

Configuración de un servidor RADIUS

PREPARACIÓN DE LA PRÁCTICA

Antes de empezar la práctica seguid las indicaciones siguientes:

→ Aseguraos de que habeis arrancado la partición “PRÁCTICA RDC LOCAL”.

→ Restaurar la configuración original de RADIUS:

```
cd /etc; sudo tar -xvzf freeradius.original.tgz
```

→ Resetead el punto de acceso proporcionado: mantened pulsado el botón trasero “Restore” hasta que la luz frontal “Power” parpade (unos 20 s). Una vez hecho esto desconectad de la corriente eléctrica y volved a conectar para poder trabajar.

Nota: Cuando editeis archivos de configuración no copiar/pegar desde un archivo pdf.

1. Introducción

RADIUS (*Remote Authentication Dial-In User Server*) es un protocolo que nos permite gestionar la autenticación, autorización y registro de usuarios remotos para controlar el acceso a servicios en red. En esta práctica vamos a estudiar RADIUS, dado que se trata de un protocolo ampliamente empleado. En particular instalaremos una solución de código abierto denominada FreeRADIUS, y la configuraremos para un uso concreto como es regular el acceso a una red inalámbrica, donde mediante el uso de un punto de acceso se creará una red con seguridad WPA2 empresarial que autenticará a través del servidor RADIUS configurado.

Un caso real en el que se utiliza RADIUS como método global de control de acceso a las redes inalámbricas de las principales instituciones académicas de Europa es el proyecto *eduroam* (*EDUcation ROAMing*), creado para facilitar el acceso a Internet a los miembros de las instituciones científico-académicas asociadas, desde cualquiera de estas instituciones.

2. El protocolo RADIUS

Como hemos dicho, RADIUS es un protocolo que nos permite gestionar la “autenticación, autorización y registro” de usuarios remotos sobre un determinado recurso. La tupla “autenticación, autorización y registro” se conoce como AAA, al ser éste su acrónimo de su denominación original inglesa: “Authentication, Authorization, and Accounting”. Veamos con más detalle a qué se refiere cada uno de estos términos.

Autenticación (*authentication*) hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.

Un tipo habitual de credencial es el uso de una contraseña (o password) que junto al nombre de usuario nos permite acceder a determinados recursos. El nombre de usuario es nuestra identidad, que puede ser públicamente conocida, mientras que la contraseña se mantiene en secreto, y sirve para que nadie suplante nuestra identidad. Otros tipos más avanzados de credenciales son los certificados digitales.

Existen muchos métodos concretos que implementan el proceso de la autenticación. Algunos de ellos, soportados por RADIUS, son:

- Autenticación de sistema (system authentication), típica en un sistema Unix, normalmente realizada mediante el uso del fichero `/etc/passwd`;
- Protocolos PAP (*Password Authentication Protocol*), y su versión segura CHAP (*Challenge Handshake Authentication Protocol*), que son métodos de autenticación usados por proveedores de servicios de Internet (ISPs) accesibles vía PPP;
- LDAP (*Lightweight Directory Access Protocol*), un protocolo a nivel de aplicación (sobre TCP/IP) que implementa un servicio de directorio ordenado, y muy empleado como base de datos para contener nombres de usuarios y sus contraseñas;
- Kerberos, el famoso método de autenticación diseñado por el MIT;
- EAP (*Extensible Authentication Protocol*), que no es un método concreto sino un entorno universal de autenticación empleado frecuentemente en redes inalámbricas y conexiones punto a punto;
- Por último, también se permite la autenticación basada en ficheros locales de configuración del propio servidor RADIUS.

Autorización (*authorization*) se refiere a conceder servicios específicos (entre los que se incluye la “negación de servicio”) a un determinado usuario, basándose para ellos en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como, por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples “logins” de un mismo usuario. El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio (QoS) que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

Los métodos de autorización soportados habitualmente por un servidor de RADIUS incluyen bases de datos LDAP o SQL, o incluso el uso de ficheros de configuración locales al servidor.

No se debe confundir los términos autenticación con autorización. Mientras que la autenticación es el proceso de verificar un derecho reclamado por una entidad (persona u ordenador), la autorización es el proceso de verificar que una entidad ya autenticada tiene la autoridad para efectuar una determinada operación.

