

12. ПОДГОТОВКА СЕНСОРА NETFLOW

Сенсор Netflow используется в работе теста Netflow, который предоставляет возможность анализа сетевого трафика на уровне сеансов, делая запись о каждой транзакции TCP/IP. Сенсор представляет собой устройство, собирающее статистику по проходящему через него трафику. Собранные данные отправляются в формате Netflow 5 на коллектор Netflow.

Сенсор может быть развёрнут на оборудовании под управлением Unix-совместимой операционной системы, через которое проходит трафик, и которое позволяет установить пакеты `fprobe` и `tcrdump`. Брандмауэр должен позволять исходящие соединения на порт UDP 9996. Пользователь должен входить в `sudoers` и иметь возможность выполнения команд с повышенными привилегиями без ввода пароля.

Подготовка сенсора к работе

1) Выяснить IP-адрес коллектора Netflow

Адрес такой же, как у сервера приложений wiSLA. Запуск коллектора описан в разделе «Действия по обслуживанию wiSLA»;

2) Установить пакет `fprobe`.

Для установки рекомендуется обратиться к руководству администратора соответствующей операционной системы. Примеры команды для грп-совместимых дистрибутивов Linux:

2.1 Для Debian/Ubuntu/Astra, deb-совместимых дистрибутивов Linux:

2.1.1 Обновите список пакетов:

```
$ sudo apt update
```

2.1.2 Установите `fprobe` (для Debian/Ubuntu, deb-совместимых дистрибутивов Linux):

```
$ sudo apt install fprobe
```

2.2 Для CentOS/RHEL:

2.2.1 Установите EPEL-репозиторий (если еще не установлен):

```
$ sudo yum install epel-release
```

2.2.2 Установите `fprobe`:

```
$ sudo yum install fprobe
```

ИЛИ

```
$ sudo dnf install fprobe
```

3) Настройка fprobe

После установки необходимо настроить fprobe для мониторинга трафика на конкретном интерфейсе и отправки данных на коллектор.

3.1 Для Debian/Ubuntu/Astra

3.1.1 Откройте файл конфигурации:

```
$ sudo nano /etc/default/fprobe
```

3.1.2 Приведите файл к следующему виду:

```
# fprobe default configuration file

INTERFACE="eth0"           # Интерфейс для мониторинга (например, eth0)
FLOW_COLLECTOR="192.168.1.100:9996" # Адрес коллектора (IP и порт-9996)

# Дополнительные параметры (опционально)
OTHER_ARGS="-fip"
```

где:

- **INTERFACE**: Укажите интерфейс, который нужно мониторить. Если нужно мониторить все интерфейсы, укажите `any`.
- **FLOW_COLLECTOR**: Укажите IP-адрес и порт коллектора (сервер wiSLA).
- **OTHER_ARGS** указывает прочие опции.
 - Например, можно перехватывать только IP-пакеты, указав `-fip`;

3.1.3 Сохраните файл и выйдите из редактора (в nano: `Ctrl+O`, затем `Ctrl+X`).

3.1.4 В случае внесении корректировок в файл при запущенном fprobe, чтобы применить настройки, необходимо перезапустить fprobe.

3.2 Для CentOS/RHEL:

3.2.1 Откройте файл конфигурации:

```
$ sudo nano /etc/sysconfig/fprobe
```

3.2.2 Приведите файл к следующему виду:

```
OPTIONS="-ieth0 -B4096 -r2 -q10000 -t10000:10000000 192.168.1.100:9996"
```

где:

- `-ieth0`: Интерфейс для мониторинга (например, eth0).
- `192.168.1.100:9996`: Адрес коллектора (IP и порт).

3.2.3 Сохраните файл и выйдите из редактора.

4) Запуск и управление fprobe

- Для Debian/Ubuntu/Astra:

```
sudo systemctl start fprobe
```

- Для CentOS/RHEL:

```
sudo service fprobe start
```

5) Автозапуск при загрузке системы:

- Для Debian/Ubuntu/Astra:

```
sudo systemctl enable fprobe
```

- Для CentOS/RHEL:

```
sudo chkconfig fprobe on
```

5) Проверка статуса fprobe:

- Для Debian/Ubuntu/Astra:

```
sudo systemctl status fprobe
```

- Для CentOS/RHEL:

```
sudo service fprobe status
```

Дополнительно:

Остановка fprobe:

- Для Debian/Ubuntu/Astra:

```
sudo systemctl stop fprobe
```

- Для CentOS/RHEL:

```
sudo service fprobe stop
```

Перезапуск fprobe:

- Для Debian/Ubuntu/Astra:

```
sudo systemctl restart fprobe
```

- Для CentOS/RHEL:

```
sudo service fprobe restart
```

Проверка что fprobe установлен:

```
which fprobe
```

Если команда возвращает путь (например, `/usr/sbin/fprobe`), значит, `fprobe` установлен.

Иные команды для управления службой fprobe

Запуск сенсора:

```
$ /etc/init.d/fprobe start
```

Остановка сенсора:

```
$ /etc/init.d/fprobe stop
```

Перезапуск сенсора:

```
$ /etc/init.d/fprobe restart
```

Пример файла настройки fprobe:

- В **deb-совместимых дистрибутивах Linux**

Расположение: **/etc/default/fprobe**

```
#fprobe default configuration file
INTERFACE="eth0"
FLOW_COLLECTOR="192.168.1.10:9996"
#fprobe can't distinguish IP packet from other (e.g. ARP)
OTHER_ARGS="-fip"
```

- В **rpm-совместимых дистрибутивах Linux**

Расположение: **/etc/sysconfig/fprobe**

```
OPTIONS="-ieth0 -B4096 -r2 -q10000 -t10000:10000000 192.168.1.10:9996 -fip"
```

Проверка работы fprobe

Проверка отправки данных на коллектор:

1. На сервере коллектора (wiSLA), с помощью утилиты tcpdump, выполните команду:

```
$ sudo tcpdump -nni any udp and port 9996
```

Если данные поступают, вы увидите строки вида:

```
18:57:41.010226 IP 192.168.1.10.52861 > 192.168.1.100.9996: UDP, length 120
```

2. На сервере с fprobe проверьте, отправляются ли данные:

```
$ sudo netstat -tunap | grep fprobe
```

Или:

```
$ sudo ss -tunap | grep fprobe
```

Полное удаление fprobe на линукс: `sudo apt-get purge fprobe`

По итогу

Поздравляю, теперь fprobe настроен и готов к работе. Он будет собирать данные о трафике на указанном интерфейсе и отправлять их на коллектор NetFlow.
