rgw - Backport #19704

civetweb-worker segmentation fault

04/20/2017 04:05 AM - Ben Hines

Status:	Resolved	**Spent time:**	0.00 hour
Priority:	High		
Assignee:	Yehuda Sadeh		
Target version:	v11.2.1		
Release:	kraken	**Crash signature:**	

Description

https://github.com/ceph/ceph/pull/14960

History

#1 - 04/20/2017 06:10 PM - Yehuda Sadeh

It'd be great if you could provide more info here. Also, maybe try to install the debug package to include symbols so that we could get some more info? Thanks

#2 - 04/20/2017 06:10 PM - Yehuda Sadeh

- Priority changed from Normal to High

#3 - 04/24/2017 05:15 PM - Ben Hines

Yehuda Sadeh wrote:

> It'd be great if you could provide more info here. Also, maybe try to install the debug package to include symbols so that we could get some more info? Thanks

I installed ceph-debuginfo and got the crash again, but the stack in the log still doesn't have symbols. Is there something that needs to be done to get it to print them? (or perhaps it will work now that it's died/restarted once post-symbol-install?)

-Ben

#4 - 04/24/2017 07:10 PM - Yehuda Sadeh

If you got core from the crash you can now try to get a backtrace from gdb. If not, then next time hopefully you'll get the backtrace in the logs.

#5 - 05/03/2017 10:24 PM - Ben Hines

Managed to get a core dump. Is there somewhere I can upload it for you? Here's the backtrace:

(gdb) bt
#0 0x00007fd857d8d23b in raise () from /lib64/libpthread.so.0
#1 0x00007fd862b2fe95 in reraise_fatal (signum=11) at /usr/src/debug/ceph-11.2.0/src/global/signal_handler.cc:72
#2 handle_fatal_signal (signum=11) at /usr/src/debug/ceph-11.2.0/src/global/signal_handler.cc:134
#3 <signal handler called>
#4 0x00007fd856652e71 in __strlen_sse2_pminub () from /lib64/libc.so.6
#5 0x00007fd8628760f2 in handle_request (conn=conn@entry=0x7fd86ca87000)
at /usr/src/debug/ceph-11.2.0/src/civetweb/src/civetweb.c:9632

#6 0x00007fd862877eb9 in process_new_connection (conn=0x7fd86ca87000)
at /usr/src/debug/ceph-11.2.0/src/civetweb/src/civetweb.c:11917
#7 worker_thread_run (thread_func_param=0x7fd86bedb800) at /usr/src/debug/ceph-11.2.0/src/civetweb/src/civetweb.c:12084
#8 worker_thread (thread_func_param=0x7fd86bedb800) at /usr/src/debug/ceph-11.2.0/src/civetweb/src/civetweb.c:12121
#9 0x00007fd857d85dc5 in start_thread () from /lib64/libpthread.so.0
#10 0x00007fd8565e673d in clone () from /lib64/libc.so.6

Here's my ceph.conf settings:

[client.sm-cephrgw5]
host = sm-cephrgw5
keyring = /etc/ceph/ceph.client.radosgw.keyring
log file = /var/log/ceph/client.<snip>.log
rgw thread pool size = 800
debug civetweb = 20
rgw frontends = civetweb enable_keep_alive=yes port=80 num_threads=500 error_log_file=/var/log/ceph/civetweb.error.log
access_log_file=/var/log/ceph/civetweb.access.log
rgw num rados handles = 32
rgw cache lru size = 30000
rgw cache enabled = true
rgw override bucket index max shards = 23
rgw dns name = <snip>
rgw_dns_s3website_name = <snip>
rgw enable apis = s3
debug rgw = 20
rgw lifecycle work time = 20:00-09:00
rgw enable ops log = False

#6 - 05/04/2017 05:43 PM - Yehuda Sadeh

fails on the following line:

```
uri_len = (int)strlen(ri->local_uri);
```

#7 - 05/04/2017 05:53 PM - Yehuda Sadeh

The problem seems to be in the civetweb version that is in kraken. We should move it to whatever we currently have in master (commit: 46ced9ddd2795f00f014e22e5637070b49e7a6d5)

