Ryzom - Bug # 1345

Status:	New	**Priority:**	Normal
Author:	Potlatch	**Category:**	
Created:	08/17/2011	**Assignee:**	
Updated:	08/17/2011	**Due date:**	
Subject:	Crash while idling (afk)		

Description

Crash while idle (afk). Using PPA from kervala on Ubuntu Lucid.

- glibc detected * /**usr**/**games**/**ryzom_client: free(): invalid next size (fast): 0x00007fffd1e41770 ***======= Backtrace: =========

/lib/libc.so.6(+0x775b6)[0x7ffff33a45b6]
/lib/libc.so.6(cfree+0x73)[0x7ffff33aae83]
/usr/lib/libnel3d.so.0(*ZN4NL3D9CMaterialD1Ev+0x5f)[0x7ffff6ea094f]*
/usr/lib/libnel3d.so.0(_ZN4NL3D17CMeshBaseInstanceD2Ev+0x238)[0x7ffff6bc96e8]
/usr/lib/libnel3d.so.0(_ZN4NL3D16CMeshMRMInstanceD0Ev+0x188)[0x7ffff6e21cb8]
/usr/lib/libnel3d.so.0(_ZN4NL3D6CScene11deleteModelEPNS_10CTransformE+0xc8)[0x7ffff6a9e158]
/usr/lib/libnel3d.so.0(_ZN4NL3D6CScene14deleteInstanceEPNS_15CTransformShapeE+0x22)[0x7ffff6a9e1c2]
/usr/lib/libnel3d.so.0(_ZN4NL3D10CSceneUser14deleteInstanceERNS_9UInstanceE+0x46)[0x7ffff6e98c56]
/usr/games/ryzom_client(_ZN9CEntityCLD2Ev+0x170)[0x659420]
/usr/games/ryzom_client(_ZN12CCharacterCLD0Ev+0x439)[0x6d6849]
/usr/games/ryzom_client(_ZN14CEntityManager6removeEjb+0x129)[0x7a2409]
/usr/games/ryzom_client(_ZN11CNetManager6updateEv+0x33f)[0x80e26f]
/usr/games/ryzom_client(_Z8mainLoopv+0xf2a)[0x681c6a]
/usr/games/ryzom_client(main+0x567)[0x6c8087]
*/lib/libc.so.6(*_libc_start_main+0xfd)[0x7ffff334bc4d]
/usr/games/ryzom_client[0x62ec09]======= Memory map: ========
00400000-01039000 r-xp 00000000 fc:00 527389 /usr/games/ryzom_client
01239000-0123a000 r--p 00c39000 fc:00 527389 /usr/games/ryzom_client
0123a000-0123e000 rw-p 00c3a000 fc:00 527389 /usr/games/ryzom_client
0123e000-3fff3000 rw-p 00000000 00:00 0 [heap]
40000000-4005f000 rw-p 00000000 00:05 1368 /dev/zero
4005f000-40061000 rwxp 00000000 00:05 1368 /dev/zero
7fffc7339000-7fffc8000000 rw-p 00000000 00:00 0
7fffc8000000-7fffc84f3000 rw-p 00000000 00:00 0
7fffc84f3000-7fffcc000000 ---p 00000000 00:00 0
7fffcc0a6000-7fffd3400000 rw-p 00000000 00:00 0
7fffd3400000-7fffd3600000 rw-s 5262d000 00:05 7471 /dev/nvidia0
7fffd369d000-7fffd3b00000 rw-p 00000000 00:00 0
7fffd3bbe000-7fffd4000000 rw-p 00000000 00:00 0
7fffd4000000-7fffd7322000 rw-p 00000000 00:00 0
7fffd7322000-7fffd8000000 ---p 00000000 00:00 0
7fffd80cd000-7fffd82cd000 rw-s 55698000 00:05 7471 /dev/nvidia0
7fffd82cd000-7fffd84cd000 rw-s 1282fe000 00:05 7471 /dev/nvidia0
7fffd84cd000-7fffd86cd000 rw-s 8fce3000 00:05 7471 /dev/nvidia0
7fffd86cd000-7fffdb1ad000 rw-p 00000000 00:00 0
7fffdb1ad000-7fffdb52d000 rw-s 11b029000 00:05 7471 /dev/nvidia0
7fffdb52d000-7fffde8bd000 rw-p 00000000 00:00 0
7fffde8bd000-7fffde8be000 ---p 00000000 00:00 0
7fffde8be000-7fffdf0be000 rw-p 00000000 00:00 0

```
7fffdf0e7000-7fffdfd52000 rw-p 00000000 00:00 0
