Subject: Node Crashes on 64 bit owing to a single file.
Posted by Ligesh on Thu, 11 Jan 2007 14:36:22 GMT
View Forum Message <> Reply to Message

Thu, Jan 11, 2007 at 08:04:35PM +0530, Ligesh wrote:

I have encountered a bug in the 64 bit openvz. I am now not able to access the system, so all I can do now is describe the general conditions. I will send the specific details later.

The problem seems to be with one single file, Mostly a paramater of the file is overflowing the variable in which it is stored, and I think it could be due the 32<->64 bit compatibility issues.

The result:

-> ls -al in /vz/private/100 and /vz/private/400 shows large integer values in place of last modified time.

-> Once this particular vps containing the bad file is started, all applications--IN THE NODE--start segfaulting. An strace show it happening after getftime, so I think it could be related to modified time of the file.

The thing is, once this vps is stopped, the others are working fine. I think the problem is with a specific file because we did a backup in cpanel, destroyed the old vps, created a new one, and restored the cpanel backup. The server was working fine midway the restore, but it started segfaulting when we were halfway through the cpanel restore.

I will send the kernel dmesg and the strace one I am able to login back to the server.

Thanks.

Subject: Re: Node Crashes on 64 bit owing to a single file.
Posted by dev on Thu, 11 Jan 2007 16:09:54 GMT
View Forum Message <> Reply to Message

Ligesh,

Would be nice to provide exact messages and details when you have an access.
Also please specify kernel version you use.

> I have encountered a bug in the 64 bit openvz. I am now not able to access the system, so all I can do now is describe the general conditions. I will send the specific details later.
> The problem seems to be with one single file, Mostly a paramater of the file is overflowing the variable in which it is stored, and I think it could be due the 32<->64 bit compatibility issues.
> The result:
>
> -> ls -al in /vz/private/100 and /vz/private/400 shows large integer values in place of last modified time.

> -> Once this particular vps containing the bad file is started, all applications--IN THE NODE--start segfaulting. An strace show it happening after getftime, so I think it could be related to modified time of the file.
how did you strace it if you say that *ALL* applications start segfaulting?
strace doesn't segfault?

> The thing is, once this vps is stopped, the others are working fine. I think the problem is with a specific file because we did a backup in cpanel, destroyed the old vps, created a new one, and restored the cpanel backup. The server was working fine midway the restore, but it started segfaulting when we were halfway through the cpanel restore.
>
> I will send the kernel dmesg and the strace one I am able to login back to the server.
would be very helpfull!

Thanks,
Kirill

Subject: Re: Node Crashes on 64 bit owing to a single file.
Posted by Ligesh on Sat, 13 Jan 2007 17:48:02 GMT
View Forum Message <> Reply to Message

On Thu, Jan 11, 2007 at 07:19:52PM +0300, Kirill Korotaev wrote:
> Ligesh,
>
> >
> > -> ls -al in /vz/private/100 and /vz/private/400 shows large integer values in place of last modified time.
> > -> Once this particular vps containing the bad file is started, all applications--IN THE NODE--start segfaulting. An strace show it happening after getftime, so I think it could be related to modified time of the file.
> how did you strace it if you say that *ALL* applications start segfaulting?
> strace doesn't segfault?

Hehe. All _system_ applications crash. As I said, it crashes somewhere while reading time, here's the trace:

strace w.

```
open("/proc/19241/stat", O_RDONLY) = 4
read(4, "19241 (w) R 19240 19240 14483 34"..., 1023) = 227
read(4, "w\0", 2047) = 2
close(4) = 0
getdents64(3, /* 0 entries */, 1024) = 0
close(3) = 0
open("/etc/localtime", O_RDONLY) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=0, ...}) = 0
fstat(3, {st_mode=S_IFREG|0644, st_size=0, ...}) = 0
```

mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x2a983ab000
read(3, "", 4096) = 0
close(3) = 0
munmap(0x2a983ab000, 4096) = 0
--- SIGSEGV (Segmentation fault) @ 0 (0) ---
+++ killed by SIGSEGV +++
Process 19241 detached

The kernel is the latest stable 64bit one. ovzkernel-smp-2.6.9-023stab037.3.x86_64.rpm

> >
> > I will send the kernel dmesg and the strace one I am able to login back to the server.
> would be very helpfull!

