TANet無線網路漫遊交換中心

Freeradius使用SSL憑證安裝手冊

政府憑證入口網(GCP)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.unitname.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 | server.key | 1.生成憑證請求檔(CSR)的伺服器私鑰2.需要產生伺服器私鑰之密碼 |
| 2 | GCP | ABCD1234(hash).cer(名稱會有32個hash的值) | GCP中心發的伺服器憑證 |
| 3 | GCP | eCA1\_GTLSCA.crt | GCP中心發的中繼憑證 |

# 設定流程

## 將server.key、ABCD1234(hash).cer、eCA1\_GTLSCA.crt複製到/tmp/目錄裡面

## 再/etc/raddb/cert/增資料夾→gcp

|  |
| --- |
| mkdir /etc/raddb/cert/gcp |

## 將/tmp目錄的server.key、ABCD1234(hash).cer、eCA1\_GTLSCA.crt移動到gcp資料夾

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

## 對伺服器憑證轉碼

|  |
| --- |
| openssl x509 -in ABCD1234(hash).cer -inform DER -out server.crt |

## 匯出無密碼的伺服器私鑰

|  |
| --- |
| openssl rsa -in server.key -out server\_nopass.key |

## 設定資料夾群組

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

## 設定資料夾權限

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

## 修改EAP設定

|  |
| --- |
| vim /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/gcp/server\_nopass.key   #certificate\_file = ${certdir}/server.pem #註解 certificate\_file = /etc/raddb/certs/gcp/server.crt   #ca\_file = ${cadir}/ca.pem #註解 ca\_file = /etc/raddb/certs/gcp/eCA1\_GTLSCA.crt …略… |

## 重新啟動服務

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

# 使用載具測試

## 使用Android 14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

