Education Roaming
Movilidad segura para la comunidad académica

Manual de Instalación y configuración para nodos pilotos de EDUROAM-LA

Módulo 3 Servidor RADIUS Local (12 ½ horas)

Detalles a tener en consideración:

- El archivo “sources.list” donde se enlistan las fuentes o repositorios, debe estar configurado “solo” de la siguiente manera:

```
deb http://ftp.es.debian.org/debian/ squeeze main
deb-src http://ftp.es.debian.org/debian/ squeeze main

deb http://security.debian.org/ squeeze/updates main
deb-src http://security.debian.org/ squeeze/updates main

deb http://ftp.es.debian.org/debian/ squeeze-updates main
deb-src http://ftp.es.debian.org/debian/ squeeze-updates main
```

- Descargar las fuentes necesarias con wget:

a. Descargar la fuente para obtener la versión 0.98 estable del paquete openssl desde **ftp://ftp.openssl.org/snapshot/**
b. Descargar la fuente para obtener la última versión del paquete freeradius desde **ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.1.12.tar.gz**
c. Descargar la fuente para obtener la última versión del paquete rsyslog desde **http://rsyslog.com/files/download/rsyslog/rsyslog-4.8.0.tar.gz**

- Desinstalación de paquetes innecesarios

  apt-get remove openssl y rsyslog

1. Instalar los paquetes necesarios para la configuración de una autoridad certificadora con formato estándar X.509 y creación de certificados digitales para los servidores RADIUS y usuarios itinerantes. (3h)

   Instalación de paquetes y librerías necesarias:

```
apt-get install make pkg-config vim nmap mysql-server mysql-client libssl-dev libgnutls-dev libsnmp-dev libmysqlclient-dev libldap-dev
```

En el siguiente paso, vamos a instalar el paquete openssl para la creación de una autoridad certificadora para la emisión de certificados digitales al servidor radius.

```
tar -zxvf openssl*
./config --prefix=/usr/local --openssldir=/usr/local/openssl
make && make test && make install
/sbin/ldconfig -v
```

Comprobar que el paquete *openssl* fue instalado en forma correcta:

```
root@test-eduroam:~# openssl
OpenSSL> version
OpenSSL 0.9.8s xx XXX xxxx
```

En los siguientes pasos detallaremos los procedimientos a seguir para la creación de una autoridad certificadora, y las firmas digitales de los certificados emitidos hacia el servidor RADIUS.

1.1 Crearemos un directorio con nombre *eduroam* dentro de la carpeta "/etc".

```
mkdir /etc/eduroam
```

Dentro del directorio /etc/eduroam, crear los siguientes directorios y archivos:

```
mkdir private newcerts
touch index.txt
echo '01' > serial
```

1.2 Creación de la llave pública y privada para el establecimiento de una autoridad certificadora. (ejemplo: ver figura ca.jpg de la carpeta imágenes-eduroam)

```
openssl req -new -x509 -extensions v3_ca -keyout private/ca.key -out ca.crt
```

Comentario [r1]: ca.key -> Llave privada de la Autoridad Certificadora, la cual firmará las peticiones de certificados.

Comentario [r2]: ca.crt -> Llave pública del CA.

1.3 Creación del certificado de consulta para el servidor RADIUS (ejemplo: ver figura radius-req.jpg de la carpeta imágenes-eduroam).

```
openssl  req -new -keyout radius.key -out radius.<dom_institución>.csr -days 3650
```

Comentario [r3]: radius.key -> Llave privada del servidor radius por lo que debería ser guardada.

Comentario [r4]: Dominio institucional, por ejemplo, inictel-uni.edu.pe para la institución del INICTEL-UNI en Perú.

1.4 Obtención del archivo "xpextensions"

```
cp /usr/local/etc/raddb/certs/xpextensions /etc/eduroam/
```

1.5 Firma del certificado de consulta para el servidor RADIUS (ejemplo: ver figura radius-ca.jpg de la carpeta imágenes-eduroam)

```
openssl ca -policy policy_anything -out radius.<dom_institución>.crt -extensions
xpserver_ext -extfile xpextensions -infiles radius.<dom_institución>.csr
```

Comentario [r5]: Clave pública del servidor radius, el cuál se alojará en la carpeta certs.

