

3.0基站产品测试 - 错误 #2918

Pre1T5版本多终端业务后出现cu coredump问题

2025-03-03 13:58 - 孙浩

|         |           |           |            |
|---------|-----------|-----------|------------|
| 状态:     | 已关闭       | 开始日期:     | 2025-03-03 |
| 优先级:    | 普通        | 计划完成日期:   |            |
| 指派给:    | 孙浩        | % 完成:     | 0%         |
| 类别:     |           | 预期时间:     | 0.00 小时    |
| 目标版本:   |           | 耗时:       | 0.00 小时    |
| 问题归属:   | CU        | 目标解决问题版本: | Rel_3.0.0  |
| 发现问题版本: | Rel_3.0.0 |           |            |

描述

【问题描述】Pre1T5版本（3月3号早上发布版本）多终端业务后出现cu coredump问题；

```
#1 gnb::rm_up::delete_mgr (this=this@entry=0x2b71af20, gnb_mgr_id=..., gnb_mgr_id@entry=...)
  at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/rm/build/./src/rm_up_db.cpp:83
83  /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/rm/build/./src/rm_up_db.cpp: No such file or directory.
(gdb) bt
#0  gnb::gnb_ue_id::operator== (gnb_ue_id=<synthetic pointer>..., this=<optimized out>)
  at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/rm/build/./src/common/include/gnb_common_types.h:238
#1  gnb::rm_up::delete_mgr (this=this@entry=0x2b71af20, gnb_mgr_id=..., gnb_mgr_id@entry=...)
  at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/rm/build/./src/rm_up_db.cpp:83
#2  0x000000000000bee494 in gnb::ue_conn_state::ue_conn_release_initiated::on_bearer_context_release_complete_event (this=<optimized out>, ue_conn=0x2bd566a0,
trans_id=3, bearer_context_release_complete=<optimized out>) at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/ue_conn_mgr/build/./src/ue_conn_mgr_conn_release.cpp:740
#3  0x000000000000c1aef4 in gnb::ue_conn_trans::process_event (this=this@entry=0x2bc81580, ue_conn=ue_conn@entry=0x2bd566a0, msg=msg@entry=0x2bd918b0,
event=event@entry=gnb::ue_conn_event::UE_CONN_BEARER_CONTEXT_RELEASE_COMPLETE_EVENT)
  at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/ue_conn_mgr/build/./src/ue_conn_mgr_trans.cpp:914
#4  0x000000000000c07118 in gnb::ue_conn_trans_mgr::process_trans (this=this@entry=0x2bd566a0, ue_conn=ue_conn@entry=0x2bd566a0, msg=msg@entry=0x2bd918b0,
event=event@entry=gnb::ue_conn_event::UE_CONN_BEARER_CONTEXT_RELEASE_COMPLETE_EVENT)
  at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/ue_conn_mgr/build/./src/ue_conn_mgr_trans_mgr.cpp:1059
#5  0x000000000000bf12c0 in gnb::conn_mgmt::process_bearer_context_release_complete_info (this=this@entry=0x7f7c8857e0,
bearer_context_release_complete=bearer_context_release_complete@entry=0x2bd918b0)
  at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/ue_conn_mgr/build/./src/ue_conn_mgr_el_msg.cpp:133
#6  0x000000000000c35b34 in gnb::ue_conn_mgr_msg_hdlr::process_bearer_mgr_bearer_context_release_complete (this=<optimized out>,
bearer_mgr_bearer_context_release_complete=0x2bd8d5c30) at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/ue_conn_mgr/build/./src/ue_conn_mgr_msg_hdlr.cpp:738
#7  0x000000000000a112c in gnb::ue_cntrl_thread::handle_bearer_mgr_bearer_context_release_complete_msg (this=0x2b9e52c0, message=<optimized out>)
  at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/app/build/./src/ue_cntrl_thread.cpp:339
#8  0x00000000000089fd38 in std::function<gnb::ret (ngp::message*)>::operator()(ngp::message*) const (_args#0=<optimized out>, this=0x7f7c885930)
  at /opt/gcc-linaro-7.5.0-2019.12-x86_64_aarch64-linux-gnu/aarch64-linux-gnu/include/c++/7.5.0/bits/std_function.h:706
#9  gnb::ue_cntrl_thread::process_message (this=<optimized out>, message=0x2b7b4f90)
  at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/app/build/./src/ue_cntrl_thread.cpp:71
#10 0x0000000000008a9c20 in ngp::comm_thread::run (this=0x2b9e52c0) at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/app/build/./src/ngp/include/ngp_comm_thread.h:300
#11 0x000000000000c86028 in ngp::thread_entry_function (param=0x2b9e52c0) at /root/yl/cu/nr_hl_cu/ngp/thread/build/./src/ngp_sys_thread.cpp:121
#12 ngp::thread_start (param=0x2b9e52c0) at /root/yl/cu/nr_hl_cu/ngp/thread/build/./src/ngp_sys_thread.cpp:134
#13 0x000000007fa21587e4 in start_thread (arg=0x7fdd4810ef) at pthread_create.c:486
#14 0x000000007fa20af70c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
(gdb) f 1
#1  gnb::rm_up::delete_mgr (this=this@entry=0x2b71af20, gnb_mgr_id=..., gnb_mgr_id@entry=...)
  at /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/rm/build/./src/rm_up_db.cpp:83
83  in /root/yl/cu/nr_hl_cu/cu/nr_hl_cu/rm/build/./src/rm_up_db.cpp
(gdb) i local
itr = <optimized out>
__for_range = std::map with 2 elements = {[1] = 0x2bd93470, [2] = 0x2bd85d40}
__for_begin = <optimized out>
__for_end = <optimized out>
iterator = {first = {ue_control_thread_inst_id = 0, rm_thread_inst_id = 0, conn_type = 0, ue_id = 3}, second = 0x2b95f460}
up_ue = 0x2b95f460
(gdb) quit
```

