Apache?????

- Ubuntu20.04????Apache?DoS???????(mod_evasive)????
- Ubuntu????Mod_Security????
- Mod_Security??????????????Nextcloud?????????
- Ubuntu 24.04????mod_dosdetector????

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
    #かなり緩く設定して、後で狭めていった方が偽陽性を防げます。
    DOSPageInterval     1
    DOSSiteInterval     1
    DOSBlockingPeriod   10

    #DOSEmailNotify      you@yourdomain.com
    #メール通知を行わないため、ここを省いています
    DOSSystemCommand    "sudo ufw deny proto tcp from %s to any port 80,443"
    # 検証時に自分のサイトがブロックされるのを防ぐため、ポートは80/443に絞っています
    DOSLogDir           "/var/log/mod_evasive"
    DOSWhitelist        127.0.0.1
    DOSWhitelist        xx.xx.xx.xx
```

```
    # □□□□□□□IP□□□□□□□□□□□□□
```

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

Ubuntu????Mod_Security????

Apache?WAF????????mod_security???????

- AWS Lightsail??????????????
- ?????IP???????????

??????????????????????????????Web Arena???????????????

??

- Ubuntu 24.04 (20.04????????????)
- Apache 2.4

? ????????aptitude??????????????apt???????????

?????????

1. mod_security?????????????
2. mod_security?????????
3. Apache??????????mod_security????????
4. ???????????????

mod_security?????????????

- ??????????????

```
sudo aptitude update
```

- mod_security??????

```
sudo aptitude install libapache2-mod-security2
```

- ????????

```
sudo apache2ctl -M |grep security
```

```
security2_module (shared)
```

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

ModSecurity???

- ??????????

```
sudo mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

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

OWASP Core Rule Set (CRS)??????????

- ????????

```
cd /usr/share/modsecurity-crs && pwd
```

- ?????????????

```
sudo git clone https://github.com/coreruleset/coreruleset.git
```

- ?????????????

```
sudo mv /usr/share/modsecurity-crs/coreruleset/crs-setup.conf.example /usr/share/modsecurity-crs/coreruleset/crs-setup.conf
```

mod_security??????CRS??????????

- ????????

```
cd /etc/apache2/mods-available/ && pwd
```

- ???????????

```
sudo cp -pi security2.conf /path/to/backup/directory/security2.conf.$(date +%Y%m%d)
```

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

- ????????

```
diff -u /path/to/backup/directory/security2.conf.$(date +%Y%m%d) security2.conf
```

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

- ??????

`/etc/apache2/mods-available/security2.conf` ??????????????????????????????????????root???

```
- </IfModule>
+       # Include OWASP ModSecurity CRS rules if installed
+       IncludeOptional /usr/share/modsecurity-crs/*.load
+</IfModule>
```

- ???????????

```
sudo apache2ctl configtest
```

`Syntax OK`???????

- Apache???

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

- Apache?????

```
systemctl status apache2.service
```

`active (running)` ???????

Apache???????????

?????Apache??

- ????????

```
cd /etc/apache2/sites-available && pwd
```

- ??????????????????????

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

.conf???????????????????????????????

- ????????

```
diff -u /path/to/backup/directory/your_site.conf.$(date +%Y%m%d) your_site.conf
```

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

- ??????

`/etc/apache2/sites-available/your_site.conf` ????????????????????????????????????root???

```
# Mod Security


## ModSecurity有効化
SecRuleEngine On
## ModSecurity検知モード
### 検知モードで動かす場合はSecRuleEngine Onをコメントアウトしてこちらを有効化します
```

```
#SecRuleEngine DetectionOnly

## ファイルのアップロードをできるようにします。
SecRequestBodyInMemoryLimit 524288000
SecRequestBodyLimit 524288000

## テスト用の検知パラメータを付け加えます。
    SecRule ARGS:modsecparam "@contains test" "id:4321,deny,status:403,msg:'ModSecurity test rule has triggered'"
```