1.6 Creación del certificado de consulta para un usuario en itinerancia (ejemplo: ver figura user-req.jpg de la carpeta imágenes-eduroam).

```
openssl req -new -keyout test.key -out test.<dom_institución>.csr –days 3650
```

1.7 Firma del certificado de consulta para un usuario en itinerancia (ejemplo: ver figura user-ca.jpg de la carpeta imágenes-eduroam).

```
openssl ca -policy policy_anything -out test.<dom_institución>.crt -extensions
xpclient_ext -extfile xpextensions -infiles test.<dom_institución>.csr
```

Comentario [r6]: Clave pública del usuario en itinerancia.

1.8 Creación del certificado PKCS12 para un usuario Windows (ejemplo: ver figura user-p12.jpg de la carpeta imágenes-eduroam).

```
openssl pkcs12 -export -in test.<dom_institución>.crt -inkey test.key -out test.p12 -
clcerts
```

1.9 Creación del archivo DER para Windows (ejemplo: ver figura otros.jpg de la carpeta imágenes-eduroam).

```
openssl x509 -inform PEM -outform DER -in ca.crt -out ca.der
```

1.10 Creación del archivo diffie-hellman para la negociación de llaves de sesión TLS (ejemplo: ver figura otros.jpg de la carpeta imágenes-eduroam).

```
openssl dhparam -check -text -5 512 -out dh
```

1.11 Creación del archivo random bitstream usado en las operaciones TLS (ejemplo: ver figura otros.jpg de la carpeta imágenes-eduroam).

```
dd if=/dev/urandom of=random count=2
```

1.12 Copiar los siguientes archivos al directorio /usr/local/etc/raddb/certs/ del servidor radius.

```
cp ca.crt /usr/local/etc/raddb/certs/ -v
cp radius.key /usr/local/etc/raddb/certs/ -v
cp radius.inictel-uni.edu.pe.crt /usr/local/etc/raddb/certs/ -v
cp dh /usr/local/etc/raddb/certs/
cp random /usr/local/etc/raddb/certs/
```

2. Instalar un servidor RADIUS en Linux y configurar algunos parámetros necesarios en la configuración del RADIUS (1h).

```
./configure --with-openssl-includes=/usr/local/openssl/include --with-openssl-
libraries=/usr/local/openssl/lib --prefix=/usr/local/
make && make install
```

Comprobar que el paquete freeradius fue instalado de forma correcta

```
root@test-eduroam:~# radiusd -v
radiusd: FreeRADIUS Version 2.1.12, for host i686-pc-linux-gnu, built on Sep 26 2011 at
11:02:06
Copyright (C) 1999-2010 The FreeRADIUS server project and contributors.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License.
```

3. Generación de claves GPG para el intercambio de secretos entre los servidores RADIUS (30')

3.1 Creación de llaves privadas y públicas

- gpg --gen-key

Para visualizar la generación de claves:

- ls ..gnupg/

3.2 Listar las claves públicas y privadas y obtener el ID correspondiente

- gpg --edit-key

3.3 Compartición de claves públicas entre los participantes del curso de EDUROAM.

Para esto, publicaremos nuestra llave al internet, de la siguiente manera:

- gpg –send-keys "ID" --keyserver hkp://subkeys.pgp.net

Comentario [r7]: Servidor de claves públicas GPG.

3.4 Importación de claves públicas de todos los participantes del curso de EDUROAM.

Para esto, haremos una búsqueda hacia el servidor de claves GPG e importaremos la clave desde el internet de la siguiente manera:

- gpg --keyserver hkp://subkeys.pgp.net –search-keys "ID"

3.5 Intercambio de claves cifradas por cada NREN.

Para esto, debemos cifrar en un archivo de texto la clave compartida y enviarla por correo electrónico al servidor radius correspondiente.

- gpg –e file.txt

4. Configurar las claves locales y remotas para un servidor RADIUS (30') (ver figura 1)

Las directivas de configuración del cliente es:

```
client <nombre_institución_remota> {
 ipaddr = <IP_RADUIS_REMOTO>
 netmask=32
 require_message_authenticator=no
 secret = <secreto>
 shortname = org-"NREN"
 }
```

Comentario [r8]: Dirección IP del servidor radius remoto.

Comentario [r9]: Cambiar NREN por la institución de su país, por ejemplo para el Perú es: org-RAAP

Las directivas de configuración de realm y proxy radius son:

```
proxy server {
 default_fallback       = yes
}
realm <nombre_institución>.edu.<dom_país> {
  type = radius
  authhost = LOCAL
  accthost = LOCAL
 }
realm LOCAL {
 nostrip
 }
realm NULL {
  nostrip
}
realm <nombre_institución_remota>.edu.<dom_país_remoto> {
  type = radius
  authhost = <IP_RADIUS_REMOTO>:1812
  accthost = <IP_RADIUS_REMOTO>:1813
  secret = <secreto>
  nostrip
  }
```

Comentario [r10]: Si una consulta de autenticación contiene un realm que no esta explícitamente listado líneas abajo, entonces esto es proxiado al realm Default.

