

netflow-nfsen-ejercicio

NetFlow - NFSen - Exercise

0. Instalar herramientas primero:

=====

```
# 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
```

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
```

Preparar config:

=====

Editar nfsen.conf:

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

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

2. Busca PREFIX, y cambia el camino que permite hallar las herramientas nfdump:

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

3. Preparar usuarios:

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

4. Configure tamaño del buffer a algo mas pequeño, para ver los datos más rapido

```
$BUFFLEN = 2000;
```

5. Hallar la cadena "%sources" para definir fuente de información de flujos:

```
%sources = (
    'gw-rtr'    => { 'port'    => '2002', 'col' => '#ff0000' },
);
```

6. Salvar y cerrar fichero

Crear un usuario "netflow" en Ubuntu

=====

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

Configurar nfsen

=====

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

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

Lanzar Nfsen

=====

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

Conectarse

=====

<http://127.0.0.1/nfsen/nfsen.php>