Ceph - Bug #10425

RadosClient::connect leaks Objecter if called twice

12/23/2014 03:40 AM - Loic Dachary

Status:	Resolved		**Start date:**	12/23/2014
Priority:	Normal		**Due date:**	
Assignee:	Loic Dachary		**% Done:**	0%
Category:	librados		**Estimated time:**	0.00 hour
Target version:			**Spent time:**	0.00 hour
Source:	other		**Reviewed:**	
Tags:			**Affected Versions:**	
Backport:	firefly		**ceph-qa-suite:**	
Regression:	No		**Pull request ID:**	
Severity:	3 - minor			

Description

http://workbench.dachary.org/ceph/ceph/blob/giant/src/librados/RadosClient.cc#L226

If RadosClient::connect is called a second time (maybe after fixing an error condition), the Objecter allocated by the first call will be leaked.

Associated revisions

Revision 624c056d - 02/01/2015 08:36 PM - Radoslaw Zarzynski

librados: fix resources leakage in RadosClient::connect().

If RadosClient::connect was called a second time (which could
happen as a part of recovery from failure), the instances
of Objecter and Messenger allocated by the first call were leaked.

Additionally, the implementation of the method wrongly reported
memory allocation problems -- it throwed std::bad_alloc exception
instead of returning -ENOMEM error code.

Fixes: #10425
Signed-off-by: Radoslaw Zarzynski <rzarzynski@mirantis.com>

Revision 1b266721 - 02/27/2015 06:14 PM - Radoslaw Zarzynski

librados: fix resources leakage in RadosClient::connect().

If RadosClient::connect was called a second time (which could
happen as a part of recovery from failure), the instances
of Objecter and Messenger allocated by the first call were leaked.

Additionally, the implementation of the method wrongly reported
memory allocation problems -- it throwed std::bad_alloc exception
instead of returning -ENOMEM error code.

Fixes: #10425
Signed-off-by: Radoslaw Zarzynski <rzarzynski@mirantis.com>
(cherry picked from commit 624c056da093c8741242892413438a291c03c7d5)

Conflicts:
src/librados/RadosClient.cc
resolve adding (std::nothrow) that failed because the
prototype of the constructor is not the same

History

#1 - 01/19/2015 05:11 AM - Radoslaw Zarzynski

I am working on this bug.

#2 - 01/19/2015 06:42 AM - Loic Dachary

- Status changed from Verified to In Progress

- Assignee set to Loic Dachary

Cool, thanks. I assign it to myself to track this, let me know if you need any help.

#3 - 01/21/2015 12:04 PM - Radoslaw Zarzynski

- File 20150121_10425_fix_v1.patch added

I am attaching the first proposal of patch for your review.

Besides rectifying the Objecter leak, two additional things have been done in the body of RadosClient::connect method:

1. Switch from throwing variant of "new" to the non-throwing one. I think that handling memory allocation problems via std::bad_alloc exception was
   unintentional behavior, especially due to the usage of ENOMEM return code across the whole method. It might lead to stuck in CONNECTING
   state in some circumstances.
2. Leak of Messenger instance. The issue is very similar to the main problem so I am proposing to fix it together.

Could you please tell me about guard (objecter != NULL) on RadosClient::wait_for_osdmap method? Does the check need to base on assumption
about objecter? Maybe the explicit state verification (like in other methods of the class) should be performed?

#4 - 01/28/2015 05:09 PM - Radoslaw Zarzynski

Link to pull request: https://github.com/ceph/ceph/pull/3513

#5 - 02/01/2015 12:49 PM - Loic Dachary

tests https://github.com/ceph/ceph/pull/3519

#6 - 02/01/2015 01:08 PM - Loic Dachary

- Backport set to dumpling,firefly

#7 - 02/09/2015 02:26 PM - Loic Dachary

- Status changed from In Progress to Testing

#8 - 02/10/2015 09:16 PM - Loic Dachary

- Status changed from Testing to Pending Backport

#9 - 03/26/2015 03:31 PM - Loic Dachary

- Backport changed from dumpling,firefly to firefly

dumpling is end of life

#10 - 03/26/2015 03:31 PM - Loic Dachary

[1b26672](#) librados: fix resources leakage in RadosClient::connect(). (in firefly),

#11 - 03/26/2015 03:31 PM - Loic Dachary

- Status changed from Pending Backport to Resolved

Files

20150121_10425_fix_v1.patch	1.06 KB	01/21/2015	Radoslaw Zarzynski