Comentario [r11]: Realm institucional referente al radius institucional conectado a eduroam. Por ejemplo: inictel-uni.edu.pe es el realm de INICTEL-UNI del Perú.

Comentario [r12]: Si no especificamos un pool server entonces el realm es Local.

Comentario [r13]: Para consultas que no tienen un realm explicito.

Comentario [r14]: Realm del servidor remoto.

5. Configurar el archivo *file users* del servidor RADIUS local (30')

```
DEFAULT
        User-Name = `%{User-Name}`,
        Fall-Through = yes
user    Cleartext-Password := "pass"
#DEFAULT Auth-Type = LDAP
#       Fall-Through = 1
#DEFAULT Auth-Type = SQL
#       Fall-Through = 1
```

Comentario [r15]: Usuarios generalmente de pruebas en texto plano

Comentario [r16]: Descomentar en caso que todos los usuarios estén almacenados en un servidor LDAP

Comentario [r17]: Descomentar en caso que todos los usuarios estén almacenados en un servidor SQL.

Evaluación 1: Validación entre servidores RADIUS usando protocolos PAP o CHAP desde "file users" (30') (5%)

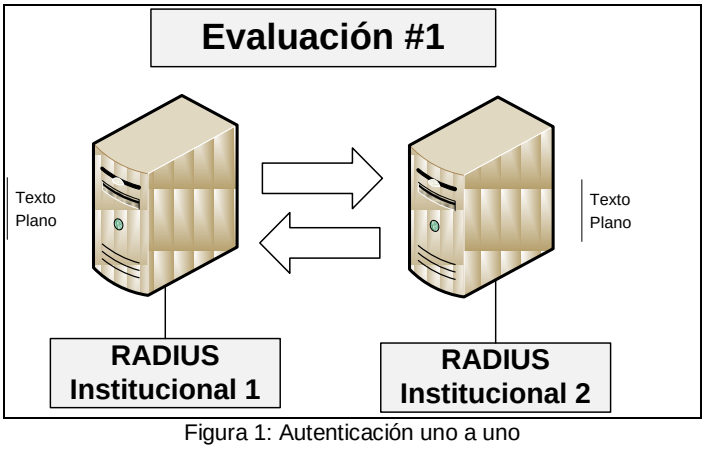

Figura 1: Autenticación uno a uno

6. Instalar un servidor de base de datos MySQL (30')

   apt-get install mysql mysql-client

7. Configurar un cliente MySQL para el servidor RADIUS (30')

```
sql { …
      database = "mysql"
      driver = "rlm_sql_${database}"
      server = 127.0.0.1
      port = 3306
      login = "eduroam"
      password = "eduroam"
      radius_db = "freeradius"
… }
```

Comentario [r18]: Como ejemplo usaremos: user= eduroam y clave=eduroam

Comentario [r19]: Base de datos por default, donde se almacenará los eventos de conexión de usuarios.

Ahora importe el esquema "schema.sql" hacia el servidor base de datos:

```
root@test-eduroam:/usr/local/etc/raddb/sql/mysql# mysql -h 127.0.0.1 -p freeradius < schema.sql
Enter password:
root@test-eduroam:/usr/local/etc/raddb/sql/mysql#
```

Asigne los permisos correspondientes:

Pruebas de MySQL a nivel cliente

```
root@test-eduroam:/usr/local/etc/raddb# mysql -u root -p
Enter password:
mysql> create user eduroam identified by 'eduroam';
Query OK, 0 rows affected (0.00 sec)

mysql> create database freeradius;
Query OK, 1 row affected (0.02 sec)

mysql> grant all privileges on freeradius.* to 'eduroam'@'127.0.0.1' identified by 'eduroam' with grant option;
Query OK, 0 rows affected (0.00 sec)
mysql> use freeradius;
mysql> insert into radcheck values (1,'user1','User-Password','==','pass1');
Query OK, 1 row affected (0.00 sec)
mysql> quit
```

Comentario [r20]: Usuario de prueba para la autenticación de usuarios, éstos se encontrarán en la tabla radcheck de la base de datos.