#8 - 05/04/2017 05:58 PM - Yehuda Sadeh

- Status changed from New to Pending Backport

- Backport set to kraken

https://github.com/ceph/ceph/pull/14960

#9 - 05/04/2017 08:18 PM - Nathan Cutler

- Tracker changed from Bug to Backport

- Description updated

- Status changed from Pending Backport to In Progress

- Assignee set to Yehuda Sadeh

description

We're encountering this crash when nessus scans our gateways. I'll attempt to track down the exact request which is causing it, if that's useful.

```
   -23> 2017-04-19 18:50:47.985157 7f441c6fc700  1 ====== starting new request req=0x7f441c6f6340 =====
   -22> 2017-04-19 18:50:47.985186 7f441c6fc700  2 req 12676657:0.000029::GET /::initializing for trans_id = t
x000000000000000c16e31-0058f813f7-41ca13a-default
   -21> 2017-04-19 18:50:47.985535 7f441c6fc700  2 req 12676657:0.000378:s3:GET /::getting op 0
   -20> 2017-04-19 18:50:47.985546 7f441c6fc700  2 req 12676657:0.000389:s3:GET /:list_buckets:authorizing
   -19> 2017-04-19 18:50:47.985552 7f441c6fc700  2 req 12676657:0.000395:s3:GET /:list_buckets:normalizing buc
kets and tenants
   -18> 2017-04-19 18:50:47.985556 7f441c6fc700  2 req 12676657:0.000399:s3:GET /:list_buckets:init permission
s
   -17> 2017-04-19 18:50:47.985571 7f441c6fc700  2 req 12676657:0.000414:s3:GET /:list_buckets:recalculating t
arget
   -16> 2017-04-19 18:50:47.985577 7f441c6fc700  2 req 12676657:0.000419:s3:GET /:list_buckets:reading permiss
ions
   -15> 2017-04-19 18:50:47.985585 7f441c6fc700  2 req 12676657:0.000428:s3:GET /:list_buckets:init op
   -14> 2017-04-19 18:50:47.985588 7f441c6fc700  2 req 12676657:0.000431:s3:GET /:list_buckets:verifying op ma
sk
   -13> 2017-04-19 18:50:47.985603 7f441c6fc700  2 req 12676657:0.000440:s3:GET /:list_buckets:verifying op pe
rmissions
   -12> 2017-04-19 18:50:47.985613 7f441c6fc700  2 req 12676657:0.000456:s3:GET /:list_buckets:verifying op pa
rams
   -11> 2017-04-19 18:50:47.985615 7f441c6fc700  2 req 12676657:0.000458:s3:GET /:list_buckets:pre-executing
   -10> 2017-04-19 18:50:47.985617 7f441c6fc700  2 req 12676657:0.000460:s3:GET /:list_buckets:executing
    -9> 2017-04-19 18:50:47.985692 7f441c6fc700  1 -- 10.30.1.13:0/1280116751 --> 10.30.1.124:6814/26162 -- os
d_op(unknown.0.0:619994 7.d72ef9c4 anonymous.buckets [call user.list_buckets] snapc 0=[] ack+read+known_if_red
irected e136543) v7 -- 0x7f45ac354000 con 0
    -8> 2017-04-19 18:50:47.985719 7f441c6fc700  2 Event(0x7f459819f480 nevent=5000 time_id=304012).wakeup
    -7> 2017-04-19 18:50:47.986499 7f457b9ba700  5 -- 10.30.1.13:0/1280116751 >> 10.30.1.124:6814/26162 conn(0
x7f45ad4e7800 :-1 s=STATE_OPEN_MESSAGE_READ_FOOTER_AND_DISPATCH pgs=197075 cs=1 l=1). rx osd.108 seq 76 0x7f45