7fffdfd52000-7fffdfdd2000 rw-s 8ef1e000 00:05 7471                       /dev/nvidia0
7fffdfdd2000-7fffdffd2000 rw-s bba7e000 00:05 7471                       /dev/nvidia0
7fffdffd4000-7fffe00d4000 rw-p 00000000 00:00 0
7fffe00d4000-7fffe02d4000 rw-s 139aa7000 00:05 7471                      /dev/nvidia0
7fffe02d4000-7fffe05b1000 rw-s 1283e4000 00:05 7471                      /dev/nvidia0
7fffe05b1000-7fffe05b2000 ---p 00000000 00:00 0
7fffe05b2000-7fffe0db2000 rw-p 00000000 00:00 0
7fffe0db2000-7fffe0db3000 ---p 00000000 00:00 0
7fffe0db3000-7fffe15b3000 rw-p 00000000 00:00 0
7fffe15b3000-7fffe15b4000 ---p 00000000 00:00 0
7fffe15b4000-7fffe15b7000 rw-p 00000000 00:00 0
7fffe15b7000-7fffe15b8000 ---p 00000000 00:00 0
7fffe15b8000-7fffe1db8000 rw-p 00000000 00:00 0
7fffe1db8000-7fffe5db9000 rw-s 00000000 00:10 4566986                    /dev/shm/pulse-shm-2718903593
7fffe5db9000-7fffe5dba000 ---p 00000000 00:00 0
7fffe5dba000-7fffe65ba000 rw-p 00000000 00:00 0
7fffe65ba000-7fffe677d000 r-xp 00000000 fc:00 565936                     /usr/lib/libvorbisenc.so.2.0.6
7fffe677d000-7fffe697d000 ---p 001c3000 fc:00 565936                     /usr/lib/libvorbisenc.so.2.0.6
7fffe697d000-7fffe6994000 r--p 001c3000 fc:00 565936                     /usr/lib/libvorbisenc.so.2.0.6
7fffe6994000-7fffe6995000 rw-p 001da000 fc:00 565936                     /usr/lib/libvorbisenc.so.2.0.6
7fffe6995000-7fffe69de000 r-xp 00000000 fc:00 565934                     /usr/lib/libFLAC.so.8.2.0
7fffe69de000-7fffe6bde000 ---p 00049000 fc:00 565934                     /usr/lib/libFLAC.so.8.2.0
7fffe6bde000-7fffe6bdf000 r--p 00049000 fc:00 565934                     /usr/lib/libFLAC.so.8.2.0
7fffe6bdf000-7fffe6be0000 rw-p 0004a000 fc:00 565934                     /usr/lib/libFLAC.so.8.2.0
7fffe6be0000-7fffe6bf7000 r-xp 00000000 fc:00 1054429                    /lib/libnsl-2.11.1.so
7fffe6bf7000-7fffe6df6000 ---p 00017000 fc:00 1054429                    /lib/libnsl-2.11.1.so
7fffe6df6000-7fffe6df7000 r--p 00016000 fc:00 1054429                    /lib/libnsl-2.11.1.so
7fffe6df7000-7fffe6df8000 rw-p 00017000 fc:00 1054429                    /lib/libnsl-2.11.1.so
7fffe6df8000-7fffe6dfa000 rw-p 00000000 00:00 0
7fffe6dfa000-7fffe6e37000 r-xp 00000000 fc:00 1046691                    /lib/libdbus-1.so.3.4.0
7fffe6e37000-7fffe7037000 ---p 0003d000 fc:00 1046691                    /lib/libdbus-1.so.3.4.0
7fffe7037000-7fffe7038000 r--p 0003d000 fc:00 1046691                    /lib/libdbus-1.so.3.4.0
7fffe7038000-7fffe7039000 rw-p 0003e000 fc:00 1046691                    /lib/libdbus-1.so.3.4.0
7fffe7039000-7fffe7097000 r-xp 00000000 fc:00 529700                     /usr/lib/libsndfile.so.1.0.21
7fffe7097000-7fffe7297000 ---p 0005e000 fc:00 529700                     /usr/lib/libsndfile.so.1.0.21
7fffe7297000-7fffe7299000 r--p 0005e000 fc:00 529700                     /usr/lib/libsndfile.so.1.0.21
