Ryzom - Bug # 1016

Status:	Validated	**Priority:**	High
Author:	ashly	**Category:**	Services: General
Created:	07/13/2010	**Assignee:**	
Updated:	04/11/2012	**Due date:**	
Subject:	entities_game_service segfault in ubuntu 64biten		

Description

Console Text:

src/entities_game_service/entities_game_service
INF 0b251720 command.cpp 145 registerNamedCommandHandler <Unknown> : CCommandRegistry : adding commands handler for class 'CModuleManager'
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'AdminExecutorService' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'AdminExecutorServiceClient' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'AdminService' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'AnimSessionManager' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'CharNameMapperClient' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'CharacterControl' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'ClientCommandForwader' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'GuildUnifier' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'LocalGateway' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'LoggerServiceClient' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'ShardUnifierClient' factory
INF 0b251720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'StandardGateway' factory
INF 0b251720 service.cpp 252 cbDirectoryChanged EGS : SERVICE: 'ConfigDirectory' changed to '/home/elantia/server/code/ryzom/server/'
Segmentation fault

Debug Info:
@
gdb src/entities_game_service/entities_game_service
GNU gdb (GDB) 7.1-ubuntu
Copyright (C) 2010 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law. Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
Reading symbols from /home/elantia/server/code/ryzom/server/src/entities_game_service/entities_game_service...(no debugging symbols found)...done.
(gdb) run
Starting program: /home/elantia/server/code/ryzom/server/src/entities_game_service/entities_game_service
[Thread debugging using libthread_db enabled]
INF f7fdd720 command.cpp 145 registerNamedCommandHandler <Unknown> : CCommandRegistry : adding commands handler for class 'CModuleManager'
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'AdminExecutorService' factory

INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'AdminExecutorServiceClient' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'AdminService' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'AnimSessionManager' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'CharNameMapperClient' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'CharacterControl' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'ClientCommandForwader' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'GuildUnifier' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'LocalGateway' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'LoggerServiceClient' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'ShardUnifierClient' factory
INF f7fdd720 module_manager.cpp 228 addModuleFactoryRegistry <Unknown> : Adding module 'StandardGateway' factory
INF f7fdd720 service.cpp 252 cbDirectoryChanged EGS : SERVICE: 'ConfigDirectory' changed to '/home/elantia/server/code/ryzom/server/'

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7694976 in NLNET::cbDirectoryChanged (var=...) at /home/elantia/server/code/nel/src/net/service.cpp:266
warning: Source file is more recent than executable.
266 instance->_DirectoryChangedCBI->onVariableChanged(var);
(gdb) bt
#0 0x00007ffff7694976 in NLNET::cbDirectoryChanged (var=...) at /home/elantia/server/code/nel/src/net/service.cpp:266
#1 0x00007ffff769bef0 in NLMISC::CVariable<std::string>::set (this=0x1bf1670, serviceShortName=<value optimized out>, serviceLongName=0x13d8cdc "entities_game_service", servicePort=0,
configDir=<value optimized out>, logDir=<value optimized out>, compilationDate=0x13d8cf2 "Jul 13 2010 00:25:29") at /home/elantia/server/code/nel/include/nel/misc/variable.h:454
#2 NLMISC::CVariable<std::string>::operator= (this=0x1bf1670, serviceShortName=<value optimized out>, serviceLongName=0x13d8cdc "entities_game_service", servicePort=0,
configDir=<value optimized out>, logDir=<value optimized out>, compilationDate=0x13d8cf2 "Jul 13 2010 00:25:29") at /home/elantia/server/code/nel/include/nel/misc/variable.h:428
#3 NLNET::IService::main (this=0x1bf1670, serviceShortName=<value optimized out>, serviceLongName=0x13d8cdc "entities_game_service", servicePort=0, configDir=<value optimized out>,
logDir=<value optimized out>, compilationDate=0x13d8cf2 "Jul 13 2010 00:25:29") at /home/elantia/server/code/nel/src/net/service.cpp:601
#4 0x0000000000adaa09 in main ()
(gdb)
@

I think its Target version 0.8.0 its whatever is in the hg branch..

Related issues:

duplicates Ryzom - Bug # 987: EGS Segmentation fault under ubuntu x64	**Rejected**	**06/20/2010**

History

#1 - 07/14/2010 04:19 am - ashly

- File strace.dump added

Also heres a strace dump of the entities_game_service

#2 - 07/14/2010 05:30 pm - promethium

It looks like a duplicate of #987

#3 - 07/29/2010 02:17 pm - Naush

This is a GCC <=4.4.4 issue, upgrade your GCC to 4.5.0 and you will not have this error any more

#4 - 07/30/2010 09:12 am - kervala

Please someone could try if it still happens after adding : -fno-strict-aliasing at the end of flags line 231 in code/nel/CMakeModules/nel.cmake ?

