Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2018 pp. 5-15 *Correo: editor@istvidanueva.edu.ec*
Volumen 2, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: agosto 2018 *Fecha de aceptación: octubre 2018*

Aplicación de Servidor Radius en la Distribución Linux Mint

Aguas Luis [1]; Bucheli Fabiola[2]

[1] *Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, aguaszoft@outlook.es*
[2] *Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, fgbl_02@hotmail.com*

Resumen: En primer lugar, RADIUS (del inglés Remote Access Dial In User Service) es un protocolo que destaca sobre todo por ofrecer un mecanismo de seguridad, flexibilidad, capacidad de expansión y una administración simplificada de las credenciales de acceso a un recurso de red. Tras la breve introducción, hay que decir que el protocolo se utiliza en esquema cliente-servidor. Es decir, un usuario con unas credenciales de acceso al recurso se conecta contra un servidor que será el que se encargue de verificar la autenticidad de la información y ser el encargado de determinar si el usuario accede o no al recurso compartido. Ya hemos mencionado que se utiliza sobre todo por los operadores de red, pero es cierto que en las redes Wi-Fi de hoteles u otros establecimientos también es habitual encontrarse con esto.

Palabras clave: Tecnología, Servidor, Linux, Radius

Radius Server Application on Linux Mint Distribution

Abstract: First, RADIUS (Remote Access Dial in User Service) is a protocol that stands out above all for offering a security mechanism, flexibility, expandability, and simplified management of network resource access credentials. After the brief introduction, it must be said that the protocol is used in client-server schema. That is, a user with resource access credentials connects to a server that will be responsible for verifying the authenticity of the information and being responsible for determining whether or not the user accesses the share. We have already mentioned that it is mainly used by network operators, but it is true that in the Wi-Fi networks of hotels or other establishments it is also common to encounter this.

Keywords: Technology, Server, Linux, Radius

1. INTRODUCCIÓN

Decidimos usar virtualización para minimizar el equipamiento físico necesario. Lo primero fue descargar Linux Mint 14.1 en el equipo que sería el hospedero para la máquina virtual de Radius. Es importante mencionar también que todo el procedimiento se lo ha realizado por CLI pues es el medio que nos resulta más cómodo, así que abrimos una consola en el hospedero y ejecutamos wget para descargar el ISO de Linux Mint: Bhaiji, Y. (2003)

```
$ wget -c --limit-rate=100k
http://mirror.jmu.edu/pub/linuxmint/ima
ges//stable/14/linuxmint-14.1-mate-dvd-
64bit.iso
```

Nota

Para la virtualización usamos una máquina virtual en VirtualBox. El proceso de instalación no lo describimos pues no es el objetivo primario de este trabajo y además es bastante sencillo e intuitivo. O'Reilly Media (2007)

1. Magíster en Redes de Comunicaciones, aguaszoft@outlook.es
2. Magíster en Gerencia Educativa, fgbl_02@hotmail.com

Luego de instalada, siempre es bueno mandarle a actualizar (esto toma cierto tiempo):

```
# apt-get update    (actualiza los
repositorios)
# apt-get upgrade    (actualiza
paquetes)
```

Nota

Vimos que entre los paquetes que se actualizaron, se instaló un nuevo kernel, así que reiniciamos para que lo use y de inmediato mandamos a instalar el freeRadius:

```
# apt-get install freeradius
```

Con esto ya tenemos lo necesario instalado y listo para comenzar.

2. METODOLOGÍA

Una vez instalado, el manejador de paquetes por defecto activará y arrancará el servidor freeradius, por ahora no nos conviene que esté ejecutándose pues necesitamos realizar una serie de pruebas de funcionamiento, entonces lo detenemos:

```
# /etc/init.d/freeradius stop
```

freeRadius ya viene prácticamente listo para usarse, por lo que los pasos a continuación son bastante elementales, pero necesarios:

Primero creamos las credenciales de un usuario para pruebas, editando **/etc/freeradius/users**:

```
# vi /etc/freeradius/users
```

y al final agregamos la siguiente línea, donde prueba es el nombre de usuario y probando es la contraseña:

prueba Cleartext-Password := "probando"

ahora arrancamos el servidor freeRadius en modo de depuración:

```
# freeradius -X
```

Esta consola quedará inútil para otras operaciones mientras el servidor freeRadius esté corriendo en modo debug,. Se puede presionar Ctrl+C para detenerlo en cualquier momento y volver al *prompt*. Hassell, J. (2002)
Aparecerán una gran cantidad de líneas de información, esto es normal, lo importante es ver al final algo como:

```
...
Listening on authentication address *
port 1812
Listening on accounting address * port
1813
Listening on authentication address
127.0.0.1 port 18120 as server inner-
tunnel
Listening on proxy address * port 1814
Ready to process requests.
```

3. RESULTADOS Y DISCUSIÓN

3.1. Primera prueba de autenticación (local).

Abrimos otra consola en el mismo equipo, enviamos a ejecutar un pedido de autenticación de prueba con las credenciales que creamos antes:

```
# radtest prueba probando localhost 0
testing123
```

Obtendremos una salida similar a la siguiente:

```
Sending Access-Request of id 114 to
127.0.0.1 port 1812
    User-Name = "prueba"
    User-Password = "probando"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 0
    Message-Authenticator =
0x00000000000000000000000000000000
rad_recv: Access-Accept packet from
host 127.0.0.1 port 1812, id=114,
length=20
```

La última línea dice claramente que el acceso fue aceptado.

En la consola del servidor veremos muchas líneas salir, Sankar, K. (2004), pero la parte medular está cerca del final y dirá algo como:

```
[pap] login attempt with password
"probando"
[pap] Using clear text password
"probando"
[pap] User authenticated successfully
++[pap] returns ok
```

Que nos indica éxito en la autenticación. Si probamos con una clave errónea como poner la "P" mayúscula en la clave:

```
# radtest prueba Probando localhost 0
testing123
```

Obtendremos en el log 3 intentos de autenticación y al final la última línea contendrá un "Access-Reject" bastante claro.

3.2. Segunda prueba de autenticación (remota).

En el siguiente paso realizamos un intento de autenticación remota, es decir en un equipo diferente (un fedora 18 en este caso) lanzamos una prueba remota de conexión. Para ello necesitamos primero indicarle al freeRadius que este equipo estará autorizado para consultarle:

```
# vi /etc/freeradius/clients.conf
```

Al final del archivo agregamos la configuración como NAS para el equipo desde el que lanzaré la prueba:

```
client 192.168.9.7 {
      secret = 123456
      shortname = aspire
   }
```

Donde le decimos que el equipo con la IP 192.168.9.7 le realizará consultas con la palabra secreta 123456. shortname realmente ya no se necesita, aunque sí se requería en versiones anteriores del freeRadius, sin embargo, es útil para fines informativos y de organización interna. Cisco. (s.f.).

En el mismo archivo, más arriba, podremos ver que ya éste contenía la configuración para "localhost", por eso funcionó enseguida sin mayores configuraciones. Cisco. (s.f.). Debug Authentications.Es importante fijarse también que ahí justamente está especificada testing123 como secret, o palabra secreta de autenticación, que es la que proporcionamos en la prueba anterior (local).

Volvemos a levantar el server en modo de depuración e intentamos autenticarnos desde el equipo remoto:

```
[pbernal@aspire ~]$ radtest prueba
probando 192.168.9.66 0 123456
```

El resultado será el mismo que en el ejemplo anterior con la salvedad de que en este caso responderá indicando que la petición se hizo desde la IP 192.168.9.7 del equipo remoto. Si el equipo no estuviese en la lista de clientes (NAS) aceptados obtendríamos algo como:

```
Ignoring request to authentication
address * port 1812 from unknown client
192.168.9.7 port 57500
```

3.3. Notas sobre el firewall de Linux:

En Linux Mint, por ser una distro orientada al usuario final, el firewall no viene activado por defecto, pero si por cualquier circunstancia hiciera falta darle de baja se podría con:

```
# iptables -F
```

3.4. Implementación de PEAP.

Dado que PEAP utiliza un túnel TLS para encapsular la autenticación, requiere el uso de certificados digitales. En un entorno real deberíamos adquirir este certificado, pero freeRadius trae ya un certificado digital autogenerado, que no es válido en la vida real pues

Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2018 pp. 5-15 *Correo: editor@istvidanueva.edu.ec*
Volumen 2, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: agosto 2018 *Fecha de aceptación: octubre 2018*

no existe entidad certificadora que lo valide, pero que para todos los demás fines es perfectamente funcional.
La única diferencia práctica entre usar un certificado auto-firmado como este y uno real que pudimos comprar, es que con éste último, los sistemas operativos de los equipos que se conecten, no emitirán una advertencia de seguridad al momento de la conexión, como sí sucede con el auto-firmado, tal cual lo veremos más adelante. Más allá de esa pequeña molestia y para un entorno de pruebas, este es más que suficiente.

Para activar el protocolo de autenticación PEAP, editamos el archivo /etc/freeradius/eap.conf y cambiamos la línea que dice:

default_eap_type = **md5**

Por:

default_eap_type = **peap**

Hacemos las pruebas respectivas, idénticas a las ya realizadas y todo debería seguir funcionando igual, pues las configuraciones necesarias para PEAP ya vienen establecidas, sólo había que decirle a freeRadius que las use.

3.5. Pruebas con un AP y equipos remotos.

Hasta ahora hemos realizado pruebas satisfactorias sólo con el radtest, tanto local como remotamente, lo que nos permite estar seguros de que el servidor está bien configurado; pero requerimos que ahora sí el sistema trabaje conjuntamente con un equipo NAS y los equipos realmente se autentiquen y conecten a la red por ésta vía. Para esto usaremos un ruteador Linksys WRT54G2 / GS2 al cual se le cambió el firmware por el de DD-WRT v24-sp2, hace varios años ya. Aún cuando detallamos el que usamos, no es demasiado importante la marca/modelo del AP que usemos, cualquiera que soporte WPA2 Enterprise como método de autenticación, debería servir igualmente.

