% Monitorización de Netflow con NFSen
%
% Gestión de Redes

Introducción

Metas

* Aprender como instalar las herramientas Nfdump y Nfsen

Notas

* Los comandos precedidos por "$" implican que debe ejecutar el comando como usuario genérico -
* Los comandos precedidos por "#" implican que deberá estar trabajando como usuario root.
* Los comandos con inicios de li≠nea más específicos como "rtrX>" o "mysql>" indican que debe ej

Configure el colector

Nota: si está trabajando en parejas entonces sólo el PC que está recibiendo
paquetes netflow necesita instalar nfdump y nfsen. Sin embargo, usted puede instalar
en el otro pc también, sólo para practicar.

Instale nfdump y el software asociado

Nfdump es parte de las herramientas del colector de flujo Netflow, que incluye:

nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgen

Hay un paquete en Ubuntu, pero es demasiado viejo - por lo que vamos a instalar
desde el código fuente. En primer lugar, compruebe que dispone de las herramientas y dependencia

~~~~~~
```
$ sudo apt-get install build-essential
$ sudo apt-get install rrdtool mrtg librrds-perl librrdp-perl librrd-dev \
       libmailtools-perl php5 bison flex
```
~~~~~~

Ahora proceda a descargar y construir. Tenga en cuenta que sólo el último paso
(make install) tiene que hacerse como root.

~~~~~~
```
$ cd
$ wget http://noc.ws.nsrc.org/downloads/nfdump-1.6.10p1.tar.gz
$ tar xvzf nfdump-1.6.10p1.tar.gz
$ cd nfdump-1.6.10p1
$ ./configure --help      # optional, shows the build settings available
$ ./configure --enable-nfprofile --enable-nftrack
$ make
$ sudo make install
```
~~~~~~

Testing nfcapd and nfdump

~~~~~~
```
$ mkdir /tmp/nfcap-test
$ nfcapd -E  -p 9001 -l /tmp/nfcap-test
```
~~~~~~

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

... después de un tiempo, una serie de flujos deben ser descargados en la pantalla.

Detenga la herramienta con CTRL + C y luego revise el contenido en /tmp/nfcap-test

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ ls -l /tmp/nfcap-test
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Debería ver uno o más archivos llamados `nfcapd. <A—O> <MES> <DÕA> <HR> <min>`

Procesar el/los archivo(s) con nfdump:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
nfdump -r /tmp/nfcap-test/nfcapd.2013wwxxyyzz | less
nfdump -r /tmp/nfcap-test/nfcapd.2013wwxxyyzz -s srcip/bytes
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Deben obtener alguna información.

Instalación y configuración de NFSen

Descargar y compilar. El parche es para arreglar un problema reportado en
<http://sourceforge.net/p/nfsen/bugs/31/>

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ cd
$ wget http://noc.ws.nsrc.org/downloads/nfsen-1.3.6p1.tar.gz
$ tar xvzf nfsen-1.3.6p1.tar.gz
$ cd nfsen-1.3.6p1
$ wget http://noc.ws.nsrc.org/downloads/nfsen-socket6.patch
$ patch -p0 < nfsen-socket6.patch
$ cd etc
$ cp nfsen-dist.conf nfsen.conf
$ editor nfsen.conf
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Ajuste la variable $ BASEDIR

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$BASEDIR = "/var/nfsen";
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Ajuste los usuarios como corresponde, para que Apache pueda acceder a los archivos:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$WWWUSER = 'www-data';
$WWWGROUP = 'www-data';
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Ajuste el tamaÒo del büfer a algo pequeÒo, y observara datos rapidamente.
No se recomienda hacer esto en un sistema de produccion.

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
# Receive buffer size for nfcapd - see man page nfcapd(1)
$BUFFLEN = 2000;
```

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Encuentre la definición de fuentes (%sources), y cámbiela a:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
%sources=(
'rtrX' => {'port'=>'9001','col'=>'#0000ff','type'=>'netflow'},
 );
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

(sustituir el router de su grupo para rtrX, y descomente
las fuentes existentes de muestra). Ahora, guarde y salga del archivo.

Cree el usuario netflow en el sistema

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo useradd -d /var/nfsen -G www-data -m -s /bin/false netflow
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Instale NFSen e iniciarlo

Cambie al directorio origen

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ cd
$ cd nfsen-1.3.6p1
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Ahora, finalmente, instalamos:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo perl install.pl etc/nfsen.conf
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Presione ENTER cuando se le pida la ruta de Perl.

Instalar el script de inicio

Con el fin de que nfsen se inicie y se detenga automáticamente cuando se inicie el sistema,
se tiene que agregar un enlace al diretorio init.d apuntando al script de inicio nfsen:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
# sudo ln -s /var/nfsen/bin/nfsen /etc/init.d/nfsen
# sudo update-rc.d nfsen defaults 20
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Iniciar Nfsen

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo service nfsen start
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Compruebe que el proceso nfcapd se ha inciado:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ ps auxwww | grep nfcapd
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Ver los flujos a través de la web:

Puede encontrar la página nfsen aquí:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
http://pcX.ws.nsrc.org/nfsen/nfsen.php
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Si está trabajando en parejas, entonces ambos deben apuntar su navegador web
al PC que está recibiendo flujos.

Es posible que aparezca un mensaje como:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Frontend - Backend version missmatch!
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Esto desaparecerá si vuelve a cargar la página, no es un problema.

¡Ya está! Continüe en el tercer laboratorio, ejercicio3-NFSen-PortTracker

* NOTAS:

Adición de fuentes

Si tuvieras varios enrutadores en la red todos enviando los flujos al misma
colector, puede o bien configurarlos para que envíen a diferentes puertos del
colector, o le puede decir a NFSen la dirección IP de origen de cada router. esto
permite a Nfsen mostrar datos diferentes de cada origen.

NO HACERLO AHORA!!! Ya que sólo tiene un ünico router, pero si necesita,
lo haría de la siguiente manera:

- Editar /var/nfsen/etc/nfsen.conf y agregar la(s) fuente(s), por ejemplo:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
%sources = (
    'rtrX'  => { 'port' => '9001', 'col' => '#0000ff', 'type' => 'netflow' },
    'rtrY'  => { 'port' => '9002', 'col' => '#00ff00', 'type' => 'netflow' },
    'gw'    => { 'port' => '9996', 'col' => '#ff0000', 'type' => 'netflow' },
);
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

- Reconfigurar Nfsen.

Usted tendrá que ejecutar esto cada vez que modifique '/var/nfsen/etc/nfsen.conf':

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
$ sudo /etc/init.d/nfsen reconfig
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Deberia ver:

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
New sources to configure : gw rtrY
Continue? [y/n] y

Add source 'gw'
```

```
Add source 'rtrY'

Start/restart collector on port '9002' for (rtr2)[pid]
Start/restart collector on port '9996' for (gw)[pid]

Restart nfsend:[pid]
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```