

Table of Contents

ipfixreceiver2: IPFIX/NetflowV9 collector	3
<i>Introduction</i>	3
<i>Installation and Upgrading</i>	3
CentOS	3
<i>ipfixreceiver2 files</i>	3
Параметры запуска программы	5
Конфигурация	5
Примеры конфигураций	8

ipfixreceiver2: IPFIX/NetflowV9 collector

Introduction

ipfixreceiver2 is an IPFIX/NetflowV9 collector with the following functionality

- Allows to save the received data with the required format in a text file.
- Allows to redirect received data to other IPFIX collectors.

Installation and Upgrading

CentOS

1. Add the VAS Experts repository according to the p.1 of the [DPI installation instruction](#).
2. Add the [EPEL](#) repository
3. Install the ipfixreceiver2:

```
yum install -y ipfixreceiver2
```

4. In order to upgrade ipfixreceiver2 issue the following command:

```
yum update -y ipfixreceiver2
```

ipfixreceiver2 files

- Files describing the types of ipfix data fields:

```
/etc/rcollector/xml/ipfix_raw.xml - ipfix data field types used in fullflow.  
/etc/rcollector/xml/ipfix_url.xml - ipfix data field types used in clickstream (http requests).  
/etc/rcollector/xml/ipfix_sip.xml - ipfix data field types used in SIP connections.  
/etc/rcollector/xml/ipfix_aaa.xml - ipfix data field types used in AAA events.  
/etc/rcollector/xml/ipfix_nat.xml - ipfix data field types used in NAT events.
```

- Examples of configuration files describing ipfix data import and export models:

```
/etc/rcollector/ipfixreceiver_raw.ini is responsible for ipfix data import and export for fullflow.  
/etc/rcollector/ipfixreceiver_raw_new.ini is responsible for ipfix data import and export for the VAS Experts DPI version 8.1 and higher.
```

```
/etc/rcollector/ipfixreceiver_url.ini is responsible for ipfix data
import and export for clickstream.
/etc/rcollector/ipfixreceiver_sip.ini is responsible for ipfix data
import and export for SIP connections.
/etc/rcollector/ipfixreceiver_aaa.ini is responsible for ipfix data
import and export for AAA events.
/etc/rcollector/ipfixreceiver_nat.ini is responsible for ipfix data
import and export for NAT events.
```

- Executable file,:

```
/usr/bin/ipfixreceiver2
```

CentOS 6

- Scripts used to run the process of importing and exporting ipfix data:

```
/etc/init.d/ipfix_raw - ipfixreceiver2 startup script with
corresponding '/etc/rcollector/ipfixreceiver_raw.ini' configuration
file.
/etc/init.d/ipfix_url - Скрипт запуска ipfixreceiver2 с конфигурационным
файлом /etc/rcollector/ipfixreceiver_url.ini.
/etc/init.d/ipfix_sip - Скрипт запуска ipfixreceiver2 с конфигурационным
файлом /etc/rcollector/ipfixreceiver_sip.ini.
/etc/init.d/ipfix_aaa - Скрипт запуска ipfixreceiver2 с конфигурационным
файлом /etc/rcollector/ipfixreceiver_aaa.ini.
```

CentOS 7

- Сервисные файлы для запуска процессов импорта и экспорта данных ipfix:

```
/usr/lib/systemd/system/ipfix_raw.service - Сервисный файл для запуска
ipfixreceiver2 с конфигурационным файлом
/etc/rcollector/ipfixreceiver_raw.ini.
/usr/lib/systemd/system/ipfix_url.service - Сервисный файл для запуска
ipfixreceiver2 с конфигурационным файлом
/etc/rcollector/ipfixreceiver_url.ini.
/usr/lib/systemd/system/ipfix_sip.service - Сервисный файл для запуска
ipfixreceiver2 с конфигурационным файлом
/etc/rcollector/ipfixreceiver_sip.ini.
/usr/lib/systemd/system/ipfix_aaa.service - Сервисный файл для запуска
ipfixreceiver2 с конфигурационным файлом
/etc/rcollector/ipfixreceiver_aaa.ini.
```

Параметры запуска программы

Программа ipfixreceiver2 имеет следующие параметры запуска:

```
usage: ipfixreceiver2 <-f config file> [options]
где
--daemon           Запуск программы в фоновом режиме.
--umask=mask       Установить umask (восьмиричн., по умолчанию 027).
--pidfile=path     Путь к pid файлу.
-h, --help         Вывести краткую справку.
-fFILE, --config-file=FILE Путь к конфигурационному файлу.
-v, --version      Вывести версию программы.
```

Конфигурация

Параметры работы программы задаются в .ini файле.

Секция [connect]

В данной секции задаются параметры для приема данных ipfix.

- protocol - IP протокол (tcp или udp)



При использовании протокола udp необходимо убедиться, что размер ipfix записи не превышает размер MTU (clickstream данные можно принимать только по протоколу tcp).

- host - интерфейс, на котором будет осуществляться прием данных
- port - номер порта
- flow_type - тип принимаемого потока: ipfix или netflow9. В случае использования netflow9 protocol может быть только udp.

Секция [dump]

В данной секции задаются параметры дампа принятых данных в файл.

- delimiter - символ разделителей данных в файле.
- rotate_minutes - через сколько минут закрывать временный файл и переименовывать его в постоянный.
- rotate_flows - через какое количество ipfix записей закрывать временный файл и переименовывать его в постоянный. 0 - отключение данного вида ротации.
- dumpfiledir - каталог для размещения файлов с дампом.
- fileprefix - префикс имени файла с дампом.
- rotateformat - формирует имя файла с дампом.
- extension - расширение файла с дампом.
- temp_file_suffix - суффикс имени временного файла.