Originalmente este NAS descrito estaba proveyendo el servicio de Internet a la LAN de mi casa (pbernal) a través de WPA2 Personal. Para que trabaje con el radius, sólamente se le cambió el tipo de seguridad Inalámbrica a **WPA2 Enterprise** y se le llenó los datos según lo configurado en el servidor Radius:

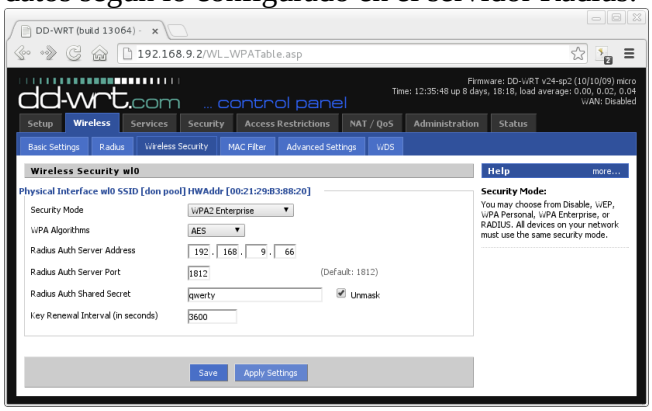

Ilustración 1. Implementación.
Fuente: (Xiaodan & Junhao, 2014)

Luego de darle click en el botón de “Apply Changes” y de unos segundos de refresco, ya tenemos la red “don pool” (este es el SSID) disponible en cualquier equipo dentro del rango de cobertura. Deploying RADIUS Partnerships. (s.f.).

La primera prueba la realizamos con un Fedora 18 como cliente de este AP, donde seleccionamos conectar la red “don pool” y obtuvimos la ventana de solicitud de detalles de autenticación para esta conexión:

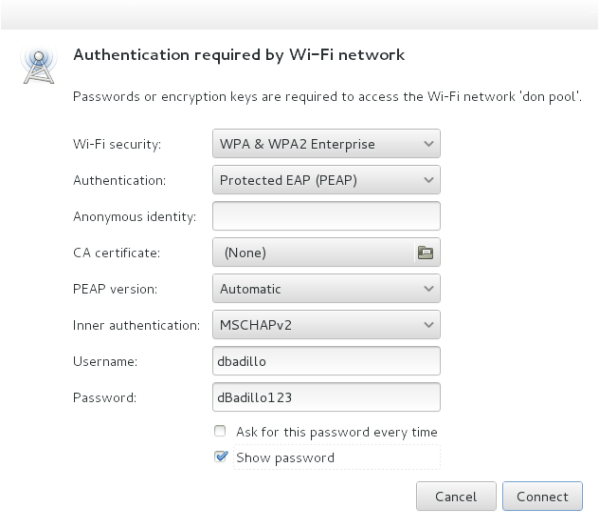

Ilustración 2: Wifi Network
Fuente: (Xiaodan & Junhao, 2014)

Luego de llenar el usuario, la clave (el cual debe coincidir con un usuario y clave definido en el radius) y seleccionar el botón “Connect”, obtenemos una ventana de advertencia del certificado no válido (cosa de la que ya hablamos

Revista Nexos Científicos *ISSN: 2773-7489*
Julio –Diciembre 2018 pp. 5-15 *Correo: editor@istvidanueva.edu.ec*
Volumen 2, Número 2 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: agosto 2018 *Fecha de aceptación: octubre 2018*

antes) pues es uno autogenerado que viene para pruebas con el propio freeradius:

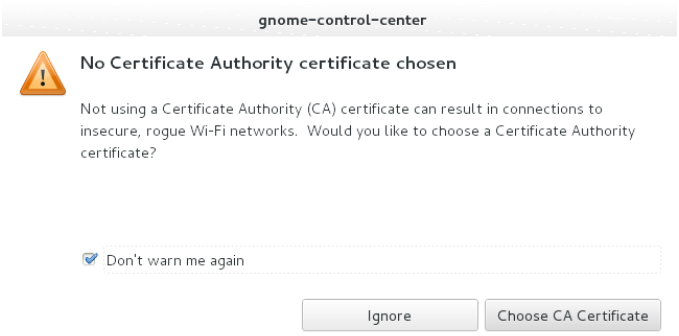

Ilustración 3: Certificado.
Fuente: (Xiaodan & Junhao, 2014)

Simplemente le decimos que la Ignore y el equipo se autenticó exitosamente y entró a la red enseguida. Probamos también con Windows, pero para no redundar, dejamos la documentación de esta demostración de la prueba con Windows para el final (ver más abajo) donde aprovechamos para probar otras características adicionales.

3.6. Radius con MySQL.

En el siguiente paso decidimos activar el trabajo con MySQL, es decir, dejar de lado los archivos de texto como medios de manejo de cuentas para los NAS y para los Usuarios. Al manejar esto con MySQL tenemos la ventaja, entre muchas otras, de por ejemplo poder poner algún sistema Web de administración Radius y facilitar y profesionalizar el manejo de las cuentas.

