





MariaDB Server

MDEV-26402

A SEGV in

Item_field::used_tables/update_depend_map_for_order or Assertion `fixed == 1`

▼ Details

Type:	 Bug
Status:	CLOSED (View Workflow)
Priority:	 Blocker
Resolution:	Fixed
Affects Version/s:	10.4, 10.5, 10.6, 10.7
Fix Version/s:	10.4.25 , 10.5.16 , 10.6.8 , (3)
Component/s:	Optimizer
Labels:	regression
Environment:	Linux version 5.13.0-1-MANJARO (builduser@LEGION) (gcc (GCC) 11.1.0, GNU ld (GNU Binutils) 2.36.1) #1 SMP PREEMPT Mon Jun 7 06:16:10 UTC 2021 x86_64

▼ Description

PoC:

```
CREATE TABLE v0 AS SELECT STRCMP ( 'x' , 'x' ) AS v1 ORDER BY ( v1 + v1 LIKE 'x' AND  
REPLACE INTO v0 SELECT * FROM v0 ;  
CHECK TABLE v0 EXTENDED ;  
SELECT * FROM v0 GROUP BY v1 HAVING v1 = 'x' IN ( v1 IS NULL AND 'x' = 0 , 10 , -1  
OPTIMIZE TABLE v0 , v0 ;  
LOCK TABLE v0 WRITE , v0 WRITE ;
```

Log:

```
2021-08-16 15:06:2021-08-16 14:41:38 0 [Note] InnoDB: Compressed tables use zli ▲  
2021-08-16 14:41:38 0 [Note] InnoDB: Number of pools: 1  
2021-08-16 14:41:38 0 [Note] InnoDB: Using crc32 + pclmulqdq instructions  
2021-08-16 14:41:38 0 [Note] mysqld: O_TMPFILE is not supported on /tmp (disabl  
2021-08-16 14:41:38 0 [Note] InnoDB: Using liburing  
2021-08-16 14:41:38 0 [Note] InnoDB: Initializing buffer pool, total size = 134  
2021-08-16 14:41:38 0 [Note] InnoDB: Completed initialization of buffer pool  
2021-08-16 14:41:38 0 [Note] InnoDB: 128 rollback segments are active.  
2021-08-16 14:41:38 0 [Note] InnoDB: Creating shared tablespace for temporary t  
2021-08-16 14:41:38 0 [Note] InnoDB: Setting file './ibtmp1' size to 12 MB. Phy
```

```
2021-08-16 14:41:38 0 [Note] InnoDB: File './ibtmp1' size is now 12 MB.
2021-08-16 14:41:38 0 [Note] InnoDB: 10.7.0 started; log sequence number 42161;
2021-08-16 14:41:38 0 [Note] InnoDB: Loading buffer pool(s) from /home/fuboa/m
2021-08-16 14:41:38 0 [Note] Plugin 'FEEDBACK' is disabled.
2021-08-16 14:41:38 0 [Note] InnoDB: Buffer pool(s) load completed at 210816 14
2021-08-16 14:41:38 0 [Note] Server socket created on IP: '0.0.0.0'.
2021-08-16 14:41:38 0 [Note] Server socket created on IP: '::'.
2021-08-16 14:41:38 0 [Note] /usr/local/mysql/bin//mysqld: ready for connection
Version: '10.7.0-MariaDB' socket: '/tmp/0.socket' port: 3306 Source distribu
```









Coredump

```
GNU gdb (GDB) 10.2
Copyright (C) 2021 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-pc-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from /usr/local/mysql/bin//mysqld...
[New LWP 1386618]
[New LWP 1349958]
[New LWP 1382444]
```

▼ Issue Links

is duplicated by

- | | |
|---|---|
|  MDEV-26401 A SEGV in Optimizer Component |  CLOSED |
|  MDEV-26403 A SEGV in Optimizer Component |  CLOSED |
|  MDEV-28080 Crash when using HAVING with NOT EXIST predicate in an ... |  CLOSED |
|  MDEV-28082 Crash when using HAVING with IS NULL predicate in an eq... |  CLOSED |

relates to

[Show 1 more links](#) (1 links to)

▼ Activity

5 older comments

- ▼  [Sergei Petrunia](#) added a comment - 2022-04-21 16:50 - **edited**

Can we get rid of such complex-constant Items?

I mean if I run

```
explain SELECT * FROM t1 where i IN ( i IS NULL AND 'x' = 0);
```

I can see that the value of the constant is cached:

```
"attaching_conditions_to_tables": {  
  "original_condition": "t1.i = <cache>(/*always not null*/ 1 is n
```

This is done by this code:


```
conds->compile(thd, &Item::cache_const_expr_analyzer, (uchar **)&analyzer_  
               &Item::cache_const_expr_transformer, (uchar *)&cache_flag);
```

Can we do the same in `st_select_lex::pushdown_from_having_into_where` to get all complex constants replaced with their values?

A: no, it doesn't seem to work for `Item_equal` object. When I added this code, the compilation didn't do anything.

`Item_equal` inherits `Item_func::compile` but has `args=NULL`, `arg_count=0`. Because of that, `Item_func::compile` won't try to "compile" `Item_equal`'s multiple equality members.

(Attempting to get it to compile seems like a hard problem: suppose a multiple equality member, an `Item_field` get compiled to something that isn't an `Item_field`? Also, multiple equality code has `Item`-pointer spaghetti architecture so it's hard to add any local changes.

- ▼  [Sergei Petrunia](#) added a comment - 2022-04-21 17:34

Another approach: if we are marking an item with `IMMUTABLE_FL`, mark the entire item [sub]tree with this.


Then, we won't have the fixed-item-contains-unfixed-items issue.

✓  Sergei Petrunia added a comment - 2022-04-21 19:51

<https://github.com/MariaDB/server/commit/ba1c6577a36b078a41289f6259880ce77fe28711>

✓  Sergei Petrunia added a comment - 2022-04-21 19:51

Oleksandr Byelkin, please review.

✓  Oleksandr Byelkin added a comment - 2022-04-22 10:48


OK to push

▼ People

Assignee:

 Sergei Petrunia

Reporter:

 Zhiyong Wu

Votes:

0 Vote for this issue

Watchers:

5 Start watching this issue

▼ Dates

Created:

2021-08-19 02:02

Updated:

2022-04-29 17:37

Resolved:

2022-04-22 15:27

▼ Git Integration

 Error rendering 'com.xiplink.jira.git.jira_git_plugin:git-issue-webpanel'. Please contact your Jira administrators.