Subject: VPS can not be entered
Posted by leobrown on Tue, 05 Jan 2010 11:44:16 GMT
View Forum Message <> Reply to Message

Hi

I have an issue where a fairly new VPS stops serving HTTP/SSH requests and can not be entered into.

The problem is resolved by issuing a restart, though the restart takes 1 minute, and the restart 3 minutes, much slower than its' similar counterpart VPSs.

Quotas seem to be fine for the VPS:

vzmemcheck

```
 LowMem  LowMem     RAM MemSwap MemSwap   Alloc   Alloc   Alloc
   util  commit    util    util  commit    util  commit   limit
  12.83   61.93   65.51   21.70   79.67   44.89   81.14  137.95
```

vzcalc

```
Resource     Current(%)  Promised(%)  Max(%)
Memory          11.16       8.67      25.40
```

vzquota stat

```
   resource          usage       softlimit      hardlimit    grace
  1k-blocks        2303448        10485760       10485760
     inodes          60714          200000         220000
```

When the server is restarted, it can not be entered due to Unable to open pty: No such file or directory and must be repaired with:

```
vzctl exec 110 /sbin/MAKEDEV pty
vzctl exec 110 /sbin/MAKEDEV tty
```

Before it can be used again.

Does anyone have any clues what this might be symptomatic of?

Thanks
Leo

openvz-kernel-rhel5

```
Linux ***** 2.6.18-53.1.13.el5.028stab053.10 #1 SMP Tue Apr 1 14:58:47 MSD 2008 i686 i686
i386 GNU/Linux
vzctl version 3.0.22
```

Subject: Re: VPS can not be entered

Posted by defiancenl on Wed, 06 Jan 2010 13:38:43 GMT

View Forum Message <> Reply to Message

Is this a migrations from real server to VZ?
Because all i ever seen this before is with migration from real to container.

What container template are you using?

what you could also do (its a nasty workaround),

```
cp /dev/tty* /vz/private/110/dev/
cp /dev/pty* /vz/private/110/dev/
```

on the hwnode.

Subject: Re: VPS can not be entered

Posted by leobrown on Wed, 06 Jan 2010 14:11:20 GMT

View Forum Message <> Reply to Message

Hi

No, this is not a migration, it's a new build.

Are there any other diagnostic steps I can take to find out why when I try to 'vzctl enter' the VPS I immediately receive 'Killed', and am stuck on my host system?

Leo

Subject: Re: VPS can not be entered

Posted by defiancenl on Wed, 06 Jan 2010 14:15:32 GMT

View Forum Message <> Reply to Message

What are the normal logs saying on the host?
/var/log/messages etc.....

And plz answer all the questions i make.....

What template is the container based on?

Subject: Re: VPS can not be entered
Posted by leobrown on Wed, 06 Jan 2010 14:18:42 GMT
View Forum Message <> Reply to Message

Nothing regarding that VPS! Only one TCP error logged:

TCP: time wait bucket table overflow (CT110)

Subject: Re: VPS can not be entered
Posted by defiancenl on Wed, 06 Jan 2010 14:19:47 GMT
View Forum Message <> Reply to Message

AGAIN !, plz ..... or ill stop responding ....

Answer the questions i have plz !

WHAT TEMPLATE IS THE CONTAINER BASED ON.

and you say nothing? what logs did you check ?

Subject: Re: VPS can not be entered
Posted by leobrown on Wed, 06 Jan 2010 14:30:10 GMT
View Forum Message <> Reply to Message

Hi

Sorry, defiancenl. After the first question I tried to find out, it took a bit longer than I expected. When you reply to the message on this forum, you don't see the original email above, so it's easy to forget a question!

OSTEMPLATE="centos-5-i386-default"

The host log I checked was /var/log/messages (dmesg).

Let me know if you need anything else.
Leo

Subject: Re: VPS can not be entered
Posted by defiancenl on Wed, 06 Jan 2010 14:38:05 GMT
View Forum Message <> Reply to Message

ok no problem

what does /var/log/vzctl.log give?

Subject: Re: VPS can not be entered
Posted by leobrown on Wed, 06 Jan 2010 21:48:51 GMT

View Forum Message <> Reply to Message

Right....

Nothing for that time. Just the VPS restart messages when I restarted it...

And then... grepped ALL host logs for that VPS. Nothing.

And THEN, grepped all VPS logs, and got this:

```
Jan  5 11:32:25 my-hostname xinetd[3780]: Started working: 0 available services
Jan  5 11:32:28 my-hostname avahi-daemon[3957]: Found user 'avahi' (UID 70) and group 'avahi' (GID 70).
Jan  5 11:32:28 my-hostname avahi-daemon[3957]: Successfully dropped root privileges.
Jan  5 11:32:28 my-hostname avahi-daemon[3957]: avahi-daemon 0.6.16 starting up.
Jan  5 11:32:28 my-hostname avahi-daemon[3957]: WARNING: No NSS support for mDNS detected, consider installing nss-mdns!
Jan  5 11:32:28 my-hostname avahi-daemon[3957]: dbus_bus_get(): Failed to connect to socket /var/run/dbus/system_bus_socket: No such file or directory
Jan  5 11:32:28 my-hostname avahi-daemon[3957]: WARNING: Failed to contact D-Bus daemon.
Jan  5 11:32:28 my-hostname init: no more processes left in this runlevel
```

Avahi was new to me, but I see it is a service discovery layer. This is clearly malicious and possibly the result of a rootkit. What do you think?!?

If so, manual exploit attempt, or automated? I am not seeing high numbers of reports on this approach.

After restart, I am not seeing any unusual open ports, just 22 and 80.

I am presuming you believe like me this is non-OpenVZ, so happy to close this up, but if you have any useful feedback I'd obviously be keen to hear it.

Best regards
Leo