RADOS - Bug #24486

osd: segv in Session::have_backoff

06/10/2018 06:34 PM - Sage Weil

Status:	Resolved	**% Done:**	0%
Priority:	High	**Spent time:**	0.00 hour
Assignee:			
Category:			
Target version:			
Source:		**Affected Versions:**	
Tags:		**ceph-qa-suite:**	
Backport:	mimic,luminous	**Component(RADOS):**	
Regression:	No	**Pull request ID:**	
Severity:	3 - minor	**Crash signature (v1):**	
Reviewed:		**Crash signature (v2):**	

Description

```
2018-06-09 23:36:57.443 7f871a82e700 -1 *** Caught signal (Segmentation fault) **
 in thread 7f871a82e700 thread_name:tp_osd_tp

 ceph version 14.0.0-421-g63faa8d (63faa8df3753877bdbf212fbe724730aa68b0086) nautilus (dev)
 1: (()+0x8ed7f0) [0x55c35fdd37f0]
 2: (()+0xf6d0) [0x7f87433d16d0]
 3: (cmp(hobject_t const&, hobject_t const&)+0x25) [0x7f87469cc8d5]
 4: (Session::check_backoff(CephContext*, spg_t, hobject_t const&, Message const*)+0x134) [0x55c35
fa9dec4]
 5: (PrimaryLogPG::do_op(boost::intrusive_ptr<OpRequest>&)+0x374) [0x55c35fa2ef14]
 6: (PrimaryLogPG::do_request(boost::intrusive_ptr<OpRequest>&, ThreadPool::TPHandle&)+0xc45) [0x5
5c35fa35e35]
 7: (OSD::dequeue_op(boost::intrusive_ptr<PG>, boost::intrusive_ptr<OpRequest>, ThreadPool::TPHand
le&)+0x1b7) [0x55c35f8993a7]
 8: (PGOpItem::run(OSD*, OSDShard*, boost::intrusive_ptr<PG>&, ThreadPool::TPHandle&)+0x62) [0x55c
35fb06cd2]
 9: (OSD::ShardedOpWQ::_process(unsigned int, ceph::heartbeat_handle_d*)+0x592) [0x55c35f8b6f12]
 10: (ShardedThreadPool::shardedthreadpool_worker(unsigned int)+0x3d3) [0x7f874687b813]
 11: (ShardedThreadPool::WorkThreadSharded::entry()+0x10) [0x7f874687c400]
 12: (()+0x7e25) [0x7f87433c9e25]
```

/a/sage-2018-06-09_21:47:39-rados-wip-sage3-testing-2018-06-09-1439-distro-basic-smithi/2647006/a/sage-2018-06-09_21:47:39-rados-wip-sage3-testing-2018-06-09-1439-distro-basic-smithi/2647006

gdb shows

```
(gdb) f 6
#6  have_backoff (oid=..., pgid=..., this=0x55c362932600) at /usr/src/debug/ceph-14.0.0-421-g63faa
8d/src/osd/Session.h:180
180             p->first > oid) {
(gdb) list
175         if (i == backoffs.end()) {
176           return nullptr;
177         }
178         auto p = i->second.lower_bound(oid);
179         if (p != i->second.begin() &&
180             p->first > oid) {
181           --p;
182         }
```

```
183         if (p != i->second.end()) {
184           int r = cmp(oid, p->first);
```

It looks like p is i->second.end() and we are dereferencing p->first.

Related issues:

Copied to RADOS - Backport #24494: mimic: osd: segv in Session::have_backoff	**Resolved**
Copied to RADOS - Backport #24495: luminous: osd: segv in Session::have_backoff	**Resolved**

History

#1 - 06/10/2018 06:41 PM - Sage Weil

- Status changed from 12 to Fix Under Review

- Backport set to mimic,luminous

https://github.com/ceph/ceph/pull/22497

#2 - 06/12/2018 03:22 AM - Sage Weil

- Status changed from Fix Under Review to Pending Backport

#3 - 06/12/2018 08:00 AM - Nathan Cutler

- Copied to Backport #24494: mimic: osd: segv in Session::have_backoff added

#4 - 06/12/2018 08:00 AM - Nathan Cutler

- Copied to Backport #24495: luminous: osd: segv in Session::have_backoff added

#5 - 10/03/2018 09:32 PM - Nathan Cutler

- Status changed from Pending Backport to Resolved