????????? ?????? SPAN-??????? ?? Central Node ? Sensor

Руководство по настройке KATA/NDR 7.1

> **Информация:** Приведенная на данной странице информация, является разработкой команды **pre-sales** и/или **AntiAPT Community** и **НЕ является** официальной рекомендацией вендора.

- **Версия решения:** 7.1
- **Тип инструкции:** Настройка источников данных SPAN

> **Важно!**
> Интеграция в локальную сеть позволяет получать и анализировать зеркалированный трафик SPAN, ERSPAN и RSPAN. Извлекаются объекты и метаданные HTTP, HTTP2, FTP, SMTP, DNS, SMB и NFS протоколов. Зеркалируемый трафик перенаправляется с одного порта коммутатора на другой (локальное зеркалирование) или на удаленный коммутатор (удалённое зеркалирование). Администратор сети выбирает, какую часть трафика направлять в Kaspersky Anti Targeted Attack Platform.
>
> Kaspersky Anti Targeted Attack Platform принимает зеркалированный трафик от агрегирующих устройств, таких как брокеры сетевых пакетов и сетевые отводы (Network tap). Фильтрация трафика, поступающего через эти устройства, влияет на аппаратные требования платформы. Для точного определения этих требований рекомендуется провести пилотное тестирование.

---

1. Подготовка

1.1. Обязательные условия

Перед настройкой приёма SPAN-трафика убедитесь, что:

- ☐ Установлена и настроена **Central Node**

- ☐ Активирована одна из лицензий: **KATA**, **NDR** или **KATA/NDR**

- ☐ Добавлен **дополнительный сетевой интерфейс**, на который будет подан SPAN. (кроме Management)

- ☐ Интерфейс находится в состоянии **«Не инициализирован» (при подаче ESRPAN указывается IP адрес)**

- ☐ Имеется доступ к веб-интерфейсу под учётной записью `**admin**`

1.2. Лицензии и функциональность

Лицензия	**Требуется для**
KATA	Анализ периметра сети: сетевая песочница (Network Sandbox), пограничный IDS, анализ SMTP/ICAP-трафика
NDR	Защита внутренней сети: NTA-анализ, ретроспективный поиск, выявление горизонтального перемещения, **запись и хранение SPAN-трафика**
KATA/NDR	Комбинированный функционал: защита периметра + внутренней сети

□□ Подробное описание функционала

□□KATA

- Обеспечивает **защиту периметра IT-инфраструктуры**

- Включает **сетевую песочницу (Network Sandbox)** — автоматическую проверку подозрительных объектов

- Реализует функции **пограничного IDS**

- Поддерживает анализ трафика от почтовых шлюзов (SMTP), прокси и NGFW (ICAP)

- Позволяет анализировать трафик на границе сети

□□NDR (Network Detection and Response)

- Предназначен для **обнаружения сложных атак во внутренней сети**

- Выполняет **глубокий анализ сетевого трафика (NTA)**:

    - Построение карты сетевой активности

    - Выявление скрытых C2-каналов

    - Обнаружение **горизонтального перемещения** злоумышленника

    - Ретроспективный анализ событий за весь период хранения данных

- **Записывает и хранит обрабатываемый SPAN-трафик**

- Использует правила IDS для детектирования аномалий во внутреннем трафике

- Интегрируется с EDR-агентами для корреляции событий

□□KATA/NDR

- Объединяет возможности KATA и NDR

- Позволяет **одновременно защищать периметр и внутреннюю сеть**

- Центральный узел может принимать данные как от периметровых источников, так и от Sensor, анализирующих внутренний трафик

- Поддерживает единый интерфейс управления, корреляцию событий между периметром и внутренней сетью

> ⚠**ВАЖНО:**
> - Без активации соответствующей лицензии функционал **приёма и обработки SPAN-трафика будет недоступен**.
> - Для записи и хранения сырого трафика требуется **лицензия NDR или KATA/NDR**.

> **□□Рекомендация:**
> - Для оптимальной работы лучше выбрать комбинированную лицензию **KATA/NDR**. Она позволяет контролировать как периметр, так и внутреннюю сеть.

1.3. Сетевые требования

Данный пункт описывает процесс настройки Central Node для анализа копии трафика, поданного с внутреннего или внешнего сегмента сети.

> ⚠**ВАЖНО:**
> - Для включения анализа сетевого трафика обязательно должен быть добавлен дополнительный интерфейс.

> **iПримечание:**
> - В версию KATA 7.1 добавлена возможность записи, хранения и выгрузки копий сырого сетевого трафика. В данном документе этот функционал описан не будет, только настройка приема SPAN. Детально по данному функционалу можно ознакомиться в онлайн документации.
>
> Добавить!

□□Минимальные и максимальные требования к объёму SPAN-трафика

Конфигурация	Минимальный объём SPAN-трафика	Максимальный объём SPAN-трафика
Физический сервер + выделенный Sensor	100 Мбит/с	10 000 Мбит/с
Виртуальная платформа + выделенный Sensor	100 Мбит/с	4 000 Мбит/с
Central Node со встроенным Sensor (Embedded Sensor)	100 Мбит/с	1 000 Мбит/с

> **iПояснение:**
> - Значение **100 Мбит/с** указано как **рекомендуемый порог**, используемый при сайзинге и проектировании.
> - Это значение **не является жёстким ограничением**, а служит ориентиром для расчёта ресурсов.
> - При объёмах ниже 100 Мбит/с **сайзинг не изменяется** — аппаратные требования остаются теми же.

Масштабирование через распределённую архитектуру

Если объём SPAN-трафика превышает возможности одной инсталляции:

- На виртуальной платформе: максимум **4000 Мбит/с на одну Central Node с Sensor**

- На физической платформе: максимум **10 000 Мбит/с на одну Central Node с Sensor**

> **Примечание:** Количество сенсоров, подключенных к одному центральному узлу, ограничено только общим объемом поступающего на них трафика SPAN.

> **При необходимости обработать больший объём:**
> 1. Разделите трафик между несколькими независимыми инсталляциями
> 2. Используйте физическую платформу
> 3. Объедините инсталляции в иерархическую структуру **(PCN + SCN)**

> **Подробнее:** Распределённое решение и мультитенантность

1.4. Проверка настройки функционала обработки SPAN-трафика

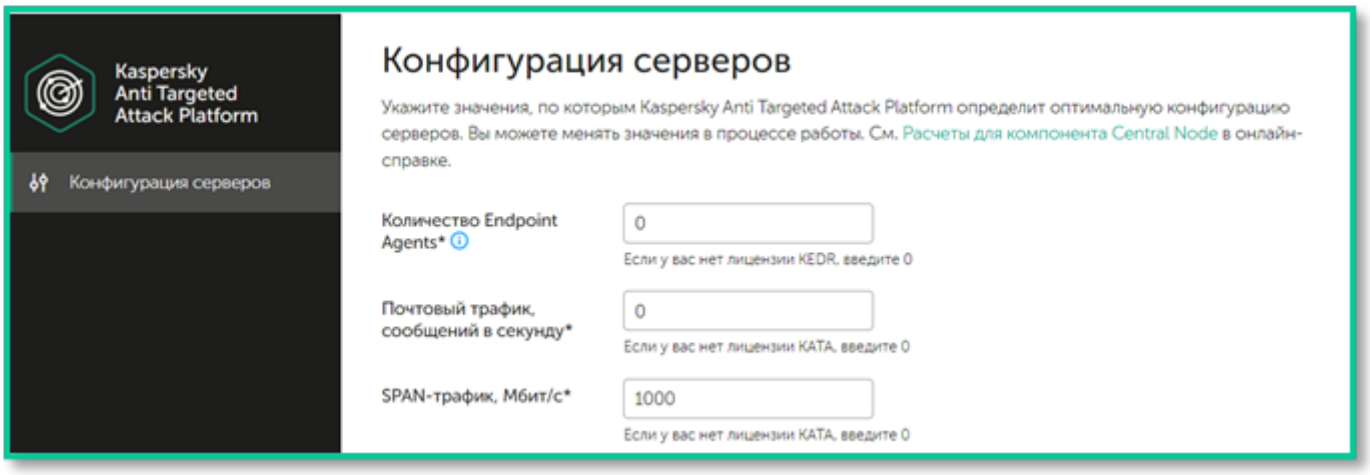
1. Перейдите в веб-интерфейс Central Node под учётной записью `**admin**`.

2. Перейдите: **Конфигурация серверов**.

3. Проверьте, что в поле «**SPAN-трафик, Мбит/с**» указан **общий объем** планируемого к обработке трафика со SPAN-портов.