Por último, **registro** (*accounting*) se refiere a llevar un registro del consumo de recursos que realizan los usuarios. El registro suele incluir la identidad del usuario, la naturaleza del servicio prestado, así como el registro temporal del uso del servicio correspondiente.

Es interesante el uso del protocolo RADIUS cuando tenemos redes de dimensiones considerables sobre las que queremos proporcionar un servicio de acceso centralizado. Por este motivo, uno de los principales usos de RADIUS se encuentra en empresas que proporcionan acceso a Internet o grandes redes corporativas, en un entorno con diversas tecnologías de red (incluyendo módems, xDSL, VPNs y redes inalámbricas) no sólo para gestionar el acceso a la propia red, sino también para servicios propios de Internet.

Un uso de RADIUS que queremos enfatizar, al ser el que realizaremos en esta práctica, es la autenticación en redes inalámbricas (Wi-Fi), sustituyendo métodos más simples de clave compartida (pre-shared key, PSK), que son bastante limitados al gestionar una red cuando ésta alcanza un determinado volumen.

3. Topología de la red

La topología de la red a desplegar en esta práctica se muestra en la figura. Así, conectaremos el PC donde instalaremos el servidor RADIUS a la red de infraestructura del punto de acceso. Para ello desconectad el cable amarillo de la roseta de la pared y conectadlo al punto de acceso (puerto standard, no WAN). El PC deberá recibir una dirección IP en la red 192.168.1.0/24 por DHCP desde el router. Si no es así, aseguraos de que está activada la conexión “DCLAN eth1-DHCP” en el “Network Manager” (icono en el panel superior).



4. El servidor FreeRADIUS

FreeRADIUS es un paquete de software de código abierto y libre distribución que implementa un servidor RADIUS modular para facilitar su extensión, y muy escalable, presentando prácticamente todas las opciones que un usuario puede necesitar. Por ejemplo, para realizar las tareas de autenticación y autorización puede almacenar y acceder a la información por medio de múltiples bases de datos: LDAP (AD, OpenLDAP,...), SQL (MySQL, PostgreSQL, Oracle,...) y ficheros de texto (fichero local de usuarios, fichero de sistema /etc/passwd,...).

5. Configuración del servidor

La configuración del servidor se realiza mediante el fichero “radiusd.conf” ubicado en el directorio “/etc/freeradius/”. Para aprovecharnos de la modularidad y evitar una excesiva longitud del fichero, éste se suele dividir en varios ficheros enlazados mediante la directiva “\$INCLUDE”. Entre otros destacamos:

- clients.conf: Contiene la lista de dispositivos clientes (p.ej., un punto de acceso) que están autorizados para usar los servicios de autenticación.
- eap.conf: Se utiliza para configurar las características de la autenticación EAP a emplear.
- sql.conf: Para configurar el acceso a las bases de datos SQL.
- policy.conf, etc.

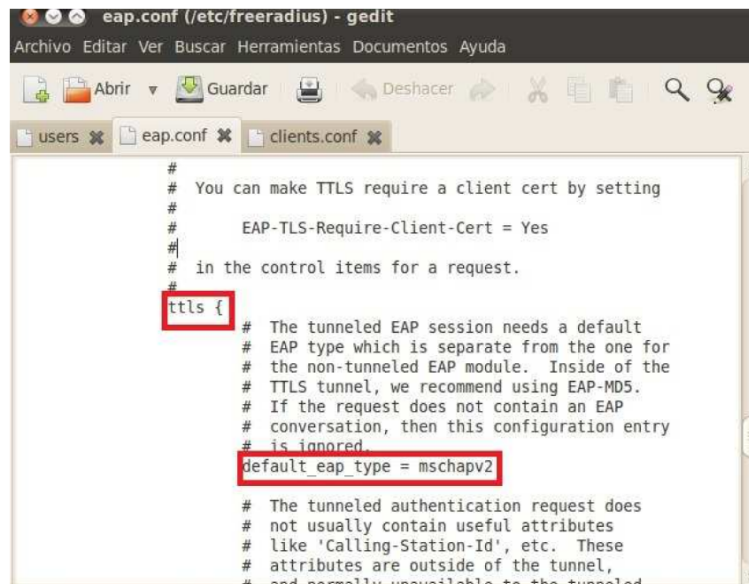
Además, el fichero “users” contiene información sobre la autenticación de suplicantes (usuarios). Aquí podremos añadir credenciales en forma de nombre de usuario y contraseña de una manera sencilla. Para empezar abrid el fichero “users” con un editor de textos (por ejemplo gedit):

```
$ sudo gedit /etc/freeradius/users &
```

