DragonFlyBSD - Bug #2171

DFBSD v2.13.0.151.gdc8442 - panic: assertion "(*ptep & (PG_MANAGED|PG_V)) == PG_V"

10/30/2011 06:58 PM - tuxillo

Status:	New	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			

Description

Hi,

Under KVM an infinite loop of make -j48 buildkernel in a 4-cpu virtual machine:

pmap_scan: caught race func 0xffffffff8075dcc2, resolved ok
[diagnostic] cache_lock: blocked on 0xffffffe0462512c8 "pcivar.h"
[diagnostic] cache_lock: unblocked pcivar.h after 2 secs
panic: assertion "(*ptep & (PG_MANAGED|PG_V)) == PG_V" failed in pmap_scan at
/usr/src/sys/platform/pc64/x86_64/pmap.c:2815
cpuid = 2
Trace beginning at frame 0xffffffe04bc536a8
panic() at panic+0x1ed
panic() at panic+0x1ed
pmap_scan() at pmap_scan+0x899
pmap_remove() at pmap_remove+0x16
vm_map_delete() at vm_map_delete+0x271
vm_map_remove() at vm_map_remove+0x72
kmem_free() at kmem_free+0x1f
pipe_free_kmem() at pipe_free_kmem+0x3a
pipespace() at pipespace+0xc1
pipe_write() at pipe_write+0x172
kern_pwritev() at kern_pwritev+0x16e
sys_write() at sys_write+0x66
syscall2() at syscall2+0x330
Xfast_syscall() at Xfast_syscall+0xbf

Fatal trap 12: page fault while in kernel mode
cpuid = 2; lapic->id = 02000000
fault virtual address = 0x4008
fault code = supervisor read data, page not present
instruction pointer = 0x8:0xffffffff80730d29
stack pointer = 0x10:0xffffffe04bc53540
frame pointer = 0x10:0xffffffe04bc53558
code segment = base 0x0, limit 0xfffff, type 0x1b
= DPL 0, pres 1, long 0, def32 0, gran 1
processor eflags = interrupt enabled, resume, IOPL = 0
current process = 47093
current thread = pri 10 (CRIT)
kernel: type 12 trap, code=0

CPU2 stopping CPUs: 0x0000000b
stopped
Physical memory: 2018 MB
Dumping 825 MB: 810 794 778 762 746 730 714 698 682 666 650 634 618 602 586 570
554 538 522 506 490 474 458 442 426 410 394 378 362 346 330 314 298 282 266 250
234 218 202 186 170 154 138 122 106 90 74 58 42 26 10

sudo ubuntu-vm-builder kvm hardy --addpkg vim --addpkg screen --mem 256

History

#1 - 10/30/2011 06:59 PM - tuxillo

I have the dump available under demand. Btw, you can ignore the trailing sudo command :P

#2 - 11/04/2011 05:06 PM - tuxillo

Hi,

I'm missing some bits of the history here. With commit 23b4bd448a61a8934fb2354d2d0add3c20c0c392 I got this panic. I shared it with Matt.

Unread portion of the kernel message buffer:
panic: bad *ptep 0000000000000000 sva ffffffe04b78e000 pte_pv NULL
cpuid = 2
Trace beginning at frame 0xffffffe04742b728
panic() at panic+0x1ed
panic() at panic+0x1ed
pmap_scan() at pmap_scan+0x83f
pmap_remove() at pmap_remove+0x16
vm_map_delete() at vm_map_delete+0x271
vm_map_remove() at vm_map_remove+0x72
kmem_free() at kmem_free+0x1f
pipe_free_kmem() at pipe_free_kmem+0x3a
pipeclose() at pipeclose+0x278
pipe_close() at pipe_close+0x31
fdrop() at fdrop+0xf1
closef() at closef+0x154
kern_close() at kern_close+0x13c
sys_close() at sys_close+0xc
syscall2() at syscall2+0x330
Debugger("panic")

After that, Matt committed this one: a505393fd1a1920367affae433de8573462fe68c

I tried to do my test again and I finally got infinite messages saying:

swap_pager: indefinite wait buffer: offset xxx size 4096

The virtual machine was not responding anymore and I couldn't escape to DDB either.

Cheers,
Antonio Huete