New issue

Jump to bottom

A malicious node becomes a leader and set the view to a very large one, blocks cannot be processed #2312

Closed **fCorleone** opened this issue on Mar 28 · 1 comment

Labels bug consensus resolved viewchange

fCorleone commented on Mar 28

Describe the bug

I setup a group with 10 nodes. One of them are malicious one. First, the malicious node starts, and after that all the other nodes start. Then I start the press testing program to send transactions to the group. And it stuck here:

```
====== PerformanceOk trans, count: 10000, qps:50, groupId: group
====== Deploy Ok ======
====== Deploy Ok succ, address: 0xe706C8E63BCD23391170AF882Af06fC57cf1e5c6 ======
====== PerformanceOk trans start ======
Already sended: 1000/10000 transactions
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
                                                        |received:10%
Already sended: 2000/10000 transactions
                                                        |received:20%
                                                        |received:20%
Already sended: 3000/10000 transactions
Already sended: 4000/10000 transactions
Already sended: 5000/10000 transactions
Already sended: 6000/10000 transactions
Already sended: 7000/10000 transactions
Already sended: 8000/10000 transactions
Already sended: 9000/10000 transactions
Already sended: 10000/10000 transactions
```

To Reproduce

Steps to reproduce the behavior:

1. setup 10 nodes
2. start press testing program
3. the bug occurs

Expected behavior

The system should not stuck and keep changing the view.

Screenshots

Environment (please complete the following information):

- OS: Ubuntu 20.04
- FISCO BCOS Version 3.0.0-rc2

Additional context

There maybe an integer overflow during the viewchange and the malicious node can always be the leader.

Merged

cyjseagull commented on Mar 28 • edited ▾ Contributor

The problem is triggered because the view overflows:

1. The loki node starts first and broadcasts a large viewchange message packet (view = int64_max) to other nodes;
2. After other nodes receive this message packet and find that the view is larger than their own view, they will trigger quick view switching, and try to switch to this view, and set toView to view+1. At this time, toView overflows and reset to 0;
3. After that, everyone basically maintained this largest view, resulting in an abnormal consensus.

We try to fix this issue by PR #2311

cyjseagull added consensus bug bug fix **viewchange** resolved and removed bug fix labels on Mar 28

cyjseagull closed this as completed on Mar 30

Assignees

No one assigned

Labels

bug consensus resolved **viewchange**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants