Содержание

Сборка IPFIX потоков rcollector

Введение

Утилита предназначена для дополнения данными вспомогательных потоков таких как clickstream, SIP из потока сессий (netflow).

Инсталляция и обновление

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 rcollector:

```
yum install -y rcollector
```

3. настройте файлы конфигурации в директории /etc/rcollector см. далее

Файлы поставки

1. примеры конфигурации:

```
/etc/rcollector/ipfixreceiver2.conf - пример конфигурации для clickstream (http запросы)
/etc/rcollector/ipfixreceiverflow2.conf - пример конфигурации для получения информации о сессиях (аналог netflow)
/etc/rcollector/ipfixreceiversip2.conf - пример конфигурации для получения информации о sip соединениях
/etc/rcollector/rcflowprocess - пример исполняемого файла для обработки сессий (netflow)
/etc/rcollector/rcurlprocess - пример исполняемого файла для обработки HTTP сессий
/etc/rcollector/rcsipprocess - пример исполняемого файла для обработки SIP сессий
```

2. файлы программы располагаются в директории:

```
/usr/local/lib/rcollector.d/
```

3. вспомогательные файлы:

```
/etc/dpiui/port_proto.txt - информация о трансляции идентификатора протокола в наименование,
```

используется в утилите для получения текстового имени протокола

4. ссылки на исполняемый модуль:

```
/usr/local/bin/rcollector -> линк на
/usr/local/lib/ipfixreceiver.d/rcollector
```

Настройка конфигурации

1. создайте директории для размещения файлов ipfixreceiver и rcollector
   пример для устройства 111:

```
mkdir -p /var/dump/111/ipfixflow
mkdir -p /var/dump/111/ipfixsip
mkdir -p /var/dump/111/ipfixurl

mkdir -p /var/collector/111/email
mkdir -p /var/collector/111/ftp
mkdir -p /var/collector/111/http_requests
mkdir -p /var/collector/111/raw_flow
mkdir -p /var/collector/111/sip
mkdir -p /var/collector/111/ssh
```

2. скопируйте примеры конфигурационных файлов /etc/rcollector в директорию /etc/rcollector/<NNN>, <NNN> - идентификатор устройства
   пример для устройства 111:

```
mkdir -p /etc/rcollector/111
cp /etc/rcollector/* /etc/rcollector/111
chmod a+x /etc/rcollector/111/rc*
```

3. настройте конфигурационные файлы ipfixreceiver:
   В файлах ipfixreceiver2.conf, ipfixreceiverflow2.conf, ipfixreceiversip2.conf:
   1. устанавливаем данные портов приема потоков в зависимости от конфигурации DPI, **например** для clickstream 1501: *port=1501*
   2. установите обработчик принятого файла, например для clickstream устройства 111: processcmd=/etc/collector/111/rcurlprocess%%s
   3. установите директорию для полученных файлов, например для clickstream: dumpfiledir=/var/dump/111/ipfixurl/
4. настройте конфигурационные файлы rcollector. Пример для устройства 111, локальные ASN=47438,57451,56613,65535 устанавливаем следующие значения переменных в файлах rcflowprocess, rcurlprocess, rcsipprocess:

```
chome="/var/collector/111"
cipfix="/etc/rcollector/111"
localASN="47438,57451,56613,65535"
devuid="111"
```

   где
   chome - корневая директория результирующих файлов коллектора

cipfix - корневая директория файлов конфигурации
localASN - локальные автономные системы оператора связи
devuid - номер устройства

5. создайте файл для ротации логов

```
cat /etc/logrotate.d/ipfix
/var/log/dpiui*.log
/var/log/rflowcollector.log
{
    rotate 5
    missingok
    notifempty
    compress
    size 10M
    daily
    copytruncate
    nocreate
    postrotate
    endscript
}
```

6. создайте задания перемещающие файлы в архив или удаляющие их как в примере:

```
# dell collector data after 1.5 and 1 days
15 * * * * /bin/find /var/collector/ -name url_\*gz -cmin +2160 -delete
> /dev/null 2>&1
05 * * * * /bin/find /var/db/rcollector/ -name \*.val -cmin +120 -
delete > /dev/null 2>&1
15 * * * * /bin/find /var/dump/ -name url_\*gz -cmin +1440 -delete >
/dev/null 2>&1
```