I wonder if it's related to that, because we used this flag for Ryzom and not for NeL.

#5 - 08/12/2010 05:22 am - ashly

I tried both, updating to GCC 4.5.x and adding the -fno-strict-aliasing, still nothing... I get the same thing, segfault in compile

#6 - 09/25/2010 01:07 pm - Naush

"EGS-128 : SERVICE: Service ready" on ubuntu 10.04 LTS x86_64

Well, here is how I've build gcc 4.5.0 :
- install package : libmpfr-dev libmpc-dev zip libgmp3-dev libgmpxx4ldbl
- download : gcc-4.5.0 gmp-5.0.1 mpc-0.8.2

build mpc : http://slackbuilds.org/slackbuilds/13.1/libraries/libmpc/libmpc.SlackBuild

```
./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var/lib --disable-static --mandir=/usr/man --program-prefix= --program-suffix=
--build=x86_64-slackware-linux
```

build gmp :

```
./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var/lib --disable-static --mandir=/usr/man --program-prefix= --program-suffix=
--build=x86_64-slackware-linux
```

- create a directory and do :

```
../gcc-4.5.0/configure --prefix=/usr --libdir=/usr/lib64 --enable-shared --enable-bootstrap --enable-languages=c,c++,objc --enable-threads=posix
--enable-checking=release --with-system-zlib --with-python-dir=/lib64/python2.6/site-packages --disable-libunwind-exceptions
--enable-__cxa_atexit --enable-libssp --with-gnu-ld --verbose --disable-multilib --target=x86_64-slackware-linux --build=x86_64-slackware-linux
--host=x86_64-slackware-linux
```

clean, rebuild every things, Enjoy :)

PS: target, build and host is x86_64-linux-gnu for Ubuntu

#7 - 09/27/2010 01:20 pm - molator

I've justed Naush solution.

I finally succeeded in building the server on ubuntu 8.04 x86_64 but the solution is some what special.

Tthe native gcc is 4.2.4, so i've build gcc 4.5 from source.
I've build nel and all services except backup_services with gcc 4.5.
But i got nelligo issues for backup_service, so i built that service with gcc 4.2.4 (using symbolic link).
After that no more crash with egs but many others services instead.
I had to add missing var in various services config, set to empty string, var i never had to add before.

I added in code/ryzom/server/frontend_service.cfg

> *DefaultUserPriv = "";*

> *AcceptInvalidCookie = "";*

> *TimeBeforeEraseCookie = "";*

In code/ryzom/server/sheet_pack_cfg/input_output_service.cfg (during compilation) and code/ryzom/server/input_output_service.cfg:

> *MaxDistSay = "";*

> *MaxDistShout = "";*

> *ReadWorkOnly = "";*

In code/ryzom/server/tick_service.cfg:

> *GameTime = "";*

> *GameCycle = "";*

> *TickTimeStep = "";*

> *GameTimeStep = "";*

In code/ryzom/server/welcome_service.cfg

> *FrontEndAddress = "";*

Those services were crashing asking for those vars.

#8 - 10/05/2010 05:46 pm - kervala

- File egs_crash.patch added

I renamed some CVariable to avoid a nlstopex.

Please someone could apply my patch and tell me if it fixes the crash or not ? Thanks :)

#9 - 10/06/2010 12:02 pm - kervala

- File egs_crash_2.patch added

#10 - 10/06/2010 12:02 pm - kervala

- File deleted (egs_crash.patch)

#11 - 10/06/2010 05:41 pm - molator

Ok my last result, here some part of the logs.

```
INF 905f6700 command.cpp 145 registerNamedCommandHandler 178.32.114.249/AS-0 : CCommandRegistry : adding commands handler for class 'CModuleBase'
terminate called after throwing an instance of 'NLNET::ESocketConnectionFailed'
  what():  Socket error: Connection to 127.0.0.1:46702 (127.0.0.1) failed (111: Connection refused)
/home/ryzom/code/ryzom/tools/scripts/linux/service_launcher.sh: line 102:  3466 Aborted                 (core dumped) $CTRL_CMDLINE

INF 71c17700 command.cpp 145 registerNamedCommandHandler 178.32.114.249/EGS : CCommandRegistry : adding commands handler for class 'CUnifiedNetwork'
terminate called after throwing an instance of 'NLNET::ESocketConnectionFailed'
  what():  Socket error: Connection to 127.0.0.1:50000 (127.0.0.1) failed (111: Connection refused)
/home/ryzom/code/ryzom/tools/scripts/linux/service_launcher.sh: line 102:  3547 Aborted                 (core dumped) $CTRL_CMDLINE

CMDLINE          = src/mirror_service/mirror_service -C. -L. --nobreak --writepid
There are 2 commands that have the same name in the project (command name 'MainNbEntities'), skip the second definition
/home/ryzom/code/ryzom/tools/scripts/linux/service_launcher.sh: line 102:  3713 Aborted                 (core dumped) $CTRL_CMDLINE

INF 501a7700 unified_network.cpp 779 addService 178.32.114.249/SU-0 : HNETL5: addService BS-256 '127.0.0.1:49990 (127.0.0.1)'
terminate called after throwing an instance of 'NLNET::ESocketConnectionFailed'
  what():  Socket error: Connection to 127.0.0.1:49990 (127.0.0.1) failed (111: Connection refused)
/home/ryzom/code/ryzom/tools/scripts/linux/service_launcher.sh: line 102:  3738 Aborted                 (core dumped) $CTRL_CMDLINE

CMDLINE          = src/frontend_service/frontend_service -C. -L. --nobreak --writepid
2010/10/06 17:33:57 <Unknown> AST 4973a700 factory.h 81 : "_FactoryRegisters.find(key) == _FactoryRegisters.end()"
--------------------------------
/home/ryzom/code/ryzom/tools/scripts/linux/service_launcher.sh: line 102:  3748 Aborted                 (core dumped) $CTRL_CMDLINE
```