历史记录

#1 - 2025-03-03 14:27 - 杨杨乐

- 状态 从 新建 变更为 进行中

#2 - 2025-03-03 14:40 - 杨杨乐

- 状态 从 进行中 变更为 转测试

- 指派给 从 杨杨乐 变更为 孙浩

【问题原因】

问题描述：如下的释放的伪代码

- 1.使用了for (auto &: rm\_rb\_list) {  
delete\_rb(rb\_id);  
}  
2.在delete\_rb里面会删除rm\_rb\_list里的某个内容  
3.这样会导致迭代器失效，从而导致崩溃

该问题属于修改新问题引入的问题：  
之前pdu  
Session释放的问题#2824的修改，引入了该问题；之前的代码在删除一次后进行delete，所以没有问题，但是#2824问题的修改，删除了delete，导致了崩溃

【修改方案】  
收集所有需要删除的gnb\_rb\_id，然后循环调用delete\_rb进行删除

【回归方法和注意事项】  
接入多余一个ue，然后在做业务的过程中，多次释放和接入；如果问题不再出现，则关闭问题单

#3 - 2025-03-03 16:00 - 孙浩

- 状态从 转测试 变更为 已解决

重新打包的Rel\_3.0.0\_Pre1T5版本，反复接入2到3个终端并灌包业务，暂未出现cu coredump现象，问题解决。

#4 - 2025-03-11 11:47 - 孙浩

- 状态从 已解决 变更为 已关闭

Rel\_3.0.0\_Pre1T7版本，反复接入2个终端并灌包业务，未出现cu coredump现象，问题关闭。

文件

|                         |        |            |    |
|-------------------------|--------|------------|----|
| coredump截图.jpg          | 543 KB | 2025-03-03 | 孙浩 |
| cu coredump日志1-0303.rar | 277 KB | 2025-03-03 | 孙浩 |