OBSERVATIONS of Freeze Issue. CQ: **MobC00423019**

## Conclusion:

**Memory is very low and all the processes with adj value 117 and above can be killed to recover memory. There are 20 processes with adj value greater than 117, out of which 10 are already in zombie state and rest 10 are having mm\_struct set to NULL. Hence lowmem\_shrinker loops and goes backs, just eating up the CPU time.**

**But the real problem what “android.io” application was holding a mutex lock and enters a infinite while loops. So none of the other task where able to proceed.**

## Runqueue:

crash> runq

CPU 0 RUNQUEUE: c1e02480

CURRENT: PID: 17492 TASK: d69b3740 COMMAND: "kworker/u4:5"

RT PRIO\_ARRAY: c1e02560

[no tasks queued]

CFS RB\_ROOT: c1e024f0

[120] PID: 1580 TASK: edfe0880 COMMAND: **"sh"**

[120] PID: 1557 TASK: edec5980 COMMAND: **"gpsd"**

[120] PID: 490 TASK: edfe2ec0 COMMAND: **"kswapd0"**

[112] PID: 1518 TASK: ed1ff300 COMMAND: "surfaceflinger"

[112] PID: 1836 TASK: edf56ec0 COMMAND: "SensorService"

[101] PID: 1676 TASK: edde0440 COMMAND: "AudioOut\_2"

[120] PID: 1394 TASK: edf7bb80 COMMAND: **"healthd"**

CPU 1 RUNQUEUE: c1e0b480

CURRENT: PID: 1523 TASK: ed1fd540 COMMAND: "atparser"

RT PRIO\_ARRAY: c1e0b560

[no tasks queued]

CFS RB\_ROOT: c1e0b4f0

[120] PID: 8 TASK: edc65dc0 COMMAND: "rcu\_preempt"

[120] PID: 17359 TASK: d69b1540 COMMAND: "kworker/1:2"

[125] PID: 491 TASK: ed404cc0 COMMAND: "ksmd"

[120] PID: 2 TASK: edc64440 COMMAND: **"kthreadd"**

[120] PID: 1606 TASK: edde1dc0 COMMAND**: "adbd"**

[120] PID: 1843 TASK: edd4e200 COMMAND: "android.io"

**Below threads are preempted out while in lowmem\_shrink.**

PID: 2 TASK: edc64440 CPU: 1 COMMAND: "kthreadd"

PID: 490 TASK: edfe2ec0 CPU: 0 COMMAND: "kswapd0"

PID: 1394 TASK: edf7bb80 CPU: 0 COMMAND: "healthd"

PID: 1557 TASK: edec5980 CPU: 0 COMMAND: "gpsd"

PID: 1580 TASK: edfe0880 CPU: 0 COMMAND: "sh"

PID: 1606 TASK: edde1dc0 CPU: 1 COMMAND: "adbd"

**Here is bt of one among them,**

PID: 2 TASK: edc64440 CPU: 1 COMMAND: "kthreadd"

#0 [<c07142f8>] (\_\_schedule) from [<c0714740>]

#1 [<c0714740>] (preempt\_schedule) from [<c0715588>]

#2 [<c0715588>] (\_raw\_spin\_unlock) from [<c04de388>]

#3 [<c04de388>] (lowmem\_shrink) from [<c00f17b4>]

#4 [<c00f17b4>] (shrink\_slab) from [<c00f47c4>]

#5 [<c00f47c4>] (try\_to\_free\_pages) from [<c00e9bf0>]

#6 [<c00e9bf0>] (\_\_alloc\_pages\_nodemask) from [<c0030294>]

#7 [<c0030294>] (copy\_process) from [<c0031240>]

#8 [<c0031240>] (do\_fork) from [<c003150c>]

#9 [<c003150c>] (kernel\_thread) from [<c00562e4>]

#10 [<c00562e4>] (kthreadd) from [<c0011208>]

## Low memory killer calculations:

**Below is the calculations done in lowmemorykiller.c.** [**Memory statistics**](#_MEMORY_DETAILS:) **show that,**

**other\_free = 1082**

**other\_file = 17797 - 848 - 324 = 16625**

**lowmem\_minfree = $19 =**

**{12288, 15360, 18432, 21504, 24576, 30720}**

**lowmem\_adj = $21 =**

**{0, 58, 117, 176, 529, 1000}**

**other\_file is 16625 pages, so we fall in lowmem\_adj[2] which is 117. All processes having adj value higher than 117 can be killed. Logbuf has logs around 1600 seconds but there is no trace of lowmem kills.**

