

# What is rtincident?

Daniel Quinlan  
BRTT, Inc.

# The rtincident report

**A mystery investigation**

# What is rtincident?

- run by rtxexec when task dies with a core file
- leaves file in logs directory, sends email
- rtxexec.pf:
  - ▶ `coredumpsize unlimited`
  - ▶ `email_incident_reports incidents@brtt.com`

# incident report means:

- unexpected death
- report may provide some clues

# incident report means:

- unexpected death
- report may provide some clues

Investigation required!

**From:** [rt@](#)

**Subject:** Incident report: orb2db (3155) died from signal 10: SIGBUS bus error with exit code 0 (started @2005-142 04:03:04)

**Date:** May 22, 2005 10:02:31 PM MDT

**To:** [incidents@brtt.com](mailto:incidents@brtt.com)

Where?

Incident Report (Release 4.6 SunOS 5.8 2004-03-31 )

5/23/2005 (143) 4:02:29.000 UTC

5/22/2005 (142) 21:02:29.000 Local Time

When?

What?

orb2db (3155) died from signal 10: SIGBUS bus error with exit code 0 (started @2005-142 04:03:04)

Execution line: 'orb2db -S state/orb2db -w %Y%m/0/%{sta} %{chan} %Y:%m:0:%H:%M:%S :cnsn /wicked/wf/cnsn'

How?

System Operators: [someone@somewhere.com](mailto:someone@somewhere.com)

Who?

`uname -a`

SunOS amachine 5.9 Generic\_112233-11 sun4u sparc SUNW,Sun-Fire-V240

`pwd`

/amachine/rt

`id`

uid=55555(rt) gid=55555(rt)

`ORB`

:demo

`rtchecksums orb2db`

/opt/antelope/4.6/bin/orb2db	0xd2be
/opt/antelope/4.6/lib/libPkt.so	0x3b38
/opt/antelope/4.6/lib/libforb.so	0x751d
/opt/antelope/4.6/lib/liborb.so	0xb9af
/opt/antelope/4.6/lib/libtr.so	0x94bc
/opt/antelope/4.6/lib/libds.so	0xb5c6

- First few lines of `rtincident` are fairly simple, but the whole report is rather long (~1600 lines) and rapidly becomes difficult to read.
- ***inspect\_snapshot*** helps a little: perl/tk application which breaks it apart into more manageable pieces.

```
Inspect_snapshot

id
uid=55555(rt) gid=55555(rt)

ORB
:cnsn

rtchecksuns orb2db
cat /opt/antelope/4.6/d
tail -70 logs/orb2db

/usr/sbin/swapon -s || cat /proc/meminfo
total: 220000k bytes allocated + 19240k reserved
7249248k available

top -b | head -30 && top -b | head -30 || prstat -n 20 1 2

df -k

id
uid=55555(rt) gid=55555(rt)

w
  9:02pm up 3 day(s),  5:54,  0 users,  load average: 1.03, 0.44, 0.21

User      tty          login@  idle  JCPU  PCPU  what

who
```