7fffe7299000-7fffe729a000 rw-p 00060000 fc:00 529700                     /usr/lib/libsndfile.so.1.0.21
7fffe729a000-7fffe729e000 rw-p 00000000 00:00 0
7fffe729e000-7fffe72a7000 r-xp 00000000 fc:00 1050833                    /lib/libwrap.so.0.7.6
7fffe72a7000-7fffe74a6000 ---p 00009000 fc:00 1050833                    /lib/libwrap.so.0.7.6
7fffe74a6000-7fffe74a7000 r--p 00008000 fc:00 1050833                    /lib/libwrap.so.0.7.6
7fffe74a7000-7fffe74a8000 rw-p 00009000 fc:00 1050833                    /lib/libwrap.so.0.7.6
7fffe74a8000-7fffe74a9000 rw-p 00000000 00:00 0
7fffe74a9000-7fffe74b8000 r-xp 00000000 fc:00 554547                     /usr/lib/libXi.so.6.1.0
7fffe74b8000-7fffe76b7000 ---p 0000f000 fc:00 554547                     /usr/lib/libXi.so.6.1.0
7fffe76b7000-7fffe76b8000 r--p 0000e000 fc:00 554547                     /usr/lib/libXi.so.6.1.0
7fffe76b8000-7fffe76b9000 rw-p 0000f000 fc:00 554547                     /usr/lib/libXi.so.6.1.0
7fffe76b9000-7fffe76bd000 r-xp 00000000 fc:00 1046890                    /lib/libuuid.so.1.3.0
7fffe76bd000-7fffe78bc000 ---p 00004000 fc:00 1046890                    /lib/libuuid.so.1.3.0
7fffe78bc000-7fffe78bd000 r--p 00003000 fc:00 1046890                    /lib/libuuid.so.1.3.0
7fffe78bd000-7fffe78be000 rw-p 00004000 fc:00 1046890                    /lib/libuuid.so.1.3.0
7fffe78be000-7fffe7909000 r-xp 00000000 fc:00 565944                     /usr/li[New Thread 0x7fffe65b9700 (LWP 27341)]
```

```
[New Thread 0x7fffe1db7700 (LWP 27344)]
[New Thread 0x7fffe15b6700 (LWP 27345)]
[Thread 0x7fffe15b6700 (LWP 27345) exited]
[New Thread 0x7fffe15b2700 (LWP 27348)]
[New Thread 0x7fffe0db1700 (LWP 27349)]
[New Thread 0x7fffdf0bd700 (LWP 27350)]

Program received signal SIGABRT, Aborted.
0x00007ffff3360a75 in raise () from /lib/libc.so.6
(gdb) thread apply all bt

Thread 9 (Thread 0x7fffdf0bd700 (LWP 27350)):
#0  0x00007ffff33d739d in nanosleep () from /lib/libc.so.6
#1  0x00007ffff7ae53f7 in NLMISC::nlSleep(unsigned int) ()
   from /usr/lib/libnelmisc.so.0
#2  0x00007fffe85e6ab5 in NLSOUND::CMusicChannelAL::run() ()
   from /usr/lib/nel/libnel_drv_openal.so
#3  0x00007ffff7a9a355 in ?? () from /usr/lib/libnelmisc.so.0
#4  0x00007ffff31169ca in start_thread () from /lib/libpthread.so.0
#5  0x00007ffff341370d in clone () from /lib/libc.so.6
#6  0x0000000000000000 in ?? ()

Thread 8 (Thread 0x7fffe0db1700 (LWP 27349)):
#0  0x00007ffff33d739d in nanosleep () from /lib/libc.so.6
#1  0x00007ffff7ae53f7 in NLMISC::nlSleep(unsigned int) ()
   from /usr/lib/libnelmisc.so.0
#2  0x00007ffff7b378b4 in NLMISC::CTaskManager::run() ()
   from /usr/lib/libnelmisc.so.0
#3  0x00007ffff7a9a355 in ?? () from /usr/lib/libnelmisc.so.0
#4  0x00007ffff31169ca in start_thread () from /lib/libpthread.so.0