A duplicated var remains, but that's a detail.
I will replace it and see.

#12 - 10/06/2010 06:39 pm - molator

- File MainNbEntities.patch added

Here the patch, for the last duplicated var.

#13 - 10/06/2010 10:38 pm - Naush

Some services crash

```
/opt/src/ryzom/code/ryzom/common/src/game_share/mirror.cpp:2885
if ( MirrorInstance->mirrorIsReady() )
(gdb) p MirrorInstance
$1 = (CMirror *) 0x0
(gdb) bt
#0  LocalEntitiesClass::ptr (this=0x7ffff7b517a0, pointer=0x7fffffffcbac, get=true, human=false) at
/opt/src/ryzom/code/ryzom/common/src/game_share/mirror.cpp:2885
#1  0x00007ffff785f52d in LocalEntitiesClass::toString(bool) const () from /opt/src/ryzom/code/build-server/lib/libryzom_gameshare.so.0
#2  0x00007ffff7b93cc2 in ADMIN::CAdminExecutorServiceClient::sendServiceStatus (this=0x10ce630) at
/opt/src/ryzom/code/ryzom/server/src/admin_modules/aes_client_module.cpp:401
#3  0x00007ffff7b979e6 in ADMIN::CAdminExecutorServiceClient::onModuleUpdate (this=0x10ce630) at
/opt/src/ryzom/code/ryzom/server/src/admin_modules/aes_client_module.cpp:361
#4  0x00007ffff6ad02a4 in NLNET::CModuleManager::updateModules (this=0x719520) at
/opt/src/ryzom/code/nel/src/net/module_manager.cpp:521
#5  0x00007ffff6b3b177 in NLNET::IService::main (this=0x715500, serviceShortName=<value optimized out>, serviceLongName=0x39221028
<Address 0x39221028 out of bounds>, servicePort=<value optimized out>,
    configDir=0x7fffffffd4a0 "¸\216\215\001", logDir=0x7fffffffd520 "¸\216\215\001", compilationDate=0x457aed "Oct  6 2010 19:29:23") at
/opt/src/ryzom/code/nel/src/net/service.cpp:1403
#6  0x00000000004477a3 in main (argc=1, argv=<value optimized out>) at
/opt/src/ryzom/code/ryzom/server/src/backup_service/backup_service.cpp:769
(gdb) b mirror.cpp:1499
(gdb) r
[...]
Program received signal SIGSEGV, Segmentation fault.
```

Also note on nirror.cpp:1498 nlassert with the condition (MirrorInstance==void)

```
$ ../../build-server/bin/ryzom_frontend_service
2010/10/06 22:07:21 <Unknown> AST f7fc5720 factory.h 81 : "_FactoryRegisters.find(key) == _FactoryRegisters.end()"
Program received signal SIGABRT, Aborted.
(gdb) bt
#0  0x00007ffff62e05a5 in raise () from /lib64/libc.so.6
#1  0x00007ffff62e1db0 in abort () from /lib64/libc.so.6
#2  0x00000000004ad4ea in NLMISC::CFactory<NLNET::CGatewaySecurity, std::string>::registerClass () at
/opt/src/ryzom/code/nel/include/nel/misc/factory.h:81
#3  CFactoryRegister () at /opt/src/ryzom/code/nel/include/nel/misc/factory.h:130
#4  __static_initialization_and_destruction_0 () at /opt/src/ryzom/code/ryzom/server/src/frontend_service/gateway_fes_transport.cpp:627
#5  global constructors keyed to RegisterTClientInfo () at
/opt/src/ryzom/code/ryzom/server/src/frontend_service/gateway_fes_transport.cpp:638
#6  0x00000000004ba3a6 in __do_global_ctors_aux ()
#7  0x0000000000424833 in _init ()
#8  0x00007ffff7bc7e11 in ?? () from /opt/src/ryzom/code/build-server/lib/libryzom_adminmodules.so.0
#9  0x00000000004ba335 in __libc_csu_init ()
#10 0x00007ffff62cbb00 in __libc_start_main () from /lib64/libc.so.6
#11 0x00000000004258d9 in _start () at ../sysdeps/x86_64/elf/start.S:113
(gdb) f 2
(gdb) p _FactoryRegisters
$2 = std::map with 0 elements
```