> **ВАЖНО:**
> - В этом поле указывается **общий объём SPAN-трафика**, который обрабатывается как на **Central Node**, так и на вынесенных отдельно **Sensor**.

> **Внимание:**
> Если вы не собираетесь использовать KATA и/или NDR, все равно рекомендуется указать объем обрабатываемого SPAN-трафика. Минимальный объем — 10. Это обеспечит корректную работу и логическую связность микросервисов в системе.

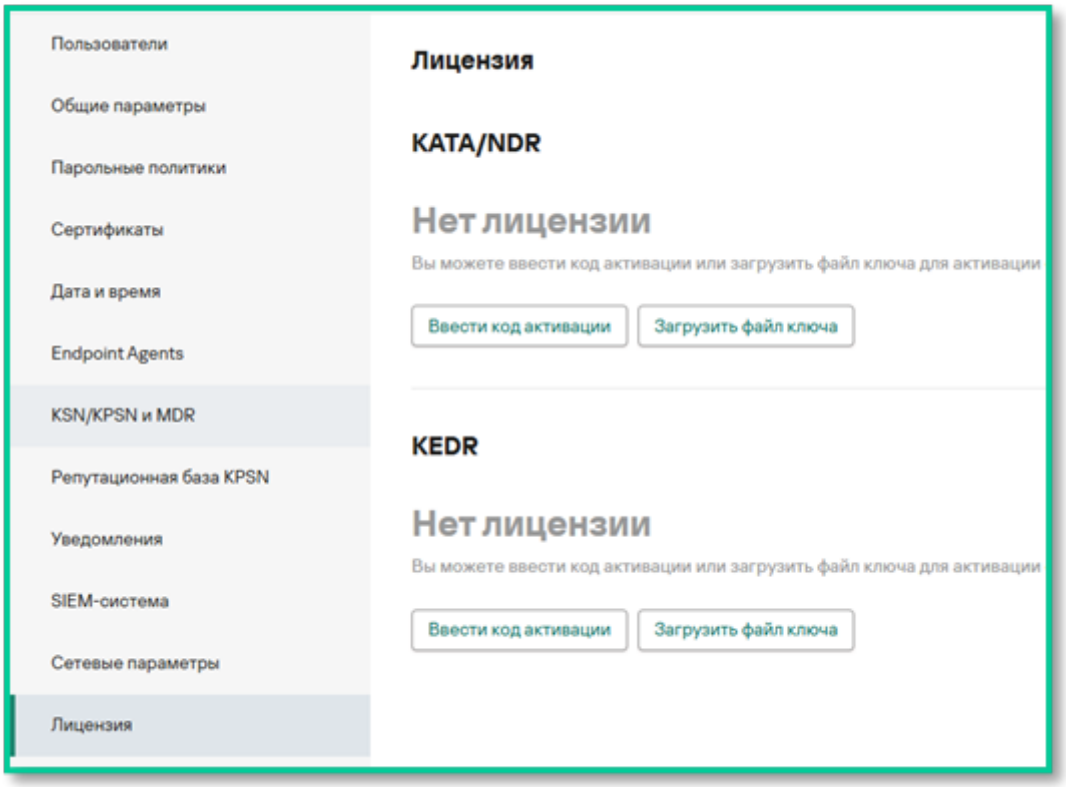


Скриншот 1: Экран "**Конфигурация серверов**" с полями: Количество Endpoint Agents, Почтовый трафик, SPAN-трафик

> **Пример заполнения:**
> На Central Node подается SPAN на выделенный интерфейс с объемом **500 Mbps** и есть выделенный Sensor, который получает SPAN объемом **1.5 Gbps**.
>
> **Настройка:**
>
> В поле **«SPAN-трафик, Мбит/с»** укажите: **2000**
>
> Это суммарный объём трафика, обрабатываемый всей системой.

4. Перейдите в раздел “**Параметры → Лицензия**”.

5. Убедитесь, что активирована лицензия **NDR** или **KATA/NDR**.



Скриншот 2: Экран ""**Параметры → Лицензия**".

1.5. Настройка объёма обрабатываемого трафика

> ⚠**Обязательно выполните эти настройки**, если на узле (CN или Sensor) получен SPAN.

