Subject: DEBIAN squeeze : "unable to handle kernel NULL pointer dereference at (null)" creating VE
Posted by SuperNaze on Sun, 02 May 2010 20:22:36 GMT
View Forum Message <> Reply to Message

hello,
I am testing openvz. the box is running debian squeeze with kernel 2.6.32-avdeyev.1. the kernel was installed using the procedure described on the wiki using the rpm package and alien.
I used ext4 over lvm.

when I create the VE, I get :

root@test-m1:/var/lib/vz/template/cache# vzctl create 2005 --ostemplate debian-5.0-x86_64
Creating container private area (debian-5.0-x86_64)
Killed
vps-create ERROR: Error in tar -z -xf /var/lib/vz/template/cache/debian-5.0-x86_64.tar.gz

Message from syslogd@test-m1 at May 2 22:08:30 ...
 kernel:Oops: 0010 [#1] SMP

Message from syslogd@test-m1 at May 2 22:08:30 ...
 kernel:last sysfs file: /sys/devices/system/cpu/cpu1/topology/thread_siblings
Received signal: 9 in /usr/sbin/vzquota
Processus arrÃªtÃ©

BUG: unable to handle kernel NULL pointer dereference at (null)

IP: [<(null)>] (null)
PGD 37a04067 PUD 6cedf067 PMD 0

Oops: 0010 [#1] SMP

last sysfs file: /sys/devices/system/cpu/cpu1/topology/thread_siblings

CPU 1
Modules linked in: vzethdev vznetdev simfs vzrst vzcpt vzdquota vzmon vzdev xt_length xt_hl xt_tcpmss xt_TCPMSS iptable_mangle xt_multiport xt_limit xt_dscp ipv6 arc4 ecb snd_hda_codec_nvhdmi snd_hda_codec_realtek ath5k snd_hda_intel snd_hda_codec mac80211 ath snd_hwdep snd_pcm cfg80211 snd_timer rfkill snd shpchp pcspkr serio_raw i2c_nforce2 soundcore wmi snd_page_alloc i2c_core forcedeth [last unloaded: scsi_wait_scan]

Pid: 1533, comm: tar Not tainted 2.6.32-avdeyev.1 #1 avdeyev Aspire R3600

RIP: 0010:[<0000000000000000>] [<(null)>] (null)

RSP: 0018:ffff88006eb139e0 EFLAGS: 00010246

RAX: ffffffffa02961c0 RBX: ffff88006b52aa80 RCX: 000000000000000c

RDX: 0000000000000000 RSI: 0000000000003000 RDI: ffff88006b63d030

RBP: ffff88006eb13a48 R08: 0000000000000001 R09: 0000000000000000

R10: 000000000000067f R11: 00000000000672ea R12: ffff88006b63d030

R13: 0000000000000000 R14: ffff88006b63cf80 R15: ffff88006b63d328

FS: 00007f91cbb5c6f0(0000) GS:ffff880001a80000(0000) knlGS:0000000000000000

CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033

CR2: 0000000000000000 CR3: 000000006db43000 CR4: 00000000000006e0

DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000

DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400

Process tar (pid: 1533, veid=0, threadinfo ffff88006eb12000, task ffff88006eb59800)

Stack:

 ffffffff81191e0f ffff880037a9ec00 0000000000000002 0000000000000003

<0> ffffffffffff0000 ffff88006b63d030 0000000000001000 ffff88006eb13a48

<0> ffffea0001a74180 ffff88006eb13a98 0000000000001000 ffff88006b63d030

Call Trace:

 [<ffffffff81191e0f>] ? ext4_da_get_block_prep+0x142/0x244

 [<ffffffff81139f62>] __block_prepare_write+0x133/0x289

 [<ffffffff81191ccd>] ? ext4_da_get_block_prep+0x0/0x244

 [<ffffffff810d0245>] ? add_to_page_cache_locked+0x7a/0xc9

 [<ffffffff8113a239>] block_write_begin+0x80/0xd2

 [<ffffffff811919ea>] ext4_da_write_begin+0x18e/0x21d

[<ffffffff81191ccd>] ? ext4_da_get_block_prep+0x0/0x244

[<ffffffff810d0c93>] generic_file_buffered_write+0x10b/0x28e

[<ffffffff810d11d4>] __generic_file_aio_write+0x251/0x286

[<ffffffff810d126c>] generic_file_aio_write+0x63/0xaf

[<ffffffff811893e9>] ext4_file_write+0x8e/0x95

[<ffffffff81110630>] ? nameidata_to_filp+0x42/0x53

[<ffffffff81112628>] do_sync_write+0xe8/0x125

[<ffffffff81070a73>] ? autoremove_wake_function+0x0/0x39

[<ffffffff8120e895>] ? __strncpy_from_user+0x1e/0x49

[<ffffffff81105508>] ? virt_to_head_page+0xe/0x2f

[<ffffffff81112bcb>] vfs_write+0xae/0x10b

[<ffffffff8111f822>] ? putname+0x32/0x3b

[<ffffffff81112d41>] sys_write+0x4e/0xc3

[<ffffffff8100bdc2>] system_call_fastpath+0x16/0x1b

Code: Bad RIP value.

RIP [<(null)>] (null)

RSP <ffff88006eb139e0>

CR2: 0000000000000000

---[end trace 9c29e24f804e60b7]---

BUG: unable to handle kernel NULL pointer dereference at (null)

IP: [<(null)>] (null)

PGD 6d854067 PUD 6e90f067 PMD 0

Oops: 0010 [#2] SMP

last sysfs file: /sys/devices/system/cpu/cpu1/topology/thread_siblings

CPU 0

Modules linked in: vzethdev vznetdev simfs vzrst vzcpt vzdquota vzmon vzdev xt_length xt_hl xt_tcpmss xt_TCPMSS iptable_mangle xt_multiport xt_limit xt_dscp ipv6 arc4 ecb snd_hda_codec_nvhdmi snd_hda_codec_realtek ath5k snd_hda_intel snd_hda_codec mac80211 ath snd_hwdep snd_pcm cfg80211 snd_timer rfkill snd shpchp pcspkr serio_raw i2c_nforce2 soundcore wmi snd_page_alloc i2c_core forcedeth [last unloaded: scsi_wait_scan]

Pid: 1032, comm: rs:main Q:Reg Tainted: G D 2.6.32-avdeyev.1 #1 avdeyev Aspire R3600

RIP: 0010:[<0000000000000000>] [<(null)>] (null)

RSP: 0018:ffff88006cdb79e0 EFLAGS: 00010246

RAX: ffffffffa02961c0 RBX: ffff88006b4dec40 RCX: 000000000000000c

RDX: 0000000000000000 RSI: 0000000000003000 RDI: ffff88006b4b3310

RBP: ffff88006cdb7a48 R08: 0000000000000001 R09: 000000000000000c

R10: 0000000000002f65 R11: 0000000000067305 R12: ffff88006b4b3310

R13: 0000000000000000 R14: ffff88006b4b3260 R15: ffff88006b4b3608

FS: 00007f943917b910(0000) GS:ffff880001a00000(0000) knlGS:0000000000000000

CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033

CR2: 0000000000000000 CR3: 000000006d85d000 CR4: 00000000000006f0

DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000

DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400

Process rs:main Q:Reg (pid: 1032, veid=0, threadinfo ffff88006cdb6000, task ffff880037ec0000)

Stack:

ffffffff81191e0f ffff880037a9ec00 0000000000000002 0000000000000003

<0> ffffffffffff0000 ffff88006b4b3310 000000000000003b ffff88006cdb7a48

<0> ffffea0001a75500 ffff88006cdb7a98 0000000000001000 ffff88006b4b3310

Call Trace:

[<ffffffff81191e0f>] ? ext4_da_get_block_prep+0x142/0x244

[<ffffffff81139f62>] __block_prepare_write+0x133/0x289

[<ffffffff81191ccd>] ? ext4_da_get_block_prep+0x0/0x244

[<ffffffff810d0245>] ? add_to_page_cache_locked+0x7a/0xc9

[<ffffffff8113a239>] block_write_begin+0x80/0xd2

[<ffffffff811919ea>] ext4_da_write_begin+0x18e/0x21d

[<ffffffff81191ccd>] ? ext4_da_get_block_prep+0x0/0x244

[<ffffffff810d0c93>] generic_file_buffered_write+0x10b/0x28e

[<ffffffff810d11d4>] __generic_file_aio_write+0x251/0x286

[<ffffffff810d126c>] generic_file_aio_write+0x63/0xaf

[<ffffffff811893e9>] ext4_file_write+0x8e/0x95

[<ffffffff81112628>] do_sync_write+0xe8/0x125

[<ffffffff8107ee3d>] ? do_uncharge_dcache+0x4d/0x56

[<ffffffff81070a73>] ? autoremove_wake_function+0x0/0x39

[<ffffffff81112bcb>] vfs_write+0xae/0x10b

[<ffffffff81112d41>] sys_write+0x4e/0xc3

[<ffffffff8100bdc2>] system_call_fastpath+0x16/0x1b

Code: Bad RIP value.