- ??????

```
diff -u /path/to/backup/directory/your_site.conf.$(date +%Y%m%d) your_site.conf
```

```
+# Mod Security
+
+## ModSecurity有効化
+SecRuleEngine On
+## ModSecurity検知モード
+### 検知モードで動かす場合はSecRuleEngine Onをコメントアウトしてこちらを有効化します
+#SecRuleEngine DetectionOnly
+
+## ファイルのアップロードをできるようにします。
+SecRequestBodyInMemoryLimit 524288000
+SecRequestBodyLimit 524288000
+
+## テスト用の検知パラメータを付け加えます。
+    SecRule ARGS:modsecparam "@contains test" "id:4321,deny,status:403,msg:'ModSecurity test rule has triggered'"
+
```

- ???????????

```
sudo apache2ctl configtest
```

`Syntax OK`???????

- Apache???

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

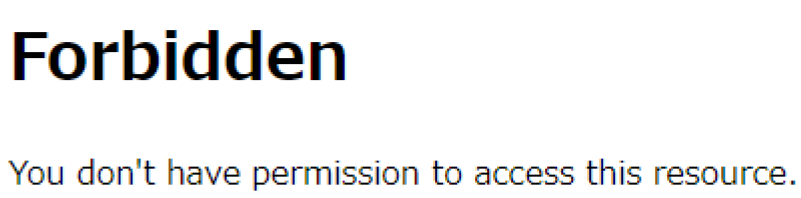
- Apache?????

```
systemctl status apache2.service
```

`active (running)` ???????

mod_security????

1. ??????????????Web?????????????????????????
2. ??????????`?modsecparam=test`?????????????



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

????????

```
sudo cat /path/to/sites_log/directory/sites_error.log
```

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

????

```
ModSecurity: Access denied with code 403 (phase 2). String match "test" at ARGS:modsecparam. [file "/etc/apache2/sites-enabled/your_site.conf"] [line "53"] [id "4321"] [msg "ModSecurity test rule has triggered"] [hostname "host_address"] [uri "/"] [unique_id "xxxxxxx"]
```

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

??

Wordpress?Redmine??Web???(???)

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

```
## ModSecurity有効化
#SecRuleEngine On
## ModSecurity検知モード
### 検知モードで動かす場合はSecRuleEngine Onをコメントアウトしてこちらを有効化します
SecRuleEngine DetectionOnly
```

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

Mod_Security??????????????Next cloud?????????

Nextcloud?mod_security??Mod_security????????????????????????????

????

1. ?????????????
2. ?????????
3. ???????????????

??????

????

`/var/log/nextcloud_error.log`??????????????????

```
[Wed Sep 11 16:35:02.048442 2024] [security2:error] [pid 32762:tid 32762] [client aaa.bbb.ccc.ddd:56994] [client aaa.bbb.ccc.ddd] ModSecurity: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "92"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 5 - SQLI=0,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 5, 0, 0, 0"] [ver "OWASP_CRS/3.3.5"] [tag "event-correlation"] [hostname "nextcloud.hoge.com"] [uri "/ocs/v2.php/apps/user_status/api/v1/heartbeat"] [unique_id "ZuFIJU_udFaqxqrJvRLaPQAAAAA"]
```

????????

- ???????IP????
- ????????ID?
- ??????????

???

???????????

???????????copilot???????awk????????????

```
awk '/ModSecurity/ {
ip = gensub(/.*\[client ([0-9.]+):.*/, "\\1", "g", $0);
rule_id = gensub(/.*\[id "([0-9]+)"\].*/, "\\1", "g", $0);
print rule_id, ip;
```

```
}' /var/log/nextcloud/nextcloud_error.log | sort | uniq -c
```

???????????Mod_Security???????????????

```
 36 911100 127.0.0.1
267 911100 aaa.bbb.ccc.ddd
 65 920420 aaa.bbb.ccc.ddd
 36 949110 127.0.0.1
267 949110 aaa.bbb.ccc.ddd
 36 980130 127.0.0.1
267 980130 aaa.bbb.ccc.ddd
```

??????????????127.0.0.1?????????aaa.bbb.ccc.ddd????????????IP??????????????????Nextcloud???????????????????