#5  0x00007ffff341370d in clone () from /lib/libc.so.6
#6  0x0000000000000000 in ?? ()

Thread 7 (Thread 0x7fffe15b2700 (LWP 27348)):
#0  0x00007ffff33d739d in nanosleep () from /lib/libc.so.6
#1  0x00007ffff7ae53f7 in NLMISC::nlSleep(unsigned int) ()
   from /usr/lib/libnelmisc.so.0
#2  0x00000000009cdb13 in CWebigNotificationThread::run() ()
#3  0x00007ffff7a9a355 in ?? () from /usr/lib/libnelmisc.so.0
#4  0x00007ffff31169ca in start_thread () from /lib/libpthread.so.0
#5  0x00007ffff341370d in clone () from /lib/libc.so.6
#6  0x0000000000000000 in ?? ()

Thread 5 (Thread 0x7fffe1db7700 (LWP 27344)):
#0  0x00007ffff33d739d in nanosleep () from /lib/libc.so.6
#1  0x00007ffff7ae53f7 in NLMISC::nlSleep(unsigned int) ()
   from /usr/lib/libnelmisc.so.0
#2  0x000000000076dc11 in CSessionBrowser::run (this=0x10c433c0)
    at /build/buildd/ryzom-core-0.8.1628~lucid0/ryzom/client/src/session_browser.cpp:171
#3  0x00007ffff7a9a355 in ?? () from /usr/lib/libnelmisc.so.0
#4  0x00007ffff31169ca in start_thread () from /lib/libpthread.so.0
#5  0x00007ffff341370d in clone () from /lib/libc.so.6
#6  0x0000000000000000 in ?? ()
```

```
Thread 4 (Thread 0x7fffe65b9700 (LWP 27341)):
#0  0x00007ffff3406f93 in poll () from /lib/libc.so.6
#1  0x00007fffe816241f in ?? () from /usr/lib/libpulse.so.0
#2  0x00007fffe8151d86 in pa_mainloop_poll () from /usr/lib/libpulse.so.0
#3  0x00007fffe8153809 in pa_mainloop_iterate () from /usr/lib/libpulse.so.0
#4  0x00007fffe81538c0 in pa_mainloop_run () from /usr/lib/libpulse.so.0
#5  0x00007fffe816221b in ?? () from /usr/lib/libpulse.so.0
#6  0x00007fffe78f60e8 in ?? () from /usr/lib/libpulsecommon-0.9.21.so
#7  0x00007ffff31169ca in start_thread () from /lib/libpthread.so.0
#8  0x00007ffff341370d in clone () from /lib/libc.so.6
#9  0x0000000000000000 in ?? ()

Thread 3 (Thread 0x7fffe8fef700 (LWP 27340)):
#0  0x00007ffff33d739d in nanosleep () from /lib/libc.so.6
#1  0x00007ffff340c844 in usleep () from /lib/libc.so.6
#2  0x00007ffff7b346d3 in NLMISC::CCoTask::yield() ()
   from /usr/lib/libnelmisc.so.0
#3  0x00000000008238fe in CLoginStateMachine::waitEvent (this=0x125c100)
    at /build/buildd/ryzom-core-0.8.1628~lucid0/ryzom/client/src/far_tp.cpp:202
#4  0x00000000008286a6 in CLoginStateMachine::run (this=0x125c100)
    at /build/buildd/ryzom-core-0.8.1628~lucid0/ryzom/client/src/far_tp.cpp:503
#5  0x00007ffff7b34bf7 in NLMISC::TCoTaskData::run() ()
   from /usr/lib/libnelmisc.so.0
#6  0x00007ffff7a9a355 in ?? () from /usr/lib/libnelmisc.so.0
#7  0x00007ffff31169ca in start_thread () from /lib/libpthread.so.0
#8  0x00007ffff341370d in clone () from /lib/libc.so.6
#9  0x0000000000000000 in ?? ()

Thread 2 (Thread 0x7fffee085700 (LWP 27339)):
#0  0x00007ffff33d739d in nanosleep () from /lib/libc.so.6
#1  0x00007ffff7ae53f7 in NLMISC::nlSleep(unsigned int) ()
