

Inner Workings of Safepoints

Johannes Bechberger
mostlynerdless.de



Kinds of Safepoints



Local Safepoint/Handshake

since 2017



Kinds of Safepoints

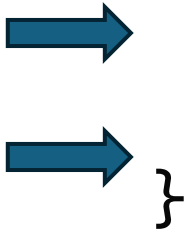


Global Safepoint/Handshake

And they get ever more
important



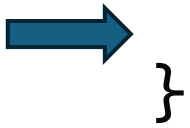
```
int mul(int a, int b) {  
    int res = 0;  
    while (b > 0) {  
        res += a;  
        b--;  
    }  
    return res;  
}
```



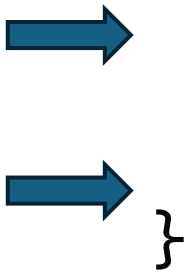
Beware of inlining



```
int mul(int a, int b) {  
    int res = 0;  
    for (int i = 0; i < b; i++) {  
        res += a;  
    }  
    return res;  
}
```




```
int mul(int a, int b) {  
    int res = 0;  
    for (int j = 0; j < b;  
        j += 1000) {  
        for (int i = j;  
            i < j + 1000; i++) {  
            res += i;  
        }  
    }  
    return res;  
}
```



Loop Strip Mining



jar profiler



jar profiler





JDK / JDK-8313419

Template interpreter produces no safepoint check for return bytecodes

Resolved ▾

Details

Type:	 Bug	Resolution:	Fixed
Priority:	 P3	Fix Version/s:	22
Affects Version/s:	22		
Component/s:	hotspot		
Labels:	interpreter		
Subcomponent:	runtime		
Resolved In Build:	b12		
CPU:	arm, aarch64, riscv		

Description

The template interpreter produces a safepoint check for return bytecodes (TemplateTable::_return(TosState state)) on x86 [1] and other platforms, but not on aarch64, arm, and riscv.

I describe the bug in more detail at <https://mostlynerdless.de/blog/2023/07/31/the-inner-workings-of-safepoints/>.

[1] https://github.com/openjdk/jdk/blob/5d193193a3a4c519e7b3d77b27e6b2bf1b11c7f9/src/hotspot/cpu/x86/templateTable_