Mod_security????????ID????????????????????

Mod_Security???????????????

Apache??????????????????????????

?????????

- ???????????

```
sudo cp -ci /etc/apache2/sites-available/nextcloud.conf /path/to/backup/directory/nextcloud.conf.$(date +%Y%m%d)
```

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

- ????????

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

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

- ??????

`/etc/apache2/sites-available/nextcloud.conf` ????????????????(?root??)

```
# Mod_security
## □□□□□□□□

SecRuleEngine DetectionOnly

## □□□□□□□□ID
```

```
SecRuleRemoveById 911100
SecRuleRemoveById 920420
SecRuleRemoveById 949110
SecRuleRemoveById 980130
```

- ????????

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

`SecRuleRemoveById ID` ??????????????????????

- ???

```
 ## 最初は検知モード

 SecRuleEngine DetectionOnly
+
+## 偽陽性と判断したID
+SecRuleRemoveById 911100
+SecRuleRemoveById 920420
+SecRuleRemoveById 949110
+SecRuleRemoveById 980130
+
 </VirtualHost>
```

???????????

- ????

```
sudo apache2ctl configtest
```

`Syntax OK` ???????

- ????

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

- Apache????

```
systemctl status apache2.service
```

`active(running)` ???????

????

??????

```
tail -f /var/log/nextcloud/nextcloud_error.log
```

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

- ????????Nextcloud???????????????
- ??????ID???????????????

Ubuntu 24.04????mod_dosdetector????

??

???Web????????????????????????????mod_dosdetector????????

mod_dosdetector ??Apache HTTP Server ?????????DoS?Denial of Service????????????????????????????????????IP????????????????????????????????????IP????????????????????????????????????

mod_evasive?????

- ?????????
- ?????????????

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

??

- Ubuntu 24.04
- Apache 2.4
  - Apache2-dev??????????????????????

?????????

1. git???????????????
2. Makefile???????????????????
3. ?????????????
4. ????????Apache????????

mod_dosdetector???????

- ??????????????

```
cd /usr/local/src && pwd
```

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

- git clone

```
sudo git clone https://github.com/stanaka/mod_dosdetector.git
```

- ?????????????

```
cd mod_dosdetector && pwd
```

Makefile???????????

- Makefile??

??????Makefile?`/usr/sbin/apxs`???????????????

```
sudo sed -i 's|^APXS=.*|APXS=/usr/bin/apxs|' Makefile
```

- ??????

```
sudo make install
```

- ????????

```
cat /etc/apache2/mods-available/dosdetector.load
```

`LoadModule dosdetector_module /usr/lib/apache2/modules/mod_dosdetector.so`????????

????????

??: [mod_dosdetector??????????????????]

```
sudo tee /etc/apache2/mods-available/dosdetector.conf > /dev/null <<EOF
<IfModule dosdetector_module>
DoSDetection on
DoSPeriod 60
DoSThreshold 5
DoSHardThreshold 10
DoSBanPeriod 60
DoSTableSize 100
DoSIgnoreContentType ^(image/|application/|text/javascript|text/css)
</IfModule>
EOF
```

- DoSDetection on
  - ??: DoS (Denial of Service) ??????????
- DoSPeriod 60
  - ??: DoS????????????????????????
- DoSThreshold 5
  - ??: DoS??????????????????????
- DoSHardThreshold 10
  - ??: ??????????????
  - 60?????IP???????10??????????????????????IP?????????????
- DoSBanPeriod 60

    - ??: DoS????????IP????????????????????????
- DoSTableSize 100
    - ??: DoS??????????IP???????????????
- DoSIgnoreContentType ^(image/|application/|text/javascript|text/css)
    - ??: DoS??????????????????????????????

??????Apache???

- mod???

```
sudo a2enmod dosdetector
```

- Web???????

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

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