Pues bien, comenzamos en LinuxMINT con la instalación del servidor de MySQL y el paquete que le provee al freeRadius del soporte para trabajo con MySQL:

```
# apt-get install freeradius-mysql mysql-server
```

Cuando el sistema de manejo de paquetes del Linux Mint (que es el mismo de Ubuntu y el mismo de Debian) ha instalado y arranca por primera vez el servidor MySQL, éste solicita una contraseña para MySQL, no es obligado ponerla, pero sí recomendable. La clave asignada (de root) fue asdfgh, la cual necesitaremos más tarde para los primeros pasos de configuración del entorno MySQL del freeRadius.

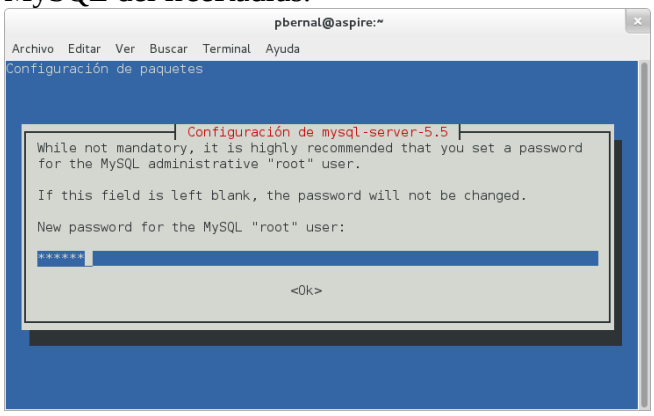

Ilustración 4: Configuración
Fuente: (Xiaodan & Junhao, 2014)

Inmediatamente el procedimiento de instalación termina ya tenemos el servidor MySQL listo y funcionando pues es muy común que los sistemas Debian y similares como Linux Mint y Ubuntu, activen y arranquen los servidores inmediata y automáticamente luego de instalarlos. Es así que simplemente procedemos a loguearnos al MySQL:

```
$ mysql -uroot -pasdfgh
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 41
Server version: 5.5.28-0ubuntu0.12.10.2 (Ubuntu)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

La última línea es el *prompt* de MySQL y nos indica que está esperando el ingreso de comandos. Entonces le creamos la base de datos radius:

```
mysql> CREATE DATABASE radius;
Query OK, 1 row affected (0.00 sec)
```

Luego le otorgamos todos los privilegios al usuario radius hacia la base de datos radius en localhost. Le seteamos además la clave radPass123 pues en la misma instrucción se está creando el usuario implícitamente y salimos de MySQL:

```
mysql> GRANT ALL ON radius.* TO
radius@localhost IDENTIFIED BY
'radPass123';
Query OK, 0 rows affected (0.00 sec)
mysql> \q
Bye
```

Dado que ya creamos la base de datos para el freeRadius y el usuario con privilegios para usarla, ya no es necesario que trabajemos como usuario root, así que en todo comando futuro se usó simplemente las credenciales del usuario radius. Lo primero fue cargar el esquema de tablas necesarias hacia la base de datos:

```
$ mysql -uradius -pradPass123 radius <
/etc/freeradius/sql/mysql/schema.sql
```

El comando anterior usa el cliente mysql para loguearse a la base de datos radius con el usuario radius y la clave radPass123 y ejecuta las instrucciones SQL contenidas en el archivo /etc/freeradius/sql/mysql/schema.sql, a través de una redirección. El resultado es sencillo: la carga del esquema de tablas necesarias hacia la base de datos. El archivo con el esquema viene con el paquete freeradius-mysql que instalamos antes.

Una vez completado, hacemos lo mismo con el esquema para el manejo de los NAS:

```
$ mysql -uradius -pradPass123 radius <
/etc/freeradius/sql/mysql/nas.sql
```

La base de datos ahora tiene todas las tablas necesarias para trabajar con freeRadius. Ahora debemos configurar el freeRadius para indicarle que trabaje con MySQL y no con archivos planos como lo hace por defecto. Para ésto, sólo debimos realizar unas pocas ediciones menores en unos pocos archivos, mismas que se describen a continuación:
En el archivo /etc/freeradius/radiusd.conf, la línea que decía:

```
#       $INCLUDE sql.conf
```

La cambiamos por:

```
        $INCLUDE sql.conf
```

Es decir, simplemente la descomentamos.
Adicionalmente, la línea que decía:

```
        $INCLUDE clients.conf
```

La cambiamos por:

```
#       $INCLUDE clients.conf
```

Es decir comentamos la línea para desactivar la lectura de NAS desde archivos.

En el archivo /etc/freeradius/sql.conf, la línea que decía:

```
        password = "radpass"
```

La cambiamos por:

```
        password = "radPass123"
```

Es decir, seteamos aquí la clave para la base de datos radius, los demás datos de conexión a MySQL no requirieron cambios. Adicionalmente descomentamos la línea:

