NGINX

NGINX相關

- Nginx 升級到 1.20.1 以上
- Nginx - 搭配 Fail2ban檢測封鎖
- Nginx 傳遞真實 IP
- Nginx 搭配 Let’s Encrypt Certbot自動更新 SSL憑證
- Nginx 代理的網站 MSIE 錯誤
- Nginx 啟用目錄列表的功能

Nginx ???1.20.1 ??

????

- **Ubuntu 20.04**

```
echo "deb http://nginx.org/packages/mainline/ubuntu `lsb_release -cs` nginx" \
    | sudo tee /etc/apt/sources.list.d/nginx.list
curl -o /tmp/nginx_signing.key https://nginx.org/keys/nginx_signing.key
sudo mv /tmp/nginx_signing.key /etc/apt/trusted.gpg.d/nginx_signing.asc

sudo apt update
sudo apt install nginx -y
```

```
nginx -v
```

因 **nginx 1.20** 不再使用 **/etc/nginx/site-enabled** 底下的設定，因此必須手動加入開啟 **/etc/nginx/nginx.conf**

```
http {
  #include /etc/nginx/conf.d/*.conf;
  include /etc/nginx/sites-enabled/*;
}
```

新的 **nginx** 使用 **nginx** 作為 **user**，取代原本的 **www-data** ，因此如有需要也可在 **nginx.conf** 內修改預設使用者

```
user  www-data;
#user  nginx;
```

```
/etc/init.d/nginx configtest

/etc/init.d/nginx restart
```

Nginx - ??Fail2ban????

????

- **Ubuntu 22.04**

??Fail2ban

```
# 安裝
apt install fail2ban -y


# 設定開機自動啟動
systemctl enable --now fail2ban


# 複製設定檔
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

??Fail2ban

編輯 `/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
```

```
抓取nginx_access_log判斷port 80 443 連線資訊
1 分鐘內, 同 IP 發生 10 次 4xx 錯誤, 封鎖 1 天
7 天內, 同 IP 因 4xx 錯誤被累計封鎖 3 次, 封鎖 7天
```

??nginx-4xx

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

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

> 只要回應 4XX都會被偵測

??nginx-4xx-repeated

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

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

```
systemctl restart fail2ban
```

```
# 顯示 Fail2ban 狀態
fail2ban-client status
# 顯示 Filter 計數
fail2ban-client status nginx-4xx
# 查詢被 ban 的 IP
fail2ban-client get nginx-4xx banip
# 解除被 ban 的 IP
fail2ban-client set nginx-4xx unbanip <IP>
# 加入白名單
fail2ban-client set nginx-4xx addignoreip <IP>
```

Nginx ????IP

Nginx??

外部 **IP**經過 **Nginx**處理後會變成 **Nginx**的 **IP**, 使用 **$remote_addr**紀錄使用者 **IP**

```
location /{
            .....
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}
```

PHP??IP??

```
if(!empty($_SERVER['HTTP_CLIENT_IP'])){
    $myip = $_SERVER['HTTP_CLIENT_IP'];
}else if(!empty($_SERVER['HTTP_X_FORWARDED_FOR'])){
    $myip = $_SERVER['HTTP_X_FORWARDED_FOR'];
}else{
    $myip= $_SERVER['REMOTE_ADDR'];
}
```

Nginx ??Let’s Encrypt Certbot ????SSL??

????

- **Ubuntu 22.04**

??certbot

```
apt install certbot python3-certbot-nginx
```

```
certbot certonly --nginx -d your_frontend_fqdn
```

輸入電子郵件用於通知

????SSL??

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Requesting a certificate for your_frontend_fqdn

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/your_frontend_fqdn/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/your_frontend_fqdn/privkey.pem
```

??Nginx??

```
listen 443 ssl;
        ssl_certificate /etc/letsencrypt/live/your_frontend_fqdn/fullchain.pem;
        ssl_certificate_key /etc/letsencrypt/live/your_frontend_fqdn/privkey.pem;
```

```
nginx -t
systemctl restart nginx
```

登入網站確認可使用 **https**瀏覽

????