program, library versions

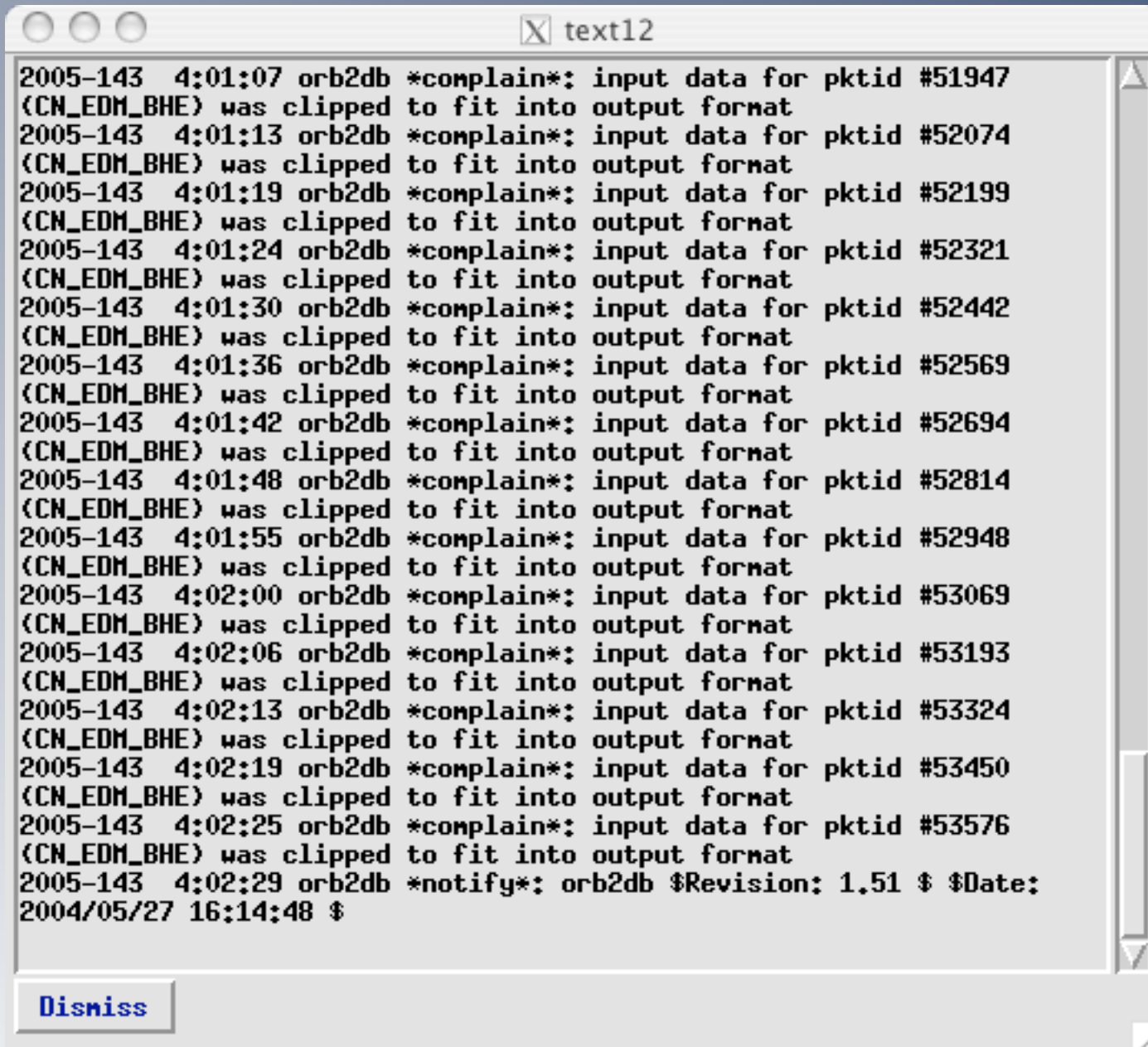
program output

memory

What else was running?

disk space

# Output from orb2db: victim's last words



```
2005-143 4:01:07 orb2db *complain*: input data for pktid #51947
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:01:13 orb2db *complain*: input data for pktid #52074
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:01:19 orb2db *complain*: input data for pktid #52199
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:01:24 orb2db *complain*: input data for pktid #52321
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:01:30 orb2db *complain*: input data for pktid #52442
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:01:36 orb2db *complain*: input data for pktid #52569
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:01:42 orb2db *complain*: input data for pktid #52694
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:01:48 orb2db *complain*: input data for pktid #52814
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:01:55 orb2db *complain*: input data for pktid #52948
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:02:00 orb2db *complain*: input data for pktid #53069
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:02:06 orb2db *complain*: input data for pktid #53193
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:02:13 orb2db *complain*: input data for pktid #53324
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:02:19 orb2db *complain*: input data for pktid #53450
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:02:25 orb2db *complain*: input data for pktid #53576
(CN_EDM_BHE) was clipped to fit into output format
2005-143 4:02:29 orb2db *notify*: orb2db $Revision: 1.51 $ $Date:
2004/05/27 16:14:48 $
```

Dismiss

# Interview witnesses

A terminal window showing a series of commands and their outputs. Yellow callouts provide context for several of the commands:

- `cat rtexec.pf`: details about system
- `tail -50 logs/rtexec`: what rtexec saw
- `last -10 reboot`: what unix saw
- `tail -10 /var/log/syslog`: (no callout)
- `/bin/ps -elo user,pid,pcpu,pmem,vsz,rss,tty,s,stime,time,args || ps`: (no callout)
- `-auwx`: (no callout)
- `orbstat -scv :cnsn`: what's in orb?
- `ls -CF`: (no callout)
- `ls -CF /opt/antelope/4.6/patched`: patched?

```
cat rtexec.pf
tail -50 logs/rtexec
last -10 reboot
tail -20 /var/adm/messages || tail -20 /var/log/messages

tail -10 /var/log/syslog

/bin/ps -elo user,pid,pcpu,pmem,vsz,rss,tty,s,stime,time,args || ps

-auwx
orbstat -scv :cnsn
ls -CF
ls -CF /opt/antelope/4.6/patched
```

sometimes complex mount schemes

```
ls -CF /opt/antelope/4.6/patch

df -k .

