Subject: Re: [patch 8/8] allow unprivileged fuse mounts
Posted by ebiederm on Sat, 21 Apr 2007 14:18:47 GMT
View Forum Message <> Reply to Message

Miklos Szeredi <miklos@szeredi.hu> writes:

> From: Miklos Szeredi <mszeredi@suse.cz>
>
> Use FS_SAFE for "fuse" fs type, but not for "fuseblk".
>
> FUSE was designed from the beginning to be safe for unprivileged
> users. This has also been verified in practice over many years. In
> addition unprivileged mounts require the parent mount to be owned by
> the user, which is more strict than the current userspace policy.
>
> This will enable future installations to remove the suid-root
> fusermount utility.
>
> Don't require the "user_id=" and "group_id=" options for unprivileged
> mounts, but if they are present, verify them for sanity.
>
> Disallow the "allow_other" option for unprivileged mounts.
>
> Signed-off-by: Miklos Szeredi <mszeredi@suse.cz>
> ---
>
> Index: linux/fs/fuse/inode.c
> ===
> --- linux.orig/fs/fuse/inode.c 2007-04-20 11:55:01.000000000 +0200
> +++ linux/fs/fuse/inode.c 2007-04-20 11:55:14.000000000 +0200
> @@ -311,6 +311,19 @@ static int parse_fuse_opt(char *opt, str
> d->max_read = ~0;
> d->blksize = 512;
>
> + /*
> + * For unprivileged mounts use current uid/gid. Still allow
> + * "user_id" and "group_id" options for compatibility, but
> + * only if they match these values.
> + */
> + if (!capable(CAP_SYS_ADMIN)) {
> + d->user_id = current->uid;
> + d->user_id_present = 1;
> + d->group_id = current->gid;
> + d->group_id_present = 1;
> +
> + }

CAP_SETUID is the appropriate capability...

This is not a dimension we have not fully explored.
What is the problem with a user controlled mount having different uid and gid values.

Yes they map into different users but how is this a problem.
The only problem that I can recall is the historic chown problem where you could give files to other users and mess up their quotas.

Or is the problem other users writing to this user controlled filesystem?

Eric

_____

Containers mailing list
Containers@lists.linux-foundation.org
https://lists.linux-foundation.org/mailman/listinfo/containers