Actually the dmesg doesn't contain any information. But here's the ls -al of /vz/private and /vz/root directory. You will see that the offending vpses have their 'mtimes' shown as very large integers. They are the vpses which, when stopped, the problem goes away.

---
ls -al /vz/private
drwxr-xr-x 20 root root 4096 Jan 13 16:54 290
drwxr-xr-x 20 root root 4096 Jan 13 16:55 310
drwxr-xr-x   3 root root 4096 Jan 13 13:40 320
drwxr-xr-x 22 root root 4096 2666130989161975770 330
drwxr-xr-x 21 root root 4096 Feb 11 2007 340
drwxr-xr-x 20 root root 4096 Feb 11 2007 350

[root@cluster /]# ls -al /vz/root
total 100
drwxr-xr-x 20 root root 4096 Jan 13 16:53 280
drwxr-xr-x 20 root root 4096 Jan 13 16:54 290
drwxr-xr-x 20 root root 4096 Jan 13 16:55 310
drwxr-xr-x 22 root root 4096 2666130989161975770 330
drwxr-xr-x 21 root root 4096 Feb 11 2007 340
drwxr-xr-x   2 root root 4096 Jan 13 02:49 350

Subject: Re: Node Crashes on 64 bit owing to a single file.
Posted by Ligesh on Mon, 15 Jan 2007 07:23:25 GMT

View Forum Message <> Reply to Message

This seems to be happening with all 64 bit installations of cpanel. The cultprit seems to be cpanel. If you install cpanel in a vps on a 64 bit, the entire machine starts segfaulting, though the funny thing is, that the other vpses are alright. Teh node and the affected vpses keep segfaulting, but the other vpses run fine. Should I file a bug report?

Thanks.

Subject: Re: Node Crashes on 64 bit owing to a single file.
Posted by Ligesh on Mon, 15 Jan 2007 07:27:07 GMT
View Forum Message <> Reply to Message

One update:

The same problem happens if cpanel is installed on the node too. It is possible that it is a bug in the linux kernel and not in openvz.

Thanks.

Subject: Re: Node Crashes on 64 bit owing to a single file.
Posted by Vasily Tarasov on Mon, 15 Jan 2007 07:31:18 GMT
View Forum Message <> Reply to Message

Just for your information, one more person has such problem:
http://forum.openvz.org/index.php?t=tree&th=1778&mid =9581&&rev=&reveal=

Kirill Korotaev wrote:
> Ligesh,
>
> Would be nice to provide exact messages and details when you have an access.
> Also please specify kernel version you use.
>
>
>> I have encountered a bug in the 64 bit openvz. I am now not able to access the system, so all I can do now is describe the general conditions. I will send the specific details later.
>> The problem seems to be with one single file, Mostly a paramater of the file is overflowing the variable in which it is stored, and I think it could be due the 32<->64 bit compatibility issues.
>> The result:
>>
>> -> ls -al in /vz/private/100 and /vz/private/400 shows large integer values in place of last modified time.
>> -> Once this particular vps containing the bad file is started, all applications--IN THE NODE--start segfaulting. An strace show it happening after getftime, so I think it could be related to modified time of the file.

>>
> how did you strace it if you say that *ALL* applications start segfaulting?
> strace doesn't segfault?
>
>
>> The thing is, once this vps is stopped, the others are working fine. I think the problem is with a specific file because we did a backup in cpanel, destroyed the old vps, created a new one, and restored the cpanel backup. The server was working fine midway the restore, but it started segfaulting when we were halfway through the cpanel restore.
>>
>> I will send the kernel dmesg and the strace one I am able to login back to the server.
>>
> would be very helpfull!
>
> Thanks,
> Kirill
>

Subject: Re: Node Crashes on 64 bit owing to a single file.
Posted by Ligesh on Sun, 21 Jan 2007 16:01:44 GMT
View Forum Message <> Reply to Message