Через SSH-консоль:

1. Подключитесь к Central Node **или Sensor** по SSH под учётной записью `**admin**`. (в зависимости от того, куда подан SPAN)

2. Перейдите: **Program settings → Configure storage**.

4. Установите значение, соответствующее вашему объёму SPAN-трафика, согласно таблице:

Объём SPAN-трафика	File storage, MB	Hot ring, MB
10000 Мбит/с	80000	10240

7000 Мбит/с	64000	8192
4000 Мбит/с	32000	1024
2000 Мбит/с	16000	1024
1000 Мбит/с	8000	1024

> **Примечание:** это размер разделов **tmpfs**, где обрабатывается и хранится трафик.

ВАЖНО!
Настройки хранилища на **Central Node** или **Sensor** учитывают только трафик, обрабатываемый **Central Node** или **Sensor**, и выполняется на **каждом узле** отдельно.
Однако настройки SPAN в конфигураторе сервера в **веб-интерфейсе** учитывают весь трафик, обрабатываемый **Central Node**, и все подключенные **внешние Sensor**.

> **Примечание:**
> - Если объём данных меньше указанного в таблице — выбирайте минимальное значение.
> - Если объём находится между двумя значениями — выбирайте **максимальное**.

ВАЖНО:
Эти настройки **обязательны** для **Central Node** и **выделенного Sensor**, независимо от того, где был подан SPAN-трафик.

1.6. Выбор протоколов для анализа

? ????: ????????? ????????? ??????? ?????? ?? ?????? ??????????.

Через SSH-консоль:

1. Подключитесь к узлу (**Central Node** или **Sensor**) по **SSH**.

2. Перейдите: **Program settings → Configure traffic capture → Setup capture protocols**.

4. Выберите протоколы, которые нужно анализировать:

- По умолчанию включены все, кроме **HTTP2**.

- Чтобы включить/отключить протокол — нажмите **Enter** на строке.

5. Нажмите **Apply and finish**.

 Сетевые протоколы для получения SPAN-трафика будут выбраны.

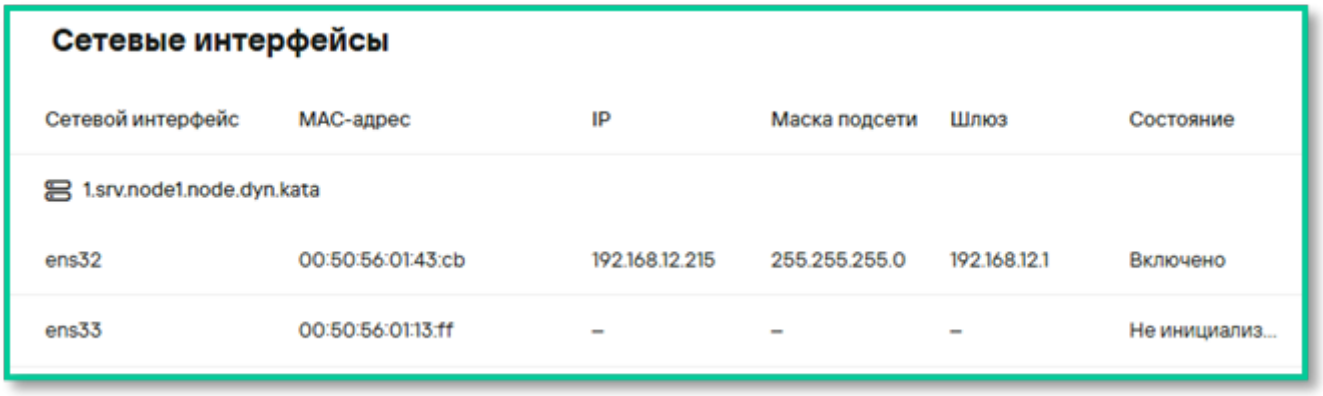
2. Включение функционала обработки SPAN

2.1. Добавление дополнительного интерфейса на Central Node

1. Войдите в веб-интерфейс Central Node под учётной записью `**admin**`.

2. Перейдите: **Параметры → Сетевые параметры → Сетевые интерфейсы**.

3. Убедитесь, что добавлен дополнительный интерфейс и он находится в состоянии «**Не инициализирован**».



