bluestore - Bug #55145

Bogus assert in SimpleBitmap

03/31/2022 10:19 AM - Gabriel BenHanokh

Status:	Resolved	**% Done:**	100%
Priority:	Immediate		
Assignee:	Gabriel BenHanokh		
Category:			
Target version:			
Source:		**Affected Versions:**	
Tags:		**ceph-qa-suite:**	
Backport:	quincy	**Pull request ID:**	45733
Regression:	No	**Crash signature (v1):**	
Severity:	3 - minor	**Crash signature (v2):**	
Reviewed:			

Description

The boundary check in SimpleBitmap is off by one causing an assert to trigger

```
2022-03-31T02:30:03.282076Z_1752ad21-6733-4266-8389-b70fb8d94408
{
    "assert_condition": "offset + length < m_num_bits",
    "assert_file":
"/home/jenkins-build/build/workspace/ceph-dev-build/ARCH/x86_64/AVAILABLE_ARCH/x86_64/AVAILABLE_DI
ST/centos8/DIST/centos8/MACHINE_SIZE/gigantic/release/17.1.0-138-g723fda64/rpm/el8/BUILD/ceph-17.1
.0-138-g723fda64/src/os/bluestore/simple_bitmap.cc",
    "assert_func": "bool SimpleBitmap::set(uint64_t, uint64_t)",
    "assert_line": 54,
    "assert_msg":
"/home/jenkins-build/build/workspace/ceph-dev-build/ARCH/x86_64/AVAILABLE_ARCH/x86_64/AVAILABLE_DI
ST/centos8/DIST/centos8/MACHINE_SIZE/gigantic/release/17.1.0-138-g723fda64/rpm/el8/BUILD/ceph-17.1
.0-138-g723fda64/src/os/bluestore/simple_bitmap.cc:
 In function 'bool SimpleBitmap::set(uint64_t, uint64_t)' thread
7f077a8913c0 time
2022-03-31T02:30:03.274438+0000\n/home/jenkins-build/build/workspace/ceph-dev-build/ARCH/x86_64/AV
AILABLE_ARCH/x86_64/AVAILABLE_DIST/centos8/DIST/centos8/MACHINE_SIZE/gigantic/release/17.1.0-138-g
723fda64/rpm/el8/BUILD/ceph-17.1.0-138-g723fda64/src/os/bluestore/simple_bitmap.cc:
 54: FAILED ceph_assert(offset + length < m_num_bits)\n",
    "assert_thread_name": "ceph-osd",
    "backtrace": [
        "/lib64/libpthread.so.0(+0x12ce0) [0x7f0778a96ce0]",
        "gsignal()",
        "abort()",
        "(ceph::__ceph_assert_fail(char const*, char const*, int, char
const*)+0x1b0) [0x56200752f4c2]",
        "/usr/bin/ceph-osd(+0x5d7685) [0x56200752f685]",
        "(SimpleBitmap::set(unsigned long, unsigned long)+0x1221)
[0x562007c26b41]",
        "(BlueStore::read_allocation_from_single_onode(SimpleBitmap*,
boost::intrusive_ptr<BlueStore::Onode>&,
BlueStore::read_alloc_stats_t&)+0x294) [0x562007b4d334]",
        "(BlueStore::read_allocation_from_onodes(SimpleBitmap*,
BlueStore::read_alloc_stats_t&)+0x8f7) [0x562007b9adb7]",
        "(BlueStore::reconstruct_allocations(SimpleBitmap*,
BlueStore::read_alloc_stats_t&)+0x5d) [0x562007b9be8d]",
        "(BlueStore::read_allocation_from_drive_on_startup()+0x99)
[0x562007baeec9]",
        "(BlueStore::_init_alloc(std::map<unsigned long, unsigned
long, std::less<unsigned long>,
```

```
std::allocator<std::pair<unsigned long const, unsigned long>
> >*)+0xaeb) [0x562007bafc2b]",
        "(BlueStore::_open_db_and_around(bool, bool)+0x321)
[0x562007be82a1]",
        "(BlueStore::_mount()+0x1ae) [0x562007beb41e]",
        "(OSD::init()+0x403) [0x56200766d523]",
        "main()",
        "__libc_start_main()",
        "_start()"
    ],
```

Related issues:

Related to bluestore - Bug #56791: crash: bool SimpleBitmap::set(uint64_t, ui...	**New**
Duplicated by RADOS - Bug #55154: Multiple OSD's during upgrade crashed with ...	**Duplicate**
Copied to bluestore - Backport #55180: quincy: Bogus assert in SimpleBitmap	**Resolved**

History

#1 - 03/31/2022 11:57 AM - Gabriel BenHanokh

- Status changed from In Progress to Fix Under Review

- % Done changed from 0 to 100

- Pull request ID set to 45733

#2 - 03/31/2022 02:10 PM - Adam Kupczyk

- Priority changed from Normal to Immediate

#3 - 03/31/2022 02:18 PM - Neha Ojha

Seen while upgrading the gibba cluster to 723fda64a662bb79871e590698268007049bcf7f

#4 - 03/31/2022 04:54 PM - Vikhyat Umrao

- Description updated

#5 - 03/31/2022 04:55 PM - Vikhyat Umrao

- Related to Bug #55154: Multiple OSD's during upgrade crashed with bluestore/simple_bitmap.cc: 54: FAILED ceph_assert(offset + length < m_num_bits)\n" added

#6 - 03/31/2022 04:56 PM - Vikhyat Umrao

- Related to deleted (Bug #55154: Multiple OSD's during upgrade crashed with bluestore/simple_bitmap.cc: 54: FAILED ceph_assert(offset + length < m_num_bits)\n")

#7 - 03/31/2022 04:56 PM - Vikhyat Umrao

- Duplicates Bug #55154: Multiple OSD's during upgrade crashed with bluestore/simple_bitmap.cc: 54: FAILED ceph_assert(offset + length < m_num_bits)\n" added

#8 - 03/31/2022 06:18 PM - Neha Ojha

Quincy backport: https://github.com/ceph/ceph/pull/45738 to expedite merge

#9 - 04/04/2022 06:38 PM - Yuri Weinstein

Neha Ojha wrote:

> Quincy backport: https://github.com/ceph/ceph/pull/45738 to expedite merge

merged

#10 - 04/04/2022 06:39 PM - Neha Ojha

- Status changed from Fix Under Review to Pending Backport

#11 - 04/04/2022 06:40 PM - Backport Bot

- Copied to Backport #55180: quincy: Bogus assert in SimpleBitmap added

#12 - 04/04/2022 06:41 PM - Neha Ojha

- Status changed from Pending Backport to Resolved

#13 - 07/28/2022 01:43 AM - Yaarit Hatuka

- Duplicated by Bug #55154: Multiple OSD's during upgrade crashed with bluestore/simple_bitmap.cc: 54: FAILED ceph_assert(offset + length < m_num_bits)\n" added

#14 - 07/28/2022 01:44 AM - Yaarit Hatuka

- Duplicates deleted (Bug #55154: Multiple OSD's during upgrade crashed with bluestore/simple_bitmap.cc: 54: FAILED ceph_assert(offset + length < m_num_bits)\n")

#15 - 07/28/2022 02:17 AM - Telemetry Bot

- Related to Bug #56791: crash: bool SimpleBitmap::set(uint64_t, uint64_t): assert(offset + length < m_num_bits) added