- processcmd - команда для запуска при ротации файла. %s задает имя постоянного файла с дампом.
- detach_child - если true, то процесс processcmd отвязывается от процесса ipfixreceiver'a.
- decode_url - декодировать символы в url при использовании decodepath.
- decode_host - декодировать idna в имени хоста при decodehost.
- decode_referer - декодировать idna в referer при decodereferer.
- reopen_time - через сколько секунд будет предпринята попытка открыть файл для записи дампа после возникшей ошибки с файлом. По умолчанию 30 секунд.
- checkdir - проверять ли на существование dumpfiledir и в случае отсутствия создать каталог (создаются все каталоги из dumpfiledir). По умолчанию true.
- fw_max_elements_in_queue - количество элементов, при котором они отправляются в очередь на запись в файл. По умолчанию 100000.
- fw_max_queue_size - максимальное количество массивов элементов в очереди. Если на момент добавления в очередь количество находящихся в очереди будет больше, то добавляемые данные будут отброшены. По умолчанию 2.
- bad_characters - символы, которые не нужно выводить при записи в файл. Могут быть указаны одиночные символы и escape последовательности. По умолчанию "\t\r\n;\x00".

Секция [InfoModel]

В данной секции задается xml файл с описанием типа данных в принимаемом потоке ipfix.

- XMLElements - путь к xml файлу с описанием типа данных в формате [IANA IPFIX Entities registry](#).

Секция [Template]

В данной секции задается порядок следования данных в принимаемом потоке ipfix и при необходимости фильтр принимаемых данных по идентификатору.

- Elements - список принимаемых данных (через запятую).
- filter_tid - только данные с данным идентификатором будут обрабатываться, а с иными будут отброшены.

Секция [ExportModel]

В данной секции определяется порядок и формат вывода полученных данных.

- Elements - список данных, которые необходимо сохранять в файле (через запятую). Возможно изменить predetermined формат вывода в файл для каждого типа данных, используя следующий формат: имя_поля:формат_вывода[:опция]. Возможны следующие типы вывода данных:

Формат_вывода	Описание
decode_unsigned	Декодировать как unsigned
decode_signed	Декодировать как signed
decodeipv4	Декодировать как IPv4 адрес
decodeipv6	Декодировать как IPv6 адрес

Формат_вывода	Описание
decode_string	Декодировать как строку
decode_seconds	Декодировать как дату и время в секундах. Формат вывода по умолчанию '%Y-%m-%d %H:%M:%S'. В опции можно задать свой формат вывода.
decode_milliseconds	Декодировать как дату и время в миллисекундах. Формат вывода по умолчанию '%Y-%m-%d %H:%M:%S'. В опции можно задать свой формат вывода.
decodehost	Декодировать как имя хоста
decodepath	Декодировать как путь в url
decodereferer	Декодировать как referer

Секция [stats]

В данной секции задаются параметры вывода статистики работы программы в telegraf.

- socket_path - путь к datagram socket telegraf'a.
- interval - через сколько секунд отправлять статистику в telegraf.
- tag - тег, выставляемый в поле ipfix_tag при отправке статистики в telegraf.

Секция [export]

- to - задаются адреса коллекторов для экспорта полученных ipfix записей. Формат ip/port/proto[,ip/port/proto]. Например:

```
[export]
to=10.0.0.2/9921/tcp, 10.0.0.3/3444/udp
```



При использовании протокола udp необходимо убедиться что одна ipfix запись не превышает размер MTU.

Секция [logging]

В данной секции задаются параметры логирования программы.

- loggers.root.level - уровень логирования
- loggers.root.channel - канал для вывода сообщений
- channels.fileChannel.class - класс канала вывода
- channels.fileChannel.path - путь к лог-файлу
- channels.fileChannel.rotation - параметр ротации
- channels.fileChannel.archive - параметр имени архивных файлов
- channels.fileChannel.purgeCount - количество архивных файлов
- channels.fileChannel.formatter.class - класс форматировщика
- channels.fileChannel.formatter.pattern - шаблон для форматировщика
- channels.fileChannel.formatter.times - время



Более подробно ознакомиться с параметрами логирования можно по ссылке [Class FileChannel](#).

Примеры конфигураций

Приём ipfix данных

В файлах `/etc/rcollector/ipfixreceiver_*.ini` приведены примеры настройки для получения различных потоков данных ipfix. Перед запуском программы необходимо изменить конфигурационный файл под ваши требования.

- При необходимости внести изменения в секцию `[connect]`, указав интерфейс, порт и протокол для приема ipfix данных.
- В секции `[dump]` указать:
 - `dumpfiledir` - каталог, где будут создаваться временный файл и файлы с данными.
 - `rotate_minutes` - время, через которое закрывать временный файл, переименовывать его в файл с постоянным именем и выполнить команду из параметра `processcmd` для действий над полученным файлом.
 - `processcmd` - команду, необходимую выполнить над файлом с данными.
 - `delimiter` - символ разделитель между полями данных.
- В секции `[ExportModel]` указать необходимый порядок следования полей в сохраняемом файле.

Экспорт ipfix данных

Для экспорта получаемых ipfix данных необходимо внести изменения в конфигурационный файл, путем добавления секции `[export]` и указания адресов назначения. Например, для отправки ipfix данных на ipfix коллектор с адресом `10.0.0.5:1501` по протоколу `tcp`, элемент конфигурации будет выглядеть следующим образом:

```
[export]
to = 10.0.0.5/1501/tcp
```

Если необходимо задать несколько ipfix коллекторов, то их можно указать через запятую. Например:

```
[export]
to = 10.0.0.5/1501/tcp, 192.168.1.200/1501/tcp
```