

【Kibana】使用 https

要在本機環境的 Kibana 自產憑證，並讓 Kibana 支援 **HTTPS**，而非預設的 **HTTP**，以下是詳細步驟：

▢ 步驟 1：產生自簽名憑證（Self-Signed Certificate）

▢ 使用 OpenSSL 產生憑證：

1. **開啟終端機**，執行以下指令來建立一個新的私鑰和自簽名憑證：

```
mkdir -p /etc/kibana/ssl
cd /etc/kibana/ssl
# 產生私鑰和自簽名憑證，設定有效期限為 365 天
openssl req -x509 -newkey rsa:4096 -keyout kibana-key.pem -out kibana-cert.pem -days 365 -nodes
# 修改擁有者，權限
chown kibana:kibana kibana-key.pem
chown kibana:kibana kibana-cert.pem
chmod 644 kibana-key.pem
chmod 600 kibana-key.pem
```

▢ 輸入相關資訊：

在執行上述指令時，OpenSSL 會要求輸入一些資訊，像是：

- **Country Name (國家代碼)**：TW
- **State or Province Name (省/市)**：Taipei
- **Locality Name (城市)**：Taipei
- **Organization Name (公司名稱)**：momo.com
- **Common Name (CN)**：apielkmonitor.momoshop.com.tw

Country Name (2 letter code) [AU]:**TW**
State or Province Name (full name) [Some-State]:**Taipei**
Locality Name (eg, city) []:**Taipei**
Organization Name (eg, company) [Internet Widgits Pty Ltd]:**momo.com**
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:**apielkmonitor.momoshop.com.tw**
Email Address []:srou@fmt.com.tw

▢ 產生的檔案：

- kibana-cert.pe：私鑰
- kibana-cert.pe：自簽名憑證

▢ 步驟 2：配置 Kibana 使用 HTTPS

▢ 編輯 Kibana 的設定檔 `kibana.yml`：

打開 `kibana.yml` 檔案（通常位於 `/etc/kibana/kibana.yml` 或你的安裝目錄下），修改以下內容：

```
# 啟用 SSL
server.ssl.enabled: true

# 設定 SSL 憑證和私鑰的路徑
server.ssl.certificate: /etc/kibana/ssl/kibana-crt.pem
server.ssl.key: /etc/kibana/ssl/kibana-key.pem
```

```
# 修改 Kibana 的監聽端口
```

```
server.port: 443
```

```
# 如果elasticsearch 使用ssl 連線(沒有則不用)
```

```
# 選擇驗證證書的方式
```

```
elasticsearch.ssl.verificationMode: full
```

```
# 這個證書在 Elasticsearch 的 HTTP 證書時已經生成。複製到 Kibana 安裝目錄下配置使用即可。
```

```
elasticsearch.ssl.certificateAuthorities: [ "/data/kibana-8.13.0/elasticsearch-ca.pem" ]
```

“ ⚠ 注意：將 `/path/to/` 替換成你實際的憑證路徑。

❑ 步驟 3：允許本機信任自簽名憑證

❑ Mac 或 Linux：

將自簽名憑證 **kibana.crt** 匯入你的系統信任區：

```
sudo cp kibana.crt /usr/local/share/ca-certificates/kibana.crt
```

```
sudo update-ca-certificates
```

❑ Windows：

1. 打開 證書管理。
2. 選擇 受信任的根憑證授權單位。
3. 匯入 **kibana.crt** 檔案。

❑ 步驟 4：重啟 Kibana

```
sudo systemctl restart kibana
```

❑ 步驟 5：透過 HTTPS 訪問 Kibana

現在，你可以使用 `https://localhost`（或指定的 IP 地址）來訪問 Kibana。

錯誤處理：

FATAL Error: listen EACCES: permission denied 0.0.0.0:443

1.

```
# 啟動服務錯誤
sudo systemctl start kibana
# 可以使用以下語法查看詳細錯誤
journalctl -u kibana -f
```

```
#如果出現以下錯誤，代表不允許非root人員啟用1024 port 以下服務
FATAL Error: listen EACCES: permission denied 0.0.0.0:443
```

```
#使用以下語法同意以下檔案綁定使用1024 port 以下服務
setcap cap_net_bind_service=+epi /usr/share/kibana/bin/kibana
setcap cap_net_bind_service=+epi /usr/share/kibana/bin/kibana-plugin
setcap cap_net_bind_service=+epi /usr/share/kibana/bin/kibana-keystore
```

```
# node以實際位置為主
```

```
setcap cap_net_bind_service=+epi /usr/share/kibana/node/glibc-217/bin/node
```

Error: EACCES: permission denied, open '/run/kibana/kibana.pid'

```
chown kibana:kibana /run/kibana/kibana.pid
```

```
setcap cap_net_bind_service=+epi /run/kibana/kibana.pid
```

🕒 修訂版本 #2

★ 由 treeman 建立於 14 🕒@🕒🕒 2025 17:33:16

✍ 由 treeman 更新於 23 🕒@🕒🕒 2025 09:35:18