

DragonFlyBSD - Bug #1907

Hammer crash in hammer_flusher_flush()

11/11/2010 05:07 AM - swildner

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

Description

I've had another hammer crash on master while running fsstress. This time it hit an assertion in hammer_flusher_flush(). The filesystem was mounted -o nohistory.

Dump is in ~swildner/crash/crash29.tbz on leaf.

Panic message is:

```
Unread portion of the kernel message buffer:
panic: assertion: flg->refs == 0 in hammer_flusher_flush
mp_lock = 00000001; cpuid = 0
Trace beginning at frame 0xd91b5d2c
panic(ffffff) at panic+0x174
panic(c05e1dd5,c060d920,c05cb4a2,d91a8124,d91a8154) at panic+0x174
hammer_flusher_master_thread(d91a8000,0,0,0,0) at
hammer_flusher_master_thread+0x345
lwkt_exit() at lwkt_exit
Debugger("panic")
```

Backtrace:

```
(kgdb) bt
#0 _get_mycpu (di=0xc07622e0) at ./machine/thread.h:83
#1 md_dumpsys (di=0xc07622e0) at
/d1/src/sys/platform/pc32/i386/dump_machdep.c:263
#2 0xc030e041 in dumpsys () at /d1/src/sys/kern/kern_shutdown.c:881
#3 0xc017d441 in db_fncall (dummy1=2, dummy2=0, dummy3=-1068125532,
dummy4=0xd91b5bd8 "") at /d1/src/sys/ddb/db_command.c:542
#4 0xc017d932 in db_command () at /d1/src/sys/ddb/db_command.c:344
#5 db_command_loop () at /d1/src/sys/ddb/db_command.c:470
#6 0xc017ffc4 in db_trap (type=3, code=0) at /d1/src/sys/ddb/db_trap.c:71
#7 0xc055b4a8 in kdb_trap (type=3, code=0, regs=0xd91b5cdc) at
/d1/src/sys/platform/pc32/i386/db_interface.c:152
#8 0xc05749b7 in trap (frame=0xd91b5cdc) at
/d1/src/sys/platform/pc32/i386/trap.c:831
#9 0xc055c827 in calltrap () at
/d1/src/sys/platform/pc32/i386/exception.s:785
#10 0xc055b2a4 in breakpoint (msg=0xc05fd655 "panic") at ./cpu/cpufunc.h:73
#11 Debugger (msg=0xc05fd655 "panic") at
/d1/src/sys/platform/pc32/i386/db_interface.c:334
#12 0xc030e8d0 in panic (fmt=0xc05e1dd5 "assertion: %s in %s") at
/d1/src/sys/kern/kern_shutdown.c:785
#13 0xc04adeb8 in hammer_flusher_flush (arg=0xd91a8000) at
/d1/src/sys/vfs/hammer/hammer_flusher.c:398
#14 hammer_flusher_master_thread (arg=0xd91a8000) at
/d1/src/sys/vfs/hammer/hammer_flusher.c:238
#15 0xc031839a in lwkt_deschedule_self (td=Cannot access memory at
address 0x8
) at /d1/src/sys/kern/lwkt_thread.c:258
Backtrace stopped: previous frame inner to this frame (corrupt stack?)
```