# OpenNebula - Bug #702
# oned crashed

06/28/2011 08:12 PM - Shi Jin

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 06/28/2011 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | | **Estimated time:** | 0.00 hour |
| **Target version:** | Release 3.0 | | |
| **Resolution:** | fixed | **Pull request:** | |
| **Affected Versions:** | | | |

**Description**

This is the latest master code built with MySQL.

[cloudadmin@devcloud spectrumVisor]$ one*** glibc detected * /**vrstorm/cloud/one3git/bin/oned: double free or corruption (fasttop): 0x00007f636c000c80** *======= Backtrace: =========
/lib64/libc.so.6[0x3705075716]
/usr/lib64/libstdc++.so.6(_ZNSs6assignERKSs+0x85)[0x371289d565]
/vrstorm/cloud/one3git/bin/oned[0x446d0a]
/usr/lib64/libxmlrpc_server++.so.4(+0x3f8e)[0x7f63c7b5df8e]
/usr/lib64/libxmlrpc_server.so.3(xmlrpc_dispatchCall+0xb3)[0x7f63c753ae63]
/usr/lib64/libxmlrpc_server.so.3(xmlrpc_registry_process_call2+0x131)[0x7f63c753b021]
/usr/lib64/libxmlrpc_server_abyss.so.3(+0x309b)[0x7f63c795709b]
/usr/lib64/libxmlrpc_abyss.so.3(+0xcc88)[0x7f63c732fc88]
/usr/lib64/libxmlrpc_abyss.so.3(+0xcd8c)[0x7f63c732fd8c]
/usr/lib64/libxmlrpc_abyss.so.3(+0x79a7)[0x7f63c732a9a7]
/usr/lib64/libxmlrpc_abyss.so.3(+0xf464)[0x7f63c7332464]
/lib64/libpthread.so.0[0x37054077e1]
/lib64/libc.so.6(clone+0x6d)[0x37050e68ed]======= Memory map: ========
00400000-004d5000 r-xp 00000000 fd:02 34365581 /vrstorm/cloud/one3git/bin/oned
006d5000-006db000 rw-p 000d5000 fd:02 34365581 /vrstorm/cloud/one3git/bin/oned
0187b000-018bd000 rw-p 00000000 00:00 0 [heap]
3704800000-3704820000 r-xp 00000000 fd:00 261655 /lib64/ld-2.12.so
3704a1f000-3704a20000 r--p 0001f000 fd:00 261655 /lib64/ld-2.12.so
3704a20000-3704a21000 rw-p 00020000 fd:00 261655 /lib64/ld-2.12.so
3704a21000-3704a22000 rw-p 00000000 00:00 0
3704c00000-3704c02000 r-xp 00000000 fd:00 261661 /lib64/libdl-2.12.so
3704c02000-3704e02000 ---p 00002000 fd:00 261661 /lib64/libdl-2.12.so
3704e02000-3704e03000 r--p 00002000 fd:00 261661 /lib64/libdl-2.12.so
3704e03000-3704e04000 rw-p 00003000 fd:00 261661 /lib64/libdl-2.12.so
3705000000-3705187000 r-xp 00000000 fd:00 261659 /lib64/libc-2.12.so
3705187000-3705387000 ---p 00187000 fd:00 261659 /lib64/libc-2.12.so
3705387000-370538b000 r--p 00187000 fd:00 261659 /lib64/libc-2.12.so
370538b000-370538c000 rw-p 0018b000 fd:00 261659 /lib64/libc-2.12.so
370538c000-3705391000 rw-p 00000000 00:00 0
3705400000-3705417000 r-xp 00000000 fd:00 261701 /lib64/libpthread-2.12.so
3705417000-3705617000 ---p 00017000 fd:00 261701 /lib64/libpthread-2.12.so
3705617000-3705618000 r--p 00017000 fd:00 261701 /lib64/libpthread-2.12.so
3705618000-3705619000 rw-p 00018000 fd:00 261701 /lib64/libpthread-2.12.so
3705619000-370561d000 rw-p 00000000 00:00 0
3705800000-3705883000 r-xp 00000000 fd:00 261716 /lib64/libm-2.12.so
3705883000-3705a82000 ---p 00083000 fd:00 261716 /lib64/libm-2.12.so