```

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/dsk/c1t0d0s7	20895703	2378358	18308388	12%	/wicked/rt

```
df -k db/. "filter -d db/2*/*"

```

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/dsk/c1t0d0s7	20895703	2378359	18308387	12%	/wicked/rt

```
df -k logs/

```

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/dsk/c1t0d0s7	20895703	2378358	18308388	12%	/wicked/rt

```
find . ! -perm -200 -ls

echo '$C;$?' | /bin/ndb logs/core.orb2db
```

run debugger on core file

# autopsy report

Trying to copy into  
mmaped file which has changed.

```
ffbf650 libstock.so.3`sncopy+0x84(fea05de6, fbf6736, 11, 7446aeff,
74650000,
74650000)
ffbf6c8 libds.so.3`dbc2d+0x184(ffbf6be0, fea05de6, 11, 6adf0, 4, 954f8)
ffbf6b4 libds.so.3`dbputv+0x514(ffbf6bfc, fbf6bf8, ff301e90,
40440000, 0,
ff301e9c)
ffbf018 libtr.so.3`wtdata+0x4ac(149cc8, 1e8a18, 1000, 758, 14a330,
14a334)
ffbf0c0 libtr.so.3`truf2disc+0x68(149cc8, 1e8a18, 1000, 758, 0, 0)
ffbf140 libtr.so.3`wtseed+0x108(14a2e0, 8d7bd, 8df15, ff2d27e8,
3e700160, 2)
ffbf1b0 libtr.so.3`stuffw+0x434(14a2e0, ff2fb2b4, 0, 0, ff2fde0c, 0)
ffbf218 libtr.so.3`cstc+0x2d4(0, ff2fb2b4, 75, 1d0, 0, 1e9aec)
ffbf278 libtr.so.3`wfwrite+0x68(10b3a8, 3c0, f0, 149cc8, 1, 71000000)
ffbf2e8 chan2db+0x6f8(15738, 149cc8, 0, 4b9f0, 10b3a8, 149cc8)
ffbf430 save_chan+0x56c(d149, ab138, 149cc8, 4d118, 0, 49410)
ffbf680 pkt2db+0x154(d149, 41d0a455, 71000000, fbf6c50, 215730, 1aa)
ffbf710 main+0x1e58(ffbf6c9c, fbf6d6c, fbf6d8c, 49000, 0, 0)
ffbf6d08 _start+0xb8(0, 0, 0, 0, 0, 0)
no process
SIGBUS: Bus Error
%g0 = 0x00000000          %i0 = 0xfea05de6
%g1 = 0xffbf6737         %i1 = 0x00000020
%g2 = 0x0000163c         %i2 = 0x0000ff00
%g3 = 0x00038884         %i3 = 0x81000000
%g4 = 0x00000002         %i4 = 0x0000006c
%g5 = 0x00000000         %i5 = 0x0000006e
%g6 = 0x00000000         %i6 = 0x7efefeff
%g7 = 0x00000000         %i7 = 0xff0f8188
%o0 = 0x00000011        %i8 = 0xfea05de6
%_1 = 0x00000011        %i9 = 0xff6c736
```

