3.0基站产品测试 - 错误 #4964

[3.0产品测试] 4UE压力测试中，du出现挂死

2026-03-05 16:12 - 黄 毅

状态:	进行中	**开始日期:**	2026-03-05
优先级:	一般	**计划完成日期:**	
指派给:	韩 伟	**% 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:	DU	**目标解决问题版本:**	Rel_3.2.1
发现问题版本:	Rel_3.2.1		

描述

测试版本：Rel3.2.1_Pre1T2版本
测试设备：军特整机192.168.8.234，网管：192.168.8.181
测试用例：4UE压力测试
基站配置：1D3U
测试终端：星创CPE*4
测试场景：基站启动正常，终端接入做上行业务。每个终端上行灌包100M
问题描述：压力测试中，du出现挂死

历史记录

#1 - 2026-03-05 17:22 - 韩 伟

- 文件 coredump调用栈信息.png 已添加

- 状态 从 新建 变更为 进行中

该问题已在定位修改中。目前看跑死位置

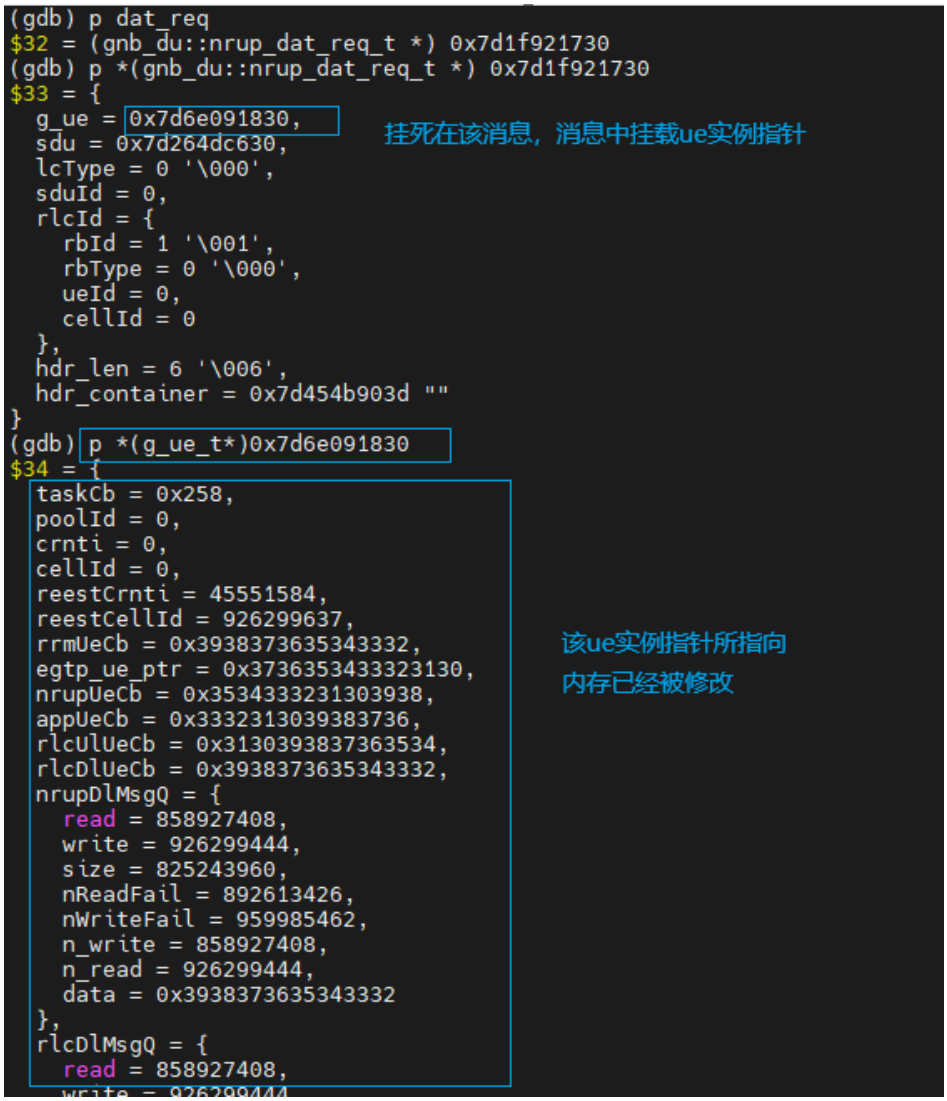
```
Using host libthread_db library "/lib/aarch64-linux-gnu/libthread_db.so.1".
Core was generated by `./gnb_du'.
Program terminated with signal SIGSEGV, Segmentation fault.
#0  gnb_du::gnb_du_nrup_msg_comm::process_data_pdu (this=this@entry=0x7d20629a34, du_msg=du_msg@entry=0x7d25788434, pktNum=0x7dd1b29234, pktNum@entry=0x7dd1b29284, pktLen=0x7dd1b29230,
    pktLen@entry=0x7dd1b29280) at /home/zlw/du_push/ran/nr_hl_du/src/du_app/nrup/build/../src/gnb_du_nrup_msg_comm.cpp:235
235     /home/zlw/du_push/ran/nr_hl_du/src/du_app/nrup/build/../src/gnb_du_nrup_msg_comm.cpp: No such file or directory.
[Current thread is 1 (Thread 0x7dd1b29b70 (LWP 2335))]
(gdb) bt
#0  gnb_du::gnb_du_nrup_msg_comm::process_data_pdu (this=this@entry=0x7d20629a34, du_msg=du_msg@entry=0x7d25788434, pktNum=0x7dd1b29234, pktNum@entry=0x7dd1b29284, pktLen=0x7dd1b29230,
    pktLen@entry=0x7dd1b29280) at /home/zlw/du_push/ran/nr_hl_du/src/du_app/nrup/build/../src/gnb_du_nrup_msg_comm.cpp:235
#1  0x00000000006ff400 in gnb_du::gnb_du_nrup_msg_comm::du_nrup_actv_tsk (tsk_info=<optimized out>)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/nrup/build/../src/gnb_du_nrup_msg_comm.cpp:118
#2  0x00000000007ce9f8 in gnb_du::gnb_du_worker_thread_instance::process_message (this=0x7d2062a034, p_task=<optimized out>, priority=<optimized out>)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../src/gnb_du_worker_thread.cpp:512
#3  0x0000000000771748 in ngp::thread_pool<gnb_du::gnb_du_worker_thread_instance, ssTskInfo>::thread_worker::run (this=0xf490af0)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../../../../../../ngp/include/ngp_thread_pool.h:426
#4  0x00000000008fd6e4 in thread_start () at /home/zlw/du_push/ngp/thread/build/../src/ngp_sys_thread.cpp:338
#5  0x0000007f7f9b77e4 in start_thread (arg=0x7ffceef8ff) at pthread_create.c:486
#6  0x0000007f7f5e970c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
```