RIP [<(null)>] (null)

RSP <ffff88006cdb79e0>

CR2: 0000000000000000

BUG: unable to handle kernel

---[end trace 9c29e24f804e60b8]---

NULL pointer dereference at (null)

IP: [<(null)>] (null)

PGD 37a06067 PUD 6db4d067 PMD 0

Oops: 0010 [#3] SMP

last sysfs file: /sys/devices/system/cpu/cpu1/topology/thread_siblings

CPU 1

Modules linked in: vzethdev vznetdev simfs vzrst vzcpt vzdquota vzmon vzdev xt_length xt_hl xt_tcpmss xt_TCPMSS iptable_mangle xt_multiport xt_limit xt_dscp ipv6 arc4 ecb snd_hda_codec_nvhdmi snd_hda_codec_realtek ath5k snd_hda_intel snd_hda_codec mac80211 ath snd_hwdep snd_pcm cfg80211 snd_timer rfkill snd shpchp pcspkr serio_raw i2c_nforce2 soundcore wmi snd_page_alloc i2c_core forcedeth [last unloaded: scsi_wait_scan]

Pid: 1536, comm: vzquota Tainted: G D 2.6.32-avdeyev.1 #1 avdeyev Aspire R3600

RIP: 0010:[<0000000000000000>] [<(null)>] (null)

RSP: 0018:ffff88006eb13c40 EFLAGS: 00010246

RAX: ffffffffa02961c0 RBX: ffff88006b619fb0 RCX: 000000000000000c

RDX: ffff880037a9f400 RSI: 0000000000003000 RDI: ffff88006b619fb0

RBP: ffff88006eb13c48 R08: 0000000000000000 R09: 0000000000000000

R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000001

R13: ffff88006b619f00 R14: ffffea0001a73900 R15: 0000000000000000

FS: 00007f832806a6f0(0000) GS:ffff880001a80000(0000) knlGS:0000000000000000

CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033

CR2: 0000000000000000 CR3: 000000006cfd0000 CR4: 00000000000006e0

DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000

DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400

Process vzquota (pid: 1536, veid=0, threadinfo ffff88006eb12000, task ffff880037d20000)

Stack:

ffffffff8118dac7 ffff88006eb13ca8 ffffffff8118dc26 ffff88006eb13cb8

<0> ffffffff00000000 0000000000000003 ffff880037a9ec00 0000000137d20000

<0> ffffea0001a73900 ffff88006b61a0d0 ffff88006b61a0d0 ffffffffffffffff

Call Trace:

[<ffffffff8118dac7>] ? vfs_dq_release_reservation_block+0x37/0x44

[<ffffffff8118dc26>] ext4_da_invalidatepage+0x152/0x16c

[<ffffffff810d8d91>] do_invalidatepage+0x25/0x27

[<ffffffff810d93a8>] truncate_inode_page+0x4b/0x7c

[<ffffffff810d94a2>] truncate_inode_pages_range+0xc9/0x316

[<ffffffff810cfffb>] ? wake_up_page+0x25/0x2a

[<ffffffffa0290213>] ? vzquota_inode_data+0x54/0xbd [vzdquota]

[<ffffffff81191a79>] ? ext4_delete_inode+0x0/0x254

[<ffffffff810d9701>] truncate_inode_pages+0x12/0x14

[<ffffffff81191adc>] ext4_delete_inode+0x63/0x254

[<ffffffff81191a79>] ? ext4_delete_inode+0x0/0x254

[<ffffffff81128b13>] generic_delete_inode+0xdb/0x15d

[<ffffffff81128bb1>] generic_drop_inode+0x1c/0x5b

[<ffffffff81127a92>] iput+0x66/0x6a

[<ffffffff81124ae7>] dentry_iput+0xb8/0xca

[<ffffffff81124bc2>] d_kill+0x26/0x46

[<ffffffff81126680>] dput+0x188/0x195

[<ffffffff81113d80>] __fput+0x1a8/0x1d4

[<ffffffff81113dc6>] fput+0x1a/0x1c

[<ffffffff81110059>] filp_close+0x68/0x73

[<ffffffff81110101>] sys_close+0x9d/0xd2

[<ffffffff8100bdc2>] system_call_fastpath+0x16/0x1b

Code: Bad RIP value.

