Аварийный дамп – чёрный ящик упавшей JVM

Андрей Паньгин
Одноклассники, ведущий инженер

Java vs. C

- ```
  nullRef.callMethod();
  ```
  ↗ NullPointerException

  ```
  nullRef->callMethod();
  ```
  ✸ Crash!

- ```
  array[999999] = 42;
  ```
  ↗ ArrayIndexOutOfBoundsException

  ```
  array[999999] = 42;
  ```
  ✸ Crash!

- ```
  int y = x / 0;
  ```
  ↗ ArithmeticException

  ```
  int y = x / 0;
  ```
  ✸ Crash!

Java пуленепробиваемая?

Не-е-ет, только не это!

```
#
# A fatal error has been detected by the Java Runtime Environment:
#
#  SIGSEGV (0xb) at pc=0x00002b47f02da0c3, pid=20644, tid=1096538432
#
# JRE version: 6.0_26-b03
# Java VM: Java HotSpot(TM) 64-Bit Server VM (20.1-b02 mixed mode linux-amd64)
# Problematic frame:
# V  [libjvm.so+0x8400c3]
#
# An error report file with more information is saved as:
# /one/bin/hs_err_pid20644.log
#
# If you would like to submit a bug report, please visit:
#   http://java.sun.com/webapps/bugreport/crash.jsp
#
```

Причины аварий

1. Проблема в native коде
2. Некорректное использование закрытого API (например, sun.misc.Unsafe)
3. Баг JVM (да, встречали не раз!)
4. Проблема с «железом» (и такое бывало!)

одноклассники

Сломаем JVM?

Заголовок

```
#
# A fatal error has been detected by the Java Runtime Environment:
#
#  SIGFPE (0x8) at pc=0x00007f1c1197b585, pid=3898, tid=139758846732032
#
# JRE version: Java(TM) SE Runtime Environment (7.0_40-b43) (build 1.7.0_40-b43)
# Java VM: Java HotSpot(TM) 64-Bit Server VM (24.0-b56 mixed mode linux-amd64 compressed oops)
#
```

код сигнала

адрес инструкции

id процесса

id потока

сборка JRE и JVM

Фрейм

```
# Problematic frame:
# C  [libdiv.so+0x585]   Java_demo1_NativeDiv_div+0x5
```

адрес инструкции (относительно DLL и символа)

тип фрейма

C	Native C frame
V	VM function
v	VM generated stub
j	Interpreted Java frame
J	Compiled Java frame

Сигнал

адрес инструкции или
обращения к памяти
(для SEGV, SIGBUS)

код сигнала

Linux	Windows
SIGSEGV	EXCEPTION_ACCESS_VIOLATION EXCEPTION_STACK_OVERFLOW
SIGBUS	EXCEPTION_ACCESS_VIOLATION EXCEPTION_DATATYPE_MISALIGNMENT
SIGILL	EXCEPTION_ILLEGAL_INSTRUCTION EXCEPTION_PRIV_INSTRUCTION
SIGFPE	EXCEPTION_INT_* EXCEPTION_FLT_*

причина сигнала

SEGV_MAPERR	отсутствующая страница
SEGV_ACCERR	нет прав доступа к странице
BUS_ADRALN	невыровненный адрес
BUS_ADRERR	несуществующий адрес
ILL_ILLOPC	неверная инструкция
ILL_PRVOPC	привилегированная инструкция
FPE_INTDIV	целочисленное деление на 0
FPE_FLTDIV	вещественное деление на 0

Регистры CPU

```
Registers:
RAX=0x00000000c5448e8f, RBX=0x00000000bd250ff0, RCX=0x0000000000000000, RDX=0x00000000ffffffff
RSP=0x00007f1c2469d798, RBP=0x00007f1c2469d7f0, RSI=0x00007f1c2469d800, RDI=0x00007f1c1c0099e8
R8 =0x0000c5448e8f8389, R9 =0x00000850b3941760, R10=0x00007f1c1901270c, R11=0x00007f1c234de260
R12=0x0000000000000000, R13=0x00000000bd250ff0, R14=0x00007f1c2469d818, R15=0x00007f1c1c009800
RIP=0x00007f1c1197b585, EFLAGS=0x0000000000010287, CSGSFS=0x0000000000000033
```

