rbd - Bug #8529

vm get killed when leveldb backend enable

06/03/2014 11:00 PM - Xinxin Shu

Status:	Resolved	**% Done:**	0%
Priority:	Normal	**Spent time:**	0.00 hour
Assignee:	Haomai Wang		
Category:			
Target version:			
Source:	Community (dev)	**Affected Versions:**	
Tags:		**ceph-qa-suite:**	
Backport:		**Pull request ID:**	
Regression:	No	**Crash signature (v1):**	
Severity:	3 - minor	**Crash signature (v2):**	
Reviewed:			

Description

hi all , i enabled leveldb backend , but i use 'attach-device' to attach rbd to vm , the vm get killed , i get a segment fault from dmesg

[1185387.398884] virbr0: port 1(vnet0) entered forwarding state
[1185387.398890] virbr0: port 1(vnet0) entered forwarding state
[1185402.342142] kvm[211895]: segfault at 7f3900000018 ip 00007f3a358bd009 sp 00007f399a7fb7f0 error 6 in librados.so.2.0.0[7f3a35570000+66b000]

the qemu log for this vm :

common/buffer.cc: In function 'ceph::buffer::ptr::ptr(const ceph::buffer::ptr&, unsigned int, unsigned int)' thread 7fc7beffd700 time 2014-06-04 05:29:20.835467
common/buffer.cc: 574: FAILED assert(_raw)
ceph version 0.80-716-g884a6b3 (884a6b374af5c08c4c8d3c5f6488f415b120a6ab)
1: (()+0x34d052) [0x7fc85a695052]
2: (ceph::buffer::list::append(ceph::buffer::ptr const&, unsigned int, unsigned int)+0x2f) [0x7fc85a6960ef]
3: (ceph::buffer::list::splice(unsigned int, unsigned int, ceph::buffer::list*)+0xba) [0x7fc85a6964ca]
4: (Striper::StripedReadResult::add_partial_sparse_result(CephContext*, ceph::buffer::list&, std::map<unsigned long, unsigned long, std::less<unsigned long>, std::allocator<std::pair<unsigned long const, unsigned long> > > const&, unsigned long, std::vector<std::pair<unsigned long, unsigned long>, std::allocator<std::pair<unsigned long, unsigned long> > > const&)+0xa49) [0x7fc85b42c689]
5: (librbd::C_AioRead::finish(int)+0xfa) [0x7fc85b3bb76a]
6: (Context::complete(int)+0x9) [0x7fc85b3bba19]
7: (librbd::AioRequest::complete(int)+0x3d) [0x7fc85b3bbaed]
8: (librados::C_AioComplete::finish(int)+0x1d) [0x7fc85a5ec7cd]
9: (Context::complete(int)+0x9) [0x7fc85b3bba19]
10: (Finisher::finisher_thread_entry()+0x1c8) [0x7fc85a67ac48]
11: (()+0x7e9a) [0x7fc8578f7e9a]
12: (clone()+0x6d) [0x7fc8576243fd]
NOTE: a copy of the executable, or `objdump -rdS <executable>` is needed to interpret this.
terminate called after throwing an instance of 'ceph::FailedAssertion'
2014-06-03 21:29:20.868+0000: shutting down

History

#1 - 06/04/2014 02:16 AM - Haomai Wang

- Status changed from New to Fix Under Review

- Assignee set to Haomai Wang

Hi xinxin,
The fix is here(https://github.com/ceph/ceph/pull/1912)

#2 - 06/07/2014 04:56 AM - Haomai Wang

- Status changed from Fix Under Review to Resolved

- Source changed from other to Community (dev)