
Subject: Access to kernel logs in VE
Posted by [Jan Tomasek](#) on Fri, 29 Dec 2006 14:11:18 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello,

I need advice how to konfigure kernel logging for VE. I'm interested in iptables logs. By default all log messages goes to log files of HW node. That can get really messy when number of VE is growing.

Is there some chance how to pass log files to VE to which they belong?

Thanks for help

--

Jan Tomasek aka Semik
<http://www.tomasek.cz/>

Subject: Re: Access to kernel logs in VE
Posted by [Mishin Dmitry](#) on Fri, 29 Dec 2006 14:18:40 GMT
[View Forum Message](#) <> [Reply to Message](#)

On Friday 29 December 2006 17:11, Jan Tomasek wrote:

> Hello,

>

> I need advice how to konfigure kernel logging for VE. I'm interested in
> iptables logs. By default all log messages goes to log files of HW node.
> That can get really messy when number of VE is growing.

It was recently fixed for devel kernels - you may use ipt_LOG for logging to per-VE log, as it is for stable kernels quite a long ago.

--

Thanks,
Dmitry.

Subject: Re: Access to kernel logs in VE
Posted by [Jan Tomasek](#) on Fri, 29 Dec 2006 14:44:04 GMT
[View Forum Message](#) <> [Reply to Message](#)

Dmitry Mishin wrote:

> On Friday 29 December 2006 17:11, Jan Tomasek wrote:

>> Hello,

>>

>> I need advice how to konfigure kernel logging for VE. I'm interested in
>> iptables logs. By default all log messages goes to log files of HW node.

>> That can get really messy when number of VE is growing.
> It was recently fixed for devel kernels

I'm using 2.6.18-028test007. Is it in there?

> - you may use ipt_LOG for logging to
> per-VE log, as it is for stable kernels quite a long ago.

I'm using in iptables:

```
$IPT -A ssh -i $EXTERNAL -p tcp -m limit --limit $LIMIT -j LOG  
--log-prefix "wiki: DROP-ssh "
```

But it ends in HW node logs. Where is syslog in VE supposed to listen?
I'm using syslog-ng with this setup:

```
source src {  
    pipe("/proc/kmsg" log_prefix("kernel: "));  
    unix-dgram("/dev/log");  
    internal();  
};
```

and it receive nothing.

Thanks for you help Dmitry!

--

Jan Tomasek aka Semik
<http://www.tomasek.cz/>

Subject: Re: Access to kernel logs in VE
Posted by [Mishin Dmitry](#) on Fri, 29 Dec 2006 16:01:12 GMT
[View Forum Message](#) <> [Reply to Message](#)

On Friday 29 December 2006 17:44, Jan Tomasek wrote:

> Dmitry Mishin wrote:

> > On Friday 29 December 2006 17:11, Jan Tomasek wrote:

> >> Hello,

> >>

> >> I need advice how to konfigure kernel logging for VE. I'm interested in
> >> iptables logs. By default all log mesages goes to log files of HW node.

> >> That can get really messy when number of VE is growing.

> > It was recently fixed for devel kernels

>

> I'm using 2.6.18-028test007. Is it in there?

No, it is git version only right now.

<http://git.openvz.org/?p=linux-2.6.18-openvz;a=commit;h=356e4674820ed23c9410f7870def17b70>

f4fddac

>
> > - you may use ipt_LOG for logging to
> > per-VE log, as it is for stable kernels quite a long ago.
>
> I'm using in iptables:
>
> \$IPT -A ssh -i \$EXTERNAL -p tcp -m limit --limit \$LIMIT -j LOG
> --log-prefix "wiki: DROP-ssh "
Yes, it is ipt_LOG target and it is fixed by above commit. Just wait for next kernel or apply above patch yourself.

>
> But it ends in HW node logs. Where is syslog in VE supposed to listen?
> I'm using syslog-ng with this setup:
>
> source src {
> pipe("/proc/kmsg" log_prefix("kernel: "));
> unix-dgram("/dev/log");
> internal();
> };
>
> and it receive nothing.

--
Thanks,
Dmitry.