RIP [<(null)>] (null)

 RSP <ffff88006eb13c40>

CR2: 0000000000000000

---[end trace 9c29e24f804e60b9]---

BUG: unable to handle kernel NULL pointer dereference at (null)

IP: [<(null)>] (null)

PGD 6eb10067 PUD 6da8f067 PMD 0
Oops: 0010 [#4] SMP
last sysfs file: /sys/devices/system/cpu/cpu1/topology/thread_siblings
CPU 1
Modules linked in: vzethdev vznetdev simfs vzrst vzcpt vzdquota vzmon vzdev xt_length xt_hl xt_tcpmss xt_TCPMSS iptable_mangle xt_multiport xt_limit xt_dscp ipv6 arc4 ecb snd_hda_codec_nvhdmi snd_hda_codec_realtek ath5k snd_hda_intel snd_hda_codec mac80211 ath snd_hwdep snd_pcm cfg80211 snd_timer rfkill snd shpchp pcspkr serio_raw i2c_nforce2 soundcore wmi snd_page_alloc i2c_core forcedeth [last unloaded: scsi_wait_scan]
Pid: 1519, comm: vzctl Tainted: G   D   2.6.32-avdeyev.1 #1 avdeyev Aspire R3600
RIP: 0010:[<0000000000000000>] [<(null)>] (null)
RSP: 0018:ffff88006ceb7c70 EFLAGS: 00010246
RAX: ffffffffa02961c0 RBX: ffff88006b619030 RCX: 000000000000000c
RDX: ffff880037a9f400 RSI: 0000000000003000 RDI: ffff88006b619030
RBP: ffff88006ceb7c78 R08: 0000000000000000 R09: ffff88006ceb7e98
R10: ffffffff00000000 R11: 0000000000a65028 R12: 0000000000000001
R13: ffff88006b618f80 R14: ffffea0001a8f580 R15: 0000000000000000
FS: 00007f9b79d016f0(0000) GS:ffff880001a80000(0000) knlGS:0000000000000000
CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 0000000000000000 CR3: 0000000037bb9000 CR4: 00000000000006e0
DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400
Process vzctl (pid: 1519, veid=0, threadinfo ffff88006ceb6000, task ffff88006eb1b000)
Stack:
 ffffffff8118dac7 ffff88006ceb7cd8 ffffffff8118dc26 ffff88006ceb7ce8
<0> ffffffff00000000 0000000000000003 ffff880037a9ec00 0000000137a9f400
<0> ffffea0001a8f580 ffff88006b619150 ffff88006b619150 ffffffffffffffff
Call Trace:
 [<ffffffff8118dac7>] ? vfs_dq_release_reservation_block+0x37/0x44
 [<ffffffff8118dc26>] ext4_da_invalidatepage+0x152/0x16c
 [<ffffffff810d8d91>] do_invalidatepage+0x25/0x27
 [<ffffffff810d93a8>] truncate_inode_page+0x4b/0x7c
 [<ffffffff810d94a2>] truncate_inode_pages_range+0xc9/0x316
 [<ffffffff811ad05e>] ? __ext4_handle_dirty_metadata+0xda/0xe3

[<ffffffff81426205>] ? mutex_lock+0x29/0x50
[<ffffffffa0290213>] ? vzquota_inode_data+0x54/0xbd [vzdquota]
[<ffffffff81191a79>] ? ext4_delete_inode+0x0/0x254
[<ffffffff810d9701>] truncate_inode_pages+0x12/0x14
[<ffffffff81191adc>] ext4_delete_inode+0x63/0x254
[<ffffffff81191a79>] ? ext4_delete_inode+0x0/0x254
[<ffffffff81128b13>] generic_delete_inode+0xdb/0x15d
[<ffffffff81128bb1>] generic_drop_inode+0x1c/0x5b
[<ffffffff81127a92>] iput+0x66/0x6a
[<ffffffff8111fd03>] do_unlinkat+0x108/0x15b
[<ffffffff814294ac>] ? do_page_fault+0x270/0x2a0
[<ffffffff8111fd6c>] sys_unlink+0x16/0x18
[<ffffffff8100bdc2>] system_call_fastpath+0x16/0x1b
Code: Bad RIP value.
RIP [<(null)>] (null)
 RSP <ffff88006ceb7c70>
CR2: 0000000000000000
---[end trace 9c29e24f804e60ba]---

can somebody advise ? thanks.