This is a widespread problem and seem to be very specific to cpanel on 64bit. It is very much reproducable. Just install cpanel in either node or inside a vps, and everything will start segfaulting.

here's the ltrace for vzctl start.

```
--------------------
start(3, 0x3106b114a6, 0x3106b0b090, 0x7472617473006c, 0xfefefefefefefeff <unfinished ...>
__libc_start_main(0x402c90, 3, 0x7fbffffa48, 0x405720, 0x405780 <unfinished ...>
init_vps_param(3, 0x7fbffffa48, 0x7fbffffa68, 32, 0x7fbffff9a0)       = 0x508010
init_vps_param(0x508010, 0, 0x508308, 0x508010, 0)                    = 0x5084e0
init_vps_param(0x5084e0, 0, 0x5087d8, 0x5084e0, 0)                    = 0x5089b0
sigemptyset(0x7fbffff7a8)                                             = 0
sigaction(13, 0x7fbffff7a0, NULL)                                     = 0
init_log(0, 0, 1, 0, 0)                                               = 0
opendir("/usr/lib/vzctl/modules/")                                    = NULL
__errno_location()                                                    = 0x2a95565ea0
logger(2, 2, 0x406910, -64, 0x7fbffffc2a)                             = 0
parse_int(0x7fbffffc30, 0x7fbffff79c, 0x406910, 0x310720ac51, 0x7fbffffc2a) = 0
vps_parse_config(3390, 0x405894, 0x508010, 0x5078e0, 0x7fbffff748)    = 0
init_log(0x509100, 3390, 1, 0, 0)                                     = 0
getopt_long(1, 0x7fbffffa58, "", 0x7fbffff570, NULL)                  = -1
get_vps_conf_path(3390, 0x7fbffff840, 256, 0, 1)                      = 24
stat_file(0x7fbffff840, 0x310721a48d, 24, 0x7fbffff858, 4)            = 1
vps_parse_config(3390, 0x7fbffff840, 0x5084e0, 0x5078e0, 4)           = 0
```

```
merge_vps_param(0x508010, 0x5084e0, 0, 0x5099a0, 128608)            = 0
merge_global_param(0x5089b0, 0x508010, 0x5086b8, 0x5081e8, 0x3106f306f8) = 0
vz_open(3390, 5, 0x508010, 0x5084e0, 0x5089b0)                      = 0x509c30
vps_lock(3390, 0x5090c0, 0x405821, -1, 32Removing stale lock file /vz/lock/3390.lck
 <unfinished ...>
 --- SIGSEGV (Segmentation fault) ---
```

---

ls -al /vz/private

```
 drwxr-xr-x  21 root root 4096 Jan 21 06:21 3350
 drwxr-xr-x  25 root root 4096 Jan 21 06:22 3360
 drwxr-xr-x  20 root root 4096 Jan 21 06:22 3370
 drwxr-xr-x  22 root root 4096 2666130989162650458 3380
```

Here's 'ltrace reboot'. The node is crashing in ctime, primarily because time(), is returning too big a number.

```
signal(22, 0x1)                                     = NULL
sigaction(2, 0x7fbffff660, NULL)                    = 0
chdir("/")                                          = 0
strchr("0", ':')                                    = NULL
__strtol_internal("0", NULL, 10)                    = 0
strncat(0x7fbffff480, 0x504a20, 319, 0, 0x1999999999999999)  = 0x7fbffff480
snprintf("", 4209868, "\377\377\377\377\377\377\377"...)     = 43
getuid()                                            = 0
getpwuid(0, 1, 0, -1, 0xfefefefefefefeff)           = 0x3106f31600
strncat(0x5048c0, 0x505010, 31, 0, 0)               = 0x5048c0
ttyname(0)                                          = "/dev/pts/1"
sprintf("", ") ")                                   = 8
time(0x7fbffff278)                                  = 2666130989162650727
ctime(0x7fbffff278)                                 = NULL
```

Subject: Re: Node Crashes on 64 bit owing to a single file.
Posted by dev on Mon, 22 Jan 2007 09:55:24 GMT
View Forum Message <> Reply to Message

Ligesh,
1. can I get an access to the node?
2. does CPanel require license? Will try to experiment locally meanwhile.