Верхушка стека

```
Top of Stack: (sp=0x00007f1c2469d798)
0x00007f1c2469d798:    00007f1c19012738 00000000bd1a53e8
0x00007f1c2469d7a8:    0000000000000000 00007f1c2469d7b0
0x00007f1c2469d7b8:    0000000000000000 00007f1c2469d818
0x00007f1c2469d7c8:    00000000bd251480 0000000000000000
0x00007f1c2469d7d8:    00000000bd250ff0 0000000000000000
0x00007f1c2469d7e8:    00007f1c2469d810 00007f1c2469d860
0x00007f1c2469d7f8:    00007f1c190061d4 00000000eb64ad68
0x00007f1c2469d808:    00007f1c1900ecd6 0000000000000000
```

Машинный код

```
Instructions: (pc=0x00007f1c1197b585)
0x00007f1c1197b565:    48 85 c0 74 0e 5d 48 8d 3d c6 08 20 00 ff e0 0f      ↑ до
0x00007f1c1197b575:    1f 40 00 5d c3 90 90 90 90 90 90 89 d0 c1 fa 1f      │
0x00007f1c1197b585:    f7 f9 c3 90 90 90 90 90 90 90 90 55 48 89 e5 53      │
0x00007f1c1197b595:    48 83 ec 08 48 8b 05 78 08 20 00 48 83 f8 ff 74      ↓ после
```

- Дизассемблер
  - http://www.onlinedisassembler.com
- Описание инструкций
  - http://www.intel.com/content/www/us/en/processors/
    architectures-software-developer-manuals.html

одноклассники

Дизассемблер

```
.data:0x00000018    90       nop
.data:0x00000019    90       nop
.data:0x0000001a    90       nop
.data:0x0000001b    89d0     mov     eax,edx
.data:0x0000001d    c1fa1f   sar     edx,0x1f
.data:0x00000020    f7f9     idiv    ecx
.data:0x00000022    c3       ret
.data:0x00000023    90       nop
.data:0x00000024    90       nop
.data:0x00000025    90       nop
.data:0x00000026    90       nop
.data:0x00000027    90       nop
```

смещение   машинный   декодированные   место падения
              код   инструкции

idiv r/m32
signed divide edx:eax by r/m32

одноклассники

Значения регистров

```
Register to memory mapping:

RAX=0x00000000c5448e8f is an unallocated location in the heap
RBX=0x00000000bd250ff0 is an oop
{method}
 - klass: {other class}
RCX=0x0000000000000000 is an unknown value
RDX=0x00000000ffffffff is an unallocated location in the heap
RSP=0x00007f1c2469d798 is pointing into the stack for thread: 0x00007f1c1c009800
RBP=0x00007f1c2469d7f0 is pointing into the stack for thread: 0x00007f1c1c009800
RSI=0x00007f1c2469d800 is pointing into the stack for thread: 0x00007f1c1c009800
RDI=0x00007f1c1c0099e8 is an unknown value
R8 =0x0000c5448e8f8389 is an unknown value
R9 =0x00000850b3941760 is an unknown value
R10=0x00007f1c1901270c is at code_begin+620 in an Interpreter codelet
method entry point (kind = native)  [0x00007f1c190124a0, 0x00007f1c19012d00]  2144 bytes
R11=0x00007f1c234de260: <offset 0x8a7260> in libjvm.so at 0x00007f1c22c37000
R12=0x0000000000000000 is an unknown value
R13=0x00000000bd250ff0 is an oop
{method}
 - klass: {other class}
R14=0x00007f1c2469d818 is pointing into the stack for thread: 0x00007f1c1c009800
R15=0x00007f1c1c009800 is a thread
```

Стек

границы стека   указатель стека

```
Stack: [0x7f1c2459e000,0x7f1c2469f000],  sp=0x7f1c2469d798,  free space=1021k

Native frames: (J=compiled Java code, j=interpreted, Vv=VM code, C=native code)
C  [libdiv.so+0x585]  Java_demo1_NativeDiv_div+0x5
j  demo1.NativeDiv.access$000(II)I+2
j  demo1.NativeDiv$1.run()V+20
j  demo1.NativeDiv.runLoop(ILjava/lang/Runnable;)V+8
j  demo1.NativeDiv.main([Ljava/lang/String;)V+21
v  ~StubRoutines::call_stub
V  [libjvm.so+0x5f8405]  JavaCalls::call_helper()+0x365
V  [libjvm.so+0x5f6e68]  JavaCalls::call()+0x28
V  [libjvm.so+0x62f8d9]  jni_invoke_static()+0x219
V  [libjvm.so+0x638962]  jni_CallStaticVoidMethod+0x162
C  [libjli.so+0x36d9]  JavaMain+0x7e9
```