**$ cat oom\_adj\_value.txt | sort -g > sort.txt**



## List of process having adj value greater than 117:

**The ones marked in red are the ones with their flags set to TIF\_MEMDIE in thread\_info. ie. Already sigkill is send to them. They count up to 10.**

PID PPID CPU TASK ST %MEM VSZ RSS COMM

117 task\_pid = 2009, 2009 1416 1 ea83e200 ZO 0.0 0 0 putmethod.latin

117 task\_pid = 30699, 30699 1416 1 e1fcd100 UN 0.0 0 0 Binder\_4

294 task\_pid = 1330, 1330 1416 1 e2244cc0 UN 0.0 0 0 Binder\_6

294 task\_pid = 25869, 25869 1416 0 e4c24880 ZO 0.0 0 0 m.android.music

529 task\_pid = 25582, 25582 1416 0 e1e62200 ZO 0.0 0 0 emui:screenshot

529 task\_pid = 25618, 25618 1416 0 e1e64cc0 UN 0.0 0 0 AsyncTask #3

529 task\_pid = 25743, 25743 1416 1 e1fcccc0 ZO 0.0 0 0 ndroid.settings

529 task\_pid = 27476, 27476 1416 0 e1ff8880 UN 0.0 0 0 pool-1-thread-1

647 task\_pid = 2239, 2239 1416 1 e4d07300 ZO 0.0 0 0 droid.deskclock

647 task\_pid = 2489, 2489 1416 1 df5fa640 UN 0.0 0 0 pool-1-thread-1

647 task\_pid = 2659, 2659 1416 1 e6687300 ZO 0.0 0 0 android.musicfx

647 task\_pid = 2671, 2671 1416 0 e2c58000 UN 0.0 0 0 Binder\_2

764 task\_pid = 17580, 17580 1416 1 e4ca1540 ZO 0.0 0 0 oadcastreceiver

764 task\_pid = 17597, 17597 1416 1 e1f66640 UN 0.0 0 0 Binder\_2

764 task\_pid = 2642, 2642 1416 1 e2245980 ZO 0.0 0 0 om.brcm.nfcutil

764 task\_pid = 2655, 2655 1416 1 dcbb2ec0 UN 0.0 0 0 Binder\_2

1000 task\_pid = 11555, 11555 1416 0 dcbb0880 ZO 0.0 0 0 d.process.acore

1000 task\_pid = 11569, 11569 1416 0 e1ff9100 UN 0.0 0 0 ContactsProvide

1000 task\_pid = 2514, 2514 1416 1 dc8a0440 ZO 0.0 0 0 .phonesettings2

1000 task\_pid = 2527, 2527 1416 1 e1e66640 UN 0.0 0 0 Binder\_2

## Memlog contex swith details:

<1>1[106324.982798330] 17359 <od\_dbs\_timer

<1>1[106324.982807792] 8 rcu\_preempt

<1>1[106324.982819022] 2 kthreadd

<1>1[106324.992737715] 1606 adbd

<1>1[106325.002739253] 1523 atparser

<1>0[106325.009298484] 591 sh-fb-vsync

<1>0[106325.009321253] 490 kswapd0

<1>1[106325.012744484] 8 rcu\_preempt

<1>0[106325.012745253] 17480 kworker/u4:1

<1>1[106325.012757715] 2 kthreadd

<1>0[106325.012759561] 17480 >pdwait\_work\_fn

<1>0[106325.012767330] 17480 <pdwait\_work\_fn

<1>0[106325.012774330] 17492 kworker/u4:5

<1>0[106325.022739253] 1580 sh

<1>1[106325.022740023] 1606 adbd

<1>0[106325.026043715] 591 sh-fb-vsync

<1>0[106325.026065407] 490 kswapd0

<1>1[106325.032742099] 17359 kworker/1:2

<1>0[106325.032742869] 17470 kworker/0:0

<1>0[106325.032755407] 17470 >od\_dbs\_timer

<1>1[106325.032756176] 17359 >od\_dbs\_timer

<1>0[106325.032776715] 17470 <od\_dbs\_timer

<1>1[106325.032780484] 17359 <od\_dbs\_timer

<1>0[106325.032785023] 1580 **sh** **-> ran 10ms before preempted by gpsd**

<1>1[106325.032787253] 1523 **atparser -> ran 10ms before preempted by rcu\_preempt**

<1>0[106325.042740638] 1557 gpsd

<1>1[106325.042746484] 8 rcu\_preempt

<1>1[106325.042760484] 2 **kthreadd** **-> ran 10ms before preempted by kworker/1:2**

