

# **B**

## **Guía de instalación del software Listry-AIGC**

## Requisitos para la instalación de Nfsen.

Nfsen ocupa las siguientes dependencias para poder ser instalado.

- Apache
- Perl y PHP
  - Perl > 5.6.0
  - PHP > 4.1
- Módulos de perl.
  - Mail:: Header, Mail:: Internet
- Herramientas RRD
  - Todos los gráficos netflow en NfSen requieren RRD. Por lo menos se requiere el módulo de Perl RRDs
- Herramientas Nfdump
  - Necesarias para recoger y procesar datos de Netflow
  - Instalar la versión 1.5.8

Todas estas dependencias se instalaron en un S.O. Centos 5.5 de 32 bits. En caso de requerir ser instalado en alguna otra versión de Linux se deberán de realizar los ajustes para dicha versión.

## Instalación apache.

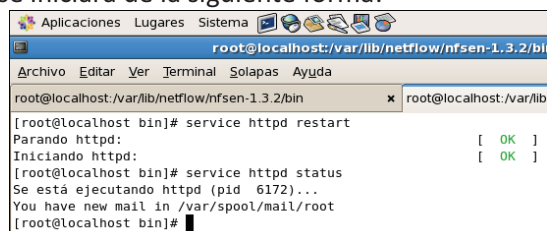
Normalmente en Centos viene instalado apache, esto se puede verificar de la siguiente forma:

```
# service httpd status
```

Si el script devuelve la leyenda “httpd: service desconocido”, significa que no se tiene instalado apache. La forma más fácil para su instalación es ejecutar el siguiente comando en una terminal:

```
# yum -y install httpd
```

Al momento de terminar la instalación, verificar que el servicio se encuentre levantado, en caso de estar detenido, se iniciara de la siguiente forma:



```
[root@localhost bin]# service httpd restart
Parando httpd:                                [ OK ]
Iniciando httpd:                              [ OK ]
[root@localhost bin]# service httpd status
Se está ejecutando httpd (pid 6172)...
You have new mail in /var/spool/mail/root
[root@localhost bin]#
```

Figura B.1 Estado del servicio httpd

Para comprobar que apache ha sido iniciado exitosamente, abrir un navegador web y escribir la siguiente URL:

```
http://localhost:80
```

```
http://IP:80
```

Aparece una ventana como la siguiente:



Figura B.2 Comprobación del servicio http en el servidor web.

Todos los archivos que se visualizan en apache están guardados en “/var/www/”, más adelante se explica el procedimiento para crear directorios virtuales y poder visualizar carpetas con diferentes rutas.

### Instalación PHP

Normalmente php viene instalado por defecto en CentOS, podemos verificar si se tiene instalado PHP, con el siguiente comando.

```
# php --version
```

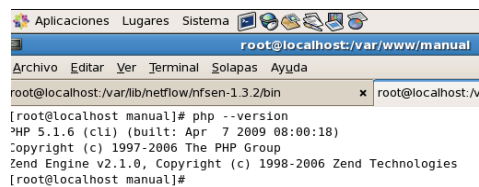


Figura B.3 Verificación de la correcta instalación de PHP.

En caso de no tener instalado php, se instalará de la siguiente forma:

```
# yum -y install php
```

Generalmente al instalarse PHP se configura automáticamente para que sea añadido a apache. Como comprobación, crear un archivo de prueba llamado “hola.php” y guardarlo en /var/www/manual

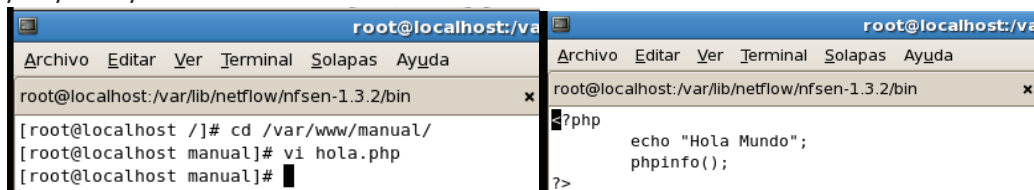


Figura B.4 Creación del script “hola.php”.

Abrir en el navegador web y escribir lo siguiente

URL: <http://localhost/manual/hola.php>

El resultado del script ejecutado es:

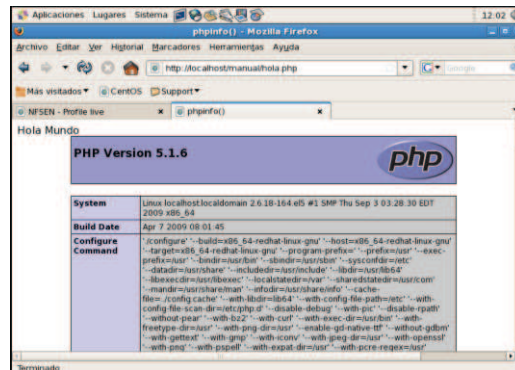


Figura B.5 Resultado de la ejecución del script “hola.php”.

