Subject: iptables LOG
Posted by massimiliano.sciabica on Mon, 19 Mar 2012 09:59:05 GMT
View Forum Message <> Reply to Message

Hello,
I have loaded the necessary modules in CT0 (debian) and implemented a
set of iptables rules in CT150 (Centos5.7).
I added a LOG before the DROP rule in order to be informed of packet
being dropped: the rule is being matched, but I can't find any log in
/var/log/messages.

I'm not sure wether the TCP stack is in CT150 or in CT0 (I would say in
CT0, as it is kernel code), but I'm quite sure that iptables logs come
from kernel.
How can I get those logs directly in CT150?
I tried the ULOG target instead of LOG, but I'm hitting the same
problem. Would adding NET_ADMIN capability help?

Thanks

Subject: Re: iptables LOG
Posted by massimiliano.sciabica on Mon, 19 Mar 2012 21:01:41 GMT
View Forum Message <> Reply to Message

Well, the problem was the template out of which I created my VPS.
I don't know why, the line to start klogd in /etc/init.d/syslog was
commented out.
Started klogd, logs are happily showing in /var/log/messages

Subject: Re: iptables LOG
Posted by massimiliano.sciabica on Mon, 19 Mar 2012 21:08:45 GMT
View Forum Message <> Reply to Message

Well, the problem was the template out of which I created my VPS.
I don't know why, the line to start klogd in /etc/init.d/syslog was
commented out.
Started klogd, logs are happily showing in /var/log/messages

Subject: Re: iptables LOG
Posted by Aleksandar Ivanisevic on Tue, 20 Mar 2012 11:14:40 GMT
View Forum Message <> Reply to Message

Massimiliano
<massimiliano.sciabica@kiiama.com>

writes:

> Well, the problem was the template out of which I created my VPS.
> I don't know why, the line to start klogd in /etc/init.d/syslog was
> commented out.
> Started klogd, logs are happily showing in /var/log/messages

Interesting, I always thought no logging is a "feature" of openvz ;)

Now I see that klogd is also commented out in my template.

Anyone care to shed some light as to why is this done?

Subject: Re: Re: iptables LOG
Posted by massimiliano.sciabica on Tue, 20 Mar 2012 11:41:36 GMT
View Forum Message <> Reply to Message

Kernel logs are available for VPS since stable kernel release =>
2.6.32.
It looks like template creator took care to avoid launching a useless
process.
Just my opinion.

On Tue, 20 Mar 2012 12:14:40 +0100, Aleksandar Ivanisevic wrote:
> Massimiliano
> <massimiliano.sciabica@kiiama.com>
> writes:
>
>> Well, the problem was the template out of which I created my VPS.
>> I don't know why, the line to start klogd in /etc/init.d/syslog was
>> commented out.
>> Started klogd, logs are happily showing in /var/log/messages
>
> Interesting, I always thought no logging is a "feature" of openvz ;)
>
> Now I see that klogd is also commented out in my template.
>
> Anyone care to shed some light as to why is this done?
>
>

Subject: Re: Re: iptables LOG
Posted by kir on Tue, 20 Mar 2012 16:55:26 GMT
View Forum Message <> Reply to Message

>
> Kernel logs are available for VPS since stable kernel release => 2.6.32.
> It looks like template creator took care to avoid launching a useless
process.
> Just my opinion.

That's right.

If you will see klogd commented out in latest templates — please file a bug

>
>
> On Tue, 20 Mar 2012 12:14:40 +0100, Aleksandar Ivanisevic wrote:
>>
>> Massimiliano
>> <massimiliano.sciabica@kiiama.com>
>> writes:
>>
>>> Well, the problem was the template out of which I created my VPS.
>>> I don't know why, the line to start klogd in /etc/init.d/syslog was
>>> commented out.
>>> Started klogd, logs are happily showing in /var/log/messages
>>
>>
>> Interesting, I always thought no logging is a "feature" of openvz ;)
>>
>> Now I see that klogd is also commented out in my template.
>>
>> Anyone care to shed some light as to why is this done?
>>
>>

Subject: Re: Re: iptables LOG
Posted by cyrolancer on Tue, 20 Mar 2012 20:45:24 GMT
View Forum Message <> Reply to Message

Hello,

The same happens in CentOS 5.8 CT0 and Debian 6.0 VZ. I have enabled
klogd in VZ and logging works in VE right now.

uname -r
2.6.32-308.el5.028stab099.3

ls /etc/rc* | grep klogd

K03sysklogd
K03sysklogd
S16sysklogd
S16sysklogd
S16sysklogd
S16sysklogd
K03sysklogd

update-rc.d klogd defaults
update-rc.d: using dependency based boot sequencing

ls /etc/rc* | grep klogd
K01klogd
K03sysklogd
K01klogd
K03sysklogd
S16sysklogd
S17klogd
S16sysklogd
S17klogd
S16sysklogd
S17klogd
S16sysklogd
S17klogd
K01klogd
K03sysklogd

Thanks,

Onur R. Bingol

On 20.03.2012 18:55, Kir Kolyshkin wrote:
>
>

> >
> > Kernel logs are available for VPS since stable kernel release => 2.6.32.
> > It looks like template creator took care to avoid launching a
> useless process.
> > Just my opinion.
>
> That's right.
>
> If you will see klogd commented out in latest templates — please file
> a bug
>

> >
> >
> > On Tue, 20 Mar 2012 12:14:40 +0100, Aleksandar Ivanisevic wrote:
> >>
> >> Massimiliano
> >> <massimiliano.sciabica@kiiama.com
> <mailto:massimiliano.sciabica@kiiama.com>>
> >> writes:
> >>
> >>> Well, the problem was the template out of which I created my VPS.
> >>> I don't know why, the line to start klogd in /etc/init.d/syslog was
> >>> commented out.
> >>> Started klogd, logs are happily showing in /var/log/messages
> >>
> >>
> >> Interesting, I always thought no logging is a "feature" of openvz ;)
> >>
> >> Now I see that klogd is also commented out in my template.
> >>
> >> Anyone care to shed some light as to why is this done?
> >>
> >>
> >> _____
> >> Users mailing list
> >> Users@openvz.org <mailto:Users@openvz.org>
> >> https://openvz.org/mailman/listinfo/users
> >
> >
> > _____
> > Users mailing list
> > Users@openvz.org <mailto:Users@openvz.org>
> > https://openvz.org/mailman/listinfo/users
>
>
>