Este paso es importante, pues nos permite comprobar la validación del servidor RADIUS hacia una base de datos MySQL.

```
root@test-eduroam:/usr/local/etc/raddb# mysql -h 127.0.0.1 -u eduroam -p freeradius
Enter password:
```

Evaluación 2: Validación entre usuarios MySQl de una base de datos(30') (5%)

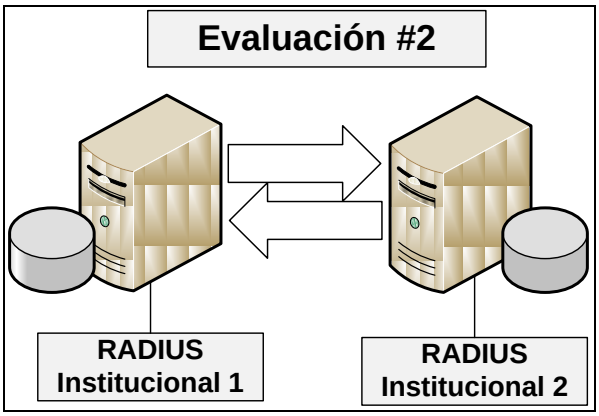

Figura 2: Autenticación uno a uno con conexión a una base de datos

8. Instalar y configurar un servidor de *logs* (1h)

- ./configure --enable-mysql --enable-gnutls --enable-snmp
- make && make install
- En el archivo /etc/init.d/rsyslogd editar lo siguiente:

Agregar:
PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/local/bin:/usr/local/sbin
Modificar:
RSYSLOGD_BIN=/usr/local/sbin/rsyslogd

9. Configurar un cliente *logs* para *eduroam* (30')

```
log {
        destination = files
        file = ${logdir}/radius.log
        syslog_facility = local1
        stripped_names = yes
        auth = yes
        auth_badpass = yes
        auth_goodpass = yes
        msg_goodpass = "Usuario Aceptado %{User-Name}"
        msg_badpass = "Usuario Rechazado"
}
```

Comentario [r21]: Usaremos como destino el archivo radius.log por defecto para los logs de autenticaciones.

Comentario [r22]: Tomaremos como referencia la facility "local1" según http://wiki.freeradius.org/Syslog-HOWTO

Pruebas de Logs

```
tail -f /usr/local/var/log/radius/radius.log

Fri Sep 30 19:06:30 2011: Auth: Login OK: [user1/pass1] (from client localhost port 111) Usuario Aceptado user1
```

Evaluación 3: Registro de *logs* en un Servidor RADIUS. (30') (10%)

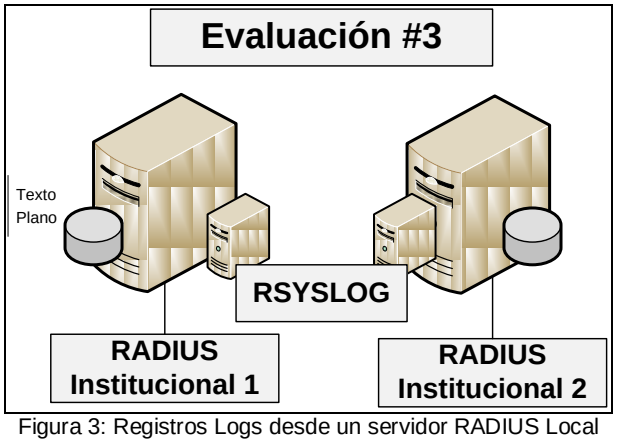

Figura 3: Registros Logs desde un servidor RADIUS Local

10. Instalar y Configurar un servidor LDAP (1h)

Primero, instalamos los siguientes paquetes:

```
openldap-servers openldap-clients, http
```

Descargar fuente LDAP:

```
wget ftp://ftp.openldap.org/pub/OpenLDAP/openldap-stable/openldap-stable-20100719.tgz
```

Copiar el archivo openldap-stable-20100719.tgz en /var/www/html/

Luego descomprimir:

```
tar –zxvf openldap*
```

Mueva el directorio generado hacia un directorio *phpldap*:

```
mv phpldapadmin* phpldap
```

Diríjase hacia /var/www/html/phpldap/config/ y realice lo siguiente:

```
cp config.php.example config.php
```

Ahora, edite el archivo config.php

Reemplace esta línea:

#$servers->setValue('server','name','My LDAP Server');

Por esta:

$servers->SetValue('server','base',array('dc=<nombre_institución>,dc=edu,dc=<dom_pais>'));

Comentario [r23]: Nombre distinguido para el servidor LDAP institucional.

