2627,8 +2627,12 @@ static int do_rename(int olddfd, const c
  if (new_dentry == trap)
   goto exit5;

+ error = mnt_want_write(oldnd.mnt);
+ if (error)
+ goto exit5;
  error = vfs_rename(old_dir->d_inode, old_dentry,
      new_dir->d_inode, new_dentry);
+ mnt_drop_write(oldnd.mnt);
 exit5:
  dput(new_dentry);
 exit4:
Index: 2.6.22-rc4-mm2-robindmount/fs/nfsd/vfs.c
===
--- 2.6.22-rc4-mm2-robindmount.orig/fs/nfsd/vfs.c
+++ 2.6.22-rc4-mm2-robindmount/fs/nfsd/vfs.c
@@ -1554,6 +1554,14 @@ out_nfserr:
  goto out_unlock;
 }

+static inline int svc_msnfs(struct svc_fh *ffhp)
+{
+#ifdef MSNFS
+ return (ffhp->fh_export->ex_flags & NFSEXP_MSNFS);
+#else
+ return 0;

```
+#endif
+}
 /*
  * Rename a file
  * N.B. After this call _both_ ffhp and tfhp need an fh_put
@@ -1615,13 +1623,20 @@ nfsd_rename(struct svc_rqst *rqstp, stru
 if (ndentry == trap)
  goto out_dput_new;

-#ifdef MSNFS
- if ((ffhp->fh_export->ex_flags & NFSEXP_MSNFS) &&
+ if (svc_msnfs(ffhp) &&
  ((atomic_read(&odentry->d_count) > 1)
   || (atomic_read(&ndentry->d_count) > 1))) {
   host_err = -EPERM;
- } else
-#endif
+  goto out_dput_new;
+ }
+
+ host_err = -EXDEV;
+ if (ffhp->fh_export->ex_mnt != tfhp->fh_export->ex_mnt)
+  goto out_dput_new;
+ host_err = mnt_want_write(ffhp->fh_export->ex_mnt);
+ if (host_err)
+  goto out_dput_new;
+
 host_err = vfs_rename(fdir, odentry, tdir, ndentry);
 if (!host_err && EX_ISSYNC(tfhp->fh_export)) {
  host_err = nfsd_sync_dir(tdentry);

--
```