```
#手動更新憑證
certbot renew
```

```
#測試更新憑證
certbot renew --dry-run
#確認憑證狀態
certbot certificates
```

??CertBot ??????

確認 **certbot.timer**是否有啟動

```
systemctl status certbot.timer
```

編輯 `/lib/systemd/system/certbot.service`, 修改 **ExecStart**

```
[Unit]
Description=Certbot
Documentation=file:///usr/share/doc/python-certbot-doc/html/index.html
Documentation=https://certbot.eff.org/docs
[Service]
Type=oneshot
ExecStart=/usr/bin/certbot -q renew --post-hook "systemctl reload nginx"
PrivateTmp=true
```

```
systemctl start certbot.service
```

如無錯誤訊息代表設定成功

```
user@nginx-proxy:~#  service certbot status
* certbot.service - Certbot
     Loaded: loaded (/lib/systemd/system/certbot.service; static)
     Active: inactive (dead) since Thu 2025-07-17 15:30:48 CST; 11min ago
TriggeredBy: * certbot.timer
       Docs: file:///usr/share/doc/python-certbot-doc/html/index.html
             https://certbot.eff.org/docs
    Process: 3737646 ExecStart=/usr/bin/certbot -q renew --post-hook systemctl reload nginx
(code=exited, status=0/SUCCESS)
   Main PID: 3737646 (code=exited, status=0/SUCCESS)
        CPU: 8.533s

Jul 17 15:28:06 nginx-proxy systemd[1]: Starting Certbot...
Jul 17 15:30:48 nginx-proxy systemd[1]: certbot.service: Deactivated successfully.
Jul 17 15:30:48 nginx-proxy systemd[1]: Finished Certbot.
```

```
Jul 17 15:30:48 nginx-proxy systemd[1]: certbot.service: Consumed 8.533s CPU time.
```

Nginx ????? MSIE ??

??

登入 **bookstack**編輯文章時，發現無法上傳圖片並報錯

```
<html> <head><title>500 Internal Server Error</title>
</head> <body> <center>
<h1>500 Internal Server Error</h1></center> <hr><center>nginx</center>
</body> </html> <!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

後續發現反向代理的所有網站皆有延遲的情況

??

查看 `/var/log/nginx/error.log`，發現有以下訊息

`[alert] 1719239#1719239: *241424 write() to "/var/log/nginx/access.log" failed (28: No space left on device) while logging request`

確認硬碟空間已滿

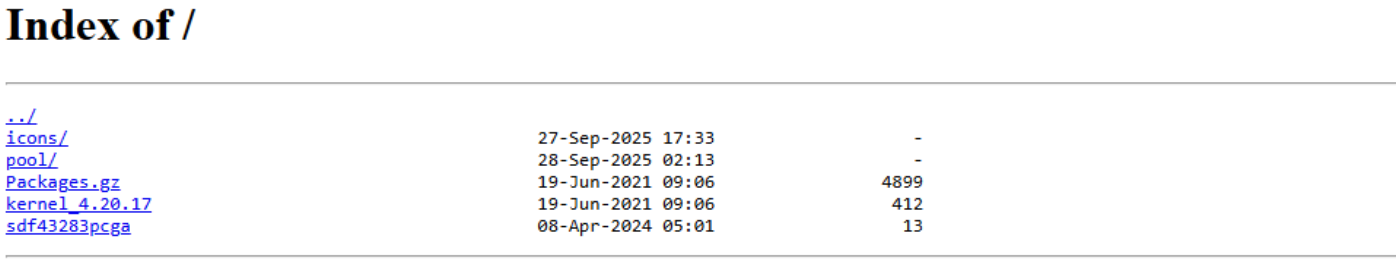
```
root@nginx-proxy:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/loop3       30G   28G     0 100% /
```

docker服務 **log**寫入異常

```
root@nginx-proxy:/var/log/nginx# service docker status
* docker.service - Docker Application Container Engine
...

Sep 01 12:40:30 nginx-proxy dockerd[344]: time="2025-09-01T12:40:30.998786583+08:00"
level=error msg="Error writing log message" driver=json-file error="error wri>
```

因為此代理主機也有運行 **docker**， **docker**的 **log**已被寫滿，由於 **docker**
服務無使用故先移除未使用容器並 **stop**後恢復正常



Nginx ?????????

Nginx預設不啟動瀏覽目錄功能，可以加入 `autoindex` 參數啟用

```
location / {
        autoindex on;
        ...
}
```

其他參數

autoindex on; 開啟瀏覽目錄
autoindex_exact_size off; 預設為 **on** 會顯示檔案大小單位為 **bytes**， **off** 單位為 **kB**、**MB**、**GB**
autoindex_localtime on; 預設為 **off** 顯示檔案修改時間為 **GMT**， **on** 則為 **Server** 地區時間。

```
nginx -t

service nginx reload
```

瀏覽網頁就會顯示目錄

Index of /

../		
icons/	27-Sep-2025 17:33	-
pool/	28-Sep-2025 02:13	-
Packages.gz	19-Jun-2021 09:06	4899
kernel_4.20.17	19-Jun-2021 09:06	412
sdf43283pcga	08-Apr-2024 05:01	13