## Instalación de perl

Normalmente Perl viene instalado por defecto en CentOS, se puede comprobar si se tiene instalado perl, tecleando en la terminal:

```
# perl -version
```

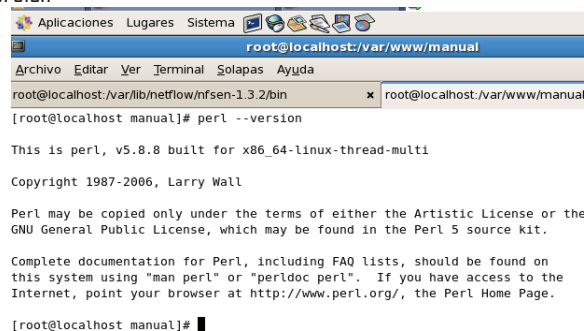


Figura B.6 Verificación de la correcta instalación de perl.

En caso de no tener instalado perl, se instala de la siguiente forma en la terminal:

```
# yum -y install perl
```

## Dependencias de perl.

Nfsen requiere de las siguientes dependencias de perl:

- Mail::Header
- Mail::Internet

Se instalan estas dependencias mediante la herramienta de perl “cpan”.

```
# perl -MCPAN -eshell
```

Esto hace que se cambie el prompt a “cpan”. Para instalar las dependencias teclear.

```
cpan> install Mail::Header
cpan> install Mail::Internet
```

Al terminar la instalación de estas dependencias, salir de cpan.

```
cpan> exit
```

## Instalación de RRDTool.

RRD (Round Robin Database) es un sistema encargado de almacenar y mostrar datos, este software se puede utilizar por medio de una terminal o en cualquier software disponible en ambiente gráfico. RRDTool es de gran utilidad debido a que genera graficas de los datos capturados.

Nfsen se apoya de RRDtool para generar graficas referentes al consumo de internet (BW ocupado, porcentaje de puertos ocupados, disponibilidad de servicios, etc.)

Para la instalación y configuración de RRDtool, realizar lo siguiente:

Dependencias requeridas por RRDtool:

- zlib
- libpng
- Cairo
- Glib
- Pango

Instalar estas dependencias mediante los siguientes comandos en la terminal:

```
# yum install cairo-devel libxml2-devel pango-devel pango libpng-devel freetype freetype-devel
libart_1gpl-devel
```

Ahora es necesario descargar y descomprimir el software RRDTool

```
# cd /opt
# wget http://oss.oetiker.ch/rrdtool/pub/rrdtool-1.4.2.tar.gz
# tar -zxvf rrdtool-versión.tar.gz
```

Compilar e instalar rrdtool, ejecutando los siguientes comandos:

- Acceder al directorio descomprimido:
 

```
# cd rrdtool-version
```
- Exportar la variable "PKG\_CONFIG\_PATH" que tiene como referencia el archivo "pkgconfig":
 

```
# export PKG_CONFIG_PATH=/usr/lib/pkgconfig
```
- Compilar el programa
 

```
# ./configure
```
- Si no arroja ningún error la compilación, instalar
 

```
# make
# make install
```
- En caso de mostrar algún error el proceso de compilación, verificar si falta alguna dependencia que utilice el software RRDtool.

**Nota:** para la instalación de RRDtool en un S.O. CentOS de 32 bits, fue necesario instalar RRDtool de repositorios contenidos en la página oficial de la siguiente forma:

Descargar los archivos:

```
# wget http://daq.wieers.com/rpm/packages/rrdtool/perl-rrdtool-1.2.23-1.el5.rf.i386.rpm
# wget http://daq.wieers.com/rpm/packages/rrdtool/rrdtool-1.2.23-1.el5.rf.i386.rpm
# wget http://daq.wieers.com/rpm/packages/rrdtool/rrdtool-devel-1.2.23-1.el5.rf.i386.rpm
```

Instalar de la siguiente forma:

```
# rpm -ivh perl-rrdtool-1.2.23-1.el5.rf.i386.rpm rrdtool-1.2.23-1.el5.rf.i386.rpm rrdtool-devel-1.2.23-1.el5.rf.i386.rpm
```

Además es necesario instalar una librería extra de la siguiente forma:

```
# yum install libcap-devel
```

**Opcional:** Crear un acceso directo hacia el directorio donde se ha instalado rrdtool:

```
# cd /usr/local
# ln -s rrdtool-versión/ rrdtool/
```

### Verificación de la instalación.

- Acceder hacia la siguiente ruta:
 

```
# cd /opt/rrdtool-version/share/rrdtool/examples
```
- Ejecutar el siguiente script para verificar el correcto funcionamiento de rrdtool
 

```
# ./stripes.pl
```
- Al momento de ejecutar este script, se genera una gráfica llamada “stripes.png”, copiar esta grafica en el directorio de apache.
 

```
# ls -l
# cp stripes.png /var/www/manual/
```
- Verificar la gráfica obtenida en el navegador web.

