
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]

```
# Default variable values
#
name = default
```
