rbd - Bug #4665

librbd: read_iterate() can overflow its return value

04/05/2013 02:50 PM - Josh Durgin

Status:	Resolved	**% Done:**	0%
Priority:	Urgent	**Spent time:**	0.00 hour
Assignee:	Sage Weil		
Category:			
Target version:	v0.61 - Cuttlefish		
Source:	Development	**Reviewed:**	
Tags:		**Affected Versions:**	
Backport:	bobtail	**ceph-qa-suite:**	
Regression:	No	**Pull request ID:**	
Severity:	3 - minor	**Crash signature:**	

Description

If the length requested is longer than int64_t, it will wrap around. This happened to someone on irc when doing an rbd export:

```
(2013-04-05 13:15:33) mrjack_: what could that be:
(2013-04-05 13:15:34) mrjack_: rbd export kvm00000000943 - | gzip >kvm00000000943.gz
(2013-04-05 13:15:34) mrjack_: rbd: export error: (-2147483648) Unknown error 18446744071562067968
```

A new version of read_iterate should be created that just returns 0 or an error code as an int, and takes a uint64_t for the length parameter.

History

#1 - 04/22/2013 11:28 AM - Ian Colle

- Priority changed from High to Urgent

#2 - 04/22/2013 11:31 AM - Ian Colle

Per Josh, this is another easy fix, let's get it into Cuttlefish.

#3 - 04/23/2013 12:18 PM - Sage Weil

- Status changed from 12 to In Progress

- Assignee changed from Josh Durgin to Sage Weil

#4 - 04/23/2013 04:12 PM - Josh Durgin

- Status changed from In Progress to Resolved

commit:857c88e017f082b6ef2a81a1890baa7d20672a31