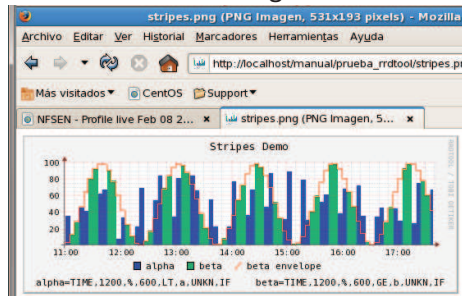


Figura B.7 Resultado de la ejecución del script “stripes.pl”.

### Instalación de Nfdump.

Nfdump es una herramienta la cual nos permite recolectar e interpretar datos provenientes de routers que soportan el protocolo Netflow, El colector Nfdump soporta las versiones 5, 7 y 9 de Netflow.

Para instalar Nfdump es necesario tener instalado los siguientes módulos de perl

- Mail::Header
- Mail::Internet

### Instalación

- Descargar el software de la página oficial.
   
<http://sourceforge.net/projects/nfdump/>
- Descomprimir el archivo descargado
 

```
# tar xzvf nfdump-versión.tar.gz
```
- Configurar Nfdump, habilitando la opción “nfprofile”:
 

```
# ./configure --enable-nfprofile
```
- Al observar que la compilación fue exitosa, instalar el software
 

```
# make
# make install
```
- En caso contrario instalar las dependencias faltantes.
- Para mayor información del software Nfdump consultar:
   
<http://nfdump.sourceforge.net/>
- Verificar la instalación en la terminal:
 

```
# nfdump -V
```

```

root@localhost:~
[root@localhost ~]# nfdump -V
nfdump: Version: 1.6 $LastChangedDate: 2010-01-12 14:53:16 +0100 (Tue, 12 Jan 2010) $
$Id: nfdump.c 40 2009-12-16 10:41:44Z haag $
[root@localhost ~]#

```

Figura B.8 Verificación de la correcta instalación del software nfdump.

## NfSen.

NfSen provee una interfaz gráfica del colector Nfdump, para poder instalar el software NfSen, es necesario tener instaladas correctamente todas las dependencias y software anteriores.

NfSen crea una instalación de acuerdo al siguiente esquema:

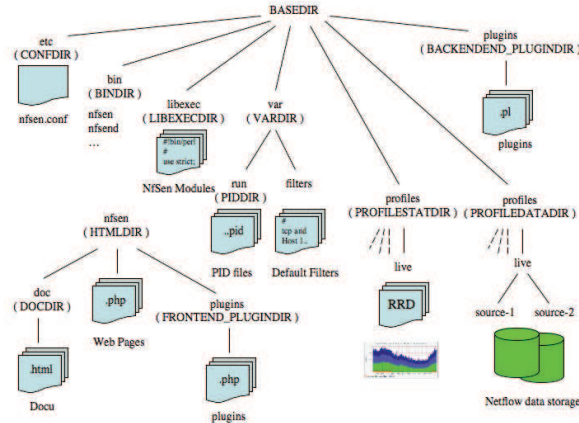


Figura B.9

Esquema de instalación del software NfSen

Donde BASEDIR es la carpeta en donde se desea instalar el software NFsen.

Antes de instalar el software NfSen, es necesario crear usuarios que solo serán utilizados por este software y configurar el archivo nfsen.conf de la siguiente forma:

### Usuarios.

NfSen corre bajo un usuario local, por defecto "netflow", por lo cual procedemos a crear el usuario "netflow" dentro del grupo APACHE.

```
# useradd -G apache -d /Lystri-AIGC/nfsen-version netflow
```

Es importante proporcionar permisos de lectura y escritura, además de cambiar al propietario de este grupo para el correcto funcionamiento del software NfSen:

```
# chown netflow:apache ~netflow
# chmod 750 ~netflow
```

### Instalación.

- Descargar el software NfSen de la página oficial y descomprimirlo:
  - <http://sourceforge.net/projects/nfsen/>
  - # tar xzvf nfsen-version.tar.gz
- NfSen requiere de un archivo de configuración especial, el cual es necesario descargarlo:
  - <http://nfsen.sourceforge.net/nfsen-dist.conf>
- Sobrescribir el contenido de nfsen.conf con el archivo nfsen-dist.conf en "etc" (se encuentra dentro del directorio de instalación no en la carpeta /etc general)
 

```
# cp nfsen-dist.conf etc/nfsen.conf
```
- Editar el archivo nfsen.conf cambiando las siguientes líneas:
  - \$BASEDIR (Poner la ruta de instalación de NfSen en este caso "/Lystri-AIGC/nfsen-version")
  - \$WWWUSER/\$WWWGROUP (Cambiar a apache)
  - %sources (Eliminar los dos ejemplos y añadir los flujos correspondientes, ver anexo C)

- Instalar Nfsen de la siguiente forma:
 

```
# ./install.pl etc/nfsen.conf
```
- El script de instalación solicita la ubicación de librerías de perl, verificar que tenga marcadas /usr/bin/perl y dar enter.
- Para ejecutar el software Nfsen, cambiar a su directorio de instalación y ejecutar el script "nfsen" para iniciar los servicios de la siguiente forma:
 

```
# cd /Lystri-AIGC/nfsen-version /bin
# ./nfsen start
```

### Configurando directorios virtuales en apache.

Debido a cuestiones de seguridad, no es posible poder mostrar en el servidor apache todos los directorios que se encuentran en "/var/www".

