

RADOS - Bug #39281

object_stat_sum_t decode broken if given older version

04/12/2019 04:58 PM - David Zafman

Status: Resolved	% Done: 0%
Priority: Urgent	Spent time: 0.00 hour
Assignee: David Zafman	
Category:	
Target version:	
Source:	Affected Versions:
Tags:	ceph-qa-suite:
Backport: nautilus	Component(RADOS):
Regression: No	Pull request ID: 27564
Severity: 3 - minor	Crash signature (v1):
Reviewed:	Crash signature (v2):
Description	
When the encode/decode for object_stat_sum_t went from version 19 to 20 the fast path wasn't updated.	
<pre>\$ ceph-objectstore-tool --op dump-import --file 1.0.export 2019-04-12 09:46:30.901 7f51b46baa00 -1 WARNING: all dangerous and experimental features are enabled. terminate called after throwing an instance of 'ceph::buffer::malformed_input' what(): buffer::malformed_input: void object_stat_sum_t::decode(ceph::buffer::v14_2_0::list::const_iterator&) decode past end of struct encoding *** Caught signal (Aborted) ** in thread 7f51b46baa00 thread_name:ceph-objectstor ceph version 15.0.0-257-g5fa9b0af82 (5fa9b0af82c87e7f80b7a78e59c0f0248c92f1c3) octopus (dev) 1: (()+0x1fbbaa4) [0x55e5c2e94aa4] 2: (()+0x12890) [0x7f51a8534890] 3: (gsignal()+0xc7) [0x7f51a7628e97] 4: (abort()+0x141) [0x7f51a762a801] 5: (()+0x8c8b7) [0x7f51a801d8b7] 6: (()+0x92a06) [0x7f51a8023a06] 7: (()+0x92a41) [0x7f51a8023a41] 8: (()+0x92c74) [0x7f51a8023c74] 9: (object_stat_sum_t::decode(ceph::buffer::v14_2_0::list::iterator_impl<true>&)+0x88f) [0x55e5c29818c1] 10: (decode(object_stat_sum_t&, ceph::buffer::v14_2_0::list::iterator_impl<true>&)+0x23) [0x55e5c29a5b84] 11: (object_stat_collection_t::decode(ceph::buffer::v14_2_0::list::iterator_impl<true>&)+0x29d) [0x55e5c2982e73] 12: (decode(object_stat_collection_t&, ceph::buffer::v14_2_0::list::iterator_impl<true>&)+0x23) [0x55e5c281528b] 13: (pg_stat_t::decode(ceph::buffer::v14_2_0::list::iterator_impl<true>&)+0x3e2) [0x55e5c2984b1c] 14: (decode(pg_stat_t&, ceph::buffer::v14_2_0::list::iterator_impl<true>&)+0x23) [0x55e5c25322f3] 15: (pg_info_t::decode(ceph::buffer::v14_2_0::list::iterator_impl<true>&)+0x350) [0x55e5c298873a] 16: (decode(pg_info_t&, ceph::buffer::v14_2_0::list::iterator_impl<true>&)+0x23) [0x55e5c2428322] 17: (metadata_section::decode(ceph::buffer::v14_2_0::list::iterator_impl<true>&)+0x2a3) [0x55e5c24349a3] 18: (dump_pg_metadata(ceph::Formatter*, ceph::buffer::v14_2_0::list&, metadata_section&)+0x4a) [0x55e5c2407711] 19: (ObjectStoreTool::dump_import(ceph::Formatter*)+0x5c1) [0x55e5c2408709] 20: (main()+0x27d3) [0x55e5c2416256] 21: (__libc_start_main()+0xe7) [0x7f51a760bb97] 22: (_start()+0x2a) [0x55e5c23fed5a]</pre>	
Related issues:	
Copied to RADOS - Backport #39320: nautilus: object_stat_sum_t decode broken ...	Resolved

History

#1 - 04/12/2019 06:40 PM - David Zafman

- Status changed from New to In Progress

- Pull request ID set to 27564

#2 - 04/16/2019 10:32 AM - Nathan Cutler

- Backport set to nautilus

#3 - 04/16/2019 10:32 AM - Nathan Cutler

- Status changed from In Progress to Pending Backport

#4 - 04/16/2019 10:32 AM - Nathan Cutler

- Copied to Backport #39320: nautilus: object_stat_sum_t decode broken if given older version added

#5 - 04/16/2019 10:32 AM - Nathan Cutler

- Status changed from Pending Backport to Fix Under Review

#6 - 04/16/2019 02:41 PM - Nathan Cutler

- Status changed from Fix Under Review to Pending Backport

#7 - 04/16/2019 02:41 PM - Nathan Cutler

- Status changed from Pending Backport to Resolved

#8 - 04/16/2019 11:08 PM - David Zafman

- Status changed from Resolved to Pending Backport

#9 - 04/16/2019 11:10 PM - David Zafman

- Status changed from Pending Backport to Resolved