Ceph - Bug #1608

osd crash in get_authorize_handler

10/07/2011 04:22 PM - Josh Durgin

Status:	Resolved	**% Done:**	0%
Priority:	Normal	**Spent time:**	0.00 hour
Assignee:			
Category:	OSD		
Target version:	v0.38		
Source:		**Reviewed:**	
Tags:		**Affected Versions:**	
Backport:		**ceph-qa-suite:**	
Regression:	No	**Pull request ID:**	
Severity:	3 - minor	**Crash signature:**	

Description

Possibly a use-after-free. From teuthology:~ teuthworker/archive/nightly_coverage_2011-10-07/251/remote/ubuntu@sepia86.ceph.dreamhost.com/log/osd.4.log.gz:

```
./common/Mutex.h: In function 'void Mutex::Lock(bool)', in thread '0x7fde32b44700'
./common/Mutex.h: 110: FAILED assert(r == 0)
 ceph version 0.36-251-g6e29c28 (commit:6e29c2826066a7723ed05b60b8ac0433a04c3c13)
 1: (get_authorize_handler(int, CephContext*)+0x658) [0x6dd1a8]
 2: (OSD::ms_verify_authorizer(Connection*, int, int, ceph::buffer::list&, ceph::buffer::list&, bo
ol&)+0x41) [0x58be51]
 3: (SimpleMessenger::verify_authorizer(Connection*, int, int, ceph::buffer::list&, ceph::buffer::
list&, bool&)+0x71) [0x614521]
 4: (SimpleMessenger::Pipe::accept()+0x1f2b) [0x6331db]
 5: (SimpleMessenger::Pipe::reader()+0x17c1) [0x636f41]
 6: (SimpleMessenger::Pipe::Reader::entry()+0x15) [0x4a3e85]
 7: (Thread::_entry_func(void*)+0x12) [0x611a92]
 8: (()+0x7971) [0x7fde45af0971]
 9: (clone()+0x6d) [0x7fde4438092d]
```

Associated revisions

Revision dc40b374 - 10/07/2011 11:47 PM - Sage Weil

auth: move AuthAuthorizeHandler registry into class

Static classes with constructors and destructors are dangerous. Explicitly
manage these as part of the server components (OSD, MDS).

Fixes: #1608
Signed-off-by: Sage Weil <sage@newdream.net>

History

#1 - 10/07/2011 04:49 PM - Sage Weil

if this was caused by global static class lameness, it should be fixed by dc40b37403298a60cb5823c030fa94518b0c6e35.

otherwise, it's some random memory corruption or something...

#2 - 10/09/2011 08:39 PM - Sage Weil

- Target version changed from v0.37 to v0.38

#3 - 10/09/2011 08:41 PM - Sage Weil

- translation missing: en.field_position set to 53

#4 - 10/11/2011 01:41 PM - Sage Weil

- Status changed from New to Resolved

I'm going to cross my fingers and call this resolved, unless/until it comes up again.