Al momento de instalar el software Nfsen se crea el directorio "/var/www/Nfsen". Es necesario realizar configuraciones en el servidor apache, para poder visualizar este directorio creado de la siguiente forma:

- Crear un archivo de configuración dentro de httpd, este archivo contendrá las opciones necesarias para poder acceder al directorio y una opción extra de seguridad que pedirá autenticarse antes de entrar a este directorio:
 

```
# vi /etc/httpd/conf.d/nfsen.conf
```
- El nuevo archivo creado tendrá lo siguiente:
 

```
Alias /nfsen /var/www/nfsen
<Directory /var/www/nfsen/>
  DirectoryIndex nfsen.php
  Options -Indexes
  AllowOverride all
  order allow,deny
  allow from all
  AuthType Basic
  AuthUserFile /etc/httpd/conf/htpasswd.nfsen
  AuthName "Access"
  require valid-user
</Directory>
```
- Estas opciones indican que para poder acceder al directorio es necesario autenticarse, además de indicar el directorio virtual al que se tendrá acceso en el servidor apache.
- Es necesario crear el archivo en donde se almacenará la contraseña correspondiente para que pueda acceder el usuario "netflow" al directorio creado.
 

```
# htpasswd -c /etc/httpd/conf/htpasswd.nfsen admin
```
- Escribir la contraseña.
- Reiniciar el servidor apache para poder visualizar los cambios realizados:
 

```
#service httpd restart
```

Acceder al software Nfsen por medio de la siguiente URL:

<http://localhost/nfsen/index.php>



### Solucionando errores presentados al momento de acceder a nfsen.

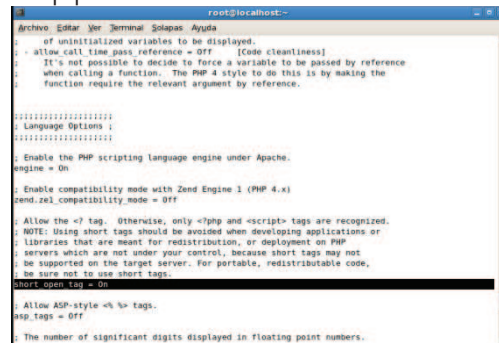
Al momento de iniciar Nfsen por primera vez, se presentaron los siguientes errores:

- ERROR: nfsen connect() error: Permission denied!
- ERROR: nfsen – conecction failed!
- ERROR: Cannot initialize globals!

Estos errores se solucionaron de la siguiente forma:

- Verificar en el archivo “php.ini” que se tenga encendida la etiqueta “short\_open\_tag=on”

```
# vi /etc/php.ini
```



```

; of uninitialized variables to be displayed.
; - allow_call_time_pass_reference = OFF [Code cleanliness]
;   It's not possible to decide to force a variable to be passed by reference
;   when calling a function. The PHP 4 style to do this is by making the
;   function require the relevant argument by reference.
;
;::::::::::::::::::::::::::
; Language Options :
;::::::::::::::::::::::::::
;
; Enable the PHP scripting language engine under Apache.
engine = On
;
; Enable compatibility mode with Zend Engine 1 (PHP 4.x)
zend.zei_compatibility_mode = Off
;
; Allow the <? tag. Otherwise, only <?php and <script> tags are recognized.
; NOTE: Using short tags should be avoided when developing applications or
; libraries that are meant for redistribution, or deployment on PHP
; servers which are not under your control, because short tags may not
; be supported on the target server. For portable, redistributable code,
; be sure not to use short tags.
short_open_tag = on
;
; Allow ASP-style <% %> tags.
asp_tags = Off
;
; The number of significant digits displayed in floating point numbers.

```

Figura B.10 Archivo “php.ini”

- Aplicar un parche en el archivo “Nfcomm.pm”:

```

“@@-770,6 +770,7@@
return undef;
    }
    chmod 0660, $socket_path;
    + chown $NFConf::UID, $NFConf::GID, $socket_path;
    } else {
        # TCP Internet socket

```

Nota: la línea + es lo que se agregara a este archivo, quedando de la siguiente forma:

```

# cd /var/lib/netflow/nfsen-versión/libexec
# vi Nfcomm.pm

```



```

769 my $socket_path = $NFConf::COMMSOCKET;
770 unlink $socket_path;
771 my $addr = sockaddr_un($socket_path);
772
773 my $sock = bind($server, $addr);
774 if ( !$sock ) {
775     $log->ERROR => $!;
776     close $server;
777     return undef;
778 }
779 chmod 0660, $socket_path;
780 #inserte
781 chown $NFConf::UID, $NFConf::GID, $socket_path;
782 #####
783 } else {
784     # TCP Internet socket
785     my $proto_tcp = getprotobyname('tcp');
786     IF ( !socket($server, PF_UNIX, SOCK_STREAM, $proto_tcp) ) {
787         $log->ERROR => $!;
788         return undef;
789     }
790 }

