TANet無線網路漫遊交換中心

Freeradius使用SSL憑證安裝手冊

( 以中華電信CHT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

## 憑證產生相關文件說明

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 生成位置 | 檔案名稱 | 說明 |
| 1 | 網頁端 | Privatekey.key | 伺服器產生的伺服器**私鑰** |
| 2 | 網頁端 | server.csr | 伺服器**私鑰**所生成的憑證請求檔(CSR) |
| 3 | 中華電信 | ROOTeCA\_64.crt | 中華電信發的根憑證檔 |
| 4 | 中華電信 | 53108993DVB6D7949CAZ0C7515E4F133.cer 簡稱 Hash32.cer | 中華電信發的伺服器憑證檔 |
| 5 | 中華電信 | PulicCA2\_64.crt | 中華電信發的中繼憑證檔 |

# 設定流程

## 將Privatekey.key、rootcer、Hash32.cer和PulicCA2\_64.crt複製到/tmp/目錄裡面

## 再/etc/raddb/cert/增資料夾→chtCA

|  |
| --- |
| mkdir /etc/raddb/cert/chtCA |

## 將/tmp目錄的Privatekey.key、ROOTeCA\_64.crt、Hash32.cer和PulicCA2\_64.crt移動到chtCA資料夾

|  |
| --- |
| mv /tmp/Privatekey.key ROOTeCA\_64.crt Hash32.cer PulicCA2\_64.crt /etc/raddb/cert/chtCA |

## 設定資料夾群組

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

## 設定資料夾權限

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

## 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/chtCA/Privatekey.key #新增 #certificate\_file = ${certdir}/server.pem #註解 certificate\_file = /etc/raddb/certs/chtCA/Hash32.cer #新增  #ca\_file = ${cadir}/ca.pem #註解 ca\_file = /etc/raddb/certs/chtCA/PulicCA2\_64.crt #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