Скриншот 3: Экран "**Сетевые интерфейсы**"

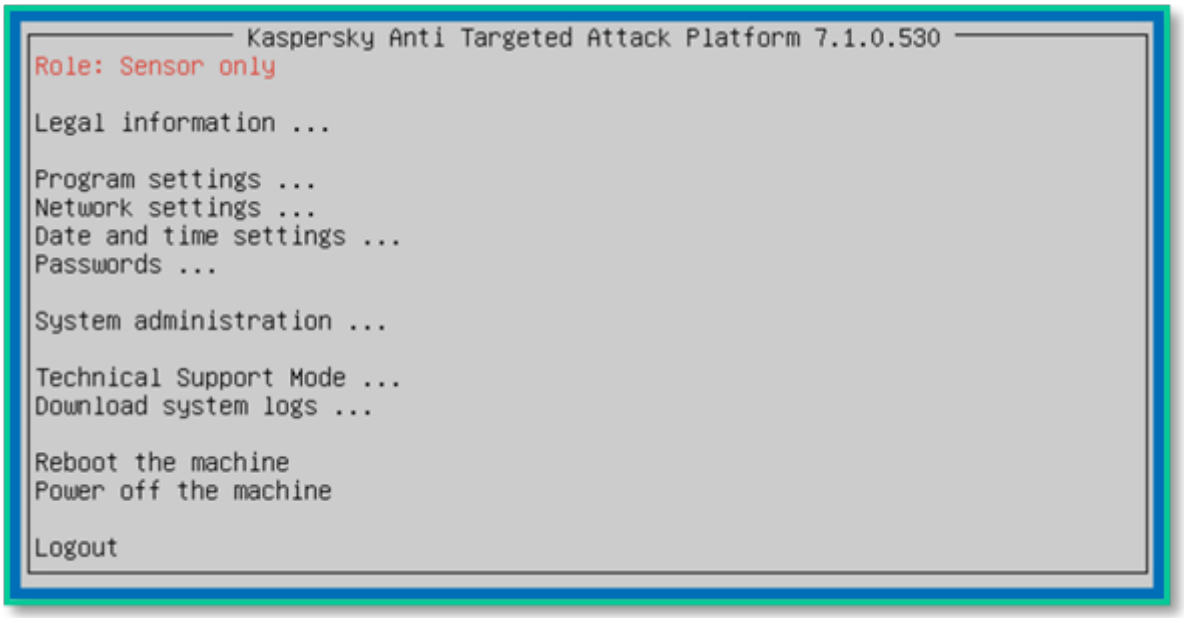
> **Примечание: ERSPAN**-трафик передаётся исключительно на IP-адрес получателя (не на конкретный интерфейс), при этом тип принимающего интерфейса может быть любым. Важно правильно указать IP-адрес назначения, так как именно он определяет маршрут доставки зеркалированного трафика через GRE-туннель.

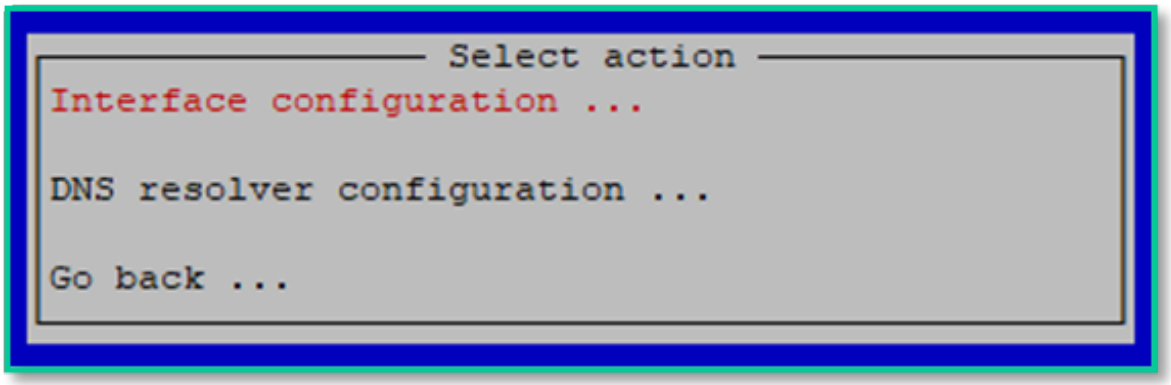
2.2. Добавление дополнительного интерфейса на Sensor

