Ceph - Tasks #4542

fix append to uninitialized buffer in FlatIndex::created and unit tests for src/os/FlatIndex.cc

03/25/2013 10:07 AM - Loic Dachary

Status:	Resolved	**% Done:**	100%
Priority:	Low	**Spent time:**	3.50 hours
Assignee:	Loic Dachary		
Category:	qa		
Target version:			
Tags:		**Affected Versions:**	
Reviewed:		**Pull request ID:**	

Description

work in progress

Create a set of unit tests in **src/test/os/FlatIndex.cc** covering the code src/os/FlatIndex.cc

Associated revisions

Revision 77230d43 - 03/26/2013 08:28 PM - Loic Dachary

fix append to uninitialized buffer in FlatIndex::created

The long_name variable is not initialized. When the append_oname function is called, it will strlen(long_name) and get a result that depends on the stack content. The long_name is truncated to a zero length string to prevent this unexpected behavior.

There is no sure way to trigger the problem by writing a unit test. Unit tests are added for all public methods of the FlatIndex class. Most of the time the tests fail if the long_name variable is not properly initialized.

- uint32_t collection_version()
- coll_t coll() const
- void set_ref(std::tr1::shared_ptr<CollectionIndex> ref)
- int cleanup()
- int init()
- int created(const hobject_t &hoid, const char *path)
- int unlink(const hobject_t &hoid)
- int lookup(const hobject_t &hoid, IndexedPath *path, int *exist)
- int collection_list(vector<hobject_t> *ls)
- int collection_list_partial(const hobject_t &start, int min_count, int max_count, snapid_t seq, vector<hobject_t> *ls, hobject_t *next)

There are a number of border cases that cannot be tested, such as the logic of the lfn_get static function. Since FlatIndex code is designed to transition from older namespace conventions, it is difficult to figure out.

The tests rely on xattr(2) and their availability is checked before running them.

http://tracker.ceph.com/issues/4542 refs #4542

Signed-off-by: Loic Dachary <loic@dachary.org>

History

#1 - 03/25/2013 10:44 AM - Loic Dachary

- Description updated

- Due date set to 03/29/2013

- % Done changed from 0 to 10

#2 - 03/26/2013 01:21 PM - Loic Dachary

- Subject changed from unit tests for src/os/FlatIndex.cc to fix append to uninitialized buffer in FlatIndex::created and unit tests for src/os/FlatIndex.cc

- % Done changed from 10 to 90

#3 - 03/28/2013 05:42 AM - Loic Dachary

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100