

## Ceph - Bug #1628

### segfault attempting to map an rbd snapshot

10/18/2011 03:18 PM - John Leach

<b>Status:</b> Resolved	<b>% Done:</b> 0%
<b>Priority:</b> Normal	<b>Spent time:</b> 0.00 hour
<b>Assignee:</b> Josh Durgin	
<b>Category:</b> librbd	
<b>Target version:</b> v0.38	
<b>Source:</b>	<b>Reviewed:</b>
<b>Tags:</b>	<b>Affected Versions:</b>
<b>Backport:</b>	<b>ceph-qa-suite:</b>
<b>Regression:</b> No	<b>Pull request ID:</b>
<b>Severity:</b> 3 - minor	<b>Crash signature:</b>
<b>Description</b>	
<pre># gdb --args rbd -n client.srv-3ucz4 --snap=two map test --user srv-3ucz4 --secret secret Reading symbols from /usr/bin/rbd...(no debugging symbols found)...done. (gdb) run Starting program: /usr/bin/rbd -n client.srv-3ucz4 --snap=two map test --user srv-3ucz4 --secret s ecret [Thread debugging using libthread_db enabled] [New Thread 0x7ffff5f75700 (LWP 1321)]  Program received signal SIGSEGV, Segmentation fault. 0x00007ffff7bcb170 in librbd::snap_set(librbd::ImageCtx*, char const*) () from /usr/lib/librbd.so. 1 (gdb) bt #0 0x00007ffff7bcb170 in librbd::snap_set(librbd::ImageCtx*, char const*) () from /usr/lib/librbd .so.1 #1 0x000000000044dd88 in main () (gdb)</pre>	
same with the test@two useage	
device maps fine on it's own, just not snapshot (not sure if I'm supposed to be able to map a snapshot, but it certainly shouldn't segfault!)	
this a build from master from a couple of days ago.	

#### History

##### #1 - 10/18/2011 03:35 PM - Josh Durgin

- Target version set to v0.38

This is a bug in the rbd command line tool - it accepts snapname but doesn't use it for map/unmap. Additionally, it doesn't check which command it's using before calling image.snap\_set(). Mapping/unmapping shouldn't call any librbd functions.

##### #2 - 10/21/2011 08:43 AM - Josh Durgin

- Assignee set to Josh Durgin

**#3 - 10/25/2011 10:35 PM - Sage Weil**

*- Status changed from New to Resolved*