```
        #readclients = yes
```

para que se vea así:

```
        readclients = yes
```

Lo siguiente fue configurar las secciones “authorize {“, “accounting {“, “session {“ y “post-auth {“ del archivo /etc/freeradius/sites-available/default para habilitarles el uso de SQL. Se puede decir que de esta forma activamos las capacidades AAA en el servidor freeRadius. Para ello, simplemente buscamos, dentro de dichas secciones, las líneas comentadas que decían sql, y las descomentamos cambiando:

```
#       sql
```

por

```
        sql
```

Realmente podríamos escoger no usar SQL para almacenar la información de alguna/s de éstas secciones, pero no es que por ello no se guarde la información que manejan, simplemente que no irían a dar a nuestra base de datos sino que se seguirían almacenando en archivos como hasta el momento. La ventaja de MySQL podría ser que así podríamos disponer de esta información a más largo plazo, pues normalmente los sistemas Linux rotan los logs y eventualmente, estos registros se perderán luego

de varios días o semanas cuando la rotación complete su ciclo.
En el siguiente paso borramos los usuarios que antes creamos en /etc/freeradius/users, pues como no hemos desactivado el módulo de uso de autenticación por archivos (identificado como "files"), estas credenciales seguirán funcionando y obtendremos falsos positivos en la autenticación.

Luego creamos el usuario en la tabla apropiada dentro de la base de datos. En este caso usamos el modificador -e para pasarle una sentencia SQL y ejecutarla sobre la base de datos radius:

```
$ mysql -uradius -pradPass123 radius -e
"INSERT INTO radcheck (UserName,
Attribute, Value) VALUES ('dbadillo',
'Password', 'dBadillo321');"
```

Nota

Igualmente lo hacemos para agregar el NAS a la tabla respectiva. Recordar que ya deshabilitamos la lectura de los NAS por archivo antes:

```
$ mysql -uradius -pradPass123 radius -e
"INSERT INTO nas
(nasname,shortname,secret)
VALUES('192.168.9.2','WRT54G2','qwerty'
);"
```

Nota

Luego de los cambios ponemos nuevamente el servidor a correr en modo debugging y probamos, obviamente lo que esperamos es, por una parte éxito en la autenticación y por otro lado una prueba de que ya el radius está trabajando con MySQL. Dado que la autenticación fue exitosa (el modo debugging así lo indicó en las últimas líneas) y considerando que ya habíamos borrado todo rastro de usuarios de los archivos, asumimos que MySQL está funcionando en este sentido. Ahora revisamos con una consulta a ver si MySQL registró la autenticación:

```
$ mysql -uradius -pradPass123 radius -e
"SELECT * FROM radpostauth;"
+----+----------+------+--------------
+---------------------+
| id | username | pass |
reply         | authdate            |
+----+----------+------+--------------
+---------------------+
|  1 | pbernal  |      | Access-Accept
| 2013-01-22 15:28:20 |
|  2 | pbernal  |      | Access-Accept
| 2013-01-22 15:28:20 |
+----+----------+------+--------------
+---------------------+
2 rows in set (0.00 sec)
```

Efectivamente, MySQL está trabajando adecuadamente con nuestro freeRadius y me indica que se le aceptó el acceso al usuario pbernal.

3.7. RADIUS ADMIN FRONTEND:

Como lo habíamos propuesto antes, una de las ventajas de usar MySQL es la de poder usar un sistema web para administrar las cuentas del servidor Radius. Por supuesto a más de aquello se pueden realizar muchas otras tareas más, como reportes y otras características avanzadas como HotSpot, pero nos centramos simplemente en la posibilidad de facilitar el manejo de cuentas de usuarios y NAS. The FreeRADIUS Server Project Sf.

Luego de una rápida búsqueda en Google, decidimos usar un sistema llamado daloRadius que está construido en PHP, pues lo vimos con varios años de existencia y con actualizaciones hasta hace sólo unos meses. Lo primero fue instalar el servidor web Apache y por supuesto PHP con algunos módulos adicionales y PEAR pues daloRadius dice requerirles en su documentación:

```
# apt-get install apache2 php5 php5-
mysql php5-gd php-pear php-db php-mail
```

Una vez instalado todo, entramos a la carpeta raíz de documentos web del servidor apache, descargamos aquí el paquete con el sistema daloRadius y lo desempaquetamos:

```
# cd /var/www
#
# wget -c
"http://downloads.sourceforge.net/proje
ct/daloradius/daloradius0.9-
9/daloradius-0.9-
```

Revista Nexos Científicos
Julio –Diciembre 2018 pp. 5-15
Volumen 2, Número 2
Fecha de recepción: agosto 2018

ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: octubre 2018