Dismiss

# Problem reports

*But please, no phone calls!*

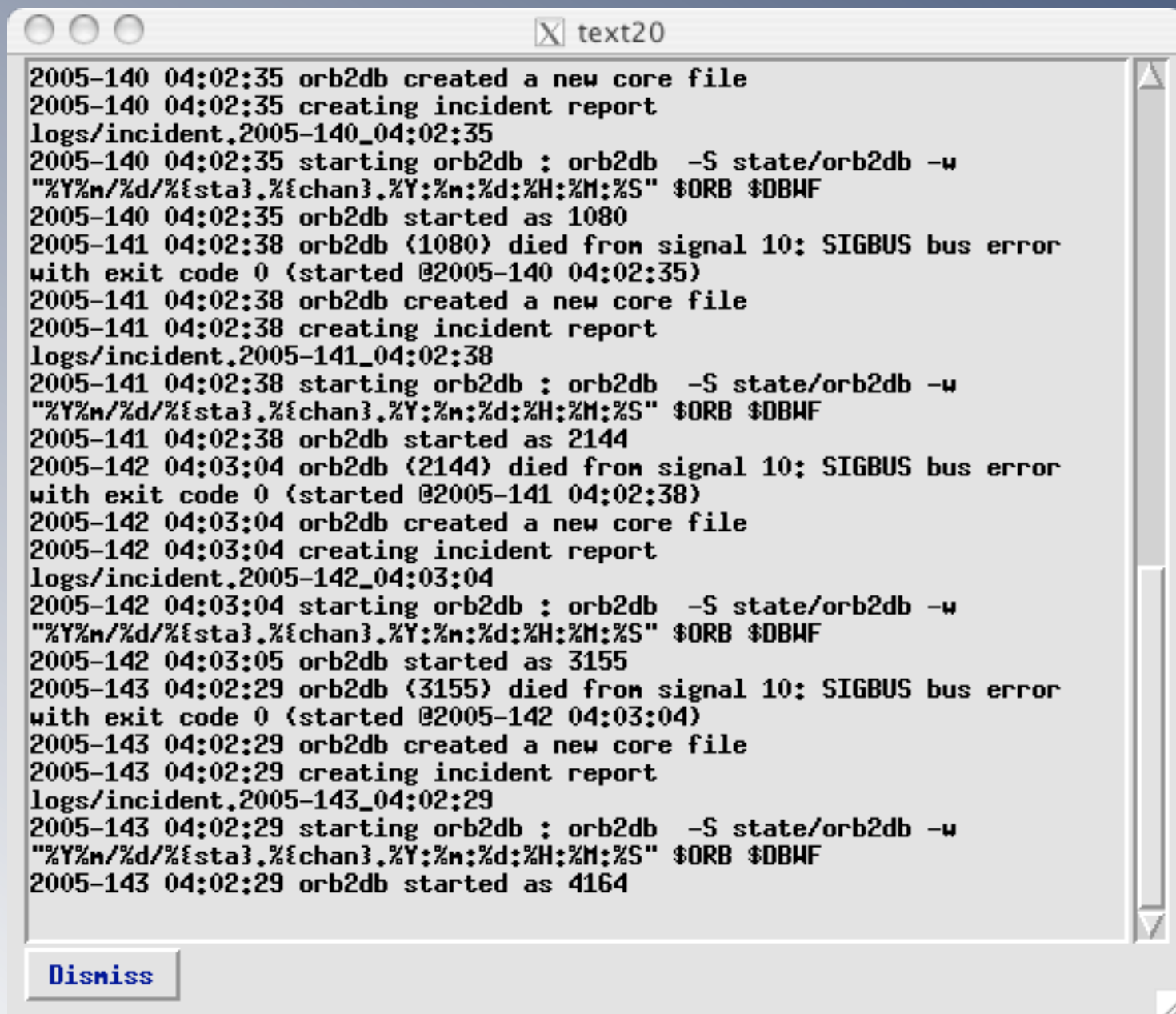
- Typical problem: email describes some of the symptoms, but misses some essential points.
- ***snapshots*** collect information that you might not consider.
- Think of it like the questionnaires you fill out at the doctor's office -- but easier

- ***dbsnapshot*** -- grabs some of the rows from a database
- ***rtsnapshot*** -- grabs log files, databases, rtexec.pf and some system files
- ***dbloc\_snapshot*** -- grabs database, dbloc2.pf, tmp directory, and location program input files
- ***sysnapshot*** -- grabs system related information

# Still missing: motive

- We need a description of what you're trying to do
- any special circumstances
- can it be reproduced (serial killer?)

# rtexec log



```
2005-140 04:02:35 orb2db created a new core file
2005-140 04:02:35 creating incident report
logs/incident.2005-140_04:02:35
2005-140 04:02:35 starting orb2db : orb2db -S state/orb2db -w
"%Y%n/%d/{sta} {chan} %Y:%n:%d:%H:%M:%S" $ORB $DBWF
2005-140 04:02:35 orb2db started as 1080
2005-141 04:02:38 orb2db (1080) died from signal 10: SIGBUS bus error
with exit code 0 (started @2005-140 04:02:35)
2005-141 04:02:38 orb2db created a new core file
2005-141 04:02:38 creating incident report
logs/incident.2005-141_04:02:38
2005-141 04:02:38 starting orb2db : orb2db -S state/orb2db -w
"%Y%n/%d/{sta} {chan} %Y:%n:%d:%H:%M:%S" $ORB $DBWF
2005-141 04:02:38 orb2db started as 2144
2005-142 04:03:04 orb2db (2144) died from signal 10: SIGBUS bus error
with exit code 0 (started @2005-141 04:02:38)
2005-142 04:03:04 orb2db created a new core file
2005-142 04:03:04 creating incident report
logs/incident.2005-142_04:03:04
2005-142 04:03:04 starting orb2db : orb2db -S state/orb2db -w
"%Y%n/%d/{sta} {chan} %Y:%n:%d:%H:%M:%S" $ORB $DBWF
2005-142 04:03:05 orb2db started as 3155
2005-143 04:02:29 orb2db (3155) died from signal 10: SIGBUS bus error
with exit code 0 (started @2005-142 04:03:04)
2005-143 04:02:29 orb2db created a new core file
2005-143 04:02:29 creating incident report
logs/incident.2005-143_04:02:29
2005-143 04:02:29 starting orb2db : orb2db -S state/orb2db -w
"%Y%n/%d/{sta} {chan} %Y:%n:%d:%H:%M:%S" $ORB $DBWF
2005-143 04:02:29 orb2db started as 4164
```

Dismiss

# Further reading

- man pages for snapshots
- bugs(5)
- reporting(5)