

## NetFlow - Ejercicio con PortTracker

# Tareas opcionales

## Instalar el plugin PortTracker

Necesitamos nfdump versión 1.6.5 o más reciente. La versión de nfdump incluida en Ubuntu 12.04 es 1.6.3p1, la cual no servirá para PortTracker.

Primero, conéctese a su máquina virtual y conviértase en root:

```
~~~~~
ssh sysadm@pcN.ws.nsrc.org
$ sudo bash
#
~~~~~
```

Ahora descargaremos la última versión de nfdump, la herramienta base para procesar los datos de netflow (esto es lo que NfSen usa también). Vamos a configurar e instalar el paquete fuente:

```
~~~~~
# cd /usr/local/src
# wget http://noc.ws.nsrc.org/downloads/nfdump-1.6.6.tar.gz
# tar xvzf nfdump-1.6.6.tar.gz
# cd nfdump-1.6.6
# ./configure --prefix /usr --enable-nfprofile --enable-nftrack
# make
# make install
~~~~~
```

\* Cree una carpeta para los datos de nftrack

```
~~~~~
# mkdir -p /var/log/netflow/porttracker
# chown www-data /var/log/netflow/porttracker
~~~~~
```

\* Configure PortTracker para encontrar la carpeta:

```
~~~~~
# editor extra/PortTracker.pm
```

Busque la línea:

```
my $PORTSDBDIR = "/data/ports-db";
```

y cámbiela a:

```
my $PORTSDBDIR = "/var/log/netflow/porttracker";
~~~~~
```

Guarde y salga.

\* Instale los plugins en la distribución de NfSen

```
~~~~~
# cp extra/PortTracker.pm /var/nfsen/plugins/
# cp /usr/local/src/nfsen-1.3.6p1/contrib/PortTracker/PortTracker.php \
  /var/www/nfsen/plugins/
~~~~~
```

\* Agregue la definición del plugin en la configuración de NfSen:

```
~~~~~
```

```
# cd /usr/local/src/nfsen-1.3.6pl
# editor etc/nfsen.conf
```

~~~~~

\* Encuentre la sección de plugins y ajústela como sigue:

```
~~~~~
@plugins = (
    [ 'live', 'PortTracker'],
);
~~~~~
```

Grabe y salga

\* Vuelva a ejecutar el instalador de NFSen. Cuando se le pregunte:

```
Perl to use: [/usr/bin/perl]
```

Oprima ENTER

```
~~~~~
# perl install.pl etc/nfsen.conf
~~~~~
```

Si ve mensajes como éste:

```
Subroutine Lookup::pack_sockaddr_in6 redefined at /usr/share/perl/5.14/Exporter.pm line 67.
at /var/nfsen/libexec/Lookup.pm line 43...
```

No se preocupe. Es un fallo en esta versión de NFSen, pero no afecta.

\* Inicialice la base de datos de PortTracker

```
~~~~~
# sudo -u www-data nftrack -I -d /var/log/netflow/porttracker
~~~~~
```

(Esto puede durar MUCHO! - Se crearán 8 GB de archivos )

\* Ajuste los permisos para que el usuario netflow que corre nfsen, y el usuario www-data que corre el servidor web, puedan acceder a los datos de porttracker:

```
~~~~~
# chown -R netflow:www-data /var/log/netflow/porttracker
# chmod -R 775 /var/log/netflow/porttracker
~~~~~
```

\* Reinicie:

```
~~~~~
# /var/nfsen/bin/nfsen reload
~~~~~
```

\* Compruebe:

```
~~~~~
# grep -i 'porttracker.*success' /var/log/syslog
Oct 12 13:19:35 pc1 nfsen[28005]: Loading plugin 'PortTracker': Success
Oct 12 13:19:35 pc1 nfsen[28005]: Initializing plugin 'PortTracker': Success
~~~~~
```

\* Espere unos minutos, y luego vaya a la interfaz web de NFSen

```
~~~~~
```

<http://pcX.ws.nsrc.org/nfsen/nfsen.php>

... vaya a la pestaña de plugins

Quizá le salga el error "No plugins installed!" - No se preocupe. Necesita esperar unos minutos para que NfSen pueda empezar a mostrar el plugin PortTracker y sus gráficos.

Al llegar aquí ha terminado. Felicitaciones!

## ## Resolución de problemas

Si le sale el error "Cannot Read Stats file", revise en el directorio de porttracker si hay dos archivos adicionales: portstat24.txt y portstat.txt, como sigue:

```
# ls -l /var/log/netflow/porttracker/portstat*
-rw-r--r-- 1 netflow www-data      677 2011-11-17 14:30 /var/log/netflow/\
porttracker/portstat24.txt
-rwxrwxr-x 1 netflow www-data      638 2011-11-17 14:30 /var/log/netflow/\
porttracker/portstat.txt
```

Asegúrese de que NfSen puede escribir en ese directorio.

## ## Si quiere agregar más fuentes

(Nota: ya debería tener dos fuentes, y no necesita hacer este paso!)

Vuelva al lugar donde desempaquetó la distribución de NfSen.

```
# cd /usr/local/src/nfsen-1.3.6pl
# editor etc/nfsen.conf
```

Actualice su %sources para reflejar cualesquiera nuevas fuentes tenga.  
(esto es un ejemplo! Sólo hágalo si tiene más fuentes)

```
%sources = (
'rtr' => { 'port' => '9000', 'col' => 'e4e4e4' },
'rtr2' => { 'port' => '9001', 'col' => '#0000ff' },
'rtr3' => { 'port' => '9002', 'col' => '#00cc00' },
'rtr4' => { 'port' => '9003', 'col' => '#000000' },
'rtr5' => { 'port' => '9004', 'col' => '#ff0000' },
'rtr6' => { 'port' => '9005', 'col' => '#ffff00' },
);
```

Grabe y salga.

Recuerde, ya ha actualizado nfsen.conf, así que debe ejecutar de nuevo el instalador:

```
# perl install.pl etc/nfsen.conf
```

Reinicie NfSen

```
# service nfsen stop
```

```
# sudo service nfsen start
```

```
~~~~~
```

```
Eso es todo amigos!
```