Ryzom - Bug # 1175

Status:	Validated	**Priority:**	High
Author:	velogfx	**Category:**	NeL: General
Created:	11/08/2010	**Assignee:**	
Updated:	07/10/2011	**Due date:**	
Subject:	Quit to Character Selection		

Description

Quit to character selection screen is causing a client crash.

Error log:
http://pastebin.com/xafDYe9t

History

#1 - 12/12/2010 02:43 am - rti

- Status changed from New to Validated

- Priority changed from Normal to High

#2 - 01/07/2011 08:44 am - Naush

It's not a specific mac os bug, maybe an OGL driver bug (NeL or Nvidia). Issue #1065 is probably the same.

```
#0  0x00007fffee5a3ce9 in glDisable () from /usr/lib64/libGL.so.1
#1  0x00007fffee5ef912 in NL3D::CDriverGL::setupScissor (this=0x39577d0, scissor=...) at
/opt/src/ryzom/code/nel/src/3d/driver/opengl/driver_opengl.cpp:1101
#2  0x00007ffff6b11439 in NL3D::CDriverUser::setupMatrixContext (this=0x364fbb0) at /opt/src/ryzom/code/nel/src/3d/driver_user.cpp:434
#3  0x00007ffff6b115e6 in NL3D::CDriverUser::setMatrixMode2D (this=0x364fbb0, frust=<value optimized out>) at
/opt/src/ryzom/code/nel/src/3d/driver_user.cpp:555
#4  0x00007ffff6b10b2f in NL3D::UDriver::setMatrixMode2D11 (this=0x364fbb0) at /opt/src/ryzom/code/nel/src/3d/driver_user.cpp:77
#5  0x00000000006f7180 in CProgress::internalProgress (this=0x1359120, value=0.5) at
/opt/src/ryzom/code/ryzom/client/src/progress.cpp:181
#6  0x000000000073cf7f in CFarTP::disconnectFromPreviousShard (this=0x1381840) at /opt/src/ryzom/code/ryzom/client/src/far_tp.cpp:1075
#7  CLoginStateMachine::run (this=0x1381840) at /opt/src/ryzom/code/ryzom/client/src/far_tp.cpp:562
#8  0x00007ffff7a9da90 in NLMISC::TCoTaskData::run (this=0x150e5c0) at /opt/src/ryzom/code/nel/src/misc/co_task.cpp:529
#9  0x00007ffff7a9ee69 in ProxyFunc (arg=0x4bbd770) at /opt/src/ryzom/code/nel/src/misc/p_thread.cpp:60
#10 0x00007ffff182b980 in start_thread () from /lib64/libpthread.so.0
#11 0x00007ffff1b2657d in clone () from /lib64/libc.so.6
```

Frame 0

```
   0x00007fffee5a3ce0 <+0>:     mov    rax,QWORD PTR fs:0xffffffffffffff68
=> 0x00007fffee5a3ce9 <+9>:     jmp    QWORD PTR [rax+0x538]
(gdb) p $rax
$1 = 0
```

Frame 1

```
   0x00007fffee5ef908 <+776>:   mov    edi,0xc11                          ; GL_SCISSOR_TEST
   0x00007fffee5ef90d <+781>:   call   0x7fffee5e9ad0 <glDisable@plt>
=> 0x00007fffee5ef912 <+786>:   jmp    0x7fffee5ef637 <NL3D::CDriverGL::setupScissor(NL3D::CScissor const&)+55>
```

I'm not able to reproduce this bug out of the box.
Render space is still in "fullscreen", not yet resized in 1024x768. I'm palying in a maximized window .

#3 - 01/07/2011 10:06 am - rti

- Category changed from OS: Mac to NeL: General

#4 - 01/07/2011 10:17 am - rti

- Subject changed from Mac - Alpha Build - Quit to Character Selection to Quit to Character Selection

#5 - 01/07/2011 10:23 am - kervala

I fixed something just before the glDisable(GL_SCISSOR_TEST) but I'm not sure it's related.

Perhaps should we put glEnable/glDisable(GL_SCISSOR_TEST) in states class to not enable/disable a state if already enabled/disabled.

Edit: see http://dev.ryzom.com/projects/ryzom/repository/revisions/1275/diff/code/nel/src/3d/driver/opengl/driver_opengl.cpp

#6 - 01/07/2011 02:27 pm - rti

when reproducing the crash on mac os i realized that the crashing gl call does not originate from the main thread like all the other calls to opengl...

