

**Apache2 : Configure mod evasive2022/05/17** 

```
Enable mod evasive module to defend from DoS attacks and so on.
[1] Install and configure mod evasive.
root@www:~#
apt -y install libapache2-mod-evasive
root@www:~#
vi /etc/apache2/mods-available/evasive.conf
# uncomment each line to configure
<IfModule mod_evasive20.c>
    # hash table size
    DOSHashTableSize
    # threshold for the number of requests for the same page per page interval
    DOSPageCount
    # threshold for the total number of requests for any object by the same client on the same listener per site interval
    DOSSiteCount
                         50
    # the interval for the page count threshold
    DOSPageInterval
    # the interval for the site count threshold
    DOSSiteInterval
                         1
    # amount of time (in seconds) that a client will be blocked for if they are added to the blocking list
    DOSBlockingPeriod
                         10
    # uncomment and configure follows if you need
    # notification address if IP address becomes blacklisted
    #DOSEmailNotify
                          root@localhost
    # possible to set any command
                           "su - someuser -c '/sbin/... %s ...'"
    #DOSSystemCommand
    # log directory
    #DOSLogDir
                           "/var/log/mod-evasive"
</IfModule>
root@www:~#
mkdir /var/log/mod-evasive
root@www:~#
chown www-data:www-data/var/log/mod-evasive
```

```
root@www:~#
systemctl reload apache2
[2] Test to access to Apache2.
root@www:~#
for ((i=1; i \le 20; i++)); do curl -I localhost; done
HTTP/1.1 200 OK
Date: Wed, 30 Nov 2022 04:10:38 GMT
Server: Apache/2.4.52 (Ubuntu)
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Wed, 30 Nov 2022 02:11:50 GMT
ETag: "29af-5eea6a09cf7d9"
Accept-Ranges: bytes
Content-Length: 10671
Vary: Accept-Encoding
Content-Type: text/html
HTTP/1.1 200 OK
Date: Wed, 30 Nov 2022 04:10:38 GMT
Server: Apache/2.4.52 (Ubuntu)
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Wed, 30 Nov 2022 02:11:50 GMT
ETag: "29af-5eea6a09cf7d9"
Accept-Ranges: bytes
Content-Length: 10671
Vary: Accept-Encoding
Content-Type: text/html
HTTP/1.1 200 OK
Date: Wed, 30 Nov 2022 04:10:38 GMT
Server: Apache/2.4.52 (Ubuntu)
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Wed, 30 Nov 2022 02:11:50 GMT
ETag: "29af-5eea6a09cf7d9"
Accept-Ranges: bytes
Content-Length: 10671
Vary: Accept-Encoding
Content-Type: text/html
# turn to "403 Forbidden" if blocked
HTTP/1.1 403 Forbidden
Date: Wed, 30 Nov 2022 04:10:38 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1
HTTP/1.1 403 Forbidden
Date: Wed, 30 Nov 2022 04:10:38 GMT
Server: Apache/2.4.52 (Ubuntu)
Content-Type: text/html; charset=iso-8859-1
. . . . .
. . . . .
# if blocked, logs are recorded
root@www:~#
11 /var/log/mod-evasive
total 12
drwxr-xr-x 2 www-data www-data 4096 Nov 30 13:16 ./
drwxrwxr-x 11 root syslog 4096 Nov 30 13:16 ../
-rw-r--r-- 1 www-data www-data 5 Nov 30 13:16 dos-127.0.0.1
# if set notification, it is sent like follows
root@www:~#
mail
Mail version 8.1.2 01/15/2001. Type ? for help.
"/var/mail/root": 1 message 1 unread
>U 1 www-data@www.srv. Wed Nov 30 13:16 20/621
& 1
Message 1:
```

5/10/24, 6:14 PM

From www-data@www.srv.world Wed Nov 30 13:16:38 2022

X-Original-To: root@localhost

To: root@localhost MIME-Version: 1.0

Content-Type: text/plain; charset="ANSI\_X3.4-1968"

Content-Transfer-Encoding: 8bit

Date: Wed, 30 Nov 2022 13:16:38 +0900 (JST) From: www-data <www-data@www.srv.world>

To: root@localhost

Subject: HTTP BLACKLIST 127.0.0.1

mod\_evasive HTTP Blacklisted 127.0.0.1

## Matched Content

## Ubuntu 22.04 : Apache2

- (16) Configure mod\_http2
- (17) Configure mod\_evasive
- (18) Log Report : AWStats
- (19) Blog System: WordPress
- (20) Web Mail: RoundCube

[ Previous Page ]

Sponsored Link

Copyright © 2007-2024 Server World All Rights Reserved.