

Содержание

- ipfixreceiver2: IPFIX/NetflowV9 collector 3**
 - Introduction* 3**
 - Installation and Upgrading* 3**
 - CentOS 3
 - ipfixreceiver2 files* 3**
 - ipfixreceiver2 startup options* 5**
 - Configuration* 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 start 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 - ipfixreceiver2 startup script with
corresponding /etc/rcollector/ipfixreceiver_url.ini configuration file.
/etc/init.d/ipfix_sip - ipfixreceiver2 startup script with
corresponding /etc/rcollector/ipfixreceiver_sip.ini configuration file.
/etc/init.d/ipfix_aaa - ipfixreceiver2 startup script with
corresponding /etc/rcollector/ipfixreceiver_aaa.ini configuration file.
```

CentOS 7

- systemd-based configuration files ([systemd](#) units) to start the process of importing and exporting ipfix data:

```
/usr/lib/systemd/system/ipfix_raw.service - systemd unit responsible
for starting ipfixreceiver2 with corresponding
/etc/rcollector/ipfixreceiver_raw.ini configuration file.
/usr/lib/systemd/system/ipfix_url.service - systemd unit responsible
for starting ipfixreceiver2 with corresponding
/etc/rcollector/ipfixreceiver_url.ini configuration file.
/usr/lib/systemd/system/ipfix_sip.service - systemd unit responsible
for starting ipfixreceiver2 with corresponding
/etc/rcollector/ipfixreceiver_sip.ini configuration file.
/usr/lib/systemd/system/ipfix_aaa.service - systemd unit responsible
for starting ipfixreceiver2 with corresponding
/etc/rcollector/ipfixreceiver_aaa.ini configuration file.
```

ipfixreceiver2 startup options

ipfixreceiver2 utility has the following startup options:

```
usage: ipfixreceiver2 <-f config file> [options]
here
--daemon                start the program as a daemon process.
--umask=mask            set umask (octal value, 027 is the default one).
--pidfile=path          set path to a pid file.
-h, --help              display a brief description.
-fFILE, --config-file=FILE set path to the configuration file.
-v, --version           display program version.
```

Configuration

Configuration options are specified in the .ini file.

Section [connect]

The section is used to specify the parameters for receiving ipfix data.

- protocol - IP protocol (tcp or udp)
 - ! Before using the udp protocol, you should make sure that the size of the ipfix record does not exceed the size of the MTU (clickstream data can be received using the tcp protocol only).
- host - interface, used to receive the data
- port - port number
- flow_type - the type of flow to receive: ipfix or netflow9. When netflow9 protocol is used the flow_type can be equal to 'udp' only.

Section [dump]

The section is used to specify the parameters of data dump received.

- delimiter - character used as delimiter within the file.
- rotate_minutes - the time period after which the temporary file will be closed and renamed to a persistent one
- rotate_flows - the ipfix records number upon the exceeding of which the temporary file will be closed and renamed to a persistent one. 0 - to disable this rotation type.
- dumpfiledir - directory used to store the dump files.
- fileprefix - dump file name prefix.
- rotateformat - generates a dump file name.
- extension - extension of a dump file.
- temp_file_suffix - name suffix of a temporary file.
- processcmd - command used to set rotate option. %s specifies the name of persistent file containing the dump.
- detach_child - when is set to true, the processcmd process will be unbound from ipfixreceiver's

process.

- `decode_url` - to decode characters in url when using `decodepath`.
- `decode_host` - to decode idna within the host name when using `decodehost`.
- `decode_referer` - to decode idna to referer when using `decoderesolver`.
- `reopen_time` - the time period upon the exceeding of which the attempt to reopen a file for recording a dump after an error occurred (when attempting to access the file) will be made. The default value is 30 seconds.
- `checkdir` - boolean parameter; is used to check whether `dumpfiledir` exists and, if it does not exist, the corresponding directories will be created (including all the `dumpfiledir` subdirectories). The default value is true.
- `fw_max_elements_in_queue` - the items number upon the exceeding of which they will be forwarded to the queue to be written to the file. The default value is 100000.
- `fw_max_queue_size` - the maximum number of arrays of elements in the queue. If the number of people at the time of adding them to the queue will be more than `fw_max_queue_size`, then the data will be discarded. The default value is 2.
- `bad_characters` - characters that do not need to be displayed when writing to a file. Single characters along with escape sequences can be specified. Default value is `"\t\r\n;\x00"`.

Section [InfoModel]

This section specifies an xml file describing the type of data within the received ipfix flow.

- `XMLElements` - path to xml file with data type description using the [IANA IPFIX Entities registry](#) format.

Section [Template]

The section is responsible for the data sequence order within the received ipfix flow and, if necessary, for the received data filtering by the given identifier.

- `Elements` - comma separated list of received data.
- `filter_tid` - only the data with the given identifier will be processed, all the other ones will be discarded.

Section [ExportModel]

This section specifies the order and format of the received data to be exported.

- `Elements` - comma separated list of data to be stored in the file. You can change the predefined export format (the data will be exported to a file) for each data type using the following format: `field_name: output_format [: option]`. The following types of data output are possible:

^Output_format^Description^

<code>decode_unsigned</code>	Decode as unsigned
<code>decode_signed</code>	Decode as signed
<code>decodeipv4</code>	Decode as IPv4 address
<code>decodeipv6</code>	Decode as IPv6 address

decode_string	Decode as string
decode_seconds	Decode as date and time in seconds. The default output format is '%Y-%m-%d %H:%M:%S'. You can specify date/time format on your own.
decode_milliseconds	Decode as date and time in milliseconds. The default output format is '%Y-%m-%d %H:%M:%S'. You can specify date/time format on your own.
decodehost	Decode as host name
decodepath	Decode as url
decoderesolver	Decode as resolver

Section [stats]

The section specifies the export options for sending ipfixreceiver2 statistics (metrics and events) to the telegraf agent.

- socket_path - path to the telegraf's datagram socket.
- interval - the time period upon the exceeding of which the statistics will be sent to the telegraf agent.
- tag - tag set in the ipfix_tag field when sending statistics to the telegraf agent.

Section [export]

- to - specifies the collector addresses to be used to export received ipfix records.
Used format: ip/port/proto[,ip/port/proto].

For example:

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

⚠ When using the udp protocol, you should make sure that one ipfix record does not exceed the size of the 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](#)

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
```