Subject: Capabilities issue
Posted by kevinm on Tue, 31 Aug 2010 14:35:44 GMT
View Forum Message <> Reply to Message

Hi All !

I appear to be having an issue with capabilities inside a openvz container..

The source code that is giving me issues is the following :

```
        /* init cap with all zeros */
        cap = cap_init();
        capval[0] = CAP_SETUID;
        capval[1] = CAP_SETGID;
        capval[2] = CAP_DAC_READ_SEARCH;
        capval[3] = CAP_SYS_CHROOT;
        cap_set_flag(cap, CAP_PERMITTED, (chroot_root >= 0 ? 4 : 3), capval, CAP_SET);
        if (cap_set_proc(cap) != 0) {
                ap_log_error(APLOG_MARK, APLOG_ERR, 0, NULL, "%s CRITICAL ERROR
ruid_child_init:cap_set_proc failed", MODULE_NAME);
        }
        cap_free(cap);
```

I have granted the following capabilities to the virtual server , and restarted it :

Quote:CAPABILITY="CHOWN:on DAC_READ_SEARCH:on DAC_OVERRIDE:on SETGID:on SETUID:on NET_BIND_SERVICE:on NET_ADMIN:on SYS_CHROOT:on SYS_NICE:on SYS_CHROOT:on "

however I get logged to apache error logs :

Quote:[Tue Aug 31 09:31:50 2010] [error] mod_ruid CRITICAL ERROR ruid_setup:cap_set_proc failed

stracing a process, shows

Quote:capset(0x19980330, 0, {CAP_DAC_OVERRIDE|CAP_DAC_READ_SEARCH, CAP_DAC_OVERRIDE|CAP_SETGID|CAP_SETUID, 0}) = -1 EPERM (Operation not permitted)

is there any reason that even though ive granted these capabilities, that im still receiving -1 EPERM (Operation not permitted) , I cant see anything wrong with the capabilities granted to the ones that are failing, any advise / assistance would be greatly appreciated.

best regards
Kev