Thanks,
Kirill

> This is a widespread problem and seem to be very specific to cpanel on 64bit. It is very much reproducable. Just install cpanel in either node or inside a vps, and everything will start segfaulting.
>
> here's the ltrace for vzctl start.
>
> ----------
> start(3, 0x3106b114a6, 0x3106b0b090, 0x7472617473006c, 0xfefefefefefefeff <unfinished ...>
> __libc_start_main(0x402c90, 3, 0x7fbffffa48, 0x405720, 0x405780 <unfinished ...>
> init_vps_param(3, 0x7fbffffa48, 0x7fbffffa68, 32, 0x7fbffff9a0) = 0x508010
> init_vps_param(0x508010, 0, 0x508308, 0x508010, 0) = 0x5084e0
> init_vps_param(0x5084e0, 0, 0x5087d8, 0x5084e0, 0) = 0x5089b0
> sigemptyset(0x7fbffff7a8) = 0
> sigaction(13, 0x7fbffff7a0, NULL) = 0
> init_log(0, 0, 1, 0, 0) = 0
> opendir("/usr/lib/vzctl/modules/") = NULL
> __errno_location() = 0x2a95565ea0
> logger(2, 2, 0x406910, -64, 0x7fbffffc2a) = 0
> parse_int(0x7fbffffc30, 0x7fbffff79c, 0x406910, 0x310720ac51, 0x7fbffffc2a) = 0
> vps_parse_config(3390, 0x405894, 0x508010, 0x5078e0, 0x7fbffff748) = 0
> init_log(0x509100, 3390, 1, 0, 0) = 0
> getopt_long(1, 0x7fbffffa58, "", 0x7fbffff570, NULL) = -1
> get_vps_conf_path(3390, 0x7fbffff840, 256, 0, 1) = 24
> stat_file(0x7fbffff840, 0x310721a48d, 24, 0x7fbffff858, 4) = 1
> vps_parse_config(3390, 0x7fbffff840, 0x5084e0, 0x5078e0, 4) = 0
> merge_vps_param(0x508010, 0x5084e0, 0, 0x5099a0, 128608) = 0
> merge_global_param(0x5089b0, 0x508010, 0x5086b8, 0x5081e8, 0x3106f306f8) = 0
> vz_open(3390, 5, 0x508010, 0x5084e0, 0x5089b0) = 0x509c30
> vps_lock(3390, 0x5090c0, 0x405821, -1, 32Removing stale lock file /vz/lock/3390.lck
> <unfinished ...>
> --- SIGSEGV (Segmentation fault) ---
>
>
> ----------
>
>
> ls -al /vz/private
>
> ----------
> drwxr-xr-x 21 root root 4096 Jan 21 06:21 3350

> drwxr-xr-x 25 root root 4096 Jan 21 06:22 3360
> drwxr-xr-x 20 root root 4096 Jan 21 06:22 3370
> drwxr-xr-x 22 root root 4096 2666130989162650458 3380
> ----------
>
>
> Here's 'ltrace reboot'. The node is crashing in ctime, primarily because time(), is returning too big a number.
>
> ---
>
> signal(22, 0x1) = NULL
> sigaction(2, 0x7fbffff660, NULL) = 0
> chdir("/") = 0
> strchr("0", ':') = NULL
> __strtol_internal("0", NULL, 10) = 0
> strncat(0x7fbffff480, 0x504a20, 319, 0, 0x1999999999999999) = 0x7fbffff480
> snprintf("", 4209868, "\377\377\377\377\377\377\377\377"...) = 43
> getuid() = 0
> getpwuid(0, 1, 0, -1, 0xfefefefefefefeff) = 0x3106f31600
> strncat(0x5048c0, 0x505010, 31, 0, 0) = 0x5048c0
> ttyname(0) = "/dev/pts/1"
> sprintf("", ") ") = 8
> time(0x7fbffff278) = 2666130989162650727
> ctime(0x7fbffff278) = NULL
>
> ---
>
>