```
9.tar.gz?r=http%3A%2F%2Fsourceforge.net
%2Fprojects%2Fdaloradius%2Ffiles%2Fdalo
radius%2Fdaloradius0.9-9%2Fdaloradius-
0.9-
9.tar.gz%2Fdownload&ts=1358886855&use_m
irror=ufpr"
#
# tar zxf daloradius-0.9-9.tar.gz
```

Nota

En estos casos es costumbre (al menos nuestra) crear un enlace simbólico con un nombre sencillo, como daloradius en este caso, para que sea más fácil de abrir en el web, en lugar de renombrar la carpeta, así, si se pusiera una versión nueva, sólo habría que cambiar el enlace simbólico. Revista Lideres. (2011). Lo creamos y entramos en la carpeta:

```
# ln -s daloradius-0.9-9 daloradius
# cd daloradius
```

Cargamos el archivo SQL que viene con el sistema dentro de la base de datos radius:

```
$ mysql -uradius -pradPass123 radius <
contrib/db/mysql-daloradius.sql
```

Finalmente editamos el archivo library/daloradius.conf.php y le colocamos los datos de acceso a la BD:

```
$configValues['CONFIG_DB_USER'] =
'radius';
$configValues['CONFIG_DB_PASS'] =
'radPass123';
$configValues['CONFIG_DB_NAME'] =
'radius';
```

Sólo nos quedó abrir la URL http://192.168.9.66/daloradius en un navegador y obtenemos:

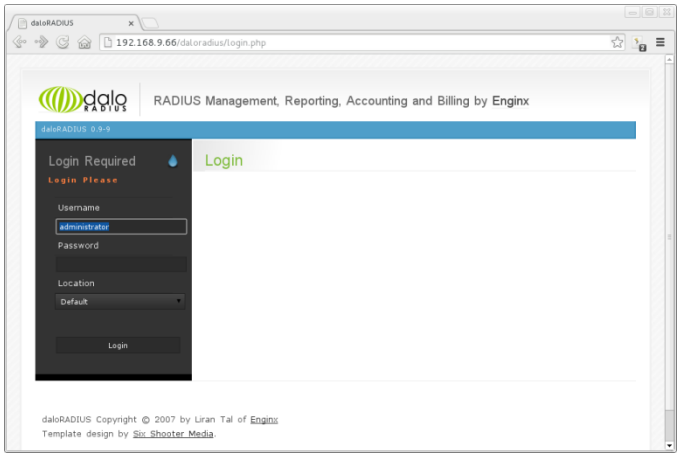

Ilustración 5: Configuración RADIUS
Fuente: (Xiaodan & Junhao, 2014)

Procedemos con los datos de login por defecto que son, username: administrator, password: radius y ya dentro pudimos ver los usuarios:

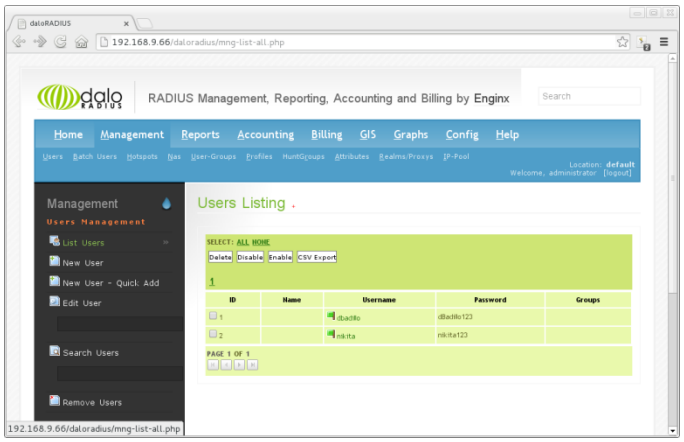

Ilustración 6: Configuración RADIUS
Fuente: (Xiaodan & Junhao, 2014)

los NAS:

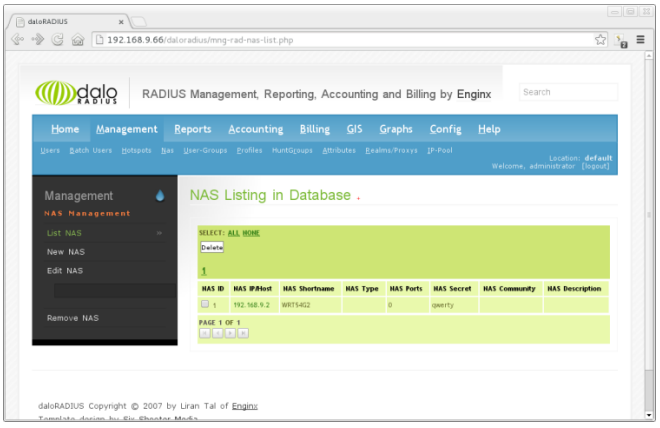

Ilustración 7: Configuración RADIUS
Fuente: (Xiaodan & Junhao, 2014)

y reportes de intentos de conexión:

Revista Nexos Científicos
Julio –Diciembre 2018 pp. 5-15
Volumen 2, Número 2
Fecha de recepción: agosto 2018
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: octubre 2018

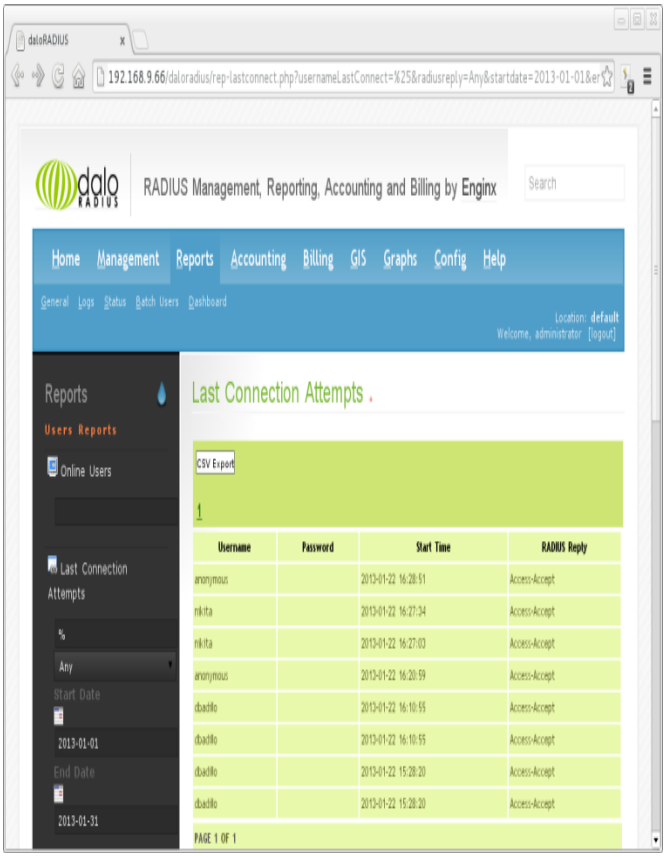

Ilustración 8: Configuración RADIUS
Fuente: (Xiaodan & Junhao, 2014)

Claro, en estas mismas interfaces podremos agregar nuevos usuarios y NAS según lo necesitemos. Es así que por esta vía agregamos el usuario nikita e intentamos conexión, esta vez desde Windows 7 Home 32 bits. Como en este equipo ya teníamos la conexión con este router creada, hubo que editarla para que trabaje con la nueva infraestructura.