смещение в байтах

индекс байткода

тип фрейма   декодированный адрес
(DLL, символ + смещение)

Потоки

```
Java Threads: ( => current thread )
  0x7f1c1c096000 JavaThread "Service Thread" daemon
                [_thread_blocked, id=3910, stack(0x7f1c11c7e000,0x7f1c11d7f000)]
  0x7f1c1c093800 JavaThread "C2 CompilerThread1" daemon
                [_thread_blocked, id=3909, stack(0x7f1c11d7f000,0x7f1c11e80000)]
  0x7f1c1c090800 JavaThread "C2 CompilerThread0" daemon
                [_thread_blocked, id=3908, stack(0x7f1c18014000,0x7f1c18115000)]
  0x7f1c1c08e800 JavaThread "Signal Dispatcher" daemon
                [_thread_blocked, id=3907, stack(0x7f1c18115000,0x7f1c18216000)]
  0x7f1c1c06f800 JavaThread "Finalizer" daemon
                [_thread_blocked, id=3906, stack(0x7f1c188f9000,0x7f1c189fa000)]
  0x7f1c1c06b800 JavaThread "Reference Handler" daemon
                [_thread_blocked, id=3905, stack(0x7f1c189fa000,0x7f1c18afb000)]
=>0x7f1c1c009800 JavaThread "main"
                [_thread_in_native, id=3899, stack(0x7f1c2459e000,0x7f1c2469f000)]
```

указатель Thread*   статус   thread id   границы стека

in_java

in_native

in_vm   тип и название

blocked

trans

одноклассники

Heap

```
Heap
 PSYoungGen      total 18944K, used 327K [0x0eb600000, 0x0ecb00000, 0x100000000)
  eden space 16384K, 2% used [0x0eb600000,0x0eb651f28,0x0ec600000)
  from space 2560K, 0% used [0x0ec880000,0x0ec880000,0x0ecb00000)
  to   space 2560K, 0% used [0x0ec600000,0x0ec600000,0x0ec880000)
 ParOldGen       total 41984K, used 0K [0x0c2200000, 0x0c4b00000, 0x0eb600000)
  object space 41984K, 0% used [0x0c2200000,0x0c2200000,0x0c4b00000)
 PSPermGen       total 21504K, used 2378K [0x0bd000000, 0x0be500000, 0x0c2200000)
  object space 21504K, 11% used [0x0bd000000,0x0bd2529f0,0x0be500000)
```

текущие границы   предел

Code Cache

```
Code Cache  [0x2aaaab977000, 0x2aaaabbe7000, 0x2aaaae977000)
 total_blobs=701 nmethods=360 adapters=295 free_code_cache=48574272 largest_free_block=20224
```

nmethods + adapters + stubs

свободное место

количество скомпилированных методов

События компилятора

```
Compilation events (10 events):
Event: 0.135 Thread 0x7fb4090800    5      java.util.Random::nextInt (7 bytes)
Event: 0.136 Thread 0x7fb4093800    6      demo1.NativeDiv$1::run (28 bytes)
Event: 0.140 Thread 0x7fb4090800 nmethod 5 0x7fb1060090 code [0x7fb10601e0, 0x7fb10602d8]
Event: 0.140 Thread 0x7fb4090800    7      java.util.Random::nextInt (60 bytes)
Event: 0.144 Thread 0x7fb4090800 nmethod 7 0x7fb105fb50 code [0x7fb105fca0, 0x7fb105fe98]
Event: 0.144 Thread 0x7fb4090800    8      demo1.NativeDiv::access$000 (6 bytes)
Event: 0.145 Thread 0x7fb4090800 nmethod 8 0x7fb1062290 code [0x7fb10623e0, 0x7fb1062448]
Event: 0.145 Thread 0x7fb4093800 nmethod 6 0x7fb105f510 code [0x7fb105f680, 0x7fb105f888]
Event: 0.146 Thread 0x7fb4090800   10 %    demo1.NativeDiv::runLoop @ 2 (20 bytes)
Event: 0.150 Thread 0x7fb4090800 nmethod 10% 0x7fb10649d0 code [0x7fb1064b40, 0x7fb1064ec8]
```

