

Android memory leak detect



2017年11月29日 15:10:39

标签：android / 内存泄露

93



What is memory leak



Native process memory leak detect



Java process memory leak detect



memleak



usage



applied



Basic Algorithm



Other memory leak detector



What is memory leak



内存泄漏指程序未能释放已经不再使用的内存。内存泄漏并非指内存在物理上的消失，而是应用程序分配内存后，由于设计错误，导致在释放该段内存之前就失去了对该段内存的控制，从而造成了内存的浪费。

当进程使用的内存随着时间的推移，越来越多，而且通常是只增不减，那么我们可以判断这个进程出现了内存泄露。

Android系统上，内存泄露有三种情况：

1. Java 进程内存泄露（java heap上的泄露）
2. Native进程或 java native heap 上泄露（JNI代码）
3. Kernel 内存泄露

这一种情况，采用了不同的方法去检测



kongxinsun

+ 关注

原创

7

粉丝

0

喜欢

0

码云

未开通



二手钢琴价格表



他的最新文章

[更多文章](#)

binder call fail caused by no address space

Decay timer of Jemalloc on android

Android show memory info cmd

android java process stack OOM

ion orphaned memory

Native process memory leak detect

目前android上，最好用的方法是android 官网上推荐的：

https://android.googlesource.com/platform/bionic/+master/libc/malloc_debug/README.md

Android 7.0以后，使用以下方法：



0



```
1 setprop libc.debug.malloc.options backtrace
2 setprop libc.debug.malloc 1
3 setprop libc.debug.malloc.program /system/bin/app_process
```

设定这个prop：libc.debug.malloc.program时，leak detect只对这个进程有效。上面的例子中，是对所有/a进程进行检测。如果没有指定这个prop，则对所有的进程进程检测。

所有的native程序申请内存时，使用的是android的libc库。所以track native memory需要使用另一版的libc：libc_malloc_debug_leak.so libc_malloc_debug_qemu.so。这两个so只在userdebug和eng版本有。其中libc_malloc_debug_qemu.so是给emulate用的。所以要debug的话，需要编个userdebug 或 eng的版本。libc.debug.malloc 这个prop的含义如下：

```
1 1 - perform leak detection
2 5 - fill allocated memory to detect overruns
3 10 - fill memory and add sentinels to detect overruns, also check memory leak
4 20 - use special instrumented malloc/free routines for the emulator
```

Libc.debug.malloc level设成10也是可以检测泄露的，但是只有在进程退出的时候才会打印没有free的内存信息。使用起来没有level 1方便。

以mediaserver为例。在设置libc.debug.malloc后，要kill mediaserver.(killall -HUP mediaserver)，让mediaserver申请内存时使用debug libc。具体步骤如下：

1. dump mediaserver's memory use dumphsys command
dumphsys media.player -m > /data/before.txt
2. Reproduce mediaserver memroy leak problem and dump again
dumphsys media player -m > /data/after.txt

加入CSDN，享受更精准的内容推荐，与500万程序员共同成长！

android

7篇

文章存档

2017年12月

4篇

2017年11月

3篇

他的热门文章

Android memory leak detect

📖 90

Android memory corruption debugger

📖 72

android java process stack OOM

📖 67

Android show memory info cmd

📖 34

binder call fail caused by no address space

📖 34



哈尔滨三日游

登录

注册



3. diff the difference
diff before.txt after.txt > diff.txt
4. Get the maps file of mediaserver
cat /proc/[pidofmediaserver]/maps > /data/maps
5. Analysis and map back the backtrace to function symbols and line number

👍 之前的版本需要做第4步，7.0之后，第4步libc默认会做的。7.0之前的版本，可以使用下面的help工具。
<https://github.com/tinypie/android-memleak-help>

☰ 之前的版本，dumpsys media.player -m 输出结果很多条，比如下面这条：

📄 1 size 1590888, dup 2, 0xb4a9a1bc, 0xb4a9a630, 0xb6eb7dc0, 0xb5077980, 0xb4eff7c4,

💬 如下：

- 分配的大小，单位 bytes
- 重复的个数
- backtrace address(up to 32)

这些backtracd地址不结合maps文件看，是没有意义的。以上面为例，假设maps如下：

```
1 b4a8d000-b4ace000 r-xp 00000000 b3:09 41059 /system/lib/libc_malloc_debug_leak
2 b4ace000-b4ad0000 r--p 00040000 b3:09 41059 /system/lib/libc_malloc_debug_leak
3 b4ad0000-b4ad3000 rw-p 00042000 b3:09 41059 /system/lib/libc_malloc_debug_leak
```

需要将backtrace地址减去map的基地址，算出偏移量。比如b4a9a1bc 在b4a8d000-b4ace000这个范围内，偏移量

```
1 b4a9a1bc - b4a8d000 = d1bc
```