```

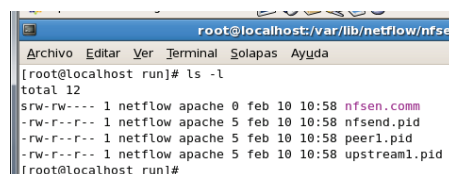
Figura B.11 Archivo “Nfcomm.pm”

Nfsen tiene un socket llamado “nfsen.comm”, el cual se encarga de la comunicación del software, este socket necesita permisos de lectura y escritura para su correcto funcionamiento. Asignar estos permisos de la siguiente forma:

```

# cd /var/lib/netflow/nfsen-versión/var/run
# chmod 660 nfsen.comm
# ls -l

```



```

root@localhost:~# cd /var/lib/netflow/nfsen
root@localhost:~# cd /var/lib/netflow/nfsen-versión/var/run
root@localhost:~# ls -l
total 12
srw-rw-r-- 1 netflow apache 0 feb 10 10:58 nfsen.comm
-rw-r--r-- 1 netflow apache 5 feb 10 10:58 nfsend.pid
-rw-r--r-- 1 netflow apache 5 feb 10 10:58 peer1.pid
-rw-r--r-- 1 netflow apache 5 feb 10 10:58 upstream1.pid
root@localhost:~#

```

Figura B.12 Verificación de la asignación de correctos permisos al socket “nfsen.comm”

Reiniciar el software Nfsen

```
# cd /Lystri-AIGC/nfsen-version /bin
# ./nfsen restart
```

Ahora será necesario detener el firewall Selinux para probar la correcta ejecución de nuestro software de la siguiente forma.

- Sistema → Administración → Nivel de seguridad y Cortafuegos
  - Deshabilitamos SELinux y las opciones de cortafuegos.

### Configuración de apache con el módulo HTTPS.

HTTPS es la versión segura del protocolo HTTP, inventada en 1996 por Netscape Communications Corporation. No es un protocolo separado de HTTP. Se trata de una combinación de este último con un mecanismo de transporte SSL o TLS, garantizando una protección razonable durante la comunicación cliente-servidor. Es ampliamente utilizado en la red mundial (WWW o World Wide Web) para comunicaciones como transacciones bancarias y pago de bienes y servicios. El servicio utiliza el puerto 443 por TCP para realizar las comunicaciones

Para la habilitación del módulo SSL en apache, es necesario realizar lo siguiente:

Instalar el módulo SSL

```
# yum -y install mod_ssl
```

A fin de mantener cierta organización, y un directorio dedicado para cada sitio virtual SSL, es conveniente crear un directorio específico para almacenar los certificados de cada sitio virtual SSL. Igualmente, por motivos de seguridad, debe ser solamente accesible para el usuario root.

```
# mkdir -mp 0700 /etc/ssl/midominio.org
```

### Generando clave y certificado.

Se debe crear una clave con algoritmo RSA de 1024 octetos y estructura x509, la cual se cifra utilizando Triple DES (Data Encryption Standard), almacenado en formato PEM de modo que sea interpretable como texto ASCII. En el proceso descrito a continuación, se utilizan 5 ficheros comprimidos con gzip, que se utilizan como semillas aleatorias que mejoran la seguridad de la clave creada (server.key).

```
# openssl genrsa -des3 -rand \
fichero1.gz:fichero2.gz:fichero3.gz:fichero4.gz:fichero5.gz \
-out server.key 1024
```

Si se utiliza este fichero (server.key) para la configuración del sitio virtual, se requerirá de interacción del administrador cada vez que se tenga que iniciar, o reiniciar, el servicio httpd, ingresando la clave de acceso de la clave RSA. Este es el procedimiento más seguro, sin embargo, debido a que resultaría poco práctico tener que ingresar una clave de acceso cada vez que se inicie el servicio httpd, resulta conveniente generar una clave sin Triple DES, la cual permita iniciar normalmente, sin interacción alguna, al servicio httpd. A fin de que no se sacrifique demasiada seguridad, es un requisito indispensable que esta clave (fichero server.pem) solo sea accesible para root. Ésta es la razón por la cual se crea el directorio /etc/ssl/midominio.org con permiso de acceso solo para root.

```
# openssl rsa -in server.key -out server.pem
```

Opcionalmente se genera un fichero de petición CSR (Certificate Signing Request) que se hace llegar a una RA (Registration Authority o Autoridad de Registro), como Verisign, quienes, tras el correspondiente pago, envían de vuelta un certificado (server.crt) firmado por dicha autoridad.

```
# openssl req -new -key server.key -out server.csr
```

Lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del anfitrión.
- Dirección de correo.
- Opcionalmente se puede añadir otra clave de acceso y nuevamente el nombre de la empresa.