конец

on-stack replacement

границы скомпилированного кода

начало

Одноклассники

Прочие события

```
GC Heap History (10 events):

Deoptimization events (10 events):

Internal exceptions (10 events):

Events (10 events):
Event: 0.113 loading class 0x7f03b86cb520
Event: 0.114 loading class 0x7f03b86cb520 done
Event: 0.114 loading class 0x7f03b869aa50
Event: 0.114 loading class 0x7f03b869aa50 done
Event: 0.115 loading class 0x7f03b8682cd0
Event: 0.115 loading class 0x7f03b8682cd0 done
Event: 0.115 loading class 0x7f03b8682c70
Event: 0.115 loading class 0x7f03b8682c70 done
Event: 0.119 loading class 0x7f03b40a6c70
Event: 0.119 loading class 0x7f03b40a6c70 done
```

Карта памяти

```
Dynamic libraries:
00400000-00401000 r-xp 00000000 08:03 156103          /usr/java/jdk1.7.0_40/bin/java
00600000-00601000 rw-p 00000000 08:03 156103          /usr/java/jdk1.7.0_40/bin/java
00bc6000-00be7000 rw-p 00000000 00:00 0               [heap]
7f1bdc000000-7f1bdc021000 rw-p 00000000 00:00 0
7f1bdc021000-7f1be0000000 ---p 00000000 00:00 0
7f1c1197b000-7f1c1197c000 r-xp 00000000 00:15 287     /media/crash/lib/libdiv.so
7f1c11b7c000-7f1c11b7d000 rw-p 00001000 00:15 287     /media/crash/lib/libdiv.so
7f1c11b7e000-7f1c11c7e000 rw-p 00000000 00:00 0       [stack:3911]
7f1c11c81000-7f1c11d7f000 rw-p 00000000 00:00 0       [stack:3910]
7f1c14000000-7f1c14021000 rw-p 00000000 00:00 0
7f1c14021000-7f1c18000000 ---p 00000000 00:00 0
7f1c20c45000-7f1c20e02000 r--s 039d3000 08:03 156934  /usr/java/jdk1.7.0_40/jre/lib/rt.jar
7f1c24494000-7f1c244b6000 r-xp 00000000 08:03 265734  /lib/x86_64-linux-gnu/ld-2.15.so
7f1c246b7000-7f1c246b9000 rw-p 00023000 08:03 265734  /lib/x86_64-linux-gnu/ld-2.15.so
```

права доступа

inode   отображаемый файл

область памяти

read
write   смещение
e**x**ecute   в файле
private
shared   id устройства
            (/dev/hda3)

Окружение

```
VM Arguments:
jvm_args: -Djava.library.path=/media/crash/lib
java_command: demo1.NativeDiv
Launcher Type: SUN_STANDARD

Environment Variables:
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/java/jdk1.7.0_40/bin
USERNAME=root
SHELL=/bin/bash
DISPLAY=:0
```