Para esto, en el administrador de conexiones, abrimos las propiedades de la conexión con clic derecho -> propiedades. Vamos a la pestaña de Seguridad y seleccionamos WPA2 Enterprise. Wikimedia Foundation, Inc. (s.f.).

En el método de autenticación de red escogemos: Cisco: PEAP porque con el que aparece por defecto el equipo intenta loguearse con el usuario y la clave del equipo y nosotros habíamos creado un usuario diferente. Esta interface puede verse en la figura siguiente:

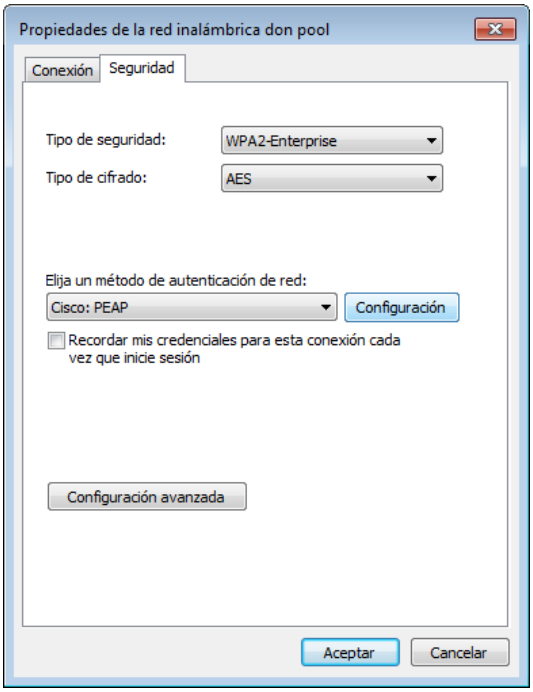

Ilustración 9: Configuración Red Inalámbrica
Fuente: (Xiaodan & Junhao, 2014)

En configuración del método de autenticación, entramos a la pestaña Credenciales de Usuario para seleccionar la opción de Solicitar nombre de usuario y contraseña automáticamente:

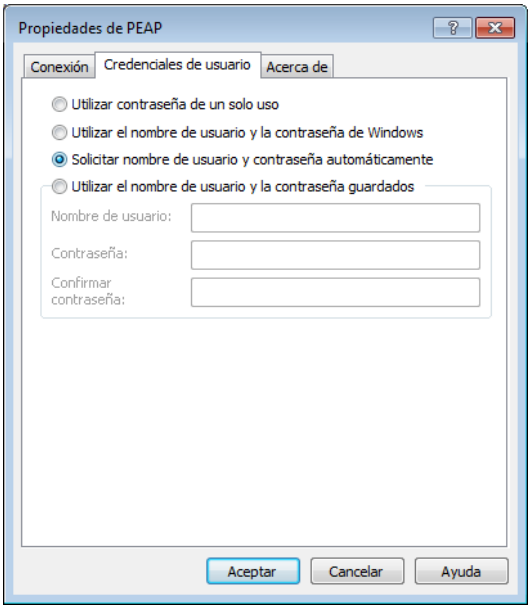

Ilustración 10: Configuración Red Inalámbrica
Fuente: (Xiaodan & Junhao, 2014)

Aceptar en ambas ventanas y damos a conectar, con lo que se nos presenta la ventana de autorización:

Revista Nexos Científicos
Julio –Diciembre 2018 pp. 5-15
Volumen 2, Número 2
Fecha de recepción: agosto 2018
ISSN: 2773-7489
Correo: editor@istvidanueva.edu.ec
URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index
Fecha de aceptación: octubre 2018

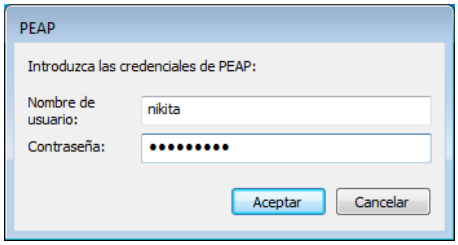

Ilustración 11: Configuración PEAP
Fuente: (Xiaodan & Junhao, 2014)

Luego, como antes en la prueba con Fedora, aparece la advertencia del certificado no válido:

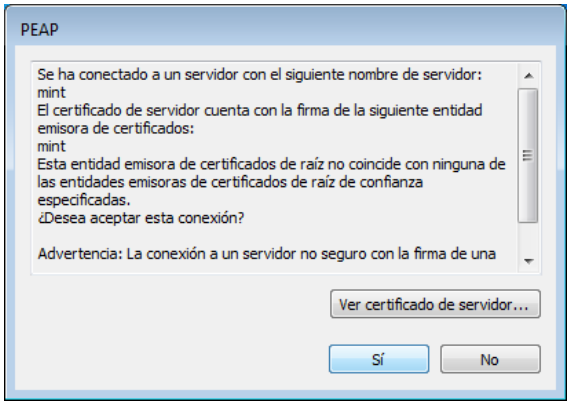

Ilustración 12: Configuración PEAP
Fuente: (Xiaodan & Junhao, 2014)

Al dar clic en Sí, el servidor le autentica y funciona correctamente.

4. CONCLUSIONES

- El mantener versiones actualizadas tanto de los sistemas operativos, de las aplicaciones que controlan los servicios así como del firmware de todos los dispositivos que forman parte de la infraestructura es una medida preventiva que tiende a reducir la indisponibilidad del servicio.

