

# CentOS 8 - A



DNF套件管理器，即將取代YUM

## Update package index

```
dnf -y update
```

## 安裝 freerADIUS

```
dnf -y install freeradius freeradius-utils
systemctl enable --now radiusd.service
```

## 設定防火牆

```
firewall-cmd --add-service=radius --permanent
firewall-cmd --reload
```

## 建立帳號轉送設定(proxy.conf & client.conf)

```
vim /etc/raddb/proxy.conf
realm eduroam.a.edu {
    authhost = LOCAL
    accthost = LOCAL
}

realm eduroam.b.edu {
    authhost = "RADIUS-B IP":1812
    accthost = "RADIUS-B IP":1813
    secret   = key
    nostrip
}

vim /etc/raddb/client.conf
client RADIUS-B {
    ipaddr = "RADIUS-B IP"
    secret = key
}
```

設定users，在RADIUS-A的internal中建立測試帳號，給RADIUS-B測試用。

```
vim /etc/raddb/users
filesA Cleartext-Password := "filesA"
```

```
systemctl restart radiusd
```

## 測試RADIUS-B的internal帳號

```
radtest filesB@eduroam.b.edu filesB 127.0.0.1 0 testing123
```

## 安裝 freeradius-mysql

```
dnf -y install mariadb-server freeradius-mysql
systemctl start mariadb
systemctl enable mariadb
```

執行mariadb安全性安裝

```
mysql_secure_installation
...
```

進入mariadb

```
mysql -u root -p
```

建立database和mysql user

```
MariaDB [(none)]> CREATE DATABASE radius;
MariaDB [(none)]> GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "password";
MariaDB [(none)]> FLUSH PRIVILEGES;
MariaDB [(none)]> quit;
```

匯入RADIUS MySQL schema到建立的database上

```
mysql -u root -p radius < /etc/raddb/mods-config/sql/main/mysql/schema.sql
```

建立sql連結到/etc/raddb/mods-enabled/

```
ln -s /etc/raddb/mods-available/sql /etc/raddb/mods-enabled/
```

設定FreeRADIUS的sql模組

```
vim /etc/raddb/mods-available/sql
driver = "rlm_sql_mysql"
dialect = "mysql"

server = "localhost"
port = 3306
login = "radius"
password = "password"

read_clients = yes
```

更改群組權限給radiusd

```
chgrp -h radiusd /etc/raddb/mods-enabled/sql
```

```
systemctl restart radiusd
```

進入mariadb insert RADIUS-A的測試帳號

```
mysql -u radius

MariaDB [(none)]> insert into radcheck (id, username, attribute, op, value) values ("1", "mysqlA", "Cleartext-Password", "=", "mysq
MariaDB [(none)]> quit
```

測試RADIUS-B的mysql帳號

```
radtest mysqlB@eduroam.b.edu mysqlB 127.0.0.1 0 testing123
```

## 安裝freeradius-ldap

```
dnf -y install freeradius-ldap freeradius-krb5
```

建立LDAP連結到/etc/raddb/mods-enabled/

```
ln -s /etc/raddb/mods-available/ldap /etc/raddb/mods-enabled/
```

LDAP module取消註解

```
vim /etc/raddb/sites-available/default
authorize {
  ldap
  if ((ok || updated) && User-Password) {
    update {
      control:Auth-Type := ldap
    }
  }
}

authenticate {
  Auth-Type LDAP {
    ldap
  }
}

post-auth {
  ldap
}

vim /etc/raddb/sites-available/inner-tunnel
authorize {
  ldap
  if ((ok || updated) && User-Password) {
    update {
      control:Auth-Type := ldap
    }
  }
}

authenticate {
  Auth-Type LDAP {
    ldap
  }
}

post-auth {
  ldap
}
```

設定LDAP server

```
vim /etc/raddb/mods-enabled/ldap
server = localhost
base_dn =
```

```
systemctl restart radiusd
```

Debug mode

```
systemctl stop radiusd.service  
radiusd -X
```

## 校時

安裝及設定chrony。在centOS 8, chrony已取代NTP。

```
dnf install -y chrony  
systemctl enable chronyd  
vim /etc/chrony.conf  
server tock.stdtime.gov.tw prefer  
server tick.stdtime.gov.tw  
server time.stdtime.gov.tw  
systemctl restart chronyd
```

## 設定時區

```
timedatectl set-timezone Asia/Taipei
```