Y al final del fichero mediante la siguiente línea añadid un usuario “pepe” y estableced su contraseña en “1234” (podéis añadir tantos usuarios como queráis):

```
pepe Cleartext-Password := "1234"
```

La autenticación de usuarios requiere de soporte PEAP y mschapv2. Para activarlo editad el fichero “/etc/freeradius/eap.conf”, y cambiad en el apartado ttls el atributo default_eap_type, de “md5” a “mschapv2” (en minúsculas), como se muestra en la figura siguiente:



```
eap.conf (/etc/freeradius) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda

Abrir Guardar Deshacer

users eap.conf clients.conf

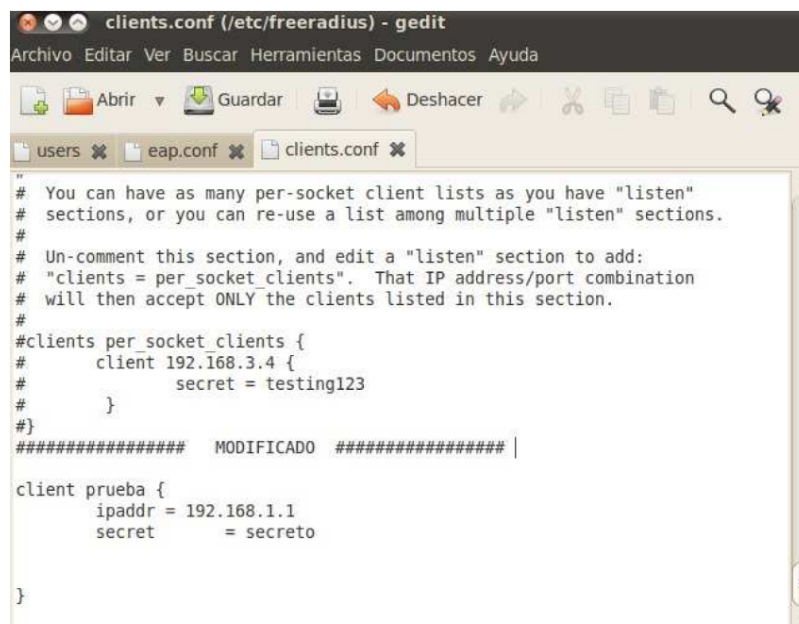
#
# You can make TTLS require a client cert by setting
#
#     EAP-TLS-Require-Client-Cert = Yes
#
# in the control items for a request.
#
tls {
# The tunneled EAP session needs a default
# EAP type which is separate from the one for
# the non-tunneled EAP module. Inside of the
# TTLS tunnel, we recommend using EAP-MD5.
# If the request does not contain an EAP
# conversation, then this configuration entry
# is ignored.
default_eap_type = mschapv2

# The tunneled authentication request does
# not usually contain useful attributes
# like 'Calling-Station-Id', etc. These
# attributes are outside of the tunnel,
# and normally unavailable to the tunneled
```

A continuación tenéis que configurar en el servidor RADIUS qué dispositivos clientes se van a conectar. En este caso será el punto de acceso inalámbrico. Al dar de alta un nuevo cliente hay que definir “un secreto” (contraseña), que permite asociar de manera segura el cliente con el servidor.

Editad el fichero `/etc/freeradius/clients.conf`. Buscad el cliente “localhost”. ¿Cuál es su IP? ¿Cuál es el “secret”?