   from /usr/lib/libnelmisc.so.0
#2  0x00000000008cfe7e in CLoginProgressTask::run() ()
#3  0x00007ffff7a9a355 in ?? () from /usr/lib/libnelmisc.so.0
#4  0x00007ffff31169ca in start_thread () from /lib/libpthread.so.0
#5  0x00007ffff341370d in clone () from /lib/libc.so.6
#6  0x0000000000000000 in ?? ()

Thread 1 (Thread 0x7ffff7fbb740 (LWP 27336)):
#0  0x00007ffff3360a75 in raise () from /lib/libc.so.6
#1  0x00007ffff33645c0 in abort () from /lib/libc.so.6
#2  0x00007ffff339a4fb in ?? () from /lib/libc.so.6
#3  0x00007ffff33a45b6 in ?? () from /lib/libc.so.6
#4  0x00007ffff33aae83 in free () from /lib/libc.so.6
#5  0x00007ffff6ea094f in NL3D::CMaterial::~CMaterial() ()
   from /usr/lib/libnel3d.so.0
#6  0x00007ffff6bc96e8 in NL3D::CMeshBaseInstance::~CMeshBaseInstance() ()
   from /usr/lib/libnel3d.so.0
#7  0x00007ffff6e21cb8 in NL3D::CMeshMRMInstance::~CMeshMRMInstance() ()
   from /usr/lib/libnel3d.so.0
#8  0x00007ffff6a9e158 in NL3D::CScene::deleteModel(NL3D::CTransform*) ()
   from /usr/lib/libnel3d.so.0
#9  0x00007ffff6a9e1c2 in NL3D::CScene::deleteInstance(NL3D::CTransformShape*)
```

```
   () from /usr/lib/libnel3d.so.0
#10 0x00007ffff6e98c56 in NL3D::CSceneUser::deleteInstance(NL3D::UInstance&) ()
   from /usr/lib/libnel3d.so.0
#11 0x0000000000659420 in ~CEntityCL (this=0x7fffcc0eede0,
    __in_chrg=<value optimized out>)
    at /build/buildd/ryzom-core-0.8.1628~lucid0/ryzom/client/src/entity_cl.cpp:579
#12 0x00000000006d6849 in ~CCharacterCL (this=0x7fffcc0eede0,
    __in_chrg=<value optimized out>)
    at /build/buildd/ryzom-core-0.8.1628~lucid0/ryzom/client/src/character_cl.cpp:420
#13 0x00000000007a2409 in CEntityManager::remove (this=0x125fde0, slot=13,
    warning=<value optimized out>)
    at /build/buildd/ryzom-core-0.8.1628~lucid0/ryzom/client/src/entities.cpp:816
#14 0x000000000080e26f in CNetManager::update (this=0x12638a0)
    at /build/buildd/ryzom-core-0.8.1628~lucid0/ryzom/client/src/net_manager.cpp:3823
#15 0x0000000000681c6a in mainLoop ()
    at /build/buildd/ryzom-core-0.8.1628~lucid0/ryzom/client/src/main_loop.cpp:1766
#16 0x00000000006c8087 in main (argc=<value optimized out>,
    argv=<value optimized out>)
    at /build/buildd/ryzom-core-0.8.1628~lucid0/ryzom/client/src/client.cpp:618
```

History

#1 - 08/17/2011 08:21 pm - sfb

- Subject changed from Crash to Crash while idling (afk)

Please attach your client log and (if applicable) your EGS log.

Also for future reference please put a more descriptive subject line.

Any other details you have handy would be helpful including ways to duplicate it.

Thanks.

#2 - 08/17/2011 11:12 pm - Potlatch

Unfortunatly, I do not know how to reproduce...

what is an EGS log?

#3 - 08/17/2011 11:32 pm - Potlatch

just in case: it happen using the "official client" from the kervala's PPA on the official server (aniro).