初步分析原因为：ue实例异常后继续被使用，直接导致挂死。

#2 - 2026-03-05 17:41 - 韩 伟

- 文件 异常ue内存.png 已添加

异常ue实例进行解引用时挂死，一下为挂死ue实例内存情况：



#3 - 2026-03-05 17:42 - 韩 伟

因为内存已经被修改，无法确定异常ue的rnti信息，暂无法确认该ue是否确实已经被释放了。

#4 - 2026-03-05 20:56 - 韩 伟

- 文件 站上在线UE信息记录查询.png 已添加

- 文件 通过环形队列确认释放UE信息.png 已添加

通过core记录信息，确认ue=0x7d6e09183确实已经释放
站上在线UE信息记录查询.png
通过环形队列确认释放UE信息.png
后通过core文件记录到的nrupDlMsgQ环形队列中信息，确认释放UE=0x7d6e091830的rnti为17116

#5 - 2026-03-05 20:57 - 韩 伟

- 文件 UE_17116_释放Log.png 已添加

后再通过Log查找，找到17116终端确实在基站挂死前进行了释放：
UE_17116_释放Log.png

#6 - 2026-03-05 21:00 - 韩 伟

基于这些信息，可以确认ue=17116已经放生了释放，但是消息队列中还缓存有该ue相关的消息待处理，在ue-17116释放后，ue实例内存释放后，缓存的消息在进行处理时，由于防护不到位，导致访问了已经释放的内存信息，直接导致挂死，针对此问题，对代码进行了修改和防护增强。

文件

20260305-160921.jpg	525 KB	2026-03-05	黄 毅
core.WORKER_0_2.rar	45.7 MB	2026-03-05	黄 毅

coredump调用栈信息.png	60.5 KB	2026-03-05	韩伟
异常ue内存.png	51.7 KB	2026-03-05	韩伟
站上在线UE信息记录查询.png	9.1 KB	2026-03-05	韩伟
通过环形队列确认释放UE信息.png	17.7 KB	2026-03-05	韩伟
UE_17116_释放Log.png	42.6 KB	2026-03-05	韩伟