Содержание

IPFIXCol2 - коллектор NetFlow v5/v9 и IPFIX

Введение

IPFIXCol2 — это гибкий, высокопроизводительный коллектор потоковых данных NetFlow v5/v9 и IPFIX, расширяемый с помощью подключаемых плагинов. Версия приложения, представленная в репозитории VAS Experts, включает в себя изменения, необходимые для оптимальной работы с потоками IPFIX со СКАТа.

Установка

1. Подключите репозиторий VAS Experts

```
rpm --import http://vasexperts.ru/centos/RPM-GPG-KEY-vasexperts.ru
rpm -Uvh http://vasexperts.ru/centos/6/x86_64/vasexperts-
repo-1-0.noarch.rpm
```

2. Установите ipfixcol2:

```
dnf install -y ipfixcol2
```

Файлы поставки

Конфигурационный файл:

```
/opt/vasexperts/etc/ipfixcol2/startup.xml
```

Исполняемый файл:

```
/opt/vasexperts/bin/ipfixcol2
```

Плагины:

```
/opt/vasexperts/lib64/ipfixcol2/libanonymization-intermediate.so
/opt/vasexperts/lib64/ipfixcol2/libfds-output.so
/opt/vasexperts/lib64/ipfixcol2/libjson-kafka-output.so
/opt/vasexperts/lib64/ipfixcol2/libudp-input.so
/opt/vasexperts/lib64/ipfixcol2/libdummy-input.so
/opt/vasexperts/lib64/ipfixcol2/libforwarder-output.so
/opt/vasexperts/lib64/ipfixcol2/libjson-output.so
/opt/vasexperts/lib64/ipfixcol2/libviewer-output.so
/opt/vasexperts/lib64/ipfixcol2/libdummy-output.so
/opt/vasexperts/lib64/ipfixcol2/libipfix-input.so
/opt/vasexperts/lib64/ipfixcol2/libtcp-input.so
```

```
/opt/vasexperts/lib64/ipfixcol2/libfds-input.so
/opt/vasexperts/lib64/ipfixcol2/libipfix-output.so
/opt/vasexperts/lib64/ipfixcol2/libtimecheck-output.so
```

Сервисный файл для запуска приложения:

```
/usr/lib/systemd/system/ipfixcol2.service
```

Параметры запуска

Программа имеет следующие параметры запуска:

```
Usage: ipfixcol2 [-c FILE] [-p PATH] [-e DIR] [-P FILE] [-r SIZE] [-vVhLd]

-c FILE Путь к файлу конфигурации
(по умолчанию: /etc/opt/vasexperts/ipfixcol2/startup.xml)

-p PATH Путь к каталогу с плагинами
(по умолчанию: /opt/vasexperts/lib64/ipfixcol2/)

-e DIR Путь к каталогу с описанием элеметов IPFIX
(по умолчанию: /etc/libfds/)

-P FILE Путь к PID файлу (без этой опции PID файл не создается)

-d Запустить как демон

-r SIZE Размер кольцевого буфера (по умолчанию: 8192)

-h Вывести краткую справку

-V Вывести версию программы

-L Вывести список плагинов и выйти

-v Увеличить уровень логирования (по умолчанию логируются только ошибки)
(может быть использовано до 3х раз для добавления warning/info/debug сообщений)
```

Конфигурация приложения для репликации потока IPFIX

В конфигурационном файле `/opt/vasexperts/etc/ipfixcol2/startup.xml` приведен пример настройки репликации одного потока IPFIX по TCP на два коллектора в режиме round robin. Конфигурационный файл составлен в формате xml.

```
<ipfixcol2>
  <!-- Input plugins -->
  <inputPlugins>
```

```
    <input>
      <name>TCP collector</name>
      <plugin>tcp</plugin>
      <params>
        <!-- List on port 1600 -->
        <localPort>1600</localPort>
        <!-- Bind to all local adresses -->
        <localIPAddress>192.168.1.183</localIPAddress>
      </params>
    </input>
  </inputPlugins>

  <outputPlugins>
    <output>
    <name>Forwarder</name>
    <plugin>forwarder</plugin>
    <params>
        <mode>roundrobin</mode>
        <protocol>tcp</protocol>
        <premadeConnections>0</premadeConnections>
        <hosts>
            <host>
                <name>Subcollector 1</name>
                <address>192.168.1.183</address>
                <port>1500</port>
            </host>
            <host>
                <name>Subcollector 2</name>
                <address>192.168.1.183</address>
                <port>1510</port>
            </host>
        </hosts>
    </params>
    </output>
  </outputPlugins>

</ipfixcol2>
```

Настройка интерфейса и порта для приема потока IPFIX осуществляется в блоке `<inputPlugins>`. Для приема потока IPFIX по протоколу TCP используется плагин `tcp` (`<plugin> tcp`). В блоке `<params>` задаются параметры плагина. В блоке `<locapPort>` плагина `tcp` указывается номер порта для приема потока IPFIX. В блоке `<localIPAddress>` IP-адрес интерфейса для приема потока TCP.

Настройка репликации входного потока IPFIX осуществляется в блоке `<outputPlugins>`. Для репликации используется плагин `forwarder` (`<plugin> forwarder`). В блоке `<params>` задаются параметры плагина. В блоке `<protocol>` указывается IP-протокол (`tcp` или `udp`). В блоке `<mode>` задается режим распределения входного потока IPFIX по заданным коллекторам (может быть `roundrobin` или `all`). В блоке `<hosts>` указываются коллекторы для репликации входного потока IPFIX. Каждый коллектор описывается отдельным блоком `<host>`. В данном блоке задается имя коллектора (блок `<name>`), IP-адрес (блок `<address>`) и порт (блок

<port>).

Внимание!
Необходимо обратить внимание на значение блока <mode>. Для репликации входного потока на **все** коллекторы необходимо указать all.

Запуск приложения

Для запуска приложения используется команда:

```
systemctl start ipfixcol2
```

Для автоматического запуска приложения при загрузке сервера необходимо выполнить следующую команду:

```
systemctl enable ipfixcol2
```

Логирование

Приложение выводит сообщения в syslog. По умолчанию в лог выводятся только сообщения об ошибках.