Guarde los cambios!

Ahora, copie el esquema del RADIUS (openldap.schema) en el directorio /etc/openldap/schema/

Edite el archivo slapd.conf

```
database        bdb
suffix          "dc=<nombre_institución>,dc=edu,dc=<dom_país>"
rootdn          "cn=admin,dc=<dom_institución>,dc=edu,dc=<dom_país>"
rootpw          <secreto>
# rootpw                {crypt}ijFYNcSNctBYg
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory       /var/lib/ldap
```

Ahora solo nos falta crear el árbol de directorio para nuestro LDAP el cuál se definirá de la siguiente forma.

11. Configurar usuarios en LDAP (30')

Primero, creamos un directorio LDIF y editamos el siguiente archivo dentro de ese directorio:

eduroam.ldif

```
# Creando la organización raíz del directorio
dn: dc=<nombre_institución>,dc=edu,dc=<dom_país>
objectClass: dcObject
objectClass: organization
dc: <nombre_institución>
o: EDUROAM-LA
description: Despliegue de EDUROAM a Nivel Latinoamericano

#Creando el Rol de Administrador
dn: cn=admin,dc=<nombre_institución>,dc=edu,dc=<dom_país>
objectClass: organizationalRole
cn: admin
description: Administrador de Directorio

#Creando la Unidad Organizativa Grupos y Usuarios
dn: ou=grupos,dc=<nombre_institución,dc=edu,dc=<dom_país>
objectClass: top
objectClass: organizationalUnit
ou: grupos
```

```
dn: ou=usuarios,dc=<nombre_institución>,dc=edu,dc=<dom_país>
objectClass: top
objectClass: organizationalUnit
ou: usuarios
```

Ahora, agregue la estructura de directorio en el LDAP (ejemplo: ver figura ldap-acceso.jpg y ldap-acceso1.jpg de la carpeta imágenes-eduroam).

```
ldapadd -x -w secret –D "cn=admin,dc=<nombre_institución>,dc=edu,dc=<dom_país>" -f eduroam.ldif

adding new entry "dc=<nombre_institución>,dc=edu,dc=<dom_país>"

adding new entry "cn=admin,dc=<nombre_institución>,dc=edu,dc=<dom_país>"

adding new entry "ou=grupos,dc=<nombre_institución>,dc=edu,dc=<dom_país>"

adding new entry "ou=usuarios,dc=<nombre_institución>,dc=edu,dc==<dom_país>"
```

12. Configurar un cliente LDAP para RADIUS (30')

Ahora editaremos el modulo *ldap* y los servidores virtuales desde el servidor RADIUS para que éste pueda conectarse con el LDAP y poder "logearse" con usuarios creados del mismo.

```
ldap {
    …
    server = <IP_LDAP>:389
    basedn = "ou=usuarios,dc=<nombre_institución>,dc=edu,dc=<dom_país>"
    filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
    base_filter = "(objectclass=radiusprofile)"
    …
    }
```

Editamos el servidor virtual por default del RADIUS:

```
authorize {
        …
        ldap
        …
        }

authenticate {
    …
    Auth-Type LDAP {
        ldap
    }
    …
            }
```

Luego, creamos un usuario desde el servidor Web LDAP y hacemos una prueba usando el programa *radtest* que ya viene incorporado en el servidor RADIUS (ejemplo: ver figura ldap-config.jpg de la carpeta imágenes-eduroam).

Evaluación 4: Validación de usuarios LDAP hacia un servidor RADIUS (30') (10%)

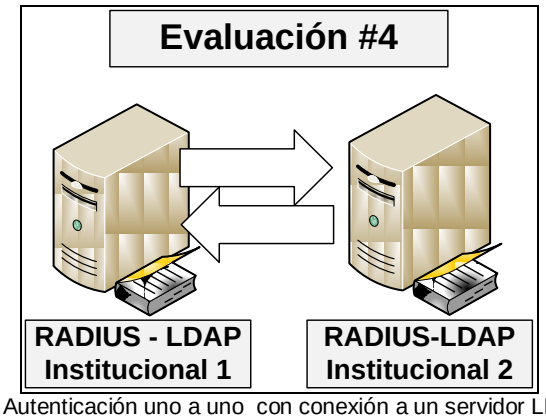

Figura 4: Autenticación uno a uno con conexión a un servidor LDAP Local