Ahora añadid el punto de acceso como cliente, con nombre “prueba”, como se muestra la figura:



```
clients.conf (/etc/freeradius) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda

Abrir Guardar Deshacer

users eap.conf clients.conf

#
# You can have as many per-socket client lists as you have "listen"
# sections, or you can re-use a list among multiple "listen" sections.
#
# Un-comment this section, and edit a "listen" section to add:
# "clients = per_socket_clients". That IP address/port combination
# will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#    client 192.168.3.4 {
#        secret = testing123
#    }
#}
##### MODIFICADO #####

client prueba {
    ipaddr = 192.168.1.1
    secret = secreto
}
```

Una vez realizados estos pasos, ya esta lista la configuración básica de nuestro servidor RADIUS, pudiendo autenticar al usuario que hayamos dado de alta en el fichero users, desde el cliente indicado, con el sistema de autenticación MSCHAPv2.

Ahora, reiniciaremos el servidor RADIUS para hacer efectivos los cambios realizados:

```
$ sudo initctl restart freeradius
```

Para comprobar que el servidor está funcionando correctamente, podéis usar la herramienta “radtest” en el PC de la siguiente manera:

```
$ radtest <usuario> <contraseña> 127.0.0.1 1812 testing123
```

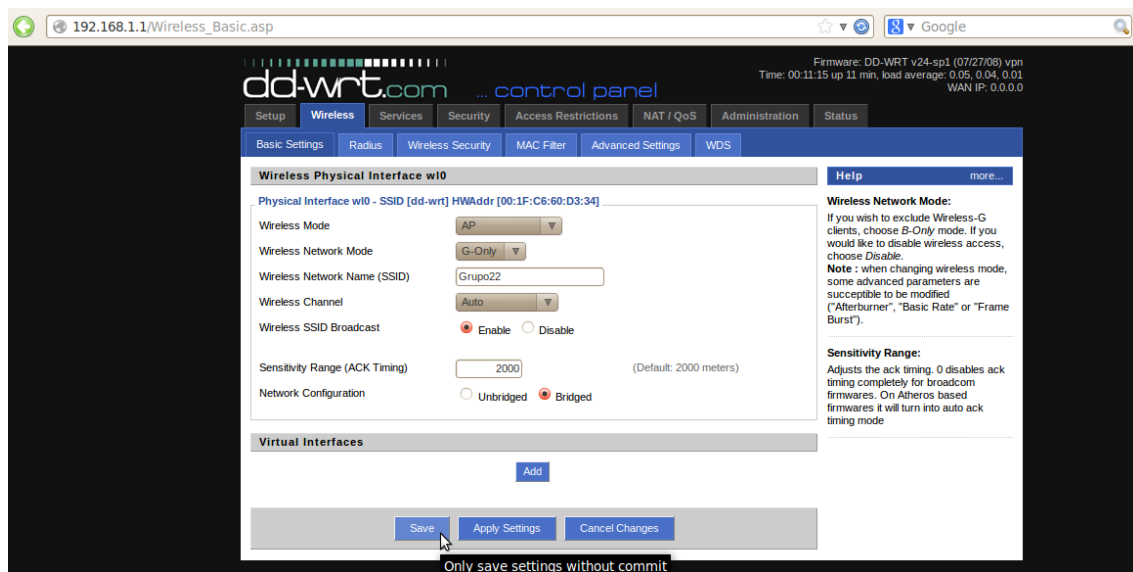
donde “usuario” y “contraseña” son las credenciales del usuario creado, “testing123” es el secreto de un supuesto cliente “localhost”, localhost o 127.0.0.1 es la dirección del servidor RADIUS, y 1812 el puerto. Si todo es correcto la respuesta debe ser “Access-Accept”, lo que confirma que el servidor RADIUS autentica a ese usuario. Si no es así, comprobad que el proceso servidor está funcionando y revisad la toda configuración anterior. *Nota: un error sintáctico en alguno de los archivos de configuración puede provocar que la conexión de prueba sea rechazada “Access-Reject” (o incluso que el servidor no arranque). Para encontrar posibles errores detened el servicio con “initctl stop freeradius” y volvedlo a iniciar en modo depuración ejecutando /usr/bin/freeradius -X.*

6. Configuración del punto de acceso

Para configurar el punto de acceso que autenticará utilizando los servicios del servidor RADIUS, conectaos al punto de acceso desde un navegador web cualquiera, tecleando en la barra de dirección su IP (normalmente 192.168.1.1), usuario (admin) y contraseña (admin)¹.

