Содержание

Utility designed to assemble the IPFIX flows

Introduction

The utility is designed to complement streams such as clickstream, SIP from the sessions stream (netflow) by auxiliary data.

Installation and upgrade

1. add the VAS Experts repository

```
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. install the rcollector:

```
yum install -y rcollector
```

3. edit the configuration files in the /etc/rcollector/ directory (see further)

Delivery files

1. configuration examples:

```
/etc/rcollector/ipfixreceiver2.conf - clickstream configuration example
(http requests)
/etc/rcollector/ipfixreceiverflow2.conf - configuration example for
retreiving the information about sessions (netflow analogue)
/etc/rcollector/ipfixreceiversip2.conf - configuration example for
retreiving the information about sip sessions
/etc/rcollector/rcflowprocess - example of executable file for session
handling (netflow)
/etc/rcollector/rcurlprocess - example of executable file for HTTP
sessions handling
/etc/rcollector/rcsipprocess - example of executable file for SIP
sessions handling
```

2. program files are located within the directory:

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

3. auxiliary files:

```
/etc/dpiui/port_proto.txt - information about the resolution of
protocol identifier to its name, it is used by the utility to obtain
```

```
the protocol text name
```

4. links to the executable module:

```
/usr/local/bin/rcollector -> symlink to the
/usr/local/lib/ipfixreceiver.d/rcollector
```

Configuration

1. create the following directories to place the ipfixreceiver and rcollector files

```
example for device 111:<code>
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. copy the /etc/rcollector sample of configuration files to the /etc/rcollector/<NNN> directory, here the <NNN> - the device identifier

```
example for device 111:<code>
mkdir -p /etc/rcollector/111
cp /etc/rcollector/* /etc/rcollector/111
chmod a+x /etc/rcollector/111/rc*
```

3. edit the ipfixreceiver configuration files:

```
In the following files: ipfixreceiver2.conf, ipfixreceiverflow2.conf,
ipfixreceiversip2.conf:<code>
1. specify the configuration of the port used to receive stream data
depending on the DPI configuration, for example, for clickstream 1501:
port=1501
2. specify the handler for the received file, for example for the
clickstream of device 111:
processcmd=/etc/collector/111/rcurlprocess %%s
3. specify the directory for the received files, for example for
clickstream:
dumpfiledir=/var/dump/111/ipfixurl/
```

4. edit configuration files rcollector. Example for device 111, local ASN = 47438,57451,56613,65535 specify the following variables values in rcflowprocess, rcurlprocess, rcsipprocess files:

```
chome="/var/collector/111"
```

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

here chome - the root directory of the resulting collector files
cipfix - root directory of configuration files
localASN - local autonomous systems of the communications provider
devuid - device number.

5. create a file for log rotation

```
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. create jobs that move files to the archive or delete them as in the example:

```
# 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
```