

Nginx - ??Fail2ban????

????

- **Ubuntu 22.04**

??Fail2ban

```
# 安装
apt install fail2ban -y

# 启动并启用
systemctl enable --now fail2ban

# 配置
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

??Fail2ban

📄 `/etc/fail2ban/jail.local`

```
[nginx-4xx]
enabled = true
port = 80,443
logpath = %(nginx_access_log)s
maxretry = 10
findtime = 1m
bantime = 1d

[nginx-4xx-repeated]
enabled = true
port = 80,443
logpath = /var/log/fail2ban.log
maxretry = 3
findtime = 7d
bantime = 7d
```

```
nginx_access_log port 80 443
1 IP 10 4xx 1
7 IP 4xx 3 7
```

??nginx-4xx

`/etc/fail2ban/filter.d/nginx-4xx.conf`

[Definition]

```
failregex = ^<HOST>.*"(GET|POST).*" (400|403|404|444) .*$
ignoreregex =
```

4XX

??nginx-4xx-repeated

`/etc/fail2ban/filter.d/nginx-4xx-repeated.conf`

[Definition]

```
failregex = \[nginx-4xx]\s+[Bb]an\s+<HOST>
ignoreregex =
```

```
systemctl restart fail2ban
```

```
# Fail2ban
fail2ban-client status

# Filter
fail2ban-client status nginx-4xx

# ban IP
fail2ban-client get nginx-4xx banip

# ban IP
fail2ban-client set nginx-4xx unbanip <IP>

#
fail2ban-client set nginx-4xx addignoreip <IP>
```

