

Messengers - Bug #40114

msg: bad address encoding when CEPH_FEATURE_MSG_ADDR2 enabled

06/03/2019 04:06 PM - Jeff Layton

Status: Resolved	% Done: 0%
Priority: Urgent	
Assignee: Jeff Layton	
Category:	
Target version: v15.0.0	
Source: Development	Affected Versions:
Tags:	ceph-qa-suite:
Backport: nautilus	Pull request ID: 28379
Regression: No	Crash signature (v1):
Severity: 3 - minor	Crash signature (v2):
Reviewed:	
Description	
On Linux, entity_addr_t::encode just copies the sockaddr as-is into the bufferlist, without fixing up the endianness of sa_family. entity_addr_t::decode copies it out in reverse cloaking the bug when the encoder and decoder are the same endianness.	
The family field should be net-endian (as it is for legacy addrs), since there is no way for the other end to know what byte-order we're using.	
Fixing this is rather simple, but how to deal with hosts already in the field?	
Related issues:	
Copied to Messengers - Backport #40227: nautilus: msg: bad address encoding w... Resolved	

History

#1 - 06/03/2019 04:24 PM - Jeff Layton

Another bug too: Apparently BSD/OSX have a sa_len field in the sockaddr, but it does not reduce the length that it encodes for the address by that amount. Sage pointed out this PR, which is related:

<https://github.com/ceph/ceph/pull/26606>

#2 - 06/03/2019 05:07 PM - Jeff Layton

So the plan I think is to just have the clients assume that the field in question is LE. That means that LE hosts without the fix will continue to work, but BE hosts may have trouble until they are all fixed. Working on a test patch now.

#3 - 06/04/2019 01:22 PM - Patrick Donnelly

- Subject changed from bad address encoding when CEPH_FEATURE_MSG_ADDR2 enabled to msg: bad address encoding when CEPH_FEATURE_MSG_ADDR2 enabled

- Status changed from New to Fix Under Review

- Assignee set to Jeff Layton

- Priority changed from Normal to Urgent

- Target version set to v15.0.0

- Start date deleted (06/03/2019)

- Source set to Development

- Backport set to nautilus

- Pull request ID set to 28379

#4 - 06/04/2019 01:24 PM - Jeff Layton

PR here: <https://github.com/ceph/ceph/pull/28379>

#5 - 06/08/2019 03:30 PM - Kefu Chai

- Status changed from Fix Under Review to Pending Backport

#6 - 06/10/2019 10:27 AM - Nathan Cutler

- Copied to Backport #40227: nautilus: msg: bad address encoding when CEPH_FEATURE_MSG_ADDR2 enabled added

#7 - 11/05/2019 01:17 PM - Nathan Cutler

- Status changed from Pending Backport to Resolved

While running with --resolve-parent, the script "backport-create-issue" noticed that all backports of this issue are in status "Resolved" or "Rejected".