A continuación, buscad la sección de configuración “wireless”, pestaña “Basic Settings”, elegid un SSID para vuestra red (figura inferior). Guardad los cambios mediante el botón “Save”.

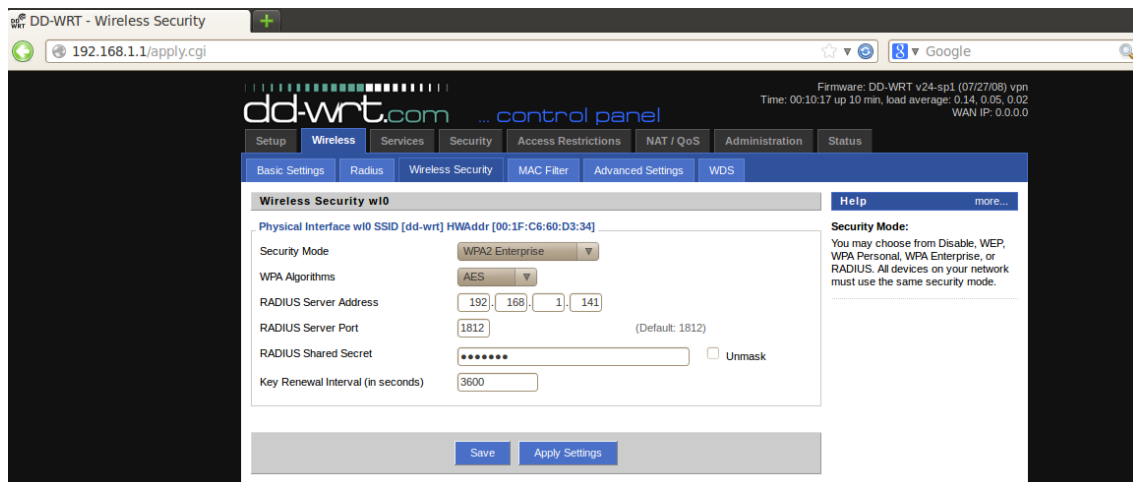
¹ Recordad usar el cable de la red interna del laboratorio (cable amarillo) para no perder la conexión exterior.



Después configurad la pestaña “Wireless security” como se ve en el ejemplo de la figura siguiente. Debéis indicar:

- método de autenticación (Security mode): “WPA2-Enterprise”;
- algoritmos de encriptación: “AES”;
- dirección IP del servidor RADIUS que se utilizará para autenticar;
- puerto en el que escucha el servidor (1812, no hay que cambiarlo);
- el “secreto” especificado en el fichero `clients.conf` para este cliente.

Finalmente pulsar “Save” y “Apply Settings”.



7. Prueba de conexión y autenticación

A continuación tendrás que comprobar que tanto el punto de acceso como el servidor RADIUS están funcionando correctamente.

Para ello, utilizando cualquier dispositivo inalámbrico (Smartphone, portatil o PC con adaptador wifi), conéctate a la red inalámbrica configurada en el apartado anterior y verifica que se te autentica correctamente una vez le proporcionas el usuario y

contraseña que configuraste en el servidor RADIUS (apartado 4). El tipo de seguridad que has de escoger es PEAP y MSCHAPv2, sin certificado (en algunos dispositivos puede funcionar con seguridad TTLS, o TLS a través de tunel).

