Subject: Using tools like fail2ban
Posted by joelee on Wed, 02 Apr 2008 17:14:34 GMT
View Forum Message <> Reply to Message

Hi All,

I am using a tool like fail2ban which automatically monitors logs and blocks IP addresses doing brute force attacks. Currently, I install this tool on a per-vps basis.

Fail2ban info can be found here: http://fail2ban.org/wiki/index.php/Main_Page

I wanted to see about using this on the OpenVZ Host Node so that I do not have to install and config on each vps. I wanted to see how others are using tools like this and what approach is being used.

From what I gather, installing this on HN will one keep the config files away from the users of VPS and only openvz HN admin would be able to view and monitor logs. Plus, nothing prevents the user of the vps to install a separate install in there vps as well.

I know it's not advised to install these types of apps on the HN but this is the most efficient. Would appreciate any comments/suggestions.

Joe

Subject: fail2ban for all containers
Posted by narcisgarcia on Mon, 20 Dec 2010 22:37:25 GMT
View Forum Message <> Reply to Message

I've tested the following and works configured on the hardware node (host):

/etc/fail2ban/jail.local
[ssh-container-777]
enabled = true
filter = sshd
logpath = /vz/private/777/var/log/auth.log
maxretry = 6
action = route

/etc/fail2ban/action.d/route.conf
Fail2Ban configuration file
#
Author: Narcis Garcia, based on FAQforge admin idea.
#
$Revision: 1 $
#

```
[Definition]

# Option:  actionstart
# Notes.:  command executed once at the start of Fail2Ban.
# Values:  CMD
#
actionstart =

# Option:  actionstop
# Notes.:  command executed once at the end of Fail2Ban
# Values:  CMD
#
actionstop =

# Option:  actioncheck
# Notes.:  command executed once before each actionban command
# Values:  CMD
#
actioncheck =

# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    <ip>  IP address
#          <failures>  number of failures
#          <time>  unix timestamp of the ban time
# Values:  CMD
#
actionban = ip route add prohibit <ip>

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    <ip>  IP address
#          <failures>  number of failures
#          <time>  unix timestamp of the ban time
# Values:  CMD
#
actionunban = ip route del prohibit <ip>

[Init]

# Defaut variable values
#
name = default
```

Subject: Re: Using tools like fail2ban
Posted by narcisgarcia on Mon, 20 Dec 2010 22:41:48 GMT
View Forum Message <> Reply to Message

I've also specified:
logpath = /vz/private/*/var/log/auth.log
and fail2ban loads all the "auth.log" files, but aren't procesed well. I suppose there is a date&time sort problem for the text lines.

I don't know how to sort properly by date and time this:
cat /vz/private/*/var/log/auth.log

Subject: Re: Using tools like fail2ban
Posted by narcisgarcia on Tue, 21 Dec 2010 09:13:22 GMT
View Forum Message <> Reply to Message

Correction:
fail2ban loads all the "auth.log" files and processes them well; not as 1 unified file, it processes one by one independly.