

Re: System panic under load (additional information)

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/hackers/2006-10/msg00193.html>

- *From:* Micah <micahjon@xxxxxxxxxx>
 - *Date:* Wed, 25 Oct 2006 10:03:00 -0700
-

Okay, I was reading the developer's handbook and trying stuff. The following may be helpful:

```
(kgdb) up 7
#7 0xc0593d34 in vfs_hash_get (mp=0xc5a53000, hash=5347783, flags=2,
td=0xc5ef9d80, vpp=0xf02ca99c, fn=0, arg=0x0)
at /usr/src/sys/kern/vfs_hash.c:73
73 if (vp->v_hash != hash)
(kgdb) list *0xc0593d34
0xc0593d34 is in vfs_hash_get (/usr/src/sys/kern/vfs_hash.c:73).
64 int
65 vfs_hash_get(struct mount *mp, u_int hash, int flags, struct thread *td, struct vnode **vpp,
vfs_hash_cmp_t *fn, void *arg)
66 {
67 struct vnode *vp;
68 int error;
69
70 while (1) {
71 mtx_lock(&vfs_hash_mtx);
72 LIST_FOREACH(vp, vfs_hash_index(mp, hash), v_hashlist) {
73 if (vp->v_hash != hash)
74 continue;
75 if (vp->v_mount != mp)
76 continue;
77 if (fn != NULL && fn(vp, arg))
(kgdb) print vp
$1 = (struct vnode *) 0xffffffff
```

I'm no expert but that doesn't look like a valid address.... I was able to get another crashdump, but kgdb locked up while trying to read it.

Thanks,
Micah

Micah wrote:

Can anyone help me in deciphering what this crashdump is telling me? My i386 6.1p3 system is panicking under heavy IO load and I'm trying to isolate the cause. I've never debugged a crashdump before, so if there's more information I can milk from the core file, let me know.

Re: System panic under load (additional information)

Thanks,
Micah

```
trisha# kgdb kernel.debug /home/crash/vmcore.0
[GDB will not be able to debug user-mode threads: /usr/lib/libthread_db.so: Undefined
symbol "ps_pglobal_lookup"]
GNU gdb 6.1.1 [FreeBSD]
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for details.
This GDB was configured as "i386-marcel-freebsd".
```

Unread portion of the kernel message buffer:

```
Fatal trap 12: page fault while in kernel mode
fault virtual address = 0x27
fault code = supervisor read, page not present
instruction pointer = 0x20:0xc0593d34
stack pointer = 0x28:0xf02ca89c
frame pointer = 0x28:0xf02ca8bc
code segment = base 0x0, limit 0xffff, type 0x1b
= DPL 0, pres 1, def32 1, gran 1
processor eflags = interrupt enabled, resume, IOPL = 0
current process = 24805 (perl5.8.8)
trap number = 12
panic: page fault
Uptime: 13h16m1s
Dumping 1534 MB (2 chunks)
chunk 0: 1MB (159 pages) ... ok
chunk 1: 1534MB (392672 pages) 1518 1502 1486 1470 1454 1438 1422 1406 1390 1374
1358 1342 1326 1310 1294 1278 1262 1246 1230 1214 1198 1182 1166 1150 1134 1118
1102 1086 1070 1054 1038 1022 1006 990 974 958 942 926 910 894 878 862 846 830 814
798 782 766 750 734 718 702 686 670 654 638 622 606 590 574 558 542 526 510 494 478
462 446 430 414 398 382 366 350 334 318 302 286 270 254 238 222 206 190 174 158 142
126 110 94 78 62 46 30 14
```

```
#0 doadump () at pcpu.h:165
165 __asm __volatile("movl %%fs:0,%0" : "=r" (td));
(kgdb) bt
#0 doadump () at pcpu.h:165
#1 0xc0535a3f in boot (howto=260) at /usr/src/sys/kern/kern_shutdown.c:402
#2 0xc0535d66 in panic (fmt=0xc0711e06 "%s")
at /usr/src/sys/kern/kern_shutdown.c:558
#3 0xc06ecf2c in trap_fatal (frame=0xf02ca85c, eva=0)
at /usr/src/sys/i386/i386/trap.c:836
#4 0xc06ecc32 in trap_pfault (frame=0xf02ca85c, usermode=0, eva=39)
at /usr/src/sys/i386/i386/trap.c:744
```