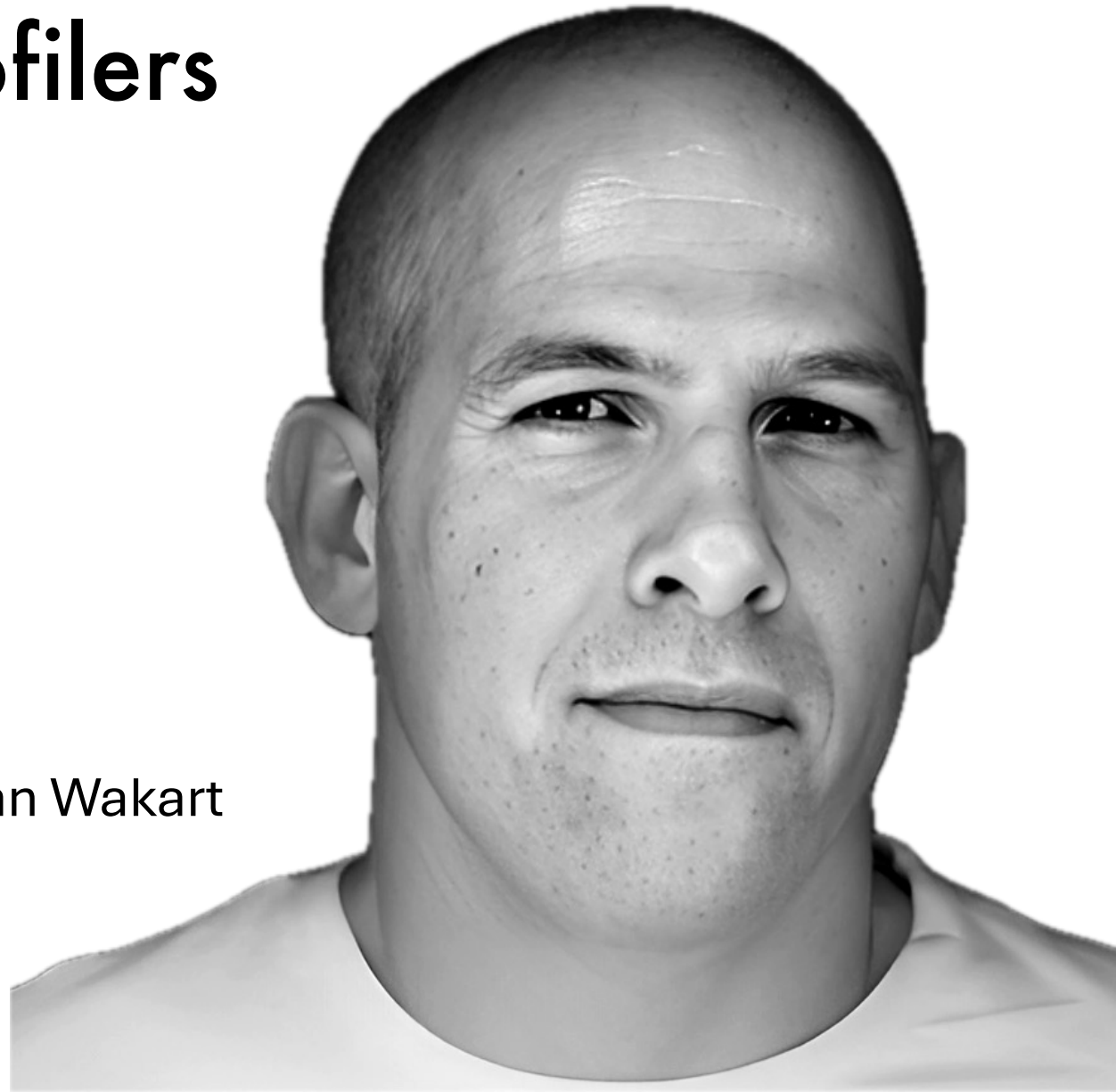
[2] https://github.com/openjdk/jdk/blob/5d193193a3a4c519e7b3d77b27e6b2bf1b11c7f9/src/hotspot/cpu/aarch64/templateTable_aarch64.cpp#L2174C27-L2174C27



**“ Safepoint biased profilers
are:**

- **Tricksy**
- **Sneaksy**
- **Filthy**
- **All of the above**

— Nitsan Wakart



Implementation

We could just...

```
if (thread->at_safepoint()) {  
    SafepointMechanism::process();  
} else {  
    // do nothing  
}
```

Slow, only in interpreted mode

Emit in MacroAssembler

```
testb(Address(thread_reg,  
JavaThread::polling_word_offset()),  
SafepointMechanism::poll_bit());  
// handshake bit set implies poll  
jcc(Assembler::notZero, slow_path);
```

We could just...

```
if (thread->at_safepoint()) {  
    SafepointMechanism::process();           rare  
} else {  
    // do nothing                             often  
}
```


We could just...

```
if (thread->at_safepoint()) {  
    SafepointMechanism::process();    slow path  
} else {  
    // do nothing                    fast path  
}
```