The same call on factory.h:81 using ryzom_entities_game_service produce the same result, this one is maybe a 64 bit issue, I will test under Ubuntu 8.04 32 bit LTS, with an uptodate "working copy" :)

#14 - 10/06/2010 11:19 pm - kervala

Thanks a lot for details, I will check them tomorrow :)

We really need to fix these server issues :)

#15 - 10/07/2010 12:41 am - molator

It's related to that crash i suppose.

```
ryzom@r33607:~/code/ryzom/server/src/frontend_service>./frontend_service
AST 48882700 factory.h 81 registerClass <Unknown> : "_FactoryRegisters.find(key) == _FactoryRegisters.end()"
------------------------------

Log with no filter:
------------------------------

Log Starting [2010/10/07 00:41:41]
2010/10/07 00:41:41 <Unknown> AST 48882700 factory.h 81 : "_FactoryRegisters.find(key) == _FactoryRegisters.end()"
------------------------------
Aborted
```

#16 - 11/23/2010 02:23 pm - molator

Looks like that issue exists for Ubuntu 10.10 x32.

So it wouldn't be a question of x64 or gcc, but an ubuntu issue.

#17 - 11/23/2010 07:21 pm - Naush

Well let me clarify a little bit,
They are two issues on this page :

First one, a GCC 4.4.0 issue. For an unknown reason when compiling, GCC 4.4.0 misalign/omit the 'cbDirectoryChanged' var, resulting in a call somewhere in the code.
An upgrade to GCC 4.5.0 solve this issue.

The second one (starting at note 7 ?) is a cmake issue. The difference between cmake and autotools reside in some library that are now built dynamically (+ some unneeded file) server_share, ai_share, game_share, etc ...
Build & link with there static version, and you will have no problem even if you are using RandomDistro@RandomABI.

Maybe we should add entry for the cmake issue and reject #987 & #1016 ? :)

#18 - 12/03/2010 01:41 pm - Krolock

After some time of investigation, my server is know running without any segfaults. The duplicated variables leaded to chain crashing in some services, but kervalas patch fixed it.
I'm now running the server on openSuse 11.3 64 bit. However, I hadn't the time yet, to connect to it with a client. But I don't think that client connection causes any further issues :)
PS: the duplicated variables were also an issue in openSUSE 32 bit.

#19 - 12/03/2010 03:18 pm - kervala

- Category changed from Build to Services: General
- Status changed from New to Assigned
- Assignee set to kervala
- Priority changed from Normal to High

#20 - 12/03/2010 03:21 pm - kervala

Thanks a lot Krolock :)

I just commited some changes, I kept the 2 duplicated variables at only one place and used "extern" for other locations.

Please could you check if it works too ?

Thanks :)

#21 - 12/03/2010 03:28 pm - kervala

- Status changed from Assigned to Rejected

That's a duplicate of #1016 and since there are more details there, we'lll use the other issue :)

#22 - 12/04/2010 01:23 pm - molator

- File patch.diff added

Following Sfb suggestion, i changed the cmake setting of the following libs to static:
game_share, serve_share, ai_share and pd_lib

I built the server with WITH_STATIC and WITH_STATIC_DRIVERS unchecked.
It seems to work as fine as what i got building everything static in the past.

#23 - 12/04/2010 02:54 pm - Krolock

Kervala,

latest revision works perfect :) Buildmode was static. I'm trying buildmode dynamic and client connection know.

#24 - 12/04/2010 02:56 pm - kervala

- Status changed from Rejected to Assigned
- Target version deleted (Version 0.8.0)

Hum I didn't want to reject this one :(

#25 - 03/03/2012 10:56 am - kervala

Please is EGS still crashing with shared libraries in 64 bits ?

#26 - 04/11/2012 06:30 pm - kervala

- Status changed from Assigned to Validated

- Assignee deleted (kervala)

Files

strace.dump	17.4 kB	07/14/2010	ashly
egs_crash_2.patch	15.2 kB	10/06/2010	kervala
MainNbEntities.patch	1.3 kB	10/06/2010	molator
patch.diff	2.2 kB	12/04/2010	molator