Si no se desea un certificado firmado por un RA, puede generarse uno certificado propio utilizando el fichero de petición CSR (server.csr). En el ejemplo a continuación, se crea un certificado con estructura X.509 en el que se establece una validez por 730 días (dos años).

```
# openssl x509 -req -days 730 -in server.csr \
-signkey server.key -out server.crt
```

Con la finalidad de que solo el usuario root pueda acceder a los ficheros creados, se deben cambiar los permisos de éstos archivos a solo lectura para root.

```
# chmod 400 /etc/ssl/midominio.org/server.*
```

### Configuración de Apache.

Crear la estructura de directorios para el sitio de red virtual.

```
# mkdir -p /var/www/midominio.org/{cgi-bin,html,logs,etc,var}
```

De todos directorios creados, solo /var/www/midominio.org/html, /var/www/midominio.org/etc, /var/www/midominio.org/cgi-bin y /var/www/midominio.org/var pueden pertenecer al usuario, sin privilegios, que administrará éste sitio de red virtual. Por motivos de seguridad, y a fin de evitar que el servicio HTTPD no sea trastornado en caso de un borrado accidental de algún directorio, tanto /var/www/midominio.org/ como /var/www/midominio.org/logs, deben pertenecer al usuario root.

Añadir al archivo /etc/httpd/conf.d/nfsen.conf el siguiente contenido:

```
NameVirtualHost *:443
<VirtualHost *:443>
  ServerAdmin root@localhost.localdomain
  DocumentRoot /var/www/localhost/html
  SSLEngine on
  SSLCertificateFile /etc/ssl/localhost/server.crt
  SSLCertificateKeyFile /etc/ssl/localhost/server.pem
  #SSLCertificateChainFile /etc/apache/domain.com/CA_issuing.crt
  ServerName localhost
<Directory /var/www/localhost>
  Options Indexes FollowSymLinks MultiViews
  AllowOverride None
  Order allow,deny
  allow from all
</Directory>
</VirtualHost>
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio httpd.

```
# service httpd restart
```

## Instalación del software OpenWebmail

OpenWebmail es un proyecto libre, de código abierto (Open Source) que permite visualizar el correo electrónico de forma gráfica. Para la instalación de Openwebmail, realizar lo siguiente:

Descargar e instalar dependencias de perl ocupadas por OpenWebmail

```
# cd /usr
# wget http://packages.sw.be/perl-Text-lconv/perl-Text-lconv-1.4-1.2.el5.rf.i386.rpm
# rpm -ivh perl-Text-lconv-1.4-1.2.el5.rf.i386.rpm
```

Añadir e instalar el repositorio oficial de OpenWebmail a los repositorios de CentOS

```
# cd /etc/yum.repos.d
# lftpget http://openwebmail.org/openwebmail/download/redhat/rpm/release/openwebmail.repo
# yum install openwebmail
```

## Instalación y configuración de MySQL y Navicat.

Verificar si se tiene instalado MySQL:

```
# rpm -q mysql mysql-server
```

En caso de no estar instalado, ejecutar:

```
# yum -y install mysql mysql-server
```

Iniciar y configurar el servicio de MySQL para que se cargue al inicio del S.O.

```
# service mysqld start
# chkconfig --level 345 mysqld on
```

Entrar a MySQL y asignar contraseña al usuario root:

```
# mysql
use mysql
update user set Password=PASSWORD('nuevo_password') where user='root';
```

Verificar que se ha asignado correctamente la contraseña y creación de la base de datos utilizada.

```
mysql -u root -p
create database anomalias;
```

Se utiliza el software Navicat para la administración de la BD creada. Descargar y descomprimir el software.

```
# cd /Listry-AIGC
# wget http://download2.navicat.com/download/navicat9_lite_en.tar.gz
# tar -xvf navicat9_lite_en.tar.gz
```

Iniciar el servicio de Navicat en modo "background":