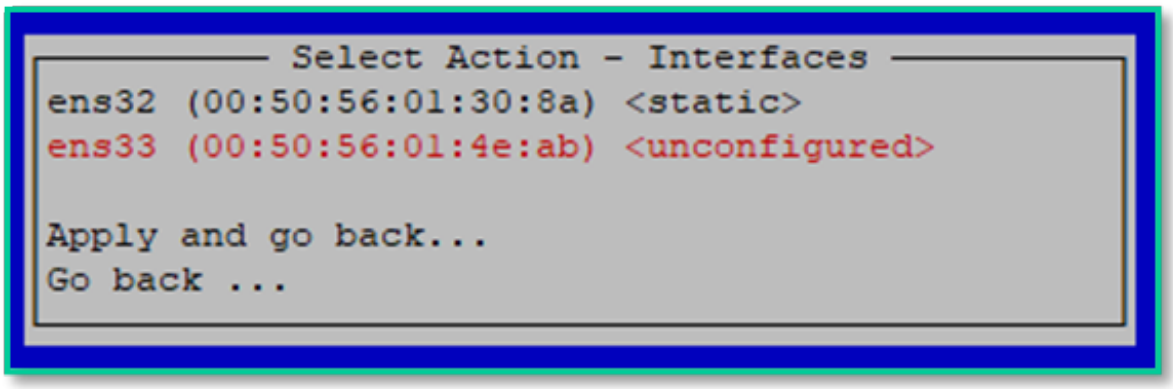
Через SSH-консоль:

1. Подключитесь к узлу **Sensor** по **SSH**.

2. Перейдите: **Network settings → Interface configuration**.







Скриншот 4: Экран "**Сетевые интерфейсы**"

> **Важно!**
> Данная настройка относится к компоненту Sensor, используемого для обработки SPAN-трафика.

2.3. Настраиваем объем обрабатываемого SPAN непосредственно на Sensor

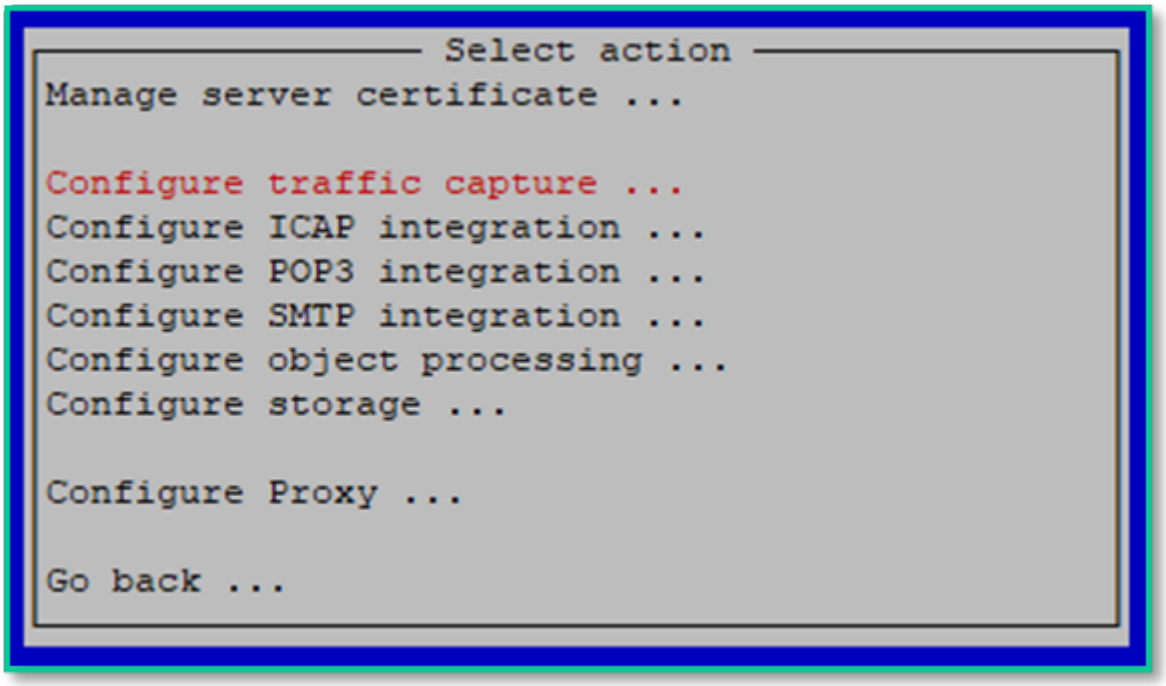
> **Пояснение:**
> Данная настройка относится к компоненту Sensor, используемого для обработки SPAN-трафика.

