Subject: Re: CSF xt_connlimit on vm failed
Posted by Dexus on Wed, 21 Mar 2012 08:56:25 GMT
View Forum Message <> Reply to Message

^
That is not the case here.

connlimit is working on the node and in the containers, only VZ tools are reporting this warning about unknown module...

This is from the host node with connlimit module loaded on CentOS 6...

```
# lsmod | grep connlimit
xt_connlimit           3446  1
nf_conntrack          80693  7
vzrst,xt_connlimit,nf_conntrack_ftp,iptable_nat,nf_nat,nf_conntrack_ipv4,xt_state

# iptables -A INPUT -p tcp --syn --dport 23 -m connlimit --connlimit-above 2 -j REJECT

# iptables --list -n | grep conn
REJECT     tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:23 flags:0x17/0x02 #conn/32 > 2
reject-with icmp-port-unreachable
```

As you can see it's working.

But there is still a warning on every vz tool execution...

```
# vzlist
Warning: Unknown iptable module: xt_connlimit, skipped
      CTID      NPROC STATUS    IP_ADDR         HOSTNAME
```

Here is vzlist trace, where you can see that vzlist is reporting warning after it load the modules list from vz.conf...

```
open("/etc/vz/vz.conf", O_RDONLY)       = 3
stat("/etc/vz/vz.conf", {st_mode=S_IFREG|0644, st_size=1392, ...}) = 0
fstat(3, {st_mode=S_IFREG|0644, st_size=1392, ...}) = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0x7fdafb187000
read(3, "## Global parameters\nVIRTUOZZO=y"..., 4096) = 1392
write(2, "Warning: Unknown iptable module:"..., 54Warning: Unknown iptable module:
xt_connlimit, skipped) = 54
write(2, "\n", 1
)                       = 1
read(3, "", 4096)                       = 0
```

close(3) = 0