8. Autenticación mediante bases de datos SQL

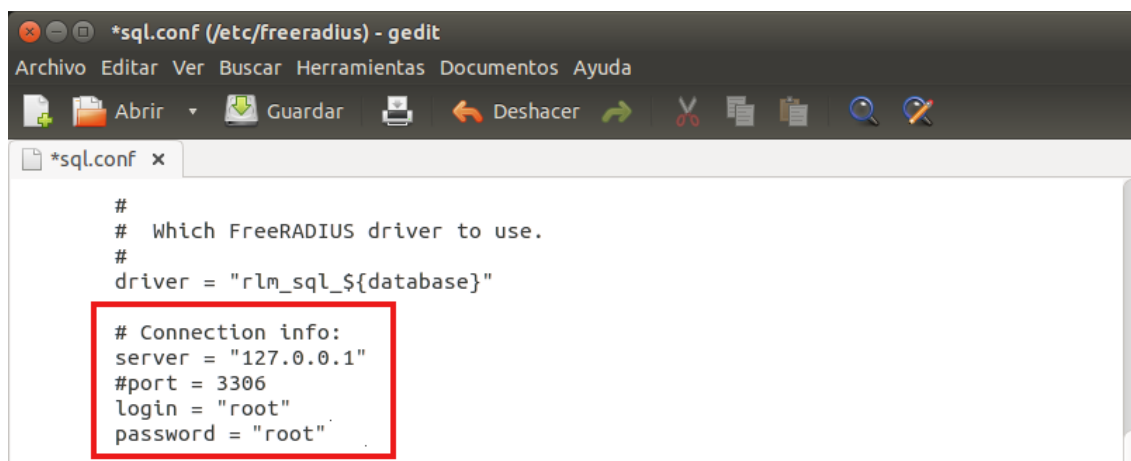
En este punto vamos a ver cómo almacenar los usuarios en una base de datos con MYSQL y configurar el servidor RADIUS para que acceda a la misma para autenticar los usuarios.

En la carpeta de freeradius esta la ruta `/etc/freeradius/sql/mysql`, en cuyo directorio encontraréis los ficheros `"schema.sql"` y `"nas.sql"`, que contienen los esquemas y tablas de la base de datos. Para permitir su correcta importación más tarde, copiad ambos ficheros al directorio *home* del usuario con el que iniciasteis sesión y cambiad el propietario a dicho usuario. Suponiendo el usuario `"redlocal"`:

```
$ sudo cp /etc/freeradius/sql/mysql/schema.sql /home/redlocal
$ sudo cp /etc/freeradius/sql/mysql/nas.sql /home/redlocal
$ sudo chown redlocal /home/redlocal/schema.sql /home/redlocal/nas.sql
```

8.1. Configuración de RADIUS para SQL

En primer lugar configuraréis el servidor RADIUS para que acceda a bases de datos SQL. Editad el archivo `"/etc/freeradius/sql.conf"` y modificad los parámetros indicados en la figura:



donde `"server"` es la dirección IP donde está instalado el servidor MySQL (en nuestro caso *localhost* o `127.0.0.1`) y `"login"` y `"password"` corresponden a un usuario de la base de datos MySQL (en nuestro caso, el usuario por defecto, `"root"`).

Más abajo en este mismo archivo descomentad los siguientes campos y asignad los siguientes valores para indicar que los dispositivos cliente deben validarse mediante la base de datos (tabla `"nas"`):

Descomentar `readclients = yes`

A continuación editaremos el fichero `/etc/freeradius/radiusd.conf` para que se utilice la configuración de las bases de datos SQL (fichero `sql.conf`) y no la del archivo `clients.conf`:

Descomentar: `$INCLUDE sql.conf`

Comentar: `$INCLUDE clients.conf`

Por último hay que configurar los tipos de autenticación, para ello id al directorio `"sites-available"` y editad los siguientes archivos:

1. Archivo `default`: Descomentad las líneas 177 y 406 para activar el uso de `sql`.
2. Archivo `inner-tunnel`: Descomentad las líneas 131, 255, 277, y 301 para activar el uso de `sql`.

8.2. Creación de la base de datos

A continuación, creareis la base de datos con la interfaz web `phpMyAdmin`. Acceded a la interfaz mediante la siguiente URL, y entrad como usuario `"root"` y contraseña `"root"`:

`http://localhost/phpmyadmin`

En la ventana de la izquierda se muestran las bases de datos existentes. Si entre ellas aparece listada `"radius"`, seleccionadla, id a la pestanya `"Operaciones"` y eliminadla (si no existe no teneis que hacer nada).