Re: System panic under load (additional information)

```
#5 0xc06ec7fd in trap (frame=
{tf_fs = 8, tf_es = 40, tf_ds = 40, tf_edi = 4, tf_esi = 4, tf_ebp = -265508676, tf_esp =
-265508728, tf_ebx = -1, tf_edx = -980369408, tf_ecx = -979030016, tf_eax = 5347783,
tf_trapno = 12, tf_err = 0, tf_eip = -1067893452, tf_cs = 32, tf_eflags = 66182, tf_esp =
-979030016, tf_ss = 5347783})
at /usr/src/sys/i386/i386/trap.c:434
#6 0xc06d9e2a in calltrap () at /usr/src/sys/i386/i386/exception.s:139
#7 0xc0593d34 in vfs_hash_get (mp=0xc5a53000, hash=5347783, flags=2,
td=0xc5ef9d80, vpp=0xf02ca99c, fn=0, arg=0x0)
at /usr/src/sys/kern/vfs_hash.c:73
#8 0xc067af59 in ffs_vget (mp=0xc5a53000, ino=5347783, flags=2,
vpp=0xf02ca99c) at pcpu.h:162
#9 0xc0683353 in ufs_lookup (ap=0xf02caa40)
at /usr/src/sys/ufs/ufs/ufs_lookup.c:572
#10 0xc0700f03 in VOP_CACHEDLOOKUP_APV (vop=0x5199c7, a=0xc590c000)
at vnode_if.c:150
#11 0xc059006a in vfs_cache_lookup (ap=0x5199c7) at vnode_if.h:82
#12 0xc0700e78 in VOP_LOOKUP_APV (vop=0xc0764f20, a=0xf02caaec)
at vnode_if.c:99
#13 0xc059547b in lookup (ndp=0xf02cabf4) at vnode_if.h:56
#14 0xc0594c08 in namei (ndp=0xf02cabf4) at /usr/src/sys/kern/vfs_lookup.c:203
#15 0xc05a672d in kern_stat (td=0xc5ef9d80,
path=0xc590c000 "\033\210Ê B\215É0£ÓÊ\020±ZÉ\020ñ\211Æ0\003\237ÊPU0Ê",
pathseg=3314597888, sbp=0x5199c7) at /usr/src/sys/kern/vfs_syscalls.c:2076
#16 0xc05a66bf in stat (td=0x5199c7, uap=0xf02cad04)
at /usr/src/sys/kern/vfs_syscalls.c:2061
#17 0xc06ed302 in syscall (frame=
{tf_fs = 59, tf_es = 59, tf_ds = 59, tf_edi = 1209537912, tf_esi = 140130588, tf_ebp =
-1077941096, tf_esp = -265507484, tf_ebx = 1209530852, tf_edx = 68, tf_ecx = 0, tf_eax =
188, tf_trapno = 12, tf_err = 2, tf_eip = 1210540343, tf_cs = 51, tf_eflags = 582, tf_esp =
-1077941140, tf_ss = 59})
at /usr/src/sys/i386/i386/trap.c:981
#18 0xc06d9e7f in Xint0x80_syscall () at /usr/src/sys/i386/i386/exception.s:200
---Type <return> to continue, or q <return> to quit---
#19 0x00000033 in ?? ()
Previous frame inner to this frame (corrupt stack?)
```

freebsd-hackers@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-hackers>

To unsubscribe, send any mail to "freebsd-hackers-unsubscribe@xxxxxxxxxxx"

freebsd-hackers@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-hackers>

To unsubscribe, send any mail to "freebsd-hackers-unsubscribe@xxxxxxxxxxx"