Ceph - Bug #38842

copy_from callback may cause ObjectContextRef leak

03/21/2019 06:21 PM - Zengran Zhang

Status:	Resolved	**Start date:**	03/21/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	OSD	**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour
Source:		**Reviewed:**	
Tags:		**Affected Versions:**	
Backport:	nautilus, mimic	**ceph-qa-suite:**	
Regression:	No	**Pull request ID:**	27084
Severity:	3 - minor		

Description

thread 1
step 1: C_Copyfrom.finishi() call pg.lock()
step 2: process_copy_chunk erase the cop from copy_ops at the end
step 3: C_Copyfrom.finishi() call pg.lock()
step 4: before deconstruct the C_Copyfrom(and the cop).

thread 2
step 1: pg.on_change.
step 2: cancel_copy_ops is not effective because cop had erased
step 3: object_contexts.clear() will leaks

thread 3
setp 1: on flushed, assert false on object_contexts.empty()

it is really rare but possible..

pr: https://github.com/ceph/ceph/pull/27084

Related issues:

Copied to Ceph - Backport #38972: mimic: copy_from callback may cause ObjectC...	**Resolved**
Copied to Ceph - Backport #38973: nautilus: copy_from callback may cause Obje...	**Resolved**

History

#1 - 03/25/2019 08:07 AM - Kefu Chai

- Status changed from New to Need Review

- Pull request ID set to 27084

#2 - 03/26/2019 04:37 PM - Sage Weil

- Status changed from Need Review to Pending Backport

- Backport set to nautilus, mimic, luminous

#4 - 03/27/2019 04:23 PM - Nathan Cutler

- Copied to Backport #38972: mimic: copy_from callback may cause ObjectContextRef leak added

#5 - 03/27/2019 04:23 PM - Nathan Cutler

- Copied to Backport #38973: nautilus: copy_from callback may cause ObjectContextRef leak added

#6 - 05/01/2019 08:57 PM - Nathan Cutler

- Backport changed from nautilus, mimic, luminous to nautilus, mimic

#7 - 05/01/2019 08:58 PM - Nathan Cutler

- Status changed from Pending Backport to Resolved

The code this is changing (struct C_CopyChunk) does not exist in luminous, so I removed the luminous backport.