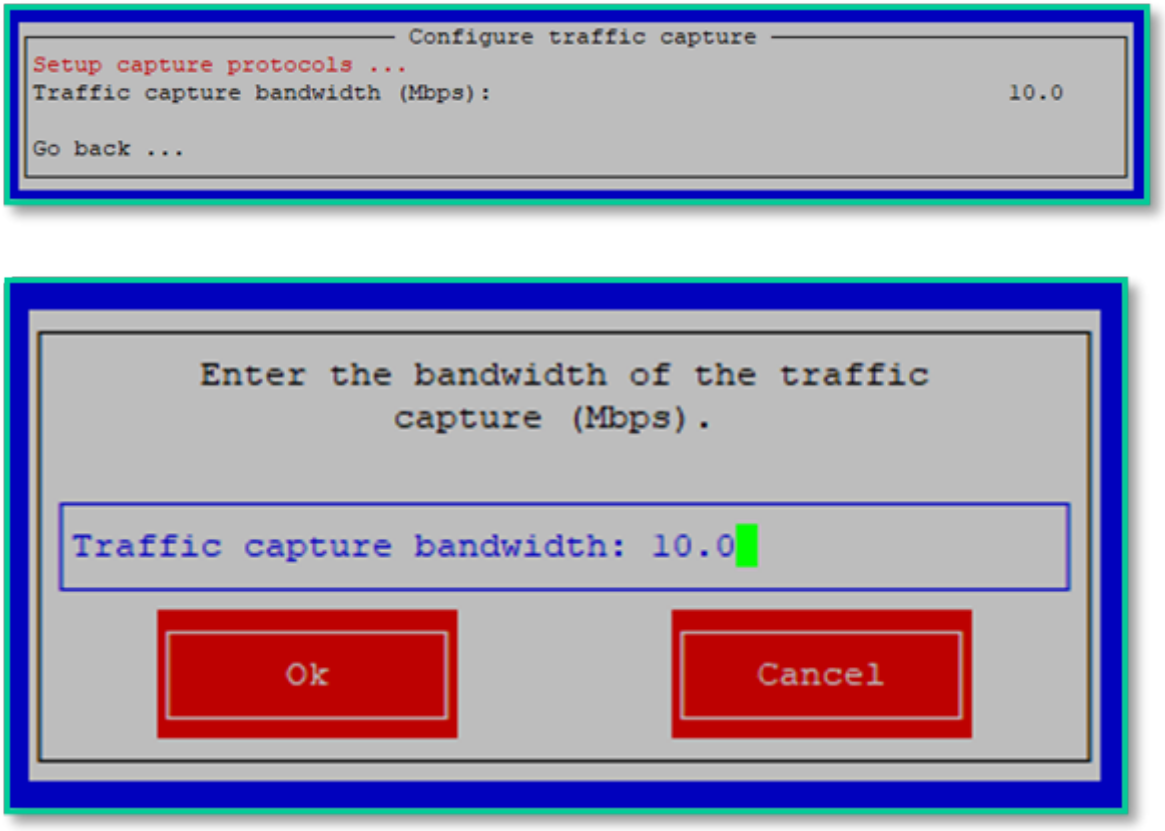
Через SSH-консоль:

1. Подключитесь к узлу **Sensor** по **SSH**.

2. Перейдите: **Program settings → Configure traffic capture**.

3. Укажите объем анализируемого сетевого трафика в разделе "**Traffic capture bandwidth (Mbps)**". Объем должен быть указан в мегабитах в секунду.





Скриншот 5: Экран "**Сетевые интерфейсы**"

> **Важно!**
> В этом разделе показан общий объем SPAN-трафика, обработанного данным сенсором.
> **Например:** сенсор может получать SPAN-трафик с нескольких источников одновременно через разные интерфейсы, подключенные к нему.