Память

```
/proc/meminfo:
MemTotal:        4048960 kB
MemFree:         2783932 kB
Buffers:          136360 kB
Cached:           437332 kB
SwapCached:            0 kB
Active:           500384 kB
Inactive:         405308 kB
Unevictable:           0 kB
Mlocked:               0 kB
SwapTotal:       1500156 kB
SwapFree:        1500156 kB
Dirty:               252 kB
Writeback:             0 kB
AnonPages:        332152 kB
Mapped:            89372 kB
Shmem:              4920 kB
Slab:             289216 kB
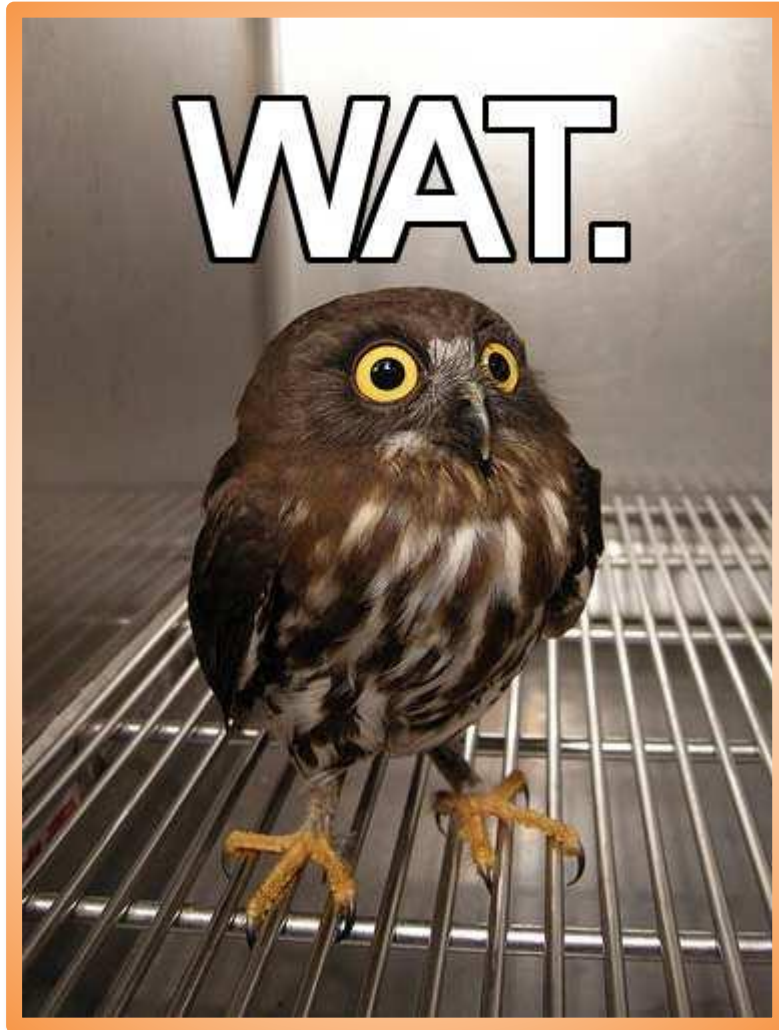SReclaimable:     269068 kB
SUnreclaim:        20148 kB
```

CPU

```
CPU:total 4 (4 cores per cpu, 1 threads per core) family 6 model 58 stepping 9, cmov, cx8,
fxsr, mmx, sse, sse2, sse3, ssse3, tsc

/proc/cpuinfo:
processor           : 0
vendor_id           : GenuineIntel
cpu family          : 6
model               : 58
model name          : Intel(R) Core(TM) i7-3517U CPU @ 1.90GHz
stepping            : 9
cpu MHz             : 2369.955
cache size          : 6144 KB
physical id         : 0
siblings            : 4
core id             : 0
cpu cores           : 4
fpu                 : yes
fpu_exception       : yes
cpuid level         : 5
wp                  : yes
flags               : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36
clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm constant_tsc rep_good nopl pni ssse3 lahf_lm
```

Передача аргументов в регистрах

- http://hg.openjdk.java.net/hsx/hotspot-main/hotspot/file/tip/ src/cpu/x86/vm/assembler_x86.hpp

JNIEnv*

jobject this
jclass holder

C args	c0	c1	c2	c3	c4	c5
Windows	RCX	RDX	R8	R9	RDI*	RSI*
Linux	RDI	RSI	RDX	RCX	R8	R9
Java args	j5	j0	j1	j2	j3	j4

* только Java

Показательные выступления

© fotografersha.livejournal.com

Управление JIT компилятором

- -Xint, -Xcomp

- -XX:CompileCommandFile=.hotspot_compiler

```
compileonly extra1/Malloc.*
compileonly sun/misc/Unsafe.*
exclude extra1/Malloc.main
print extra1/Malloc.free
```

Ошибки бывают у всех

Настройка отчёта об ошибке

- -XX:ErrorFile=./hs_err_pid%p.log

- -XX:OnError="cat hs_err_pid%p.log | mail my@email.com"

- -XX:+ShowMessageBoxOnError

- -XX:+CreateMinidumpOnCrash (только Windows)

- -XX:+UseOSErrorReporting

- -XX:+SuppressFatalErrorMessage

Спасибо!

- Блог
  - http://habrahabr.ru/company/odnoklassniki/blog/
- Наш Open Source
  - https://github.com/odnoklassniki
- Контакты
  - andrey.pangin@odnoklassniki.ru
- Работа в Одноклассниках
  - http://v.ok.ru

одноклассники