```
# /Listry-AIGC/navicat9_lite_en/start_navicat &
```

Al ejecutar el comando anterior aparece la ventana principal del software Navicat, configurar la conexión a MySQL, dar clic en "conection->MySQL" y asignar el nombre de usuario y contraseña.

Una vez realizado esto dar clic en "mysql->anomalías" para acceder a la base de datos creada.

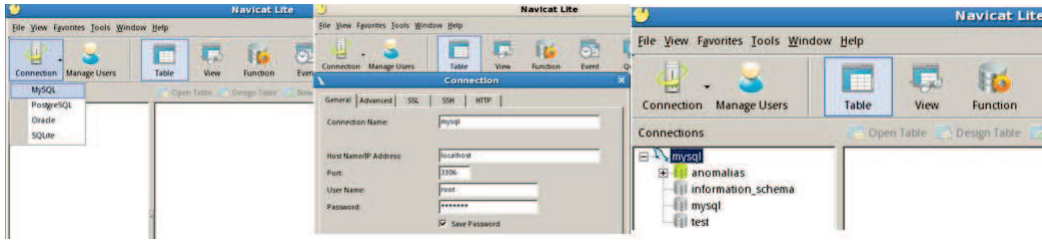


Figura B.13 Acceder al bases de datos mediante el software Navicat

Crear las tablas ‘epuertos’, ‘eips’, ‘exterior’ y ‘anomalias’.

**Tabla ‘epuertos’, ‘eips’ y ‘DoS’**

Tabla B.1 Campos creados en las tablas ‘epuertos’, ‘eips’ y ‘DoS’

Campo	Tipo	Longitud (bytes)	Llave primaria
ID	int	12	Sí
Fecha	datetime	0	Sí
Protocolo	varchar	1000	No
Ip_origen	varchar	5000	No
Ip_destino	varchar	5000	No
Pto_destino	varchar	5000	No

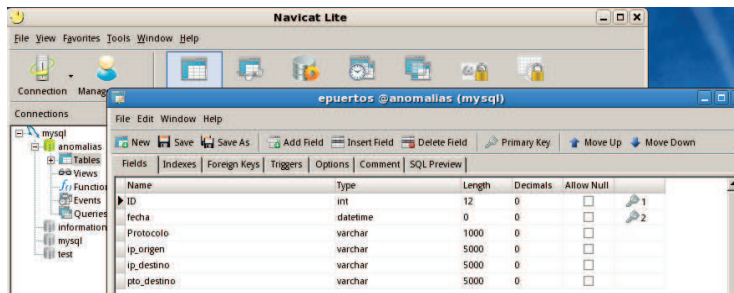


Figura B.14 Verificación de la correcta creación de las tablas ‘epuertos’, ‘eips’ y ‘DoS’

**Tabla ‘exterior’**

Tabla B.2 Campos creados en las tabla2 ‘exterior’

Campo	Tipo	Longitud (bytes)	Llave primaria
ID	int	12	Sí
Fecha	datetime	0	Sí
Protocolo	varchar	1000	No
Ip_origen	varchar	5000	No
Ip_destino	varchar	5000	No
Pto_origen	varchar	5000	No

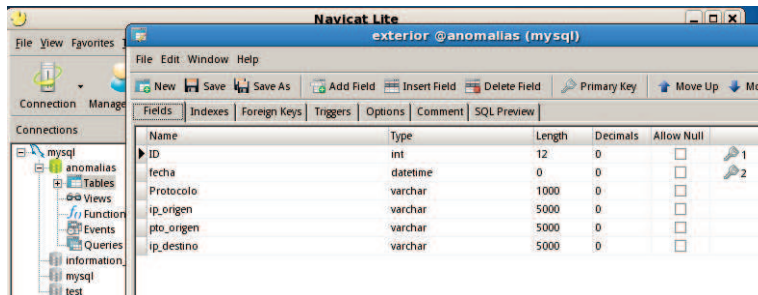


Figura B.15 Verificación de la correcta creación de la tabla ‘exterior’

## Verificación de la correcta instalación del Software “Listry-AIGC”

### Https y Nfsen.

En un navegador web, teclear la siguiente URL:

[https://ip\\_server/nfsen/nfsen.php](https://ip_server/nfsen/nfsen.php)

El navegador web indica que no es una conexión confiable, obtener el certificado de seguridad.

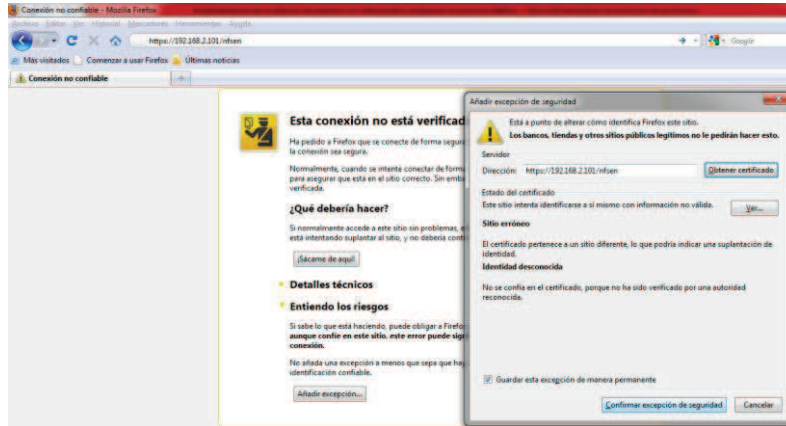


Figura B.16 Verificación de la correcta ejecución de HTTPS

Al momento de acceder aparece una ventana de autenticación, teclear:

- ✓ Usuario: admin
- ✓ Contraseña: \*\*\*\*\*,

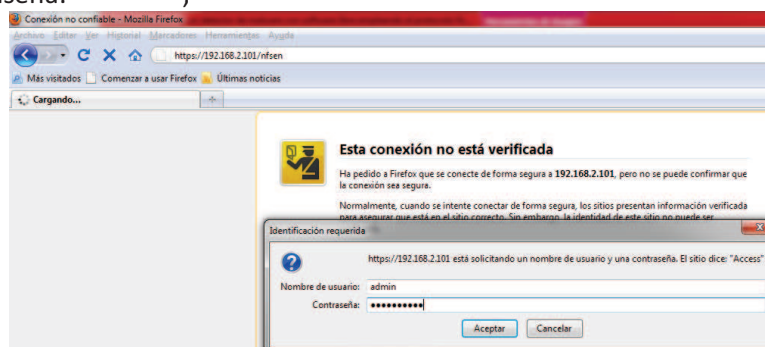


Figura B.17 Autenticación del software Nfsen

Finalmente se observa la página de inicio del software Nfsen.

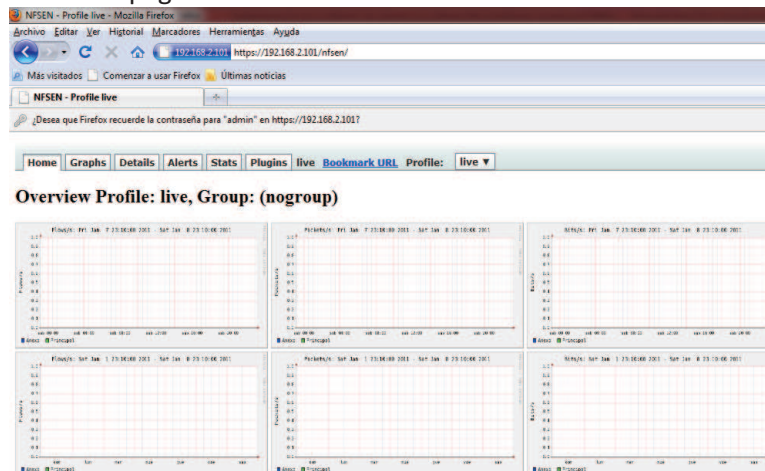


Figura B.18 Página de inicio del software Nfsen



## OpenWebmail.

Para acceder al software OpenWebmail. Teclear en un navegador web la siguiente URL [https://ip\\_server/webmail](https://ip_server/webmail)

Autenticarse con una cuenta que exista en el sistema y no sea la cuenta de root (por cuestiones de seguridad el software OpenWebmail deshabilita esta cuenta).

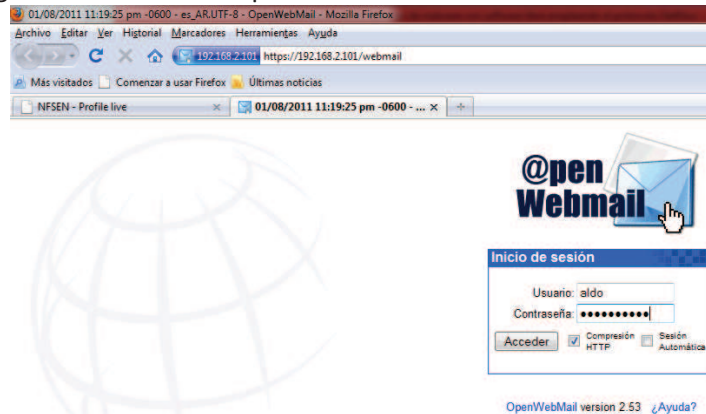


Figura B.19 Autenticación del software OpenWebmail

Para la visualización del correcto funcionamiento del software OpenWebmail, se creó un script en perl que envía un correo electrónico, este script se llama "envía\_correo.pl"