<1>0[106325.042783484] 591 sh-fb-vsync

<1>0[106325.042799869] 1557 **gpsd -> ran 10ms before preempted by kswapd0**

<1>0[106325.052738253] 490 kswapd0

<1>1[106325.052741946] 17359 kworker/1:2

<1>1[106325.052754946] 17359 >vmstat\_update

<1>1[106325.052765484] 17359 <vmstat\_update

<1>1[106325.052774176] 1606 **adbd** **-> ran 10ms before preempted by atparser**

<1>0[106325.059550330] 591 sh-fb-vsync

<1>0[106325.059570946] 17492 kworker/u4:5

<1>1[106325.062739715] 1523 atparser

**All the processes marked in red are executing lowmem\_shrinker and they are getting enough time to run (ie they are preempted only after timer tick). But lowmemory\_killer has not chosen any task to kill.**

**If you look at the** [**List**](#_Last_kill_done) **of process having adj value greater than 117, they all have the task\_size(ie rss value) of zero. So the lowmemory killer loops in lowmem\_shirnker function without selecting any process. Because there is no process with adj value greater than 117 with a non-zero rss value.**

static int lowmem\_shrink(struct shrinker \*s, struct shrink\_control \*sc)

{

----------stripped-------------------------

for\_each\_process(tsk) {

------------stripped---------------

tasksize = get\_mm\_rss(p->mm);

task\_unlock(p);

**if (tasksize <= 0)**

**continue;**

…..

}

…..

}

## Last kill done by lowmem killer:

**crash> lowmem\_deathpending\_timeout**

**lowmem\_deathpending\_timeout = $12 = 7645732**

**crash> jiffies**

**jiffies = $13 = 10602622**

**2956890 jiffies = 10602622 – 7645732**

**Our HZ value is 100 (ie 100 ticks per second)**

**2956890 jiffies = 29568900 ms = 29568.9 seconds = 8 hours, since the last kill.**

**Also there are around 1200 adbd processes in system, which is unusual.**

**crash> ps | grep adbd | wc -l**

**1148**

**Now if you look bt of adbd tasks,**

crash> bt 16198

PID: 16198 TASK: ea897300 CPU: 1 COMMAND: "adbd"

#0 [<c07142f8>] (\_\_schedule) from [<c071479c>]

#1 [<c071479c>] (schedule) from [<c0714b34>]

#2 [<c0714b34>] (schedule\_preempt\_disabled) from [<c0713508>]

#3 [<c0713508>] (\_\_mutex\_lock\_slowpath) from [<c0713630>]

#4 [<c0713630>] (mutex\_lock) from [<c0092254>]

#5 [<c0092254>] (cgroup\_lock\_live\_group) from [<c0095d58>]

#6 [<c0095d58>] (attach\_task\_by\_pid) from [<c0095fd8>]

#7 [<c0095fd8>] (cgroup\_tasks\_write) from [<c0094820>]

#8 [<c0094820>] (cgroup\_file\_write) from [<c0125d78>]

#9 [<c0125d78>] (vfs\_write) from [<c0126178>]

#10 [<c0126178>] (sys\_write) from [<c0011140>]

pc : [<00018ff8>] lr : [<00025709>] psr: 000f0010

sp : beeb1628 ip : 00000011 fp : beeb1724

r10: 000395ec r9 : 0003270c r8 : 015aad12

r7 : 00000004 r6 : 0003270c r5 : 0000003e r4 : 0002d97d

r3 : beeb1620 r2 : 00000001 r1 : 0002d97d r0 : 0000003e

Flags: nzcv IRQs on FIQs on Mode USER\_32 ISA ARM

crash>

They are sleeping on a mutex\_lock.

crash> cgroup\_mutex

cgroup\_mutex = $5 = {

count = {

counter = 0xfffffdac

},

wait\_lock = {

{

-----------stripped-----------------

},

wait\_list = {

next = 0xd7237de4,

prev = 0xd65dfde4

},

owner = 0xedd4e200,

spin\_mlock = 0x0

}

**Which is process “android.io” is holding the lock. This is in runqueue in core 1.**

Crash> task 0xedd4e200

PID: 1843 TASK: edd4e200 CPU: 1 COMMAND: "android.io"

Here is the backtrace of android.io,

crash> bt 1843

PID: 1843 TASK: edd4e200 CPU: 1 COMMAND: "android.io"

#0 [<c07142f8>] (\_\_schedule) from [<c0714b8c>]

#1 [<c0714b8c>] (preempt\_schedule\_irq) from [<c0010d00>]

#2 [<c0010d00>] (svc\_preempt) from [<c0063af0>]

#3 [<c0095638>] (cgroup\_attach\_task) from [<c0095f0c>]

#4 [<c0095f0c>] (attach\_task\_by\_pid) from [<c0095fd8>]

