

Ubuntu20.04???Apache?DoS???? ?(mod_evasive)????

??

DoS/DDoS????????Apache????????

??

- Ubuntu 20.04
- Apache 2.4?
- FW?ufw??

????????

1. mod_evasive????????
2. apache2?????(www-data)?ufw????????
3. mod_evasive????????
4. ?????????

????????????????????

mod_evasive??????

```
sudo aptitude install libapache2-mod-evasive
```

????postfix????????????????????????????????AWS????????????????????????????

apache2????????

????www-data?ufw????????????????????????????????

- sudoers????????

```
sudo cp -pi /etc/sudoers /path/to/backup/directory/sudoers.$(date +%Y%m%d)
```

????????????????

- diff????????

```
sudo diff -u /path/to/backup/directory/sudoers.$(date +%Y%m%d) /etc/sudoers
```

????????????

- ?????

```
echo 'www-data ALL=(ALL) NOPASSWD: /usr/sbin/ufw' | sudo tee -a /etc/sudoers
```

- ???????

```
sudo diff -u /path/to/backup/directory/sudoers.$(date +%Y%m%d) /etc/sudoers
```

????????????

```
+www-data ALL=(ALL) NOPASSWD: /usr/sbin/ufw
```

evasive????

- ?????????

```
sudo cp -pi /etc/apache2/mods-available/evasive.conf /path/to/backup/directory/evasive.conf.$(date +%Y%m%d)
```

- diff????????

```
sudo diff -u /path/to/backup/directory/evasive.conf.$(date +%Y%m%d) /etc/apache2/mods-available/evasive.conf
```

????????????

- ?????????????????????
 - /etc/apache2/mods-available/evasive.conf
- ??

```
DOSHashTableSize 3097
DOSPageCount     100
DOSSiteCount     100
#[]
DOSPageInterval  1
DOSSiteInterval  1
DOSBlockingPeriod 10

#DOSEmailNotify  you@yourdomain.com
#[]
DOSSystemCommand "sudo ufw deny proto tcp from %s to any port 80,443"
# []80/443[]
DOSLogDir         "/var/log/mod_evasive"
DOSWhitelist      127.0.0.1
```

DOSWhitelist xx.xx.xx.xx

[] [] [] [] [] [] P [] [] [] [] [] [] [] [] [] []

?? [Apache ? DoS???????? mod_evasive](#)

- ?????

```
sudo diff -u /path/to/backup/directory/evasive.conf.$(date +%Y%m%d) /etc/apache2/mods-available/evasive.conf
```

- ???

```
- #DOSHashTableSize 3097
- #DOSPageCount      2
- #DOSSiteCount       50
- #DOSPageInterval    1
- #DOSSiteInterval    1
- #DOSBlockingPeriod  10
+ DOSHashTableSize 3097
+ DOSPageCount      100
+ DOSSiteCount       100
+ DOSPageInterval    1
+ DOSSiteInterval    1
+ DOSBlockingPeriod  10

#DOSEmailNotify  you@yourdomain.com
- #DOSSystemCommand  "su - someuser -c '/sbin/... %s ...'"
- #DOSLogDir          "/var/log/mod_evasive"
+ DOSSystemCommand  "sudo ufw deny proto tcp from %s to any port 80,443"
+ DOSLogDir          "/var/log/mod_evasive"
+ DOSWhitelist        127.0.0.1
+ DOSWhitelist        xx.xx.xx.xx
</IfModule>
```

????

- ???

```
sudo apache2ctl configtest
```

Syntax OK ??????

- apache??

```
sudo systemctl restart apache2.service
```

????????????????????ufw????????????

Revision #1

Created 16 August 2024 11:51:27 by manualmaton

Updated 5 September 2024 11:34:59 by manualmaton