然后，用addr2line 找到代码行：

联系我们



请扫描二维码联系客服

✉ webmaster@csdn.net

☎ 400-660-0108

👤 网站客服

关于 招聘 广告服务 阿里云

©2018 CSDN 京ICP证09002463号

经营性网站备案信息


网络110报警服务

中国互联网举报中心

北京互联网违法和不良信息举报中心

```
1 addr2line -f -e symbols/system/lib/libc_malloc_debug_leak.so d1bc
2 /mnt/source/android/bionic/libc/bionic/malloc_debug_leak.cpp:282
```

Mediaserver 有dumpsys 接口，可以从libc里dump信息。如果是其它的native出现了内存泄漏，怎么办？这时就需要添加代码，仿照mediaserver里的dump接口。

 1 source file:
2 frameworks/av/media/libmediaplayerservice/MediaPlayerService.cpp
3 bionic/libc/bionic/malloc_debug_common.cpp



Java process memory leak detect



Android java 虚拟机（无论是dalvik还是art）会自己管理java heap，而JNI代码则和native 进程一样使用libc heap。所以java heap 和native heap 出现泄露时，detect方法也不一样。

Java进程 java heap 的内存泄漏就好查的多，因为有ddms这个工具可以使用。如果是Java 进程的native heap出现了内存泄漏，怎么办？

Ddms也可以查看java进程的native heap，方法如下：

Platform setup(userdebug or eng)

```
1 setprop libc.debug.malloc.options backtrace
2 setprop libc.debug.malloc 1
3 setprop libc.debug.malloc.program /system/bin/app_process
```

computer setup

1. 打开 ~/.android/ddms.cfg
2. 在这个文件的结尾添加
native=true
3. 保存文件
4. 从android sdk里单独打开ddms，确保不跑Eclipse
5. 打开Ddms，连接adb
6. Select process and track the allocation

如果没有ddms，可以使用am dumpheap命令。am dumpheap [pid or process name]，输出的文件是hprof文件，需要用MAT进行分析。如果用-n选项dump native heap的话，map backtrace的方法，上面已经介绍过了。

```

1 am dumpheap: dump the heap of a process. The given <PROCESS> argument may
2 be either a process name or pid. Options are:
3 -n: dump native heap instead of managed heap
4 --user <USER_ID> | current: When supplying a process name,
5 specify user of process to dump; uses current user if not specified.
```



memleak



核文档 Documentation/kmemleak.txt



age

打开以下kconfig

```

1 CONFIG_DEBUG_KMEMLEAK=y
2 CONFIG_DEBUG_KMEMLEAK_EARLY_LOG_SIZE=10000
```

1、如果没有挂载debugfs

```
mount -t debugfs nodev /sys/kernel/debug/
```

2、开启内核检测线程

```
echo scan > /sys/kernel/debug/kmemleak
```

3、查看leak 信息

```
cat /sys/kernel/debug/kmemleak
```

4、清除内核检测报告，新的内存泄露报告将重新写入

```
echo clear > /sys/kernel/debug/kmemleak
```

内存扫描参数可以进行修改，方法是向/sys/kernel/debug/kmemleak 节点写入参数。参数如下：

```
1 off 禁用kmemleak (不可逆)
```

- 5 scan=off 停止自动记忆扫描线程
- 6 scan=<secs> 设置n秒内自动记忆扫描，默认600s
- 7 scan 开启内核扫描
- 8 clear 清除内存泄露报告
- 9 dump=<addr> 转存信息对象在<addr>



kmemleak可以检测以下类型的memory leak



kmalloc/kzalloc



vmalloc



kmem_cache_alloc



Per_cpu

- [Page allocations and ioremap are not tracked]

Basic Algorithm

- 将所有的分配对象放到白名单里（白名单里剩余的对象稍后被认为是孤儿对象(orphan)）
- 扫描kernel data/bss 段，然后扫描所有的page和进程的stack，将匹配的地址存在PRIO搜索树。如果一个白名单对象的指针被发现，将该对象添加到灰名单中
- 扫描与灰名单对象匹配的地址（一些白名单对象可以放到灰名单里），直到灰名单结束
- 剩下的白名单对象被认为是孤儿，写入/sys/kernel/debug/kmemleak。

Other memory leak detector

Native 层的memory leak 检测还可以使用

Valgrind

Address sanitizer



目前您尚未登录，请 [登录](#) 或 [注册](#) 后参与评论



在安卓系统中侦测和调试内存泄露和越界



wlsfling 2017年03月28日 17:12 834

1.1 基本原理 使用bionc的libc初始时，会检测属性"libc.debug.malloc"，//android/bionic/libc/bionic/malloc_debug_common...



Linux kernel 加Memory leaker 检查



transformer_han 2012年08月21日 17:21 2577

1. 重新编译内核，选中 kernel hacking->kernel debug...



