CephFS - Bug #12417

segfault launching ceph-fuse with bad --name

07/21/2015 10:09 AM - John Spray

Status:	Resolved	**% Done:**	0%
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Source:	Development	**ceph-qa-suite:**	
Tags:		**Component(FS):**	
Backport:	hammer	**Labels (FS):**	
Regression:	No	**Pull request ID:**	
Severity:	3 - minor	**Crash signature (v1):**	
Reviewed:		**Crash signature (v2):**	
Affected Versions:			

Description

This is just in a vstart environment -- running ceph-fuse with no --name arg is fine.

```
./ceph-fuse --name client.a /tmp/mnt.a
ceph-fuse[2015-07-21 11:05:34.498132 7f27254ad800 -1 init, newargv = 0x4a26300 newargc=111409]: st
arting ceph client

*** Caught signal (Segmentation fault) **
 in thread 7f2718ff9700
 ceph version 9.0.2-753-g50ded2a (50ded2a363a4544ae28d3dd1f2bd13dbd58de295)
 1: (ceph::BackTrace::BackTrace(int)+0x2d) [0xf2c209]
 2: ./ceph-fuse() [0xf2b949]
 3: (()+0x10430) [0x7f2724284430]
 4: (CryptoKey::encrypt(CephContext*, ceph::buffer::list const&, ceph::buffer::list&, std::string*
) const+0x2c) [0x1244b06]
 5: (void encode_encrypt_enc_bl<CephXChallengeBlob>(CephContext*, CephXChallengeBlob const&, Crypt
oKey const&, ceph::buffer::list&, std::string&)+0xc3) [0x12464cc]
 6: (int encode_encrypt<CephXChallengeBlob>(CephContext*, CephXChallengeBlob const&, CryptoKey con
st&, ceph::buffer::list&, std::string&)+0x51) [0x12456da]
 7: (cephx_calc_client_server_challenge(CephContext*, CryptoKey&, unsigned long, unsigned long, un
signed long*, std::string&)+0x86) [0x1240d3f]
 8: (CephxClientHandler::build_request(ceph::buffer::list&) const+0x22b) [0x123c67d]
 9: (MonClient::handle_auth(MAuthReply*)+0x7e0) [0x1053b9c]
 10: (MonClient::ms_dispatch(Message*)+0x2dd) [0x1051239]
 11: (Messenger::ms_deliver_dispatch(Message*)+0xc1) [0x1251187]
 12: (DispatchQueue::entry()+0x36d) [0x12506f7]
 13: (DispatchQueue::DispatchThread::entry()+0x1c) [0x10ae8e6]
 14: (Thread::entry_wrapper()+0xa8) [0x10bac9a]
 15: (Thread::_entry_func(void*)+0x18) [0x10babe8]
 16: (()+0x7555) [0x7f272427b555]
 17: (clone()+0x6d) [0x7f2723307f3d]
2015-07-21 11:05:34.507781 7f2718ff9700 -1 *** Caught signal (Segmentation fault) **
 in thread 7f2718ff9700

 ceph version 9.0.2-753-g50ded2a (50ded2a363a4544ae28d3dd1f2bd13dbd58de295)
 1: (ceph::BackTrace::BackTrace(int)+0x2d) [0xf2c209]
 2: ./ceph-fuse() [0xf2b949]
 3: (()+0x10430) [0x7f2724284430]
 4: (CryptoKey::encrypt(CephContext*, ceph::buffer::list const&, ceph::buffer::list&, std::string*
) const+0x2c) [0x1244b06]
 5: (void encode_encrypt_enc_bl<CephXChallengeBlob>(CephContext*, CephXChallengeBlob const&, Crypt
oKey const&, ceph::buffer::list&, std::string&)+0xc3) [0x12464cc]
```

```
 6: (int encode_encrypt<CephXChallengeBlob>(CephContext*, CephXChallengeBlob const&, CryptoKey con
st&, ceph::buffer::list&, std::string&)+0x51) [0x12456da]
 7: (cephx_calc_client_server_challenge(CephContext*, CryptoKey&, unsigned long, unsigned long, un
signed long*, std::string&)+0x86) [0x1240d3f]
 8: (CephxClientHandler::build_request(ceph::buffer::list&) const+0x22b) [0x123c67d]
 9: (MonClient::handle_auth(MAuthReply*)+0x7e0) [0x1053b9c]
 10: (MonClient::ms_dispatch(Message*)+0x2dd) [0x1051239]
 11: (Messenger::ms_deliver_dispatch(Message*)+0xc1) [0x1251187]
 12: (DispatchQueue::entry()+0x36d) [0x12506f7]
 13: (DispatchQueue::DispatchThread::entry()+0x1c) [0x10ae8e6]
 14: (Thread::entry_wrapper()+0xa8) [0x10bac9a]
 15: (Thread::_entry_func(void*)+0x18) [0x10babe8]
 16: (()+0x7555) [0x7f272427b555]
 17: (clone()+0x6d) [0x7f2723307f3d]
 NOTE: a copy of the executable, or `objdump -rdS <executable>` is needed to interpret this.

   -27> 2015-07-21 11:05:34.498132 7f27254ad800 -1 init, newargv = 0x4a26300 newargc=11
     0> 2015-07-21 11:05:34.507781 7f2718ff9700 -1 *** Caught signal (Segmentation fault) **
 in thread 7f2718ff9700

 ceph version 9.0.2-753-g50ded2a (50ded2a363a4544ae28d3dd1f2bd13dbd58de295)
 1: (ceph::BackTrace::BackTrace(int)+0x2d) [0xf2c209]
 2: ./ceph-fuse() [0xf2b949]
 3: (()+0x10430) [0x7f2724284430]
 4: (CryptoKey::encrypt(CephContext*, ceph::buffer::list const&, ceph::buffer::list&, std::string*
) const+0x2c) [0x1244b06]
 5: (void encode_encrypt_enc_bl<CephXChallengeBlob>(CephContext*, CephXChallengeBlob const&, Crypt
oKey const&, ceph::buffer::list&, std::string&)+0xc3) [0x12464cc]
 6: (int encode_encrypt<CephXChallengeBlob>(CephContext*, CephXChallengeBlob const&, CryptoKey con
st&, ceph::buffer::list&, std::string&)+0x51) [0x12456da]
 7: (cephx_calc_client_server_challenge(CephContext*, CryptoKey&, unsigned long, unsigned long, un
signed long*, std::string&)+0x86) [0x1240d3f]
 8: (CephxClientHandler::build_request(ceph::buffer::list&) const+0x22b) [0x123c67d]
 9: (MonClient::handle_auth(MAuthReply*)+0x7e0) [0x1053b9c]
 10: (MonClient::ms_dispatch(Message*)+0x2dd) [0x1051239]
 11: (Messenger::ms_deliver_dispatch(Message*)+0xc1) [0x1251187]
 12: (DispatchQueue::entry()+0x36d) [0x12506f7]
 13: (DispatchQueue::DispatchThread::entry()+0x1c) [0x10ae8e6]
 14: (Thread::entry_wrapper()+0xa8) [0x10bac9a]
 15: (Thread::_entry_func(void*)+0x18) [0x10babe8]
 16: (()+0x7555) [0x7f272427b555]
 17: (clone()+0x6d) [0x7f2723307f3d]
 NOTE: a copy of the executable, or `objdump -rdS <executable>` is needed to interpret this.

ceph-fuse[1404]: mount failed: (33) Numerical argument out of domain
```