3705a82000-3705a83000 r--p 00082000 fd:00 261716 /lib64/libm-2.12.so
3705a83000-3705a84000 rw-p 00083000 fd:00 261716 /lib64/libm-2.12.so
3705c00000-3705c15000 r-xp 00000000 fd:00 261726 /lib64/libz.so.1.2.3
3705c15000-3705e14000 ---p 00015000 fd:00 261726 /lib64/libz.so.1.2.3
3705e14000-3705e15000 rw-p 00014000 fd:00 261726 /lib64/libz.so.1.2.3
3706000000-3706135000 r-xp 00000000 fd:00 1059681 /usr/lib64/mysql/libmysqlclient.so.16.0.0
3706135000-3706334000 ---p 00135000 fd:00 1059681 /usr/lib64/mysql/libmysqlclient.so.16.0.0
3706334000-3706381000 rw-p 00134000 fd:00 1059681 /usr/lib64/mysql/libmysqlclient.so.16.0.0
3706381000-3706382000 rw-p 00000000 00:00 0
3706400000-370641d000 r-xp 00000000 fd:00 261671 /lib64/libselinux.so.1
370641d000-370661c000 ---p 0001d000 fd:00 261671 /lib64/libselinux.so.1
370661c000-370661d000 r--p 0001c000 fd:00 261671 /lib64/libselinux.so.1
370661d000-370661e000 rw-p 0001d000 fd:00 261671 /lib64/libselinux.so.1
370661e000-370661f000 rw-p 00000000 00:00 0
3706c00000-3706c16000 r-xp 00000000 fd:00 261669 /lib64/libresolv-2.12.so
3706c16000-3706e16000 ---p 00016000 fd:00 261669 /lib64/libresolv-2.12.so
3706e16000-3706e17000 r--p 00016000 fd:00 261669 /lib64/libresolv-2.12.so
3706e17000-3706e18000 rw-p 00017000 fd:00 261669 /lib64/libresolv-2.12.so
3706e18000-3706e1a000 rw-p 00000000 00:00 0
3708c00000-3708c0a000 r-xp 00000000 fd:00 1059512 /usr/lib64/libxmlrpc_client.so.3.16
3708c0a000-3708e0a000 ---p 0000a000 fd:00 1059512 /usr/lib64/libxmlrpc_client.so.3.16
3708e0a000-3708e0b000 rw-p 0000a000 fd:00 1059512 /usr/lib64/libxmlrpc_client.so.3.16
3709000000-3709004000 r-xp 00000000 fd:00 1059510 /usr/lib64/libxmlrpc_util.so.3.16
3709004000-3709203000 ---p 00004000 fd:00 1059510 /usr/lib64/libxmlrpc_util.so.3.16
3709203000-3709204000 rw-p 00003000 fd:00 1059510 /usr/lib64/libxmlrpc_util.so.3.16
3709400000-3709413000 r-xp 00000000 fd:00 1059511 /usr/lib64/libxmlrpc.so.3.16
3709413000-3709613000 ---p 00013000 fd:00 1059511 /usr/lib64/libxmlrpc.so.3.16
3709613000-3709614000 rw-p 00013000 fd:00 1059511 /usr/lib64/libxmlrpc.so.3.16
370b400000-370b547000 r-xp 00000000 fd:00 1051965 /usr/lib64/libxml2.so.2.7.6
370b547000-370b746000 ---p 00147000 fd:00 1051965 /usr/lib64/libxml2.so.2.7.6
370b746000-370b750000 rw-p 00146000 fd:00 1051965 /usr/lib64/libxml2.so.2.7.6
370b750000-370b751000 rw-p 00000000 00:00 0
370f400000-370f432000 r-xp 00000000 fd:00 261910 /lib64/libidn.so.11.6.1
370f432000-370f631000 ---p 00032000 fd:00 261910 /lib64/libidn.so.11.6.1
370f631000-370f632000 rw-p 00031000 fd:00 261910 /lib64/libidn.so.11.6.1
370fc00000-370fd71000 r-xp 00000000 fd:00 1052011 /usr/lib64/libcrypto.so.1.0.0
370fd71000-370ff70000 ---p 00171000 fd:00 1052011 /usr/lib64/libcrypto.so.1.0.0
370ff70000-370ff93000 rw-p 00170000 fd:00 1052011 /usr/lib64/libcrypto.so.1.0.0
370ff93000-370ff96000 rw-p 00000000 00:00 0
3710000000-3710051000 r-xp 00000000 fd:00 1056005 /usr/lib64/libcurl.so.4.1.1vm list