- Para ambientes de producción es necesario habilitar y gestionar adecuadamente, tanto en los servidores como todos los clientes, los Certificados de Autoridad (CA) adecuados que reflejen en ellos los parámetros y características que se ajusten a la realidad de cada entorno.

- Habilitar los modos de depuración tanto en los clientes como el servidor ya que son herramientas poderosas para poder seguir el rastro de un inconveniente al momento de realizar la configuración.

- Prestar mucha atención y cuidado al momento de modificar los parámetros en los archivos de configuración ya que los mismos son del tipo texto que no permite una validación previa de su contenido.

REFERENCIAS

Bhaiji, Y. C. (s.f.). CCIE Professional Development Series Network Security Technologies and Solutions. Cisco Press. Carter, G. (March 20, 2003). LDAP System Administration.

O'Reilly Media, Inc. Carter, G., Ts, J., & Eckstein, R. (January 23, 2007). Using Samba, Third Edition.

Hassell, J. (October 8, 2002).RADIUS. O'Reilly Media, Inc.

Sankar, K., Sundaralingam, S., Balinsky, A., & Miller, D. (November 15, 2004). Cisco Wireless LAN Security.

Cisco. (s.f.). Cisco Systems, Inc. Recuperado el Febrero de 2019 de http://www.cisco.com/en/US/docs/wireless/access_point/12.3_7_JA/configuration/guide/s37cli.html

Cisco. (s.f.). Debug Authentications. Recuperado el Abril de 2011, de Document ID: 50843: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_tech_note09186a008024aa4f.shtml

Deploying RADIUS Partnerships. (s.f.). Deploying RADIUS:The book. Obtenido de http://deployingradius.com/

INEC. (s.f.). Instituto Nacional de Estadísticas y Censos. Obtenido de http://www.inec.gob.ec

Lideres, R. (s.f.). Obtenido de http://www.revistalideres.ec NetMarketShare. (s.f.). Obtenido de http://marketshare.hitslink.com/

Revista Lideres. (30 de 05 de 2011). www.revistalideres.ec. Obtenido de http://www.revistalideres.ec/2011-05-30/Informe.aspx

The FreeRADIUS Server Project. (s.f.). FreeRADIUS The world's most popular RADIUS Server. Obtenido de http://freeradius.org/

Wikimedia Foundation, Inc. (s.f.). Wikipedia. Recuperado el Octubre de 2010, de http://en.wikipedia.org/wiki/Main_Page

Zhang, Y., Zheng, J., & Ma, M. (March 31, 2008). Handbook of Research on Wireless Security. IGI Global.