

# Diadem Web Hosting Knowledgebase

You are logged in as: **anirban.das**

[Admin Area](#) | [My Account](#) | [Logout](#)

				<b>Manage</b>
<b>Knowledgebase</b>	<b>Downloads</b>	<b>Glossary</b>	<b>Diadem Technologies</b>	

Search: [Advanced search](#)

 » 

## Knowledgebase

### Linux Server Management

...

- [Setup VPS with Tomcat 7, JDK 1.7 a...](#)
- [Install http in CentOS Using YUM](#)
- [Procedure for Website & DB Backup...](#)
- [Enabling KVM with CentOS 7](#)
- [Block SSLv3 Poodle exploit in Plesk ...](#)
- [Mysql Management](#)
- [Install Linux Malware Detect \(Malde...](#)
- [Mailpiler Setup on CentOS 6.x](#)
- [Enable mod\\_evasive with Apache](#)
- [Block DDOS attacks to apache serve...](#)
- [MailerQ setup with Rabbitmq](#)
- [Zabbix Upgrade/installation Process](#)
- [Webmin DNS Server Migration Steps](#)
- [Fail2ban Configuration for Plesk VMs](#)
- [Generating Markettammer Server D...](#)
- [SAMBA - Linux to Windows file Shari...](#)
- [Howto upgrade PHP from 5.1 to 5.3...](#)
- [Spamhaus RBL Checklist + CSF conf...](#)
- [CloudLayer Storage with Linux](#)
- [Crontab Information](#)
- [Partitioning information of Linux ser...](#)
- [Resizing a partition by adding new h...](#)
- [Common MySQL Commands](#)
- [Sys Admin Activities \(Ankur\)](#)
- [Secondary DNS server overview](#)
- [Show all...](#)
- [R1Soft CDP](#)
- [Archived](#)
- [CPanel](#)
- [Linux Scripts](#)
- [Ubuntu](#)
- [Postfix MTA](#)

[KB Home](#) / [Linux Server Management](#) / Fail2ban Configuration for Plesk VMs

## Fail2ban Configuration for Plesk VMs

### Step-01

We need to download repo and using that fail2ban package can be installed (for RHEL6/CentOS6)

```
# rpm -Uvh
http://download.fedoraproject.org
/pub/epel/6/i386/epel-release-
6-7.noarch.rpm
```

Article ID: 550

Last updated: 21 Feb, 2015

Private

[Print](#)

[Export to PDF](#)

[Add comment](#)

Views: 91

Comments: 0

[Edit article](#)

[Quick edit](#)

[Category listing](#)

### Step-02

```
# yum install fail2ban <To install
package>
```

### Step-03

```
# cp /etc/fail2ban/jail.conf
/etc/fail2ban/jail.local <After installing fail2ban "jail.conf" is
configured and should be renamed as "jail.local">
```

### Step-04

Now open "jail.local" file and make necessary changes for individual service.

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

### Step-05

We will first enable the ssh filter as per below option:

```
[ssh-iptables]
enabled = true
filter = sshd
action = iptables[name=SSH, port=ssh, protocol=tcp]
        sendmail-whois[name=SSH,
dest=anirbanmukherjee1989@gmail.com,
sender=fail2ban@example.com]
logpath = /var/log/secure
maxretry = 5
```

**\*\* According to the settings if someone try to login via ssh with wrong password that ip will be blocked and notification mail be sent to mentioned email id.**

### Step-06

Restart the fail2ban service

```
# service fail2ban restart < It will show the services parameter>
```

To check wheather it is blocked - run below command

**# iptables -L <After enabling this on individul service status is found>**

#### Step-07

Now we will try to block invalid courier login (pop3) and need following entry in the configuration file- **jail.local**

##### [courierimap-iptables]

**enabled = true filter = courierlogin**

**action = iptables-multiport[name=IMAP, port="110,995,143,993"]**

**sendmail-whois[name=IMAP,**

**dest=anirbanmukherjee1989@gmail.com,**

**sender=f2b@thebengalclub.com]**

**logpath = /usr/local/psa/var/log/maillog**

**maxretry = 2**

#### Step -08

To enable this setting we need to edit below mentioned file

**# vi /etc/fail2ban/filter.d/courierlogin.conf**

and put below value

**failregex = LOGIN FAILED, ip= \[<HOST>\]\$**

#### Step 09

then save and exit

#### Step - 10

Now we will try to block invalid webmail login and need following change in configuration file,

##### [horde-iptables]

**enabled = true**

**filter = hordellogin**

**action = iptables-multiport[name=HORDE, port="80,443,143"]**

**sendmail-whois[name=HORDE,**

**dest=anirbanmukherjee1989@gmail.com,**

**sender=f2b@thebengalclub.com]**

**logpath = /var/log/psa-horde/psa-horde.log**

**maxretry = 3**

**bantime = 300**

#### Step-11

To activate this setting we need to create the below mentioned file

**# vi /etc/fail2ban/filter.d/hordellogin.conf**

and put below value

**failregex = FAILED LOGIN for \*.\* \[<HOST>\] .\*\$**

#### Step - 12

Then save and exit and restart fail2ban service.

**# service fail2ban restart**

**# chkconfig fail2ban on**

#### Note:

To forcefully unblock an IP from iptables during the duration in which it is blocked, the following commands can be used:

**# iptables-save | grep 122.160.113.253 <To View Block ip status>**

**# iptables -D fail2ban-HORDE -s 122.160.113.253/32 -j DROP <To  
release Blocked ip within the blocked duration>**

---

This article was: [Helpful](#) | [Not helpful](#)

[Add  
comment](#)

---

[Prev](#)

[Next](#)

Webmin DNS Server Migration Steps

Generating Markettammer Server  
Daily uptime to a Log file

---

[Powered by KBPublisher](#) (Knowledge base software)

