漫遊連線機制建置說明手冊

CentOS7 by ldap with EAP-802.1X

( Version 2.4 )

# 安裝OpenVPN

## 安裝epel-release和openvpn套件

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

1. **將漫遊中心的VPN金鑰「class\_number\_shortname.tar」放置/etc/openvpn解壓縮**

|  |
| --- |
| [root@openvpn]# cd /etc/openvpn  [root@openvpn]# tar -zxf class\_number\_shortname.tar |

1. **重新啟動OPENVPN服務**

|  |
| --- |
| [root@openvpn]# systemctl restart openvpn@client |

1. **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@openvpn]# 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 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 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 |

1. **設定OPENVPN開機啟動服務**

|  |
| --- |
| [root@openvpn]# systemctl enable openvpn@client |

# 安裝Freeradius

1. **安裝freeradius和freeradius-utils套件**

|  |
| --- |
| [root@freeradius]# yum install -y freeradius freeradius-utils |

1. **修改/etc/raddb目錄的clients.conf檔案**

|  |
| --- |
| [root@freeradius]# cd /etc/raddb  [root@freeradius]# 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  } |

1. **修改/etc/raddb目錄的proxy.conf檔案**

|  |
| --- |
| [root@freeradius]# 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  authhost = 10.1.77.7:1812  accthost = 10.1.77.7:1813  secret = spiradawn  nostrip  } |

1. **重新啟動Radius服務**

|  |
| --- |
| [root@freeradius]# systemctl restart radiusd |

# FreeRadius環境測試

## 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：[account@rc.edu.tw](mailto:exmaple@rc.edu.tw)

密碼：account123

測試端：127.0.0.1 (本機端)

交換密碼：testing123

|  |
| --- |
| [root@freeradius]# radtest account@rc.edu.tw password 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 |

指令 → **radtest account@rc.edu.tw password 127.0.0.1 0 testing123**

* 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 account@rc.edu.tw password 127.0.0.1 0 ABCD**

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

# **安裝及修改Ldap模組**

## 安裝套件freeradius-ldap套件

|  |
| --- |
| [root@freeradius]#yum install freeradius-ldap |

## 修改ldap模組

|  |
| --- |
| [root@freeradius]#vim /etc/raddb/mods-enabled/ldap  server = IP address  port = 389  identity = 'cn=XXX,dc=XXX,dc=XXX,dc=XXX'  password = PASSWD  base\_dn = ' dc=XXX,dc=XXX,dc=XXX' |

## 修改Freeradius的default檔案，新增LDAP驗證

|  |
| --- |
| [root@freeradius]#vim /etc/raddb/sites-enabled/default  authorize {  …略…  if (!control:Auth-Type && User-Password) {  update {  control:Auth-Type := ldap  }  }  }  authenticate {  …略…  Auth-Type LDAP {  ldap  }  …略…  } |
|  |

# **修改LDAP之EAP認證方式**

## 修改inner-tunnel檔案，新增判斷式

|  |
| --- |
| [root@freeradius]#vim /etc/raddb/sites-enabled/inner-tunnel  authenticate {  …略…  Auth-Type LDAP {  ldap  }  …略…  } |

## 修改EAP認證方式

|  |
| --- |
| [root@freeradius]#vim /etc/raddb/mod-enabled/eap  eap {  …略…  #default\_eap\_type = md5  default\_eap\_type = peap  gtc {  …略…  #auth\_type = PAP  auth\_type = ldap  …略…  }  peap{  …略…  #default\_eap\_type = mschapv2  default\_eap\_type = gtc  …略…  } |

# **FreeRadius環境測試**

## 使用漫遊中心測試帳號在本機端(127.0.0.1)測試

* 漫遊中心測試帳號相關設定

測試指令：radtest

漫遊中心測試帳號：[account@rc.edu.tw](mailto:account@rc.edu.tw)

密碼：password

測試端：127.0.0.1 (本機端)

交換密碼：testing123

|  |
| --- |
| [root@freeradius]# radtest [account@rc.edu.tw](mailto:account@rc.edu.tw) password 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 = "account@rc.edu.tw"  User-Password = "passwd"  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 |

指令 → **radtest account@rc.edu.tw password 127.0.0.1 0 testing123**

* 備註：

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

如果**secret = ABCD**那指令就要修改成

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

|  |
| --- |
| [root@freeradius]# cat /etc/raddb/clients.conf  …略…  client localhost {  …略…  **ipaddr = 127.0.0.1**  …略…  secret = testing123 #交換密碼  …略…  } |

## 使用貴單位測試帳號在本機端(127.0.0.1)測試

* 貴單位測試帳號相關設定

測試指令：radtest

貴單位測試帳號：account@xxx.edu.tw

密碼：password

測試端：127.0.0.1 (本機端)

交換密碼：testing123

|  |
| --- |
| [root@freeradius]# radtest account@XXX.edu.tw password 127.0.0.1 0 testing123  ＜radtest 貴單位測試帳號 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 = "\_\_\_\_\_@XXX.edu.tw"  User-Password = "\_\_\_\_\_"  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 |

指令 → **radtest account@xxx.edu.tw password 127.0.0.1 0 testing123**

* 備註：

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

如果**secret = ABCD**那指令就要修改成下列

指令 → **radtest account@xxx.edu.tw password 127.0.0.1 0 ABCD**

|  |
| --- |
| [root@freeradius]# cat /etc/raddb/clients.conf  …略…  client localhost {  …略…  **ipaddr = 127.0.0.1**  …略…  secret = testing123 #交換密碼  …略…  } |

## 使用貴單位測試帳號在漫遊中心伺服器(10.1.77.7)測試

* 貴單位測試帳號相關設定

測試指令：radtest

貴單位測試帳號：account@xxx.edu.tw

密碼：password

測試端： 10.1.77.7 (漫遊中心端)

交換密碼：spiradawn

|  |
| --- |
| [root@freeradius]# radtest [account@xxx.edu.tw](mailto:account@xxx.edu.tw) password 10.1.77.7 0 spiradawn  ＜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 = "account@xxx.edu.tw"  User-Password = "password"  NAS-IP-Address = 10.1.77.7  NAS-Port = 0  rad\_recv: Access-Accept packet from host 10.1.0.7 port 1812, id=234, length=20 |

指令 → **radtest** [**account@xxx.edu.tw**](mailto:account@xxx.edu.tw) **password** 10.1.77.7 **0 spiradawn**

* 備註：

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

如果**secret = ABCD**那指令就要修改成

指令 → **radtest account@xxx.edu.tw password 10.1.77.7 0 ABCD**

|  |
| --- |
| [root@freeradius]# cat /etc/raddb/clients.conf  …略…  client roamingcenter {  …略…  ipaddr = 10.1.77.7  …略…  secret = spiradawn #交換密碼  …略…  } |

## 設定開機啟動服務

|  |
| --- |
| [root@openvpn]# systemctl enable radiusd |