Memory test for the Android emulator

GPD 130

Jason Yao

OUTLINE

- Android Building
- Building Kernels

Android Building

- Downloading the Source
  - repo init -u https://android.googlesource.com/platform/manifest -b android-5.1.1_r9
- Set up environment
  - source build/envsetup.sh
  - lunch aosp_arm-eng
- Build the code
  - make –j8

Building Kernels (1)

- Source code
  - git clone https://*android.googlesource.com/kernel/goldfish.git kernel*
  - cd kernel
  - git checkout -t origin/android-goldfish-3.4 -b goldfish3.4

- Kernel Configuration
  - CONFIG_HIGHMEM=y
  - CONFIG_DEBUG_KERNEL=y
  - CONFIG_KGDB=y
  - CONFIG_DEBUG_INFO=y

Building Kernels (2)

- Build Command
  - export PATH=$TOP/prebuilts/gcc/linux-x86/arm/arm-eabi-4.8/bin:$PATH
  - export ARCH=arm
  - export SUBARCH=arm
  - export CROSS_COMPILE=arm-eabi-
  - make -C kernel goldfish_armv7_defconfig
  - time make -C kernel V=1 -j8 2>&1 | tee kernel_build.log
- vmlinux
  - **vmlinux** is a statically linked executable file.
  - zImage

Android Kernel Debugging with GDB(1)

- Using the Emulator
  - emulator -no-audio

    -verbose -show-kernel

    -kernel kernel/arch/arm/boot/zImage

    -memory 2048 -qemu -s –S

- Using the gdb
  - arm-linux-androideabi-gdb kernel/vmlinux
  - target remote localhost:1234
  - break *start_kernel
  - continue

Android Kernel Debugging with GDB(2)

```
(gdb) target remote localhost:1234
Remote debugging using localhost:1234
0x00000000 in ?? ()
(gdb) break *start_kernel
Breakpoint 1 at 0xc04534a0: file init/main.c, line 467.
(gdb) c
Continuing.
```

start_kernel is the first function that kernel runs

```
Breakpoint 1, start_kernel () at init/main.c:467
467     {
(gdb) l
462             pgtable_cache_init();
463             vmalloc_init();
464     }
465
466     asmlinkage void __init start_kernel(void)
467     {
468             char * command_line;
469             extern const struct kernel_param __start___param[], __stop___param[];
470
471             /*
(gdb)
```

Generate OOM (1)

```c
#include <stdio.h>
#include <stdlib.h>

#define MEGABYTE 1024*1024

int main(int argc, char* argv[])
{
    void* myblock = NULL;
    int count = 0;

    while (1) {
        myblock = (void*) malloc(MEGABYTE);

        if (!myblock) {
            break;
        }

        memset(myblock, 1, MEGABYTE);
        printf("Currently allocating %d MB\n", ++count);
    }

    exit(0);
}
```

```makefile
LOCAL_PATH:= $(call my-dir)
include $(CLEAR_VARS)
LOCAL_SRC_FILES:= \
    oom_test.c

LOCAL_MODULE := oom_test
include $(BUILD_EXECUTABLE)
```

```
$ tree
├── Android.mk
└── oom_test.c

$ mm
$ adb push
out/target/produ
ct/generic/syste
m/bin/oom_test
/data
```

Generate OOM (2)

- Exceute oom_test
  - adb shell
  - cd data
  - ./oom_test

```
Currently allocating 1839 MB
Currently allocating 1840 MB
Currently allocating 1841 MB
Killed
137|root@generic:/data #
```

- Kernel log
  - adb shell

  cat /proc/kmsg

```
<6>lowmemorykiller: Killing 'putmethod.latin' (555), adj 117,
<6>    to free 14432kB on behalf of 'kswapd0' (12) because
<6>    cache 18116kB is below limit 73728kB for oom_score_adj 0
<6>    Free memory is -5652kB above reserved
<6>lowmemorykiller: Killing 'android.smspush' (665), adj 58,
<6>    to free 11364kB on behalf of 'kswapd0' (12) because
<6>    cache 15184kB is below limit 73728kB for oom_score_adj 0
<6>    Free memory is -5448kB above reserved
<6>binder: undelivered transaction 21090
<6>binder: 314:314 transaction failed 29189, size 100-0
<6>lowmemorykiller: Killing 'oom_test' (1090), adj 0,
<6>    to free 1892904kB on behalf of 'kswapd0' (12) because
<6>    cache 16700kB is below limit 73728kB for oom_score_adj 0
<6>    Free memory is -4064kB above reserved
<4>healthd: battery l=50 v=0 t=0.0 h=2 st=2 chg=a
```

Generate OOM (3)

```
(gdb) b *lowmem_shrink
Breakpoint 2 at 0xc025c3bc: file drivers/staging/android/lowmemorykiller.c, line 69.
(gdb) c
Continuing.

Breakpoint 2, lowmem_shrink (s=0xc04a8448 <lowmem_shrinker>, sc=0xee25ff68) at drivers/staging/android/lowmemorykiller.c:69
59      {
(gdb) l
64                      if (lowmem_debug_level >= (level))      \
65                              pr_info(x);                     \
66              } while (0)
67
68      static int lowmem_shrink(struct shrinker *s, struct shrink_control *sc)
69      {
70              struct task_struct *tsk;
71              struct task_struct *selected = NULL;
72              int rem = 0;
73              int tasksize;
(gdb)
```

```
(gdb) bt
#0  lowmem_shrink (s=0xc04a8448 <lowmem_shrinker>, sc=0xee25ff68) at drivers/staging/android/lowmemorykiller.c:69
#1  0xc008e68c in do_shrinker_shrink (nr_to_scan=0, sc=0xee25ff68, shrinker=0xc04a8448 <lowmem_shrinker>) at mm/vmscan.c:277
#2  shrink_slab (shrink=0xee25ff68, shrink@entry=0xee25ff60, nr_pages_scanned=3993031636, lru_pages=3226034708,
    lru_pages@entry=0) at mm/vmscan.c:326
#3  0xc00913e0 in balance_pgdat (classzone_idx=<synthetic pointer>, order=0, pgdat=<optimized out>) at mm/vmscan.c:2879
#4  kswapd (p=p@entry=0xc04aff50 <contig_page_data>) at mm/vmscan.c:3180
#5  0xc003405c in kthread (_create=0xee029f3c) at kernel/kthread.c:121
#6  0xc000e128 in kernel_thread_helper ()
#7  0xc000e128 in kernel_thread_helper ()
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
(gdb)
```

Reference