

漫遊連線機制建置說明手冊

OPENVPN & Freeradius

On CentOS7

一、安裝基本環境

1. 安裝網卡管理工具和編輯工具

```
[root@clientRS]# yum install -y net-tools vim
```

2. 設定網路防火牆

```
[root@clientRS]# firewall-cmd --zone=public --add-port=1812/udp --permanent  
[root@clientRS]# firewall-cmd --zone=public --add-port=1813/udp --permanent  
[root@clientRS]# firewall-cmd --reload
```

二、安裝 OpenVPN

3. 安裝 epel-release 和 openvpn 套件

```
[root@clientRS]# yum install -y epel-release  
[root@clientRS]# yum install -y openvpn
```

4. 將漫遊中心提供的 VPN 金鑰「class_number_shortname.tar」放置/etc/openvpn 解壓

縮

```
[root@clientRS]# cd /etc/openvpn  
[root@clientRS]# tar -zxf class_number_shortname.tar
```

5. 重新啟動 OPENVPN 服務

```
[root@clientRS]# systemctl restart openvpn@client
```

6. 看 tun0 網卡是否有啟動，如 tun0 有產生 10.1.X.X 代表 VPN 連線成功

```
[root@clientRS]# ifconfig tun0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.1.X.X netmask 255.255.255.255 destination 10.1.0.2
    inet6 fe80::ab85:e6d5:df58:63c9 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3 bytes 144 (144.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

7. 設定 OPENVPN 開機啟動服務

```
[root@clientRS]# systemctl enable openvpn@client
```

三、安裝 Freeradius

1. 安裝 freeradius 和 freeradius-utils 套件

```
[root@clientRS]# yum install -y freeradius freeradius-utils
```

2. 修改/etc/raddb 目錄的 clients.conf 檔案

```
[root@clientRS]# cd /etc/raddb
[root@clientRS]# vim clients.conf
    <--於檔案最後處加入下列內容-->
client roamingcenter {
    ipaddr = 10.1.77.7
    secret = spiradawn
}
client roamingcenter-monitor{
    ipaddr = 10.1.77.11
    secret = spiradawn
}
```

3. 修改/etc/raddb 目錄的 proxy.conf 檔案

```
[root@clientRS]# vim proxy.conf
    <--於檔案最後處加入下列內容-->
realm DEFAULT { #當遇到帳號帶有 realm 時的預設動作為送至漫遊中心進行 proxy 動作
    type = radius
    authhost = 10.1.77.7:1812
    accthost = 10.1.77.7:1813
    secret = spiradawn
    nostrip
}
```

4. 重新啟動 Radius 服務

```
[root@clientRS]# systemctl restart radiusd
```

FreeRadius 環境測試

1. 使用漫遊中心測試帳號在本機端(127.0.0.1)測試

- ✓ 使用測試指令和漫遊中心測試帳號測試環境

測試指令：radtest

測試帳號：exmaple@rc.edu.tw

密碼：exmaple123

測試端：127.0.0.1 (本機端)

交換密碼：testing123

指令 → radtest exmaple@rc.edu.tw ncut123 127.0.0.1 0 testing123

```
[root@clientRS]# radtest exmaple@rc.edu.tw exmaple123 127.0.0.1 0 testing123
      < radtest      帳號      密碼      測試端 IP  測試埠  交換密碼 >
Sending Access-Request of id 234 to 10.1.0.7 port 1812
  User-Name = "XXXXXX@rc.edu.tw"
  User-Password = "XXXXXXX"
  NAS-IP-Address = 127.0.0.1
  NAS-Port = 0
rad_recv: Access-Accept packet from host 10.1.0.7 port 1812, id=234, length=20
```

備註：

交換密碼是對應/etc/raddb/clients.conf 中 ipaddr 對應的 secret

如果 secret = ABCD 那指令就要修改成

指令 → radtest exmaple@rc.edu.tw ncut123 127.0.0.1 0 ABCD

```
[root@clientRS]# cat /etc/raddb/clients.conf
...略...
client localhost {
  ...略...
  ipaddr = 127.0.0.1
  ...略...
  secret = ABCD      #交換密碼
  ...略...
}
```

2. 使用漫遊中心測試帳號在漫遊交換中心(10.1.77.7)測試

✓ 使用測試指令和漫遊中心測試帳號測試環境

測試指令：radtest

測試帳號：exmaple@rc.edu.tw

密碼：exmaple123

測試端：10.1.77.7 (漫遊交換中心)

交換密碼：spiradawn

指令 → **radtest** **exmple@rc.edu.tw** **ncut123** **10.1.77.7** **0** **spiradawn**

```
[root@clientRS]# radtest exmaple@rc.edu.tw exmaple123 10.1.77.7 0 spiradawn
< radtest      帳號          密碼  漫遊交換中心 IP  測試埠  交換密碼 >
Sending Access-Request of id 234 to 10.1.0.7 port 1812
  User-Name = "XXXXXX@rc.edu.tw"
  User-Password = "XXXXXXX"
  NAS-IP-Address = 127.0.0.1
  NAS-Port = 0
rad_recv: Access-Accept packet from host 10.1.0.7 port 1812, id=234, length=20
```

備註：

交換密碼是對應/etc/raddb/clients.conf 中的 ipaddr 對應的 secret

如果 secret = ABCD 那指令就要修改成

指令 → **radtest** **exmaple@rc.edu.tw** **ncut123** **10.1.77.7** **0** **ABCD**

```
[root@clientRS]# cat /etc/raddb/clients.conf
...略...
client localhost {
  ...略...
  ipaddr = 10.1.77.7
  ...略...
  secret = ABCD #交換密碼
  ...略...
}
```

3. 設定 Radius 開機啟動服務

```
[root@clientRS]# systemctl enable radiusd
```