**Related issues:**

| | | |
|---|---|---|
| Duplicated by Bug # 685: xmlrpc exceptions when getting pools of elements int... | **Closed** | **06/16/2011** |

### Associated revisions

**Revision 03fac909 - 07/07/2011 10:45 AM - Carlos Martín**

Bug #702: xmlrpc-c does not create a new xmlrpc_c::method class for each request.

Instead, it creates a single instance and its execute method is called for each new request.
This caused some variables to be shared by several threads, which eventually ended in
segmentation fault.

## History

#### #1 - 06/29/2011 05:17 PM - Hector Sanjuan

Hi,

can you post your OS details and xmlrpc package versions? Do you know if a particular operation is causing this or is it random? Does it happen frequently to you?

Thanks

#### #2 - 06/29/2011 08:44 PM - Shi Jin

Hi,

Here is the RHEL-6.1 box detailed information.

```
[cloudadmin@devcloud template]$ lsb_release -a
LSB Version:    :core-4.0-amd64:core-4.0-noarch:graphics-4.0-amd64:graphics-4.0-noarch:printing-4.0-amd64:printing-4.0-noarch
Distributor ID:    RedHatEnterpriseServer
Description:    Red Hat Enterprise Linux Server release 6.1 (Santiago)
Release:    6.1
Codename:    Santiago
[cloudadmin@devcloud template]$ uname -a
Linux devcloud.spectrumvisor.com 2.6.32-131.2.1.el6.x86_64 #1 SMP Wed May 18 07:07:37 EDT 2011 x86_64 x86_64 x86_64 GNU/Linux
[cloudadmin@devcloud template]$ cat /proc/version
Linux version 2.6.32-131.2.1.el6.x86_64 (mockbuild@x86-003.build.bos.redhat.com) (gcc version 4.4.5 20110214 (Red Hat 4.4.5-6) (GCC) )
#1 SMP Wed May 18 07:07:37 EDT 2011

[cloudadmin@devcloud template]$ rpm -qa|grep xmlrpc
xmlrpc-c-c++-1.16.24-1200.1840.el6.x86_64
xmlrpc-c-devel-1.16.24-1200.1840.el6.x86_64
xmlrpc-c-client-1.16.24-1200.1840.el6.x86_64
xmlrpc-c-client++-1.16.24-1200.1840.el6.x86_64
xmlrpc-c-1.16.24-1200.1840.el6.x86_64
```

The crash does not happen if I simply using the onevm CLI. It happens when I use our own code calling the XML RPC API, which works for ONE-2.x. I think there is some significant change from 2.x to 3.x and it is expected that the old code does not work. However, I would think there is still a bug in master ONE code since a legacy client shouldn't crash the server.

I am in the process of figuring out the necessary changes for our own code to work with the up coming 3.0 version. If you could provide some debugging procedure help, I am very happy to debug oned code.