ac354000 osd_op_reply(619994 anonymous.buckets [call] v0'0 uv0 ack = -2 ((2) No such file or directory)) v7
    -6> 2017-04-19 18:50:47.986532 7f457b9ba700  1 -- 10.30.1.13:0/1280116751 <== osd.108 10.30.1.124:6814/261
62 76 ==== osd_op_reply(619994 anonymous.buckets [call] v0'0 uv0 ack = -2 ((2) No such file or directory)) v7
==== 137+0+0 (542233904 0 0) 0x7f45ac354000 con 0x7f45ad4e7800
    -5> 2017-04-19 18:50:47.986706 7f441c6fc700  2 req 12676657:0.001548:s3:GET /:list_buckets:completing
    -4> 2017-04-19 18:50:47.986745 7f441c6fc700  2 req 12676657:0.001588:s3:GET /:list_buckets:op status=0
    -3> 2017-04-19 18:50:47.986751 7f441c6fc700  2 req 12676657:0.001594:s3:GET /:list_buckets:http status=200
    -2> 2017-04-19 18:50:47.986757 7f441c6fc700  1 ====== req done req=0x7f441c6f6340 op status=0 http_status=
200 ======
    -1> 2017-04-19 18:50:47.986809 7f441c6fc700  1 civetweb: 0x7f45994d1000: 10.30.1.69 - - [19/Apr/2017:18:50
:47 -0700] "GET / HTTP/1.1" 1 0 - Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
     0> 2017-04-19 18:50:47.986759 7f4466790700 -1 *** Caught signal (Segmentation fault) **
 in thread 7f4466790700 thread_name:civetweb-worker

 ceph version 11.2.0 (f223e27eeb35991352ebc1f67423d4ebc252adb7)
 1: (()+0x50bdca) [0x7f458e8e3dca]
 2: (()+0xf100) [0x7f4583b41100]
 3: (()+0x162961) [0x7f4582405961]
 4: (()+0x2520f2) [0x7f458e62a0f2]
 5: (()+0x253eb9) [0x7f458e62beb9]
 6: (()+0x7dc5) [0x7f4583b39dc5]
 7: (clone()+0x6d) [0x7f458239928d]
 NOTE: a copy of the executable, or `objdump -rdS <executable>` is needed to interpret this.

--- logging levels ---
   0/ 5 none
```

```
   0/ 1 lockdep
   0/ 1 context
   1/ 1 crush
   1/ 5 mds
   1/ 5 mds_balancer
   1/ 5 mds_locker
   1/ 5 mds_log
   1/ 5 mds_log_expire
   1/ 5 mds_migrator
   0/ 1 buffer
   0/ 1 timer
   0/ 1 filer
   0/ 1 striper
   0/ 1 objecter
   0/ 5 rados
   0/ 5 rbd
   0/ 5 rbd_mirror
   0/ 5 rbd_replay
   0/ 5 journaler
   0/ 5 objectcacher
   0/ 5 client
   0/ 5 osd
   0/ 5 optracker
   0/ 5 objclass
   1/ 3 filestore
   1/ 3 journal
   0/ 5 ms
   1/ 5 mon
   0/10 monc
   1/ 5 paxos
   0/ 5 tp
   1/ 5 auth
   1/ 5 crypto
   1/ 1 finisher
   1/ 5 heartbeatmap
   1/ 5 perfcounter
   1/ 5 rgw
   1/10 civetweb
   1/ 5 javaclient
   1/ 5 asok
   1/ 1 throttle
   0/ 0 refs
   1/ 5 xio
   1/ 5 compressor
   1/ 5 newstore
   1/ 5 bluestore
   1/ 5 bluefs
   1/ 3 bdev
   1/ 5 kstore
   4/ 5 rocksdb
   4/ 5 leveldb
   4/ 5 memdb
   1/ 5 kinetic
   1/ 5 fuse
   1/ 5 mgr
   1/ 5 mgrc
   1/ 5 dpdk
  -2/-2 (syslog threshold)
  -1/-1 (stderr threshold)
  max_recent     10000
  max_new         1000
  log_file /var/log/ceph/client.<>.log
--- end dump of recent events ---
```

#10 - 07/18/2017 09:01 PM - Nathan Cutler

- Status changed from In Progress to Resolved

- Target version set to v11.2.1