#5 [<c0095fd8>] (cgroup\_tasks\_write) from [<c0094820>]

#6 [<c0094820>] (cgroup\_file\_write) from [<c0125d78>]

#7 [<c0125d78>] (vfs\_write) from [<c0126178>]

#8 [<c0126178>] (sys\_write) from [<c0011140>]

pc : [<401253e8>] lr : [<400f9b75>] psr: 600f0010

sp : 5f911968 ip : 00000020 fp : 4026a4cf

r10: 4026a377 r9 : 00000000 r8 : 40153384

r7 : 00000004 r6 : 5f91198c r5 : 00000000 r4 : 00000000

r3 : 00000001 r2 : 00000005 r1 : 5f91198c r0 : 00000020

Flags: nZCv IRQs on FIQs on Mode USER\_32 ISA ARM

crash>

File: kernel/cgroup.c line 2006

From ramdump it is evident that ent.cgrp is equal to cgrp. And we are struck up in while loop.

do {

struct task\_and\_cgroup ent;

/\* @tsk either already exited or can't exit until the end \*/

if (tsk->flags & PF\_EXITING)

continue;

/\* as per above, nr\_threads may decrease, but not increase. \*/

BUG\_ON(i >= group\_size);

ent.task = tsk;

ent.cgrp = task\_cgroup\_from\_root(tsk, root);

/\* nothing to do if this task is already in the cgroup \*/

if (ent.cgrp == cgrp)

continue;

/\*

\* saying GFP\_ATOMIC has no effect here because we did prealloc

\* earlier, but it's good form to communicate our expectations.

\*/

retval = flex\_array\_put(group, i, &ent, GFP\_ATOMIC);

BUG\_ON(retval != 0);

i++;

if (!threadgroup)

break;

} while\_each\_thread(leader, tsk);

Issue will be fixed with this commit.

<http://mps-gerrit.sj.broadcom.com/#/c/74231/>

## MEMORY DETAILS:

crash> kmem -i

PAGES TOTAL PERCENTAGE

TOTAL MEM 218027 851.7 MB ----

FREE 5249 20.5 MB 2% of TOTAL MEM

USED 212778 831.2 MB 97% of TOTAL MEM

SHARED 24878 97.2 MB 11% of TOTAL MEM

BUFFERS 26 104 KB 0% of TOTAL MEM

CACHED 17771 69.4 MB 8% of TOTAL MEM

SLAB 35550 138.9 MB 16% of TOTAL MEM

TOTAL HIGH 42496 166 MB 19% of TOTAL MEM

FREE HIGH 442 1.7 MB 1% of TOTAL HIGH

TOTAL LOW 175531 685.7 MB 80% of TOTAL MEM

FREE LOW 4807 18.8 MB 2% of TOTAL LOW

TOTAL SWAP 38399 150 MB ----

SWAP USED 28203 110.2 MB 73% of TOTAL SWAP

SWAP FREE 10196 39.8 MB 26% of TOTAL SWAP

crash>

crash> zone\_stat\_item

enum zone\_stat\_item {

NR\_FREE\_PAGES = 0 5249

NR\_LRU\_BASE = 1 8667

NR\_INACTIVE\_ANON = 1

NR\_ACTIVE\_ANON = 2 8397

NR\_INACTIVE\_FILE = 3 7843

NR\_ACTIVE\_FILE = 4 7812

NR\_UNEVICTABLE = 5 961

NR\_MLOCK = 6 0

NR\_ANON\_PAGES = 7 15893

NR\_FILE\_MAPPED = 8 19417

NR\_FILE\_PAGES = 9 17797

NR\_FILE\_DIRTY = 10 0

NR\_WRITEBACK = 11 0

NR\_SLAB\_RECLAIMABLE = 12 9430

NR\_SLAB\_UNRECLAIMABLE = 13 26120

NR\_PAGETABLE = 14 86429

NR\_KERNEL\_STACK = 15 1882

NR\_UNSTABLE\_NFS = 16 0

NR\_BOUNCE = 17 0

NR\_VMSCAN\_WRITE = 18 31679

NR\_VMSCAN\_IMMEDIATE = 19 0

NR\_WRITEBACK\_TEMP = 20 0

NR\_ISOLATED\_ANON = 21 0

NR\_ISOLATED\_FILE = 22 0

NR\_SHMEM = 23 848

NR\_DIRTIED = 24 274975

NR\_WRITTEN = 25 306469

NR\_ANON\_TRANSPARENT\_HUGEPAGES = 26 0

NR\_FREE\_CMA\_PAGES = 27 3999

NR\_VM\_ZONE\_STAT\_ITEMS = 28

};