

NetFlow - NFSen - Ejercicio

0. Instalar herramientas primero:

=====

-Use

```
sudo su - root
para convertirse en el usuario 'root'
```

-Ahora instale las herramientas necesarias:

```
# apt-get install rrdtool
# apt-get install librrds-perl
# apt-get install librrdp-perl
```

1. Instalar nfdump

=====

[Nfdump colecciona flujos procedentes de Netflow]

Primero, exportar variables que se necesitan:

```
# export INIT_VERBOSE=yes
# export VERBOSE=yes
```

Ahora instalar:

```
# apt-get install nfdump
```

2. Instalar NFSen

=====

```
# cd
# wget http://freefr.dl.sourceforge.net/project/nfsen/stable/nfsen-1.3.2/nfsen-1.3.2.tar.gz
# tar -xzf nfsen-1.3.2.tar.gz
# cd nfsen-1.3.2
#cd etc
# cp nfsen-dist.conf nfsen.conf
```

3. Preparar config:

=====

Editar nfsen.conf:

a. Busca la variable \$BASEDIR, y cambiala a:

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

b. Busca la variable \$PREFIX, y cambiala para reflejar la localizacion correcta de las herramientas nfdump:

```
$PREFIX = '/usr/bin';
```

c. Especificar usuarios: busca las variables \$USER, \$WWWUSER, \$WWWGROUP y cambialas a:

```
$USER = "netflow"
$WWWUSER = 'www-data';
$WWWGROUP = 'www-data';
```

- d. Configure tamaño del buffer de Nfsen a un tamaño mas pequeño, para visualizar datos más rápidamente:

```
$BUFFLEN = 2000;
```

- e. Hallar la cadena "%sources", y defina la fuente de información de flujos. En nuestro caso los enrutadores rtr1, rtr2, rtr3:

```
%sources = (
    'rtr1'    => { 'port'    => '2001', 'col' => '#0000ff' },
    'rtr2'    => { 'port'    => '2002', 'col' => '#ff0000' },
    'rtr3'    => { 'port'    => '2003', 'col' => '#f000ff' },
);
```

- f. Salvar y cerrar fichero

4. Crear un usuario "netflow" en Ubuntu

```
=====
# useradd -d /var/netflow -G www-data -m -s /bin/false netflow
```

5. Configurar y compilar nfsen

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

[presione 'Enter' cuando le pregunten donde Perl está instalado]

6. Verification de directorio web

```
=====
Verifique que el directorio especificado en nfsen.conf para los datos
a visualizar esta creado con los permisos correctos:
```

```
Directorio: /var/www/nfsen
Pertenece a usuario: www-data
Pertenece a grupo:  www-data
```

7. Lanzar Nfsen

```
=====
# cd /var/nfsen/bin
# ./nfsen start
```

8. Conectarse

```
=====
http://127.0.0.1/nfsen/nfsen.php
```

Y listo!