Read from pointer

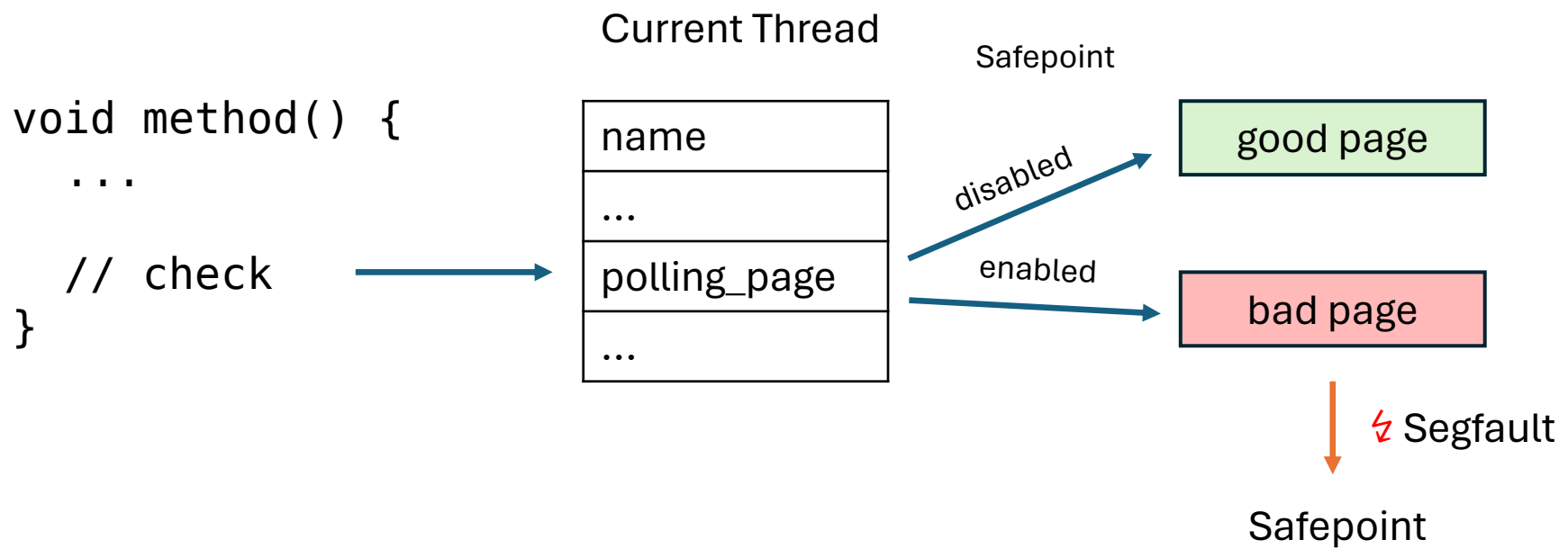


data

or



Segmentation fault





Initialize per thread

```
char* bad_page = polling_page;
char* good_page = polling_page + page_size;

os::protect_memory(bad_page, page_size, os::MEM_PROT_NONE);
os::protect_memory(good_page, page_size, os::MEM_PROT_READ);
//...
_poll_page_armed_value =
    reinterpret_cast<uintptr_t>(bad_page);
_poll_page_disarmed_value =
    reinterpret_cast<uintptr_t>(good_page);
```

Emit e.g. in C1

```
int LIR_Assembler::safepoint_poll(  
    LIR_Opr tmp, CodeEmitInfo* info) {  
  
    int offset = __ offset();  
    const Register poll_addr = rscratch1;  
  
    __ movptr(poll_addr,  
        Address(r15_thread,  
            JavaThread::polling_page_offset()));  
    // ...  
}
```


Arming local safepoints

```
void SafepointMechanism::arm_local_poll(  
    JavaThread* thread) {  
    thread->poll_data()  
        ->set_polling_word(_poll_word_armed_value);  
    thread->poll_data()  
        ->set_polling_page(_poll_page_armed_value);  
}
```

Arming global safepoints

```
_state = _synchronizing;  
for (JavaThreadIteratorWithHandle jtiwh;  
     JavaThread *cur = jtiwh.next();) {  
    SafepointMechanism::arm_local_poll(cur);  
}
```

Tracking Safepoints

- Introduction
- Flight Recorder
- JVM
- JVM: Class Loading
- JVM: Code Cache
- JVM: Compiler
- JVM: Diagnostics
- JVM: Flag
- JVM: GC: Collector
- JVM: GC: Configuration
- JVM: GC: Detailed
- JVM: GC: Heap
- JVM: GC: Metaspace
- JVM: GC: Phases
- JVM: GC: Reference
- JVM: Heap
- JVM: Internal
- JVM: Memory
- JVM: Profiling
- JVM: Runtime**
- ContinuationFreeze
- ContinuationThaw
- ContinuationFreezeFast
- ContinuationFreezeSlow
- ContinuationThawFast
- ContinuationThawSlow
- ReservedStackActivation
- SafepointBegin**
- SafepointStateSynchronization
- SafepointCleanup
- SafepointCleanupTask

