

NetFlow - Ejercicio con PortTracker

Tareas opcionales

Instalar el plugin PortTracker (opcional o como referencia)

Este ejercicio asume que ya se instalo nfdump desde las fuente con las opciones ``- enable-nfprofile`` y ``- enable-nftrack``, con nftrack instalada en `/usr/local/bin`. Si no es así, consulte el ejercicio 2.

* Cree un directorio para los datos nftrack

```
~~~~~  
$ sudo mkdir /var/ports-db  
$ sudo chown netflow /var/ports-db  
~~~~~
```

Establecer el directorio de datos nftrack en el módulo PortTracker.pm
(que se encuentra bajo la fuente nfsen)

```
~~~~~  
$ cd  
$ cd nfsen-1.3.6p1/contrib/PortTracker  
$ editor PortTracker.pm
```

Find the line:

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

and change it to:

```
my $PORTSDBDIR = "/var/ports-db";  
~~~~~
```

Save and exit from the file.

* Install the plugin into the NFSen distribution

```
~~~~~  
$ sudo cp PortTracker.pm /var/nfsen/plugins/  
$ sudo cp PortTracker.php /var/www/nfsen/plugins/  
~~~~~
```

* Añadir la definición del plugin en el archivo de configuración
nfsen.conf

```
~~~~~  
$ cd /var/nfsen/etc  
$ sudo editor nfsen.conf  
~~~~~
```

* Encuentre la sección de plugins y hacer que se vea así:

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

~~~~~  
Guarde y salga del archivo.

\* Inicialice los archivos de base de datos de PortTracker

~~~~~  
\$ sudo -u netflow nftrack -I -d /var/ports-db
~~~~~

(Esto puede tardar mucho tiempo - se creará 8 GB de archivos)

\* Establezca los permisos para que el usuario netflow que esta corriendo nfsen,  
y el usuario www-data de la Interfaz Web, puedan acceder a los datos PortTracker.

~~~~~  
\$ sudo chown -R netflow:www-data /var/ports-db
\$ sudo chmod 775 /var/ports-db
\$ sudo chmod 664 /var/ports-db/*
~~~~~

\* Reiniciar NFSen

~~~~~  
\$ sudo service nfsen reload
~~~~~

\* Compruebe que todo salio bien!!

~~~~~  
\$ 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 algunos minutos, y vaya a la GUI de nfsen

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

... y seleccione la pestaña de Plugins.

> Usted puede obtener un error de que "No hay plugins disponibles!":  
Si es así, salga y vuelva a iniciar el navegador.

>Usted puede obtener "Error reading stat". Usted tendrá que esperar  
unos minutos antes de que NFSen comience a mostrar los gráficos.

En este punto ya todo está Listo. ¡Enhorabuena!

# # Solución de problemas

Si usted recibe "Error reading stat", compruebe que en el directorio  
/ports-db/var existen 2 Archivos adicionales: portstat24.txt y portstat.txt así:

~~~~~  
\$ ls -l /var/ports-db/portstat*
~~~~~

```
-rw-r--r-- 1 netflow www-data      512 Jul 17 21:20 /var/ports-db/portstat24.txt  
                                         /var/ports-db/portstat.txt
```

~~~~~

Si faltan entonces esto va a causar problemas. Asegúrese de que nfsen puede escribir en ese directorio.

Usted puede conseguir informacion adicional estableciendo ` \$ DEBUG = 1 ` en /var/www/nfsen/conf.php, y luego revisar en /var/tmp/nfsen.log