Related issues:

Copied to CephFS - Backport #12500: segfault launching ceph-fuse with bad --name	**Resolved**	**07/21/2015**

Associated revisions

Revision 64e50410 - 07/21/2015 03:13 PM - John Spray

auth: check return value of keyring->get_secret

get_secret can fail to populate the passed CryptoKey, for example if the entity name is not found in the keyring. In this case, attempts to use the CryptoKey will lead to segfaults.

Fixes: #12417
Signed-off-by: John Spray <john.spray@redhat.com>

Revision 1e055782 - 07/28/2015 03:17 PM - John Spray

auth: check return value of keyring->get_secret

get_secret can fail to populate the passed CryptoKey, for
example if the entity name is not found in the keyring. In
this case, attempts to use the CryptoKey will lead to
segfaults.

Fixes: #12417
Signed-off-by: John Spray <john.spray@redhat.com>
(cherry picked from commit 64e5041008744362fdbb16e16bc3e049a2d426aa)

History

#1 - 07/21/2015 03:14 PM - John Spray

- Status changed from New to Fix Under Review

https://github.com/ceph/ceph/pull/5305

#2 - 07/22/2015 03:38 PM - Sage Weil

- Status changed from Fix Under Review to Pending Backport

- Source changed from other to Development

- Backport set to hammer

#3 - 09/06/2015 03:25 PM - Loïc Dachary

- Status changed from Pending Backport to Resolved