TANet無線網路漫遊交換中心

Freeradius使用SSL憑證安裝手冊

( 以Let’s encrypt為範例 )

# 準備說明

由於各連線單位的作業系統、版本和取得權限的規則都不同，建議匯入憑證前，針對相關驗證環境進行**備份**或**快照**，以減低匯入憑證失敗造成的服務異常。

# 環境準備

## 系統資源

作業系統：CentOS7.X

應用服務：freeradius 3.X

DNS綁定：wifi.roamingcenter.edu.tw ⚠️每個單位不一樣

## 需要憑證內容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 項次 | 生成位置 | 檔案名稱 | 說明 | |
| 1 | 網頁端 | privkey.pem | 生成憑證請求檔(CSR)的伺服器私鑰  (需要生產金鑰之密碼) |
| 2 | Let’s encrypt | fullchain.pem | Let’s encrypt 完整的憑證檔  (含伺服器憑證、中繼憑證) | |
| 3 | Let’s encrypt | cert.pem | Let’s encrypt中心發的伺服器憑證檔 | |
| 4 | Let’s encrypt | chain.pem | Let’s encrypt中心發的中繼憑證檔 | |

# 設定流程

## 將privkey.pem和fullchain.pem複製到/tmp/目錄裡面

## 再/etc/raddb/cert/增資料夾→letsencrypt

|  |
| --- |
| mkdir /etc/raddb/cert/letsencrypt |

## 將/tmp目錄的privkey.pem和fullchain.pem移動到letsencrypt資料夾

|  |
| --- |
| mv /tmp/server.key root.cer server.cer uca.cer /etc/raddb/cert/letsencrypt |

## 設定資料夾群組

|  |
| --- |
| chown root:radiusd /etc/raddb/cert/letsencrypt |

## 設定資料夾權限

|  |
| --- |
| chmod 655 /etc/raddb/cert/letsencrypt |

## 修改EAP設定

|  |
| --- |
| Vi /etc/raddb/mods-enabled/eap  ----------------------------------------------------------------  tls-config tls-common {  …略…  private\_key\_password = whatever #產生私鑰密碼，無密碼就不需修改  #private\_key\_file = ${certdir}/server.pem #註解  private\_key\_file = /etc/raddb/certs/letsencrypt/privkey.pem #新增    #certificate\_file = ${certdir}/server.pem #註解  certificate\_file = /etc/raddb/certs/letsencrypt/fullchain.pem #新增  …略… |

## 重新啟動服務

|  |
| --- |
| systemctl restart radiusd |

# 使用載具測試

## 使用Android 13手機測試

⚠️以下以漫遊中心環境和Pixel 7手機測試，請選擇單位內部EAP和密碼加密方式