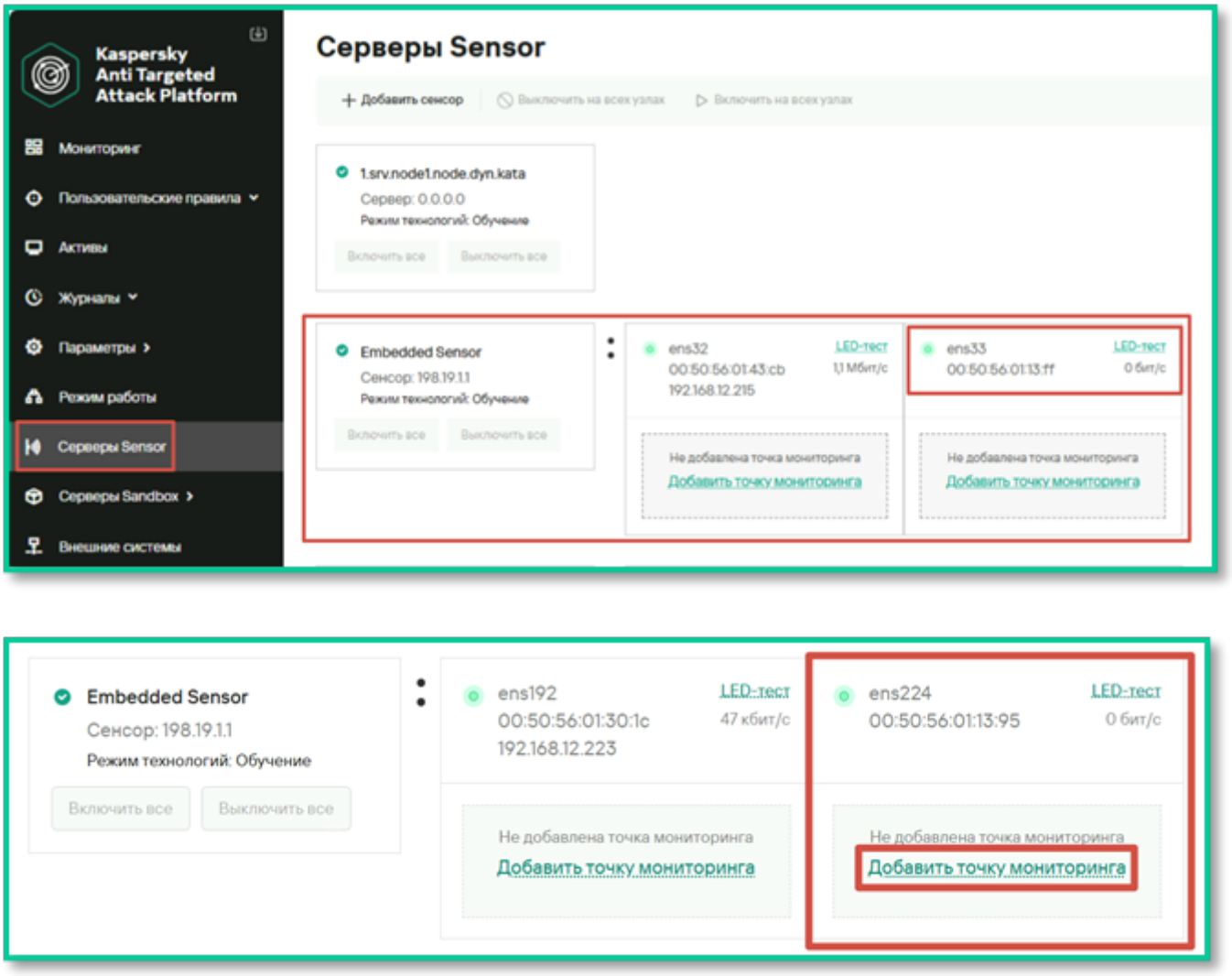
2.4. Создание точки мониторинга

Цель: создать точку мониторинга для приёма SPAN-трафика.

1. Перейдите: **Серверы Sensor**.

2. Найдите интерфейс в состоянии **«Не инициализирован»**, предназначенный для приёма SPAN.

3. Нажмите **«Добавить точку мониторинга»** на этом интерфейсе.



Скриншот 6: Кнопка "**Добавить точку мониторинга**"

4. В открывшемся окне укажите:

- **Имя точки мониторинга** (например, `**SPAN_Internal**`)

5. Нажмите «**Добавить точку мониторинга**».

> **Примечание:**
> - Точки мониторинга можно **включать и выключать** для временного прекращения наблюдения за сегментом сети.

