Содержание

Мониторинг и логи fastDPI	3
Ротация лог файлов	3
Мониторинг SNMPD	
Описание	3
Установка	
Проверка работоспособности SNMPD и вендорской ветки	5
Как прочитать файл MIB	5
Известные ограничения	6
Мониторинг через SNMP агент (Zabbix-agent)	
Настройка агента	7
настройка сервера	7
Мониторинг распределение трафика по классам	
Просмотр статистики по flow и протоколам	

Мониторинг и логи fastDPI

Логи системы представлены в виде текстовых файлов, которые располагаются в директории /var/log/dpi для модулей DPI и PCRF. Типы сообщений в логе:

- 1. [CRITICAL] критичная ошибка, работа системы невозможна без устранения неисправности
- 2. [WARNING] предупреждение, работа системы не останавливается, но стоит устранить данную неисправность
- 3. [TRACE] сообщения при включении диагностического режима трассировки
- 4. [INFO] уведомление о действиях системы
- 5. [ERROR] ошибка при подключении сервисов и полисингов, неправильная конфигурация

Процесс FastDPI по умолчанию осуществляет журналирование всех действий системы в следующие файлы логирования отладки и статистики:

- 1. /var/log/dpi/fastdpi slave.log лог процессов обработки трафика¹⁾
- 2. /var/log/dpi/fastdpi stat.log лог статистики обработки трафика
- 3. /var/log/dpi/fastdpi alert.log лог общих функций fastDPI

Счетчики по блокировкам, которые сохраняются в лог статистики

Ротация лог файлов

Ротация файлов обеспечивает ежедневное резервное копирование суточного лога. По умолчанию этот процесс осуществляется в часы с наименьшей нагрузки на систему. Глубина хранения логов определяется в конфигурации /etc/logrotate.d/fastdpi параметром maxage, значение указывается в сутках.

Мониторинг SNMPD

Описание

SNMP — протокол, позволяющий получать информацию о сервере DPI для централизованного мониторинга критически важных параметров.

Принцип работы: по SNMP отправляется запрос на сервер, он получает необходимую информацию и отправляет ее на сервер мониторинга. Сервер мониторинга эту информацию принимает и обрабатывает, после этого можно понять статус сервера — отследить, на каких уровнях находятся те или иные параметры и данные.

Пакет bngsnmp содержит скрипты, необходимые для формирования VENDOR ветки OID'ов для опроса по SNMP.

В основе лежит библиотека snmp passpersist. OID вендорской ветки: .1.3.6.1.4.1.43823

Состав вендорской ветки:

- статистика CPU, в т.ч. утилизация ядра процессами BNG;
- количество нелегитимных дропов;
- статистика дропов на диспетчере;
- список доступности RADIUS серверов (при использовании прокси или балансира в статистике будет указан этот прокси);
- количество DHCP абонентов при активном функционале;
- список VRF и активных абонентов в каждом при активном функционале;
- статистика DPDK интерфейсов (количество пакетов, ошибок, уровень сигнала и т.п.);
- статистика NAT (список профилей, список пулов, и количество трансляций на каждый публичный адрес) **при активном функционале**;
- список аппаратных модулей, установленных на материнской плате при наличии данной возможности у ВМС контроллера;
- показатели с аппаратных сенсоров (напряжение, потребляемая мощность, FAN RPMs) при наличии данной возможности у ВМС контроллера;
- утилизация пулов в DHCP сервере (поддерживается <u>только KEA-DHCP</u> сервер) **при активном функционале**.

Данный скрипт также переопределяет стандартные ветки, добавляя статистику с DPDK интерфейсов:

- .1.3.6.1.2.1.2.2.1 32 битные счетчики
- .1.3.6.1.2.1.31.1.1.1 64 битные счетчики

При необходимости можно отключить переопределение — закомментировать или удалить следующие строки из /etc/snmp/snmpd.conf:



ФАЙЛ МІВ

Установка

1. Установка:

```
yum install bngsnmp
```

2. Конфигурация:

```
/bin/cp -f /etc/snmp/snmpd.conf.example /etc/snmp/snmpd.conf
```

3. Перезапуск службы net-snmp:

```
systemctl restart snmpd
```

4. Отключить selinux (в случае ошибки при запуске SNMP):

```
vi /etc/selinux/config
...
```

```
SELINUX=disabled
```