SafepointBegin

default
profiling
startTime
duration
eventThread
11
17
21
22
23
graal vm

Category: Java Virtual Machine / Runtime / Safepoint

Safepointing begin

Configuration	enabled	threshold
default	true	10 ms
profiling	true	0 ms

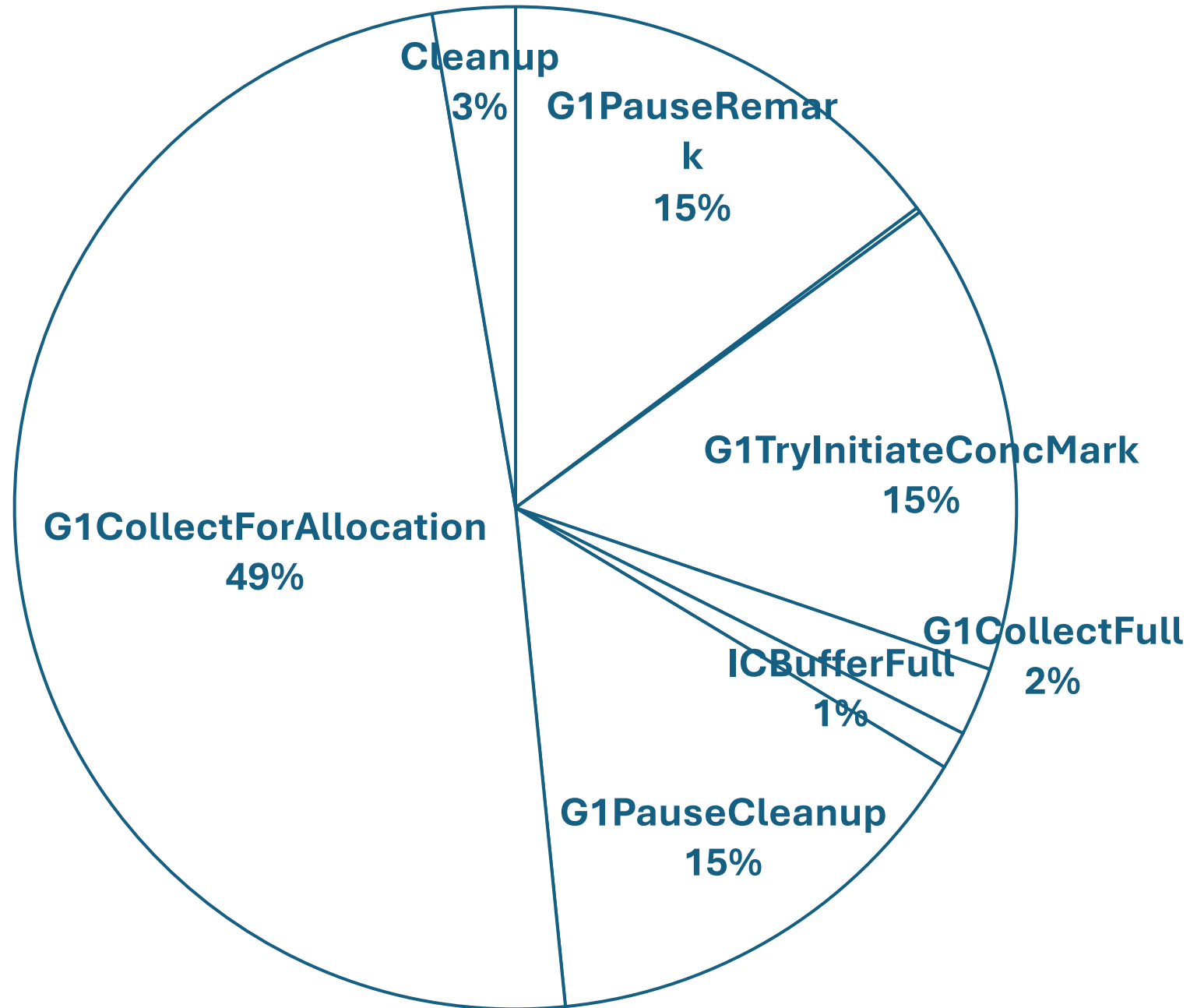
Field	Type	Description
safepointId	ulong	Safepoint Identifier
totalThreadCount	int	Total Threads The total number of threads at the start of the safe point
jniCriticalThreadCount	int	JNI Critical Threads The number of threads in JNI critical sections

