

# Мониторинг Netflow при помощи NFsen

## Contents

|                                                        |          |
|--------------------------------------------------------|----------|
| <b>1 Введение</b>                                      | <b>1</b> |
| 1.1 Цели . . . . .                                     | 1        |
| 1.2 Замечания . . . . .                                | 1        |
| <b>2 Настройте коллектор</b>                           | <b>2</b> |
| 2.1 Установите NFDump и зависимости . . . . .          | 2        |
| 2.1.1 Тестирование nfcapd и nfdump . . . . .           | 2        |
| 2.2 Установка и настройка NfSen . . . . .              | 3        |
| 2.3 Создайте пользователя netflow в системе . . . . .  | 4        |
| 2.4 Установите NfSen и запустите его . . . . .         | 4        |
| 2.5 Установите скрипт инициализации . . . . .          | 4        |
| 2.6 Посмотрите на потоки через web-интерфейс . . . . . | 5        |
| 2.7 Добавление источников потоков . . . . .            | 5        |

## 1 Введение

### 1.1 Цели

- Научиться устанавливать инструменты nfdump и NfSen

### 1.2 Замечания

- Команды, предваряемые “\$” означают, что они должны быть выполнены с правами обычного пользователя – а не администратора.
- Команды, предваряемые “#” означают, что вы должны иметь права администратора.

- Команды с более специфичными подсказками (например “rtrX>” или “mysql>”) означают что вы выполняете их либо на удаленном оборудовании, либо в какой-то другой программе.

## 2 Настройте коллектор

### 2.1 Установите NFDump и зависимости

NFDump является частью инструментария “Netflow flow collector”, который включает в себя:

```
nfcapd, nfdump, nfreplay, nfexpire, nftest, nfgn
```

В Ubuntu есть подходящий пакет, но он для слишком старой версии, поэтому мы установим его из исходников. Сначала, убедитесь что все необходимые для установки вручную инструменты и зависимости присутствуют в системе:

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

Теперь нам нужно скачать исходники и установить программу. Обратите внимание на то, что только самый последний шаг (make install) должен быть выполнен с правами администратора.

```
$ cd
$ wget http://noc.ws.nsrc.org/downloads/nfdump-1.6.10p1.tar.gz
$ tar xvfz 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
```

#### 2.1.1 Тестирование nfcapd и nfdump

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

... через какое-то время, серия потоков должна появиться на экране.

Остановите программу, нажав CTRL+C, потом посмотрите на каталог /tmp/nfcap-test

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

Вы должны увидеть один или несколько файлов вида nfcapd.<YEAR><MON><DAY><HR><MIN>

Пропустите файл(ы) через nfdump:

```
nfdump -r /tmp/nfcap-test/nfcapd.201Ywwxxyzz | less
nfdump -r /tmp/nfcap-test/nfcapd.201Ywwxxyzz -s srcip/bytes
```

Вы должны получить кое-какую полезную информацию :)

## 2.2 Установка и настройка NfSen

Скачайте и установите. Патч нужен для коррекции следующей проблемы <http://sourceforge.net/p/nfsen/bugs/31/>

```
$ cd
$ wget http://noc.ws.nsrc.org/downloads/nfsen-1.3.6p1.tar.gz
$ tar xvfz 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
```

Установите переменную \$BASEDIR

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

Укажите правильного пользователя и группу, для того чтобы Apache имел доступ к файлам:

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

Установите размер буфера в какое-нибудь небольшое значение, так что мы увидим новые данные через непродолжительное время. В реальной работе вы не будете использовать такое малое значение.

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

Найдите определение %sources, и поменяйте его на:

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

(используйте ваш групповой роутер вместо rtrX, и либо удалите либо закомментируйте существующие источники-примеры). Теперь сохраните файл и выйдите из редактора.

Наконец, если ваша систем – Ubuntu 14.04 (но не 12.04), поменяйте HTMIDIR с /var/www/nfsen/ на /var/www/html/nfsen/

```
$HTMIDIR = "/var/www/html/nfsen/";
```

## 2.3 Создайте пользователя netflow в системе

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

## 2.4 Установите NfSen и запустите его

Перейдите опять в каталог с исходниками:

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

И установите nfsen:

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

Нажмите ВВОД когда вас спросят о пути к Perl.

## 2.5 Установите скрипт инициализации

Для того чтобы nfsen запускался и останавливался автоматически когда система загружается, добавьте ссылку в каталоге init.d, указывающую на скрипт запуска nfsen:

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

Запустите NfSen

```
$ sudo service nfsen start
```

Проверьте, запущены ли процессы `nfsen`:

```
$ ps auxwww | grep nfsen
```

## 2.6 Посмотрите на потоки через web-интерфейс

Страница `nfsen` будет расположена здесь:

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

Если вы работаете в парах, то каждый из вас должен указать в браузере ту машину, которая является коллектором.

Возможно, вы увидите сообщение:

Frontend - Backend version mismatch!

Это не является проблемой, сообщение исчезнет, когда вы перезагрузите страницу в браузере.

Готово! Перейдите к третьей лабораторной работе, `exercise3-nfsen-top-talkers`.

- ЗАМЕЧАНИЯ:

## 2.7 Добавление источников потоков

Если несколько роутеров в сети шлют потоки на один и тот же коллектор, вы можете либо настроить их отправлять данные на разные порты коллектора, или вы можете сказать `nfsen` IP адреса каждого роутера. Это позволит `nfsen` показывать разную информацию от каждого источника.

НЕ ДЕЛАЙТЕ ЭТОГО СЕЙЧАС, потому что у нас есть только один роутер, но если вам это понадобится, вам нужно поступить следующим образом:

- отредактируйте `/var/nfsen/etc/nfsen.conf`, и добавьте источники, например:

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

- переконфигурируйте NfSen.

Вам нужно будет запускать следующую команду каждый раз, когда вы будете менять содержимое `/var/nfsen/etc/nfsen.conf`:

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

Вы увидите:

```
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]
```