Проверка работоспособности SNMPD и вендорской ветки

Утилита snmpwalk позволяет проверить, приходят ли данные по SNMP

1. Установка snmpwalk:

```
dnf install net-snmp-utils
```

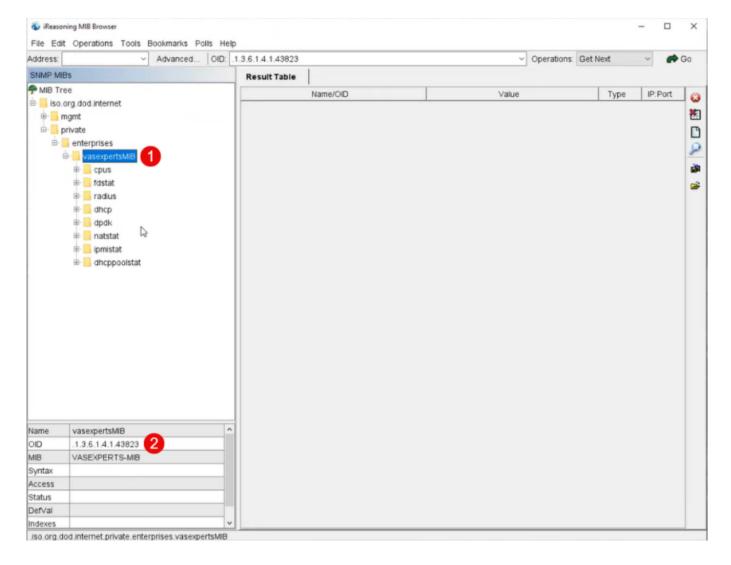
2. Команда для проверки работы SNMP:

```
snmpwalk -v 2c -c nokiamon localhost -On .1.3.6.1.4.1.43823
```

Как прочитать файл **MIB**

В случае, если необходимо увидеть файл MIB в графическом представлении, можно открыть его через MIB Browser. Там будет описана вся вендорская ветка и ее OID. На примере ниже показано:

- 1. Файл вендорской ветки
- 2. Ee OID



not8

Также в MIB Browser можно создавать собственный walk, указав адрес сервера

Известные ограничения

Поддержка on-stick девайсов доступна с версии 13.2-beta4.2.

Мониторинг через SNMP агент (Zabbix-agent)

Мы предлагаем вам следующий набор параметров, которые можно снимать с DPI CKAT:

- Ошибки в логах процесса fastDPI /var/log/dpi/fastdpi alert.log
- Ошибки в системном логе /var/log/messages
- Потери (Drop) на интерфейсах dna
- Объем трафика на интерфейсах
- Доступность интерфейсов управления
- Количество обработанных запросов по HTTP и HTTPS
- Количество заблокированных ресурсов по HTTP, HTTPS, IP
- Количество сессий РРРоЕ

Для мониторинга можно использовать Zabbix Agent.

Текущая и финальная поддерживаемая версия агента и сервера — 6.0, следует использовать Zabbix agent 1. Для более новых версий Zabbix мониторинг будет осуществляется посредством SNMP.

Настройка агента

- 1. Установить Zabbix agent 1 на сервер DPI согласно инструкции на сайте Zabbix. В первом шаге выбрать следующие значения:
 - ∘ Пакеты Zabbix
 - ∘ Версия Zabbix: 6.0+
 - ∘ Дистрибутив ОС: CentOS
 - ∘ Версия ОС: 8 STREAM
 - ∘ Компонент Zabbix: AGENT
- 2. Отредактировать конфигурационный файл /etc/zabbix/zabbix_agentd.conf: изменить параметры Server= и ServerActive= на ваш адрес сервера, hostname= на hostname сервера.
- 3. Изменить контекст файла /var/log/dpi/fastdpi stat.log:

```
chcon unconfined_u:object_r:zabbix_log_t:s0
/var/log/dpi/fastdpi_stat.log
```

- 4. Открыть порты tcp/udp 10050 и 10051 в firewall
- 5. Загрузить файл

ssg userparams.conf

в директорию /etc/zabbix/zabbix_agent.d/

6. Отредактировать файл ssg_userparams.conf заменив номер интерфейса в UserParameter

02-00.0 нужно заменить на названия интерфейсов вашего сервера! Название должно совпадать с конфигом DPI. Если у вас используется более 2 интерфейсов, необходимо добавить строчку по аналогии с существующими параметрами.

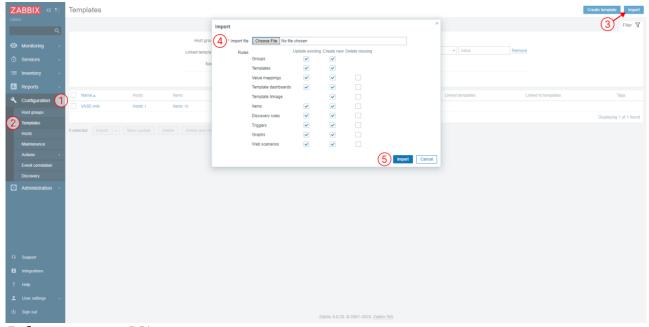
7. Сделать рестарт агента: systemctl restart Zabbix-agent