```
#!/usr/bin/perl
use strict;
my $fecha;
my @arreglo;
my $tmp;
open (MAIL,"|/usr/sbin/sendmail -t");
print MAIL "Content-Type: text/plain; charset=iso-8859-1\n";
print MAIL "To: aldo@localhost.localdomain\n";
print MAIL "From: aldo@localhost.localdomain\n";
print MAIL "Subject: Hola mensaje de prueba voy a enviar un email\n";
print MAIL "Content-Type: text/plain; charset=iso-8859-1\n";
print MAIL "Hola, este es un mensaje de prueba, saludos!!\n\n";
close (MAIL)
```

Ejecutar el script envía\_correo.pl

```
# perl envía_correo.pl
```

Observar en la página principal del software el nuevo correo.

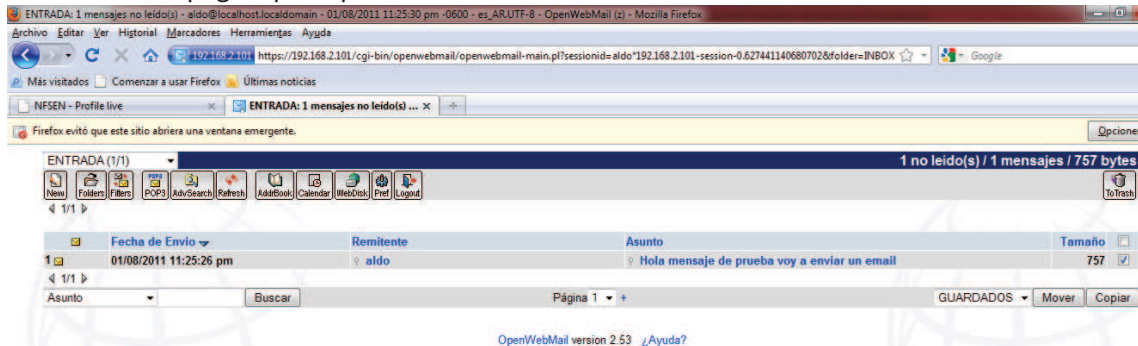


Figura B.20 Verificación del correcto funcionamiento del software Openwebmail