#7 - 01/12/2011 08:11 pm - Naush

- File 1175-oglthread.patch added

There is no many things to do :
- Release / enable context between thread using glXMakeCurrent/wglMakeCurrent/.
- Modify code, to make the rendering in thread 0

For the momment I've good results with the first method. I'm able to connect to R², but still can't switch character.
It's hard to say if it is a OGL/64 bit/linux issue :)

```
Program received signal SIGSEGV, Segmentation fault.
0x000000000075f7e3 in construct (bankStr=<value optimized out>) at
/usr/lib64/gcc/x86_64-slackware-linux/4.5.0/../../../../include/c++/4.5.0/ext/new_allocator.h:105
105           { ::new((void *)__p) _Tp(__val); }
(gdb) bt
#0  0x000000000075f7e3 in construct (bankStr=<value optimized out>) at
/usr/lib64/gcc/x86_64-slackware-linux/4.5.0/../../../../include/c++/4.5.0/ext/new_allocator.h:105
#1  std::vector<TCDBBank, std::allocator<TCDBBank> >::push_back (bankStr=<value optimized out>) at
/usr/lib64/gcc/x86_64-slackware-linux/4.5.0/../../../../include/c++/4.5.0/bits/stl_vector.h:745
#2  CCDBNodeBranch::mapNodeByBank (bankStr=<value optimized out>) at /srv/vol1/src/ryzom/code/ryzom/client/src/cdb_branch.cpp:122
#3  0x0000000000761c6f in addNode (newNode=0xbc67ac0, newName="GameTime", parent=0x13f7b170, nodes=std::vector of length 2,
capacity 2 = {...}, nodesSorted=<value optimized out>, child=@0x7fffffffc5c8, bankName="PLR", atomBranch=false,
```

clientOnly=false, progressCallBack=..., mapBanks=true) at /srv/vol1/src/ryzom/code/ryzom/client/src/cdb_branch.cpp:152
#4 0x00000000007657ae in CCDBNodeBranch::init (this=0x13f7b170, node=0xaa1d590, progressCallBack=..., mapBanks=true) at /srv/vol1/src/ryzom/code/ryzom/client/src/cdb_branch.cpp:213
#5 0x00000000008d7285 in CCDBSynchronised::init (this=<value optimized out>, fileName="data_common.bnp@database.xml", progressCallBack=...) at /srv/vol1/src/ryzom/code/ryzom/client/src/cdb_synchronised.cpp:85
#6 0x0000000000829097 in initMainLoop () at /srv/vol1/src/ryzom/code/ryzom/client/src/init_main_loop.cpp:473
#7 0x000000000078a3ef in CFarTP::sendReady (this=0x12cc460) at /srv/vol1/src/ryzom/code/ryzom/client/src/far_tp.cpp:1205
#8 0x000000000078ae30 in CFarTP::farTPmainLoop (this=0x12cc460) at /srv/vol1/src/ryzom/code/ryzom/client/src/far_tp.cpp:1457
#9 0x0000000000777485 in mainLoop () at /srv/vol1/src/ryzom/code/ryzom/client/src/main_loop.cpp:2893
#10 0x00000000008bbf17 in main (argc=<value optimized out>, argv=<value optimized out>) at /srv/vol1/src/ryzom/code/ryzom/client/src/client.cpp:618

#8 - 01/14/2011 10:37 pm - Naush

Ok It's working :)

The previous partial patch introduce a enableContext over head in the main draw loop on selection character, I will try to remove it, Also there is one enableContext missing in the ryzom/client/src/connection.cpp. It's will not cause any problem on linux, but it's an implementation problem.

For the stack trace above it's not the same issue

ryzom/client/src/cdb_branch.cpp:91:34: warning: array subscript is above array bounds

It's probably explain the testYoyo @ random crash on exit :)

I will try to bring you a full working patch (linux & windows (sorry rti :)) before Monday

#9 - 01/15/2011 09:28 pm - Naush

- File 1175-oglthread.patch added

This patch implement 2 new methods for drivers (and increment drivers revision):
- attachContext() : Attach an OpenGL context on the current thread
- detachContext() : Detach a OpenGL context from the current thread

I have not found any D3D equivalent. So those methods are abitrary returning true in the D3D driver.

This patch also fix a memory overflow in cdb_branch.

Q&A:
All drivers pass thru gDebugger with no warning/error.
A special driver have been built to ensure thread context switching is ok. Every things is ok except in connection.cpp

Platform Q&A :
Linux x64 NVidia driver: No more problem.
Seven x64 ATI : Well I don't know, it's working without this patch, so why should we take any risk ? in the other hand it's the way to do multithreaded with opengl.

Note: We must find a way to nlerror when driver revision is not in sync :)

#10 - 07/10/2011 10:02 pm - Sywindt

I have had several reports of Linux players having this problem still. It looks to be unfixed in 1.12.1, correct? Is any more information needed?

Files

1175-oglthread.patch	1.7 kB	01/12/2011	Naush
1175-oglthread.patch	7.8 kB	01/15/2011	Naush