Настройка сервера

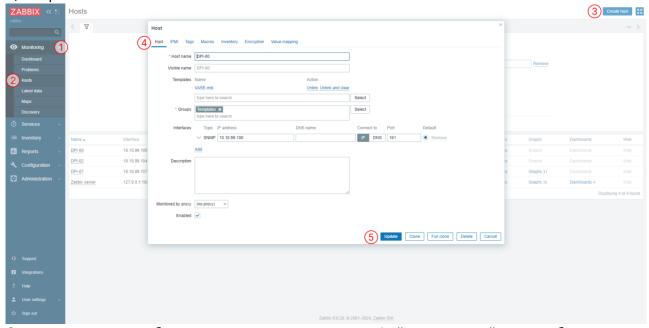
- 1. Установить и настроить Zabbix сервера согласно инструкции на официальном сайте.
- 2. Добавить шаблон

zbx export templates.xml

- 1) Перейти в раздел Configuration
- 2) Раздел Templates
- 3) Нажать "Import"
- 4) Импортировать файл шаблона
- 5) Сохранить изменения



- 3. Добавить сервер DPI в качестве хоста
 - 1) Перейти в раздел Monitoring
 - 2) Раздел Hosts
 - 3) Нажать "Create host"
 - 4) Задать необходимые параметры, имя хоста, группу и добавленный ранее шаблон
 - 5) Сохранить изменения



4. Отредактировать шаблон: изменить названия интерфейсов и ключей так, чтобы они соответствовали UserParameter.

Мониторинг распределение трафика по классам

СКАТ позволяет вывести на мониторинг распределение трафика по классам.

1. Включите приоритизацию трафика. Для примера будем использовать следующие правила приоритизации:

```
dns cs0
http cs0
https cs0
Bittorrent cs7
ICMP cs0
TCP Unknown cs7
G00GLEVIDE0 cs1
default cs2
```

2.В конфигурации /etc/dpi/fastdpi.conf установите параметр:

```
dbg_log_mask=0x4
```

3.Включите полисинг общего канала (в качестве примера приведен полисинг с ограничением на всю ширину канала):

```
htb inbound root=rate 1300mbit
htb inbound class0=rate 8bit ceil 1300mbit
htb inbound class1=rate 8bit ceil 1300mbit
htb inbound class2=rate 8bit ceil 1300mbit
htb inbound class3=rate 8bit ceil 1300mbit
htb inbound class4=rate 8bit ceil 1300mbit
htb inbound class5=rate 8bit ceil 1300mbit
htb inbound class6=rate 8bit ceil 1300mbit
htb inbound class7=rate 8bit ceil 1300mbit
htb root=rate 1300mbit
htb class0=rate 8bit ceil 1300mbit
htb class1=rate 8bit ceil 1300mbit
htb class2=rate 8bit ceil 1300mbit
htb class3=rate 8bit ceil 1300mbit
htb class4=rate 8bit ceil 1300mbit
htb class5=rate 8bit ceil 1300mbit
htb class6=rate 8bit ceil 1300mbit
htb class7=rate 8bit ceil 1300mbit
```

4. Обновите конфигурацию:

service fastdpi reload



Если полисинг для общего канала применяется впервые, необходимо сделать рестарт сервиса:

service fastdpi restart

5. Используйте следующие пользовательские параметры для zabbix агента, установленного на CKAT: 6. На сервер Zabbix импортируйте шаблон, как описано в разделе "Мониторинг через SNMP агент":

zbx export templates.xml



При необходимости измените названия интерфейсов в шаблоне и в файле с пользовательскими параметрами

Просмотр статистики по flow и протоколам

Πo flow

- 1. IPv4/IPv6
- 2. тип протокола: 0 IPv4, 1 IPv6
- 3. всего выделено записей
- 4. очередь с коротким временем жизни:
 - 1. занято записей
 - 2. готово к повторному использованию
 - 3. разница 3.1 3.2 (количество активных flow)
- 5. тоже для долгоиграющей очереди
- 6. тоже суммарно

Пример:

```
fdpi_ctrl stat --flow
IPv4 0 6784000 834 814 20 0 0 0 834 814 20
```

По протоколам

- 1. внутренний индекс статистики по протоколу
- 2. имя протокола
- 3. номер порта для протокола μ аправление subs --> inet
- 4. кол-во пакетов
- 5. объем в байтах ip total
- 6. дропнуто пакетов
- 7. дропнуто байт направление inet -→ subs кол-во пакетов и т.д.

Пример:

```
4081 'sip' 5060 0 0 0 0 2479 1170579 0 0
5812 'Bittorrent' 49165 0 0 0 0 0 0 3 495
5866 'ICMP' 65025 0 0 0 0 225 18900 0 0
5871 'TCP Unknown' 65030 0 0 0 0 41034 3448836 0 0
5880 'UDP Unknown' 65041 3900 4227600 0 0 277 24825 0 0
6000 'ARP' 65282 30 2520 0 0 30 2520 0 0
6056 'CHAMELEON' 49236 0 0 0 0 589 72475 0 0
```

1)

Под каждый обработчик создается свой fastdpi_slave лог, остальные лог файлы создаются в единственном экземпляре.