程序员不会英语怎么行？

老司机教你一个数学公式秒懂天下英语

c++ 内存泄漏(memory leak)



lee353086 2014年09月30日 09:46 1388

环境：VS2013Update3 打印详细

Linux 内核内存泄露工具使用



wuxiawang 2015年06月04日 16:20 2884

1. 内核添加内存泄漏功能选项 kernel memory leak detector kernel debugging memory leak debugg...

Linux 内核内存泄露工具使用



kehyuanyu 2015年06月04日 11:56 1531

1. 内核添加内存泄漏功能选项 kernel memory leak detector kernel debugging memory leak deb...

加入CSDN，享受更精准的内容推荐，与500万程序员共同成长！

[登录](#)

[注册](#)



@你送《趣味背单词》，学英语就是这么简单

单词背得慢？带你get英语单词速记技能！



Android native 代码内存泄露 定位方案



a332324956 2017年06月21日 21:45 570

Android native 代码内存泄露 定位方案 java代码的内存定位，暂时我们先不关注。此篇文章，主要围绕C++代码的内存泄露。 ** 欢迎留言，交流您所使用的内存泄露定位方案...



Android中内存泄漏的检测（一）最简单的方法

什么是内存泄漏内存泄漏是指程序动态申请的内存存在使用 mishifangxiangdefeng 2016年01月21日 09:12 5324

有释放，导致这段内存不能被操作系统回收再利用。

例如这段程序，申请了4个字节的空间但没有释放，有4个字节的内存泄漏。#include usi...

Linux内核内存泄漏工具使用



guoyiyan1987 2018年01月11日 13:49 17

1. 内核添加内存泄漏功能选项 kernel memory leak detector kernel debugging memory le...

Android native 内存泄露检查（libc.debug.malloc）

转自：<http://www.csdn123.com/html/blogs/20131011/81402.htm>



haima1998 2016年05月26日 17:11 4213

1. Introduction Android对内存的使用包括内存泄漏和...

Android memory corruption debugger



kongxinsun 2017年11月29日 14:10 75

memory corruption是最难搞的问题之一，这是因为：1. 破坏内存的地方和内存破坏的结果常常是分离的，所以很难定位。2. 有些破坏在特定case下才会出现，不好复现。Memor...

送你一本英语单词速记秘籍！



加入CSDN，享受更精准的内容推荐，与500万程序员共同成长！

登录

注册



【定位分享】记一次内存泄漏定位

who_you_are 2016年06月03日 10:25 947

先抛出定位结论：打开了一个socket ,但是没有去收报文，导致内存被报文占满，引起OOM。 定位过程很艰辛，但是真正找到问题所在，发现问题，只用了半个小时。多花的两天时间都是瞎忙活。 关...

Script Memory Leak Detector

china_wanglong 2012年09月29日 21:55 1635

Introduction JavaScript Memory Leak Detector (download) is a debugging tool to detect memory leak...

Android中native进程内存泄露的调试技巧（一）

L_nan 2015年02月04日 18:03 8078

Android5.0版本 Android为Java程序提供了方便的内存泄露信息和工具（如MAT），便于查找。但是，对于纯粹C/C++ 编写的native进程，却不那么容易查找内存泄露。传统的C/C...

Android中native进程内存泄露的调试技巧（一）-- libc debug

libc.debug.malloc // 1 - For memory leak detections. // 5 - For filling allocated / freed memory...

agwtpcbox 2016年11月30日 14:50 1260

Linux 下几款程序内存泄漏检查工具

youbingchen 2016年07月23日 10:15 7940

写这篇博客的原因呢是因为自己在编写基于Nginx磁盘缓存管理程序，目前已经进入测试阶段，关于这个程序的测试分为几个主要步骤：1.内存管理是否正确(因为这个程序本身开辟很多内存空间进行缓存管理，同时这个...

《社交英语》免费领，迅速扩展国际社交圈

立即领取



如何调试malloc(堆越界)问题

sandform 2016年05月26日 16:24 1886

Android native memory leak debug



ritterliu

2016年08月16日 09:58 1363

From <http://blog.chinaunix.net/uid-13614124-id-4054242.html> From http://blog.csdn.net/bd_zengxinxin...

Android中native进程内存泄露的调试技巧（一）



l_nan

2015年02月04日 18:03 8078

Android 5.0版本 Android为Java程序提供了方便的内存泄露信息和工具（如MAT），便于查找。但是，对于纯粹C/C++ 编写的native进程，却不那么容易查找内存泄露。传统的C/C...

系列一：Native memory allocation 导致JVM Crash

JVM Crash抛出如下信息：## There is insufficient memory for the JVM to continue. # Na...

使用Visual Leak Detect or 检测c/ c++ 程序内存泄漏

http://blog.sina.cn/dpool/blog/s/blog_a0f3ea9801010duw.html?vt=4 u011430225 2015年08月26日 09:56 472

1. 引言 通常的内存泄漏指堆内存泄漏[1]。堆内存指从堆中...