► Examples 3



-Xlog:safepoint

```
[0.483s][info][safepoint] Safepoint "ICBufferFull", Time since last: 350694792 ns, Reaching safepoint: 2041 ns, Cleanup: 59125 ns, At safepoint: 4375 ns, Total: 65541 ns
[0.797s][info][safepoint] Safepoint "ICBufferFull", Time since last: 313735834 ns, Reaching safepoint: 1958 ns, Cleanup: 53250 ns, At safepoint: 3792 ns, Total: 59000 ns
[1.218s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 417910666 ns, Reaching safepoint: 2042 ns, Cleanup: 8875 ns, At safepoint: 2700750 ns, Total: 2711667 ns
Creating graph database...
[1.857s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 634405583 ns, Reaching safepoint: 3875 ns, Cleanup: 61667 ns, At safepoint: 4869917 ns, Total: 4935459 ns
[2.095s][info][safepoint] Safepoint "ICBufferFull", Time since last: 238269000 ns, Reaching safepoint: 2541 ns, Cleanup: 72209 ns, At safepoint: 7041 ns, Total: 81791 ns
[2.218s][info][safepoint] Safepoint "ICBufferFull", Time since last: 122185084 ns, Reaching safepoint: 19291 ns, Cleanup: 66667 ns, At safepoint: 6792 ns, Total: 92750 ns
[2.258s][info][safepoint] Safepoint "CollectForMetadataAllocation", Time since last: 35907333 ns, Reaching safepoint: 2542 ns, Cleanup: 7541 ns, At safepoint: 4715209 ns, Total: 4725292 ns
[2.265s][info][safepoint] Safepoint "G1PauseRemark", Time since last: 4885708 ns, Reaching safepoint: 26417 ns, Cleanup: 5250 ns, At safepoint: 2122708 ns, Total: 2154375 ns
[2.268s][info][safepoint] Safepoint "G1PauseCleanup", Time since last: 2266917 ns, Reaching safepoint: 26125 ns, Cleanup: 4500 ns, At safepoint: 55500 ns, Total: 86125 ns
[2.505s][info][safepoint] Safepoint "ICBufferFull", Time since last: 237135416 ns, Reaching safepoint: 3375 ns, Cleanup: 71125 ns, At safepoint: 6209 ns, Total: 80709 ns
[2.658s][info][safepoint] Safepoint "ICBufferFull", Time since last: 152988333 ns, Reaching safepoint: 2167 ns, Cleanup: 62000 ns, At safepoint: 6500 ns, Total: 70667 ns
[2.702s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 33748791 ns, Reaching safepoint: 3167 ns, Cleanup: 34458 ns, At safepoint: 10168417 ns, Total: 10206042 ns
[2.914s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 203662417 ns, Reaching safepoint: 3500 ns, Cleanup: 28541 ns, At safepoint: 8332334 ns, Total: 8364375 ns
[3.274s][info][safepoint] Safepoint "ICBufferFull", Time since last: 359749375 ns, Reaching safepoint: 2208 ns, Cleanup: 76083 ns, At safepoint: 5334 ns, Total: 83625 ns
[3.350s][info][safepoint] Safepoint "CollectForMetadataAllocation", Time since last: 64388500 ns, Reaching safepoint: 2791 ns, Cleanup: 17209 ns, At safepoint: 12044416 ns, Total: 12064416 ns
[3.365s][info][safepoint] Safepoint "G1PauseRemark", Time since last: 11889625 ns, Reaching safepoint: 45459 ns, Cleanup: 7875 ns, At safepoint: 2815291 ns, Total: 2868625 ns
[3.376s][info][safepoint] Safepoint "G1PauseCleanup", Time since last: 6909792 ns, Reaching safepoint: 3534625 ns, Cleanup: 11333 ns, At safepoint: 134042 ns, Total: 3680000 ns
[3.763s][info][safepoint] Safepoint "ICBufferFull", Time since last: 387426708 ns, Reaching safepoint: 2875 ns, Cleanup: 71584 ns, At safepoint: 6166 ns, Total: 80625 ns
[3.780s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 1826000 ns, Reaching safepoint: 6750 ns, Cleanup: 23625 ns, At safepoint: 15108375 ns, Total: 15138750 ns
