

Hướng dẫn cài đặt Fail2Ban cho SSH trên CentOS 6

admin Sun, Apr 14, 2019 [Cài Đặt Cơ Bản & Hướng Dẫn](#) 0 1781



Fail2Ban là một ứng dụng chạy nền theo dõi log file để phát hiện những địa chỉ IP đang nhập sai password SSH nhiều lần. Sau đó, Fail2Ban sẽ dùng **iptables firewall rules** để block ngay địa chỉ IP với một khoảng thời gian ngắn nhất định.

Cài đặt Fail2Ban

Chúng ta sẽ cài đặt Fail2Ban thông qua Repo EPEL

```
# yum install epel-release# yum install fail2ban
```

Cấu hình Fail2Ban

```
# nano /etc/fail2ban/jail.conf
```

Sau khi cài đặt xong, bạn mở file cấu hình của Fail2Ban lên sẽ thấy một số thông số như sau:

```
[DEFAULT]# "ignoreip" can be an IP address, a CIDR mask or  
a DNS host. Fail2ban will not# ban a host which matches a
```

```
n address in this list. Several addresses can be# defined
using space separator.ignoreip = 127.0.0.1# "bantime" is t
he number of seconds that a host is banned.bantime = 600#
A host is banned if it has generated "maxretry" during the
last "findtime"# seconds.findtime = 600# "maxretry" is th
e number of failures before a host get banned.maxretry = 3
```

Trong đó

- **ignoreip**: không block những địa chỉ này
- **bantime**: khoảng thời gian (giây) block IP
- **findtime**: khoảng thời gian (giây) mà IP phải login thành công
- **maxretry**: số lần login thất bại

Cấu hình mặc định của Fail2Ban khá là đơn giản, chúng ta không cần thiết phải cấu hình mà chỉ cần bật theo.

Cấu hình Fail2Ban cho SSH

Tạo file cấu hình

```
# nano /etc/fail2ban/jail.local
```

Và sẽ dùng nội dung sau:

```
GNU nano 2.0.9 File: /etc/fail2ban/jail.local Modified
[ssh-iptables]
enabled = true
filter = sshd
action = iptables[name=SSH, port=ssh, protocol=tcp]
#       sendmail-whois[name=SSH, dest=root, sender=fail2ban@example.com]
logpath = /var/log/secure
maxretry = 2
bantime = 3600
```

Trong đó

- **enabled**: kích hoạt báo v?, nếu muốn tắt báo hãy chuyển thành false
- **filter**: ghi mã cảnh báo sẽ dùng file cấu hình /etc/fail2ban/filter.d/sshd.conf
- **action**: fail2ban sẽ ban địa chỉ IP nếu match filter /etc/fail2ban/action.d/iptables.conf. Nếu bạn muốn thay đổi port ssh, sẽ ảnh hưởng port=ssh bằng port mới, ví dụ port=2222
- **logpath**: đường dẫn file log fail2ban sẽ dùng theo dõi
- **maxretry**: số lần login thất bại

Khởi động Service Fail2Ban

```
# chkconfig --level 23 fail2ban on# service fail2ban start
```

Cùng check lại iptables xem đã có rule của Fail2Ban chưa:

```
# iptables -L
```

```

Running Transaction
  Installing : nano-2.0.9-7.el6.x86_64                1/1
  Verifying  : nano-2.0.9-7.el6.x86_64                1/1

Installed:
  nano.x86_64 0:2.0.9-7.el6

Complete!
[root@postbai ~]# nano /etc/fail2ban/jail.conf
[root@postbai ~]# nano /etc/fail2ban/jail.local
[root@postbai ~]# chkconfig --level 23 fail2ban on
[root@postbai ~]# service fail2ban start
Starting fail2ban:                                     [ OK ]
[root@postbai ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
f2b-SSH    tcp  --  anywhere              anywhere            tcp dpt:ssh
ACCEPT    all  --  anywhere              anywhere            state RELATED,ESTABLISH
ED
ACCEPT    icmp --  anywhere              anywhere
ACCEPT    all  --  anywhere              anywhere
ACCEPT    tcp  --  anywhere              anywhere            state NEW tcp dpt:ssh
REJECT    all  --  anywhere              anywhere            reject-with icmp-host-p
rohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
REJECT    all  --  anywhere              anywhere            reject-with icmp-host-p
rohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain f2b-SSH (1 references)
target     prot opt source                destination
RETURN    all  --  anywhere              anywhere

```

Theo dõi SSH login

Bạn có thể sử dụng lệnh sau để biết được VPS/Server đã từng bị tấn công SSH chưa:

```
# cat /var/log/secure | grep 'Failed password' | sort | un  
iq -c
```

Kết quả thường sẽ là như bên dưới, đã từng có rất nhiều kết quả như sau:

```
[root@postbai ~]# cat /var/log/secure | grep 'Failed password' | sort | uniq -c  
      1 Mar 24 04:34:07 postbai sshd[1504]: Failed password for root from 116.***.***.147  
port 17143 ssh2  
      1 Mar 24 04:34:16 postbai sshd[1504]: Failed password for root from 116.***.***.147  
port 17143 ssh2  
      1 Mar 24 04:34:19 postbai sshd[1504]: Failed password for root from 116.***.***.147  
port 17143 ssh2  
      1 Mar 24 04:39:14 postbai sshd[1588]: Failed password for root from 116.***.***.147  
port 33292 ssh2  
      1 Mar 24 04:39:23 postbai sshd[1588]: Failed password for root from 116.***.***.147  
port 33292 ssh2  
      1 Mar 24 04:39:25 postbai sshd[1588]: Failed password for root from 116.***.***.147  
port 33292 ssh2  
      1 Mar 24 04:44:57 postbai sshd[1590]: Failed password for root from 116.***.***.147  
port 41974 ssh2  
      1 Mar 24 04:44:59 postbai sshd[1590]: Failed password for root from 116.***.***.147  
port 41974 ssh2  
      1 Mar 24 04:45:01 postbai sshd[1590]: Failed password for root from 116.***.***.147  
port 41974 ssh2  
      1 Mar 24 04:50:13 postbai sshd[1593]: Failed password for root from 116.***.***.147  
port 27766 ssh2
```

Để xem IP đã bị banned bởi Fail2Ban như sau đây:

```
# fail2ban-client status ssh-iptables
```

Output thường sẽ có dạng như thế này:

```
Status for the jail: ssh-iptables|- Filter| |- Currently f  
ailed: 1| |- Total failed: 6| `-- File list: /var/log/secur  
e`- Actions|- Currently banned: 1|- Total banned: 1`- Bann  
ed IP list: 116.***.***.147(ip bị banned)
```

?? xóa IP khỏi danh sách banned, b?n s? d?ng l?nh sau

```
# fail2ban-client set ssh-iptables unbanip 116.***.***.147  
(ip mu?n xóa khỏi danh sách banned)
```

Hi v?ng v?i **Fail2Ban**, chúng ta s? ng?n ch?n ???c các cu?c t?n công s? b? vào SSH, h?n g?p l?i các b?n trong các bài ti?p theo, chúc các b?n thành công.

Online URL: <https://huongdan.maxserver.com/article-85.html>