En la pestaña `"Bases de datos"` cread una nueva base de datos con nombre `"radius"`. A continuación, en el marco izquierdo, seleccionad la base de datos `radius` que acabais de crear y desde la pestaña `"Importar"` importad las tablas incluidas en los archivos `"schema.sql"` y `"nas.sql"` que tenéis en vuestro directorio `home`:

Importando en la base de datos "radius"

Archivo a importar:

El archivo puede ser comprimido (gzip, zip) o descomprimido. Un archivo comprimido tiene que terminar en **[formato].[compresión]**. Por ejemplo: **.sql.zip**

Buscar en su ordenador: schema.sql (Máximo: 2,048KB)

Conjunto de caracteres del archivo:

Importación parcial:

☒ Permitir la interrupción de una importación en caso que el script detecte que se ha acercado al límite de tiempo PHP. (Esto podría ser un buen método para importar archivos grandes; sin embargo, puede dañar las transacciones.)

Número de filas a omitir, iniciando de la primera fila:

Formato:

Opciones específicas al formato:

Modalidad SQL compatible:

☒ No utilizar AUTO_INCREMENT con el valor 0

Finalmente, nuestra base de datos debe quedar de la siguiente manera:

Tabla	Acción	Filas	Tipo	Cotejamiento	Tamaño	Re de
<input type="checkbox"/> nas	Examinar Estructura Buscar Insertar Vaciar Eliminar	~0	InnoDB	latin1_swedish_ci	32 KB	
<input type="checkbox"/> radacct	Examinar Estructura Buscar Insertar Vaciar Eliminar	~0	InnoDB	latin1_swedish_ci	144 KB	
<input type="checkbox"/> radcheck	Examinar Estructura Buscar Insertar Vaciar Eliminar	~0	InnoDB	latin1_swedish_ci	32 KB	
<input type="checkbox"/> radgroupcheck	Examinar Estructura Buscar Insertar Vaciar Eliminar	~0	InnoDB	latin1_swedish_ci	32 KB	
<input type="checkbox"/> radgroupreply	Examinar Estructura Buscar Insertar Vaciar Eliminar	~0	InnoDB	latin1_swedish_ci	32 KB	
<input type="checkbox"/> radpostauth	Examinar Estructura Buscar Insertar Vaciar Eliminar	~0	InnoDB	latin1_swedish_ci	16 KB	
<input type="checkbox"/> radreply	Examinar Estructura Buscar Insertar Vaciar Eliminar	~0	InnoDB	latin1_swedish_ci	32 KB	
<input type="checkbox"/> radusergroup	Examinar Estructura Buscar Insertar Vaciar Eliminar	~0	InnoDB	latin1_swedish_ci	32 KB	
8 tablas	Número de filas	0	InnoDB	latin1_swedish_ci	352 KB	

☐ Marcar todos

[Vista de impresión](#) [Diccionario de datos](#)

Crear tabla

Nombre: Número de columnas:

Una vez creada la base de datos radius e importadas sus tablas, reiniciaremos el servidor RADIUS para activar la nueva configuración.

8.3. Introducción de clientes y usuarios

Ahora solo falta introducir datos en la base de datos:

1. La tabla `nas` está destinada a contener los datos de los dispositivos cliente. Una vez seleccionada introduciremos un nuevo registro con la identificación de nuestro punto de acceso (pestaña “Insertar”):

2. La tabla `radcheck` está destinada a contener los datos de los usuarios. Introduciremos los datos de uno nuevo, donde `value` es la contraseña:

3. En la tablas `radusergroup` y `radreply` deberemos replicar el usuario e introducir los siguientes valores:

username	groupname	priority
jose	admin	0

id	username	attribute	op	value
1	jose	Fall-Through	=	yes

9. Prueba de conexión y autenticación

Ahora vuelve a intentar conectarte a la red inalámbrica para comprobar el correcto funcionamiento del servidor RADIUS que utiliza ahora una base de datos para recuperar la información necesaria para la autenticación. Puedes hacer la prueba con `radtest` o con un teléfono móvil configurado con PEAP+MSCHAP2.

10. Ampliación

Puedes probar ahora a añadir un segundo cliente al servidor RADIUS, p.e el punto de acceso de un compañero. Haz los cambios apropiados en los ficheros de configuración del servidor y verifica el correcto funcionamiento.