[3.909s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 86178042 ns, Reaching safepoint: 2917 ns, Cleanup: 19375 ns, At safepoint: 43178208 ns, Total: 43200500 ns
[4.141s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 217993542 ns, Reaching safepoint: 2916 ns, Cleanup: 33250 ns, At safepoint: 13034334 ns, Total: 13070500 ns
[4.628s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 483891958 ns, Reaching safepoint: 3042 ns, Cleanup: 67541 ns, At safepoint: 3062500 ns, Total: 3133083 ns
[4.770s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 139228459 ns, Reaching safepoint: 3291 ns, Cleanup: 14084 ns, At safepoint: 3515458 ns, Total: 3532833 ns
[5.682s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 904707500 ns, Reaching safepoint: 15208 ns, Cleanup: 156375 ns, At safepoint: 6818959 ns, Total: 6990542 ns
[6.065s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 380094083 ns, Reaching safepoint: 3750 ns, Cleanup: 38292 ns, At safepoint: 2828833 ns, Total: 2870875 ns
[6.385s][info][safepoint] Safepoint "ICBufferFull", Time since last: 319451458 ns, Reaching safepoint: 3625 ns, Cleanup: 58375 ns, At safepoint: 4959 ns, Total: 66959 ns
[7.059s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 671531958 ns, Reaching safepoint: 4125 ns, Cleanup: 46583 ns, At safepoint: 2552750 ns, Total: 2603458 ns
Loading resources...
[7.095s][info][safepoint] Safepoint "G1TryInitiateConcMark", Time since last: 33920625 ns, Reaching safepoint: 4667 ns, Cleanup: 6458 ns, At safepoint: 2369542 ns, Total: 2380667 ns
[7.109s][info][safepoint] Safepoint "G1TryInitiateConcMark", Time since last: 11898000 ns, Reaching safepoint: 7458 ns, Cleanup: 4334 ns, At safepoint: 2172458 ns, Total: 2184250 ns
[7.137s][info][safepoint] Safepoint "G1TryInitiateConcMark", Time since last: 26198542 ns, Reaching safepoint: 4083 ns, Cleanup: 8125 ns, At safepoint: 1299250 ns, Total: 1311458 ns
[7.173s][info][safepoint] Safepoint "G1TryInitiateConcMark", Time since last: 34619500 ns, Reaching safepoint: 4542 ns, Cleanup: 10041 ns, At safepoint: 1458667 ns, Total: 1473250 ns
[7.245s][info][safepoint] Safepoint "G1TryInitiateConcMark", Time since last: 70525125 ns, Reaching safepoint: 8042 ns, Cleanup: 6500 ns, At safepoint: 1410250 ns, Total: 1424792 ns
[7.267s][info][safepoint] Safepoint "G1PauseRemark", Time since last: 19678250 ns, Reaching safepoint: 2458 ns, Cleanup: 6333 ns, At safepoint: 2912709 ns, Total: 2921500 ns
[7.273s][info][safepoint] Safepoint "G1PauseCleanup", Time since last: 5783375 ns, Reaching safepoint: 3541 ns, Cleanup: 1750 ns, At safepoint: 122125 ns, Total: 127416 ns
[7.598s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 289582042 ns, Reaching safepoint: 3833 ns, Cleanup: 32750 ns, At safepoint: 34895209 ns, Total: 34931792 ns
[7.904s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 235966875 ns, Reaching safepoint: 6375 ns, Cleanup: 14125 ns, At safepoint: 70280958 ns, Total: 70301458 ns
[8.116s][info][safepoint] Safepoint "G1CollectForAllocation", Time since last: 134082917 ns, Reaching safepoint: 8375 ns, Cleanup: 2500 ns, At safepoint: 78051250 ns, Total: 78062125 ns
[8.130s][info][safepoint] Safepoint "G1TryInitiateConcMark", Time since last: 2459333 ns, Reaching safepoint: 3750 ns, Cleanup: 3000 ns, At safepoint: 11200542 ns, Total: 11207292 ns
```



@parttimen3rd on Twitter
parttimenerd on GitHub
mostlynerdless.de

@SweetSapMachine
sapmachine.io