Shi

#### #3 - 06/29/2011 10:43 PM - Ruben S. Montero

Shi Jin wrote:

> *[...]*
>
> *The crash does not happen if I simply using the onevm CLI. It happens when I use our own code calling the XML RPC API, which works for ONE-2.x. I think there is some significant change from 2.x to 3.x and it is expected that the old code does not work. However, I would think there is still a bug in master ONE code since a legacy client shouldn't crash the server.*

Yes this is quite strange could you post the XML-RPC call that causes the problem?. We also plan to prepare a migration guide from 2.x to 3.x, to easily port applications...

Thanks

Ruben

#### #4 - 07/04/2011 11:17 PM - Shi Jin

Hi,

I am still trying to find exactly which XML-RPC call is causing the crash since there are so many calls.
Is there any way to log in details of the XML-RPC calls?
Right now, the one_xmlrpc.log alway shows correct information like

```
127.0.0.1:37595 - no_user - [04/Jul/2011:10:26:40 +0600] "POST" 200 4128
127.0.0.1:37595 - no_user - [04/Jul/2011:10:26:40 +0600] "POST" 200 12772
127.0.0.1:37595 - no_user - [04/Jul/2011:10:26:40 +0600] "POST" 200 518
127.0.0.1:37595 - no_user - [04/Jul/2011:10:26:40 +0600] "POST" 200 518
```

They are not very useful? Can we log the name of the function and its arguments?

Thanks.
Shi

#### #5 - 07/05/2011 06:04 PM - Shi Jin

Hi there,

Here is the code I used to reproduce the crash.

```
#!/usr/bin/ruby
require 'rexml/document'
require "xmlrpc/client"

ONE_XMLRPC=ENV["ONE_XMLRPC"]
$server = XMLRPC::Client.new("localhost", "/RPC2", 2633)
$session="<change to your session variable>"

def vminfo(id)
        param = $server.call("one.vm.info", $session, id)
        if param[0]==false
                puts "failed vminfo"
```

```
        end
        vm=REXML::Document.new(param[1]).root
        puts "VM-#{vm.elements['/VM/ID'].text.strip}: #{vm.elements['/VM/NAME'].text.strip}"

    end

    begin

        while true
            param = $server.call("one.vmpool.info", $session, -1,true,-1)
            if param[0]==false
                puts "failed vmpool"
            end
            vmList=REXML::Document.new(param[1]).root
            vmList.elements.each('/VM_POOL/VM'){|vm|
                puts "vminfo(#{vm.elements['ID'].text.strip})"
                vminfo(vm.elements['ID'].text.strip.to_i)
                #puts vm.elements['TEMPLATE/NIC/IP'].text.strip
            }
        end

    rescue XMLRPC::FaultException => e
        puts "Error:"
        puts e.faultCode
        puts e.faultString
    end
```

Running this code on the same machine as a single process is fine. The problem happens when you run two of this processes together (eg, on two terminals of the same machine).  I think the error is in the way the XML RPC server handles concurrent requests.

This problem also happens if a non-blocking XML RPC client is used (in our case, we use ColdFusion). I used two processes in this Ruby code because I think it is blocking so that all requests are processed in order.

Please let me know if you can reproduce this.
Thanks.

Shi

#### #6 - 07/05/2011 08:00 PM - Shi Jin

I should also update that I ran the same test against ONE-2.2.1 and found no problem at all.

#### #7 - 07/07/2011 10:49 AM - Carlos Martín

*- Status changed from New to Closed*

*- Resolution set to fixed*

Thank you Shi Jin for the bug report and your feedback, it should be fixed now.

#### #8 - 07/07/2011 03:02 PM - Shi Jin

Thanks.
I pull the master code but couldn't run it

> [cloudadmin@devcloud bin]$ one start
> oned failed to start

Something else breaks oned?

#### #9 - 07/07/2011 03:47 PM - Shi Jin

OK. It turned out several things have changed such as a new acl table.
Now I am able to confirm the fix. Thanks a lot.