rbd - Bug #39703
'qemu-img' seg faults on rbd_close under CentOS 7.5
05/10/2019 02:54 PM - Jason Dillaman

Status: Resolved | % Done: 0%
Priority: High | Spent time: 0.00 hour
Assignee: Jason Dillaman | 
Category: Target version: 
Source: 
Tags: 
Backport: 
Regression: No | Affected Versions: 
Severity: 3 - minor | Crash signature (v1): 
Reviewed: 

Description
#0 0x00007f56ded19277 in raise () from /lib64/libc.so.6
#1 0x00007f56ded1a968 in abort () from /lib64/libc.so.6
#2 0x00007f56e042fa66 in tcmalloc::Log(tcmalloc::LogMode, char const*, int, tcmalloc::LogItem, tcmalloc::LogItem, tcmalloc::LogItem, tcmalloc::LogItem) () from /lib64/libtcmalloc.so.4
#3 0x00007f56e0424644 in (anonymous namespace)::InvalidFree(void*) () from /lib64/libtcmalloc.so.4
#4 0x00007f56df8d7d2d in boost::lockfree::queue<librbd::io::AioCompletion*>::~queue() () from /lib64/librbd.so.1
#5 0x00007f56df8ce94a in librbd::ImageCtx::~ImageCtx() from /lib64/librbd.so.1
#6 0x00007f56df8e3e1c in librbd::ImageState<librbd::ImageCtx>::close() () from /lib64/librbd.so.1
#7 0x00007f56df89c954 in rbd_close () from /lib64/librbd.so.1
#8 0x000055f87f197a7d in qemu_rbd_close ()
#9 0x000055f87f178eb9 in bdrv_close ()
#10 0x000055f87f178d78 in bdrv_unref ()
#11 0x000055f87f178f43 in bdrv_close ()
#12 0x000055f87f178d78 in bdrv_unref ()
#13 0x000055f87f1ccdd3 in img_convert ()
#14 0x00007f56ed05445 in __libc_start_main () from /lib64/libc.so.6
#15 0x000055f87f17118d in __start ()


History
#1 - 05/10/2019 11:15 PM - Jason Dillaman
It's due to boost's use of 'aligned_alloc' which is not available in the gperftools (tcmalloc) available on RHEL/CentOS 7.5.

#2 - 05/11/2019 01:21 PM - Jason Dillaman
... actually, it's coming from the built-in C++17 'std::allocator' which can perform optional aligned allocations via 'operator new(unsigned long, std::align_val_t)'.

#3 - 05/11/2019 02:12 PM - Jason Dillaman
https://bugzilla.redhat.com/show_bug.cgi?id=1569391

#4 - 05/14/2019 01:38 PM - Jason Dillaman

06/06/2021
- Status changed from In Progress to Fix Under Review
- Pull request ID set to 28093

#5 - 05/21/2019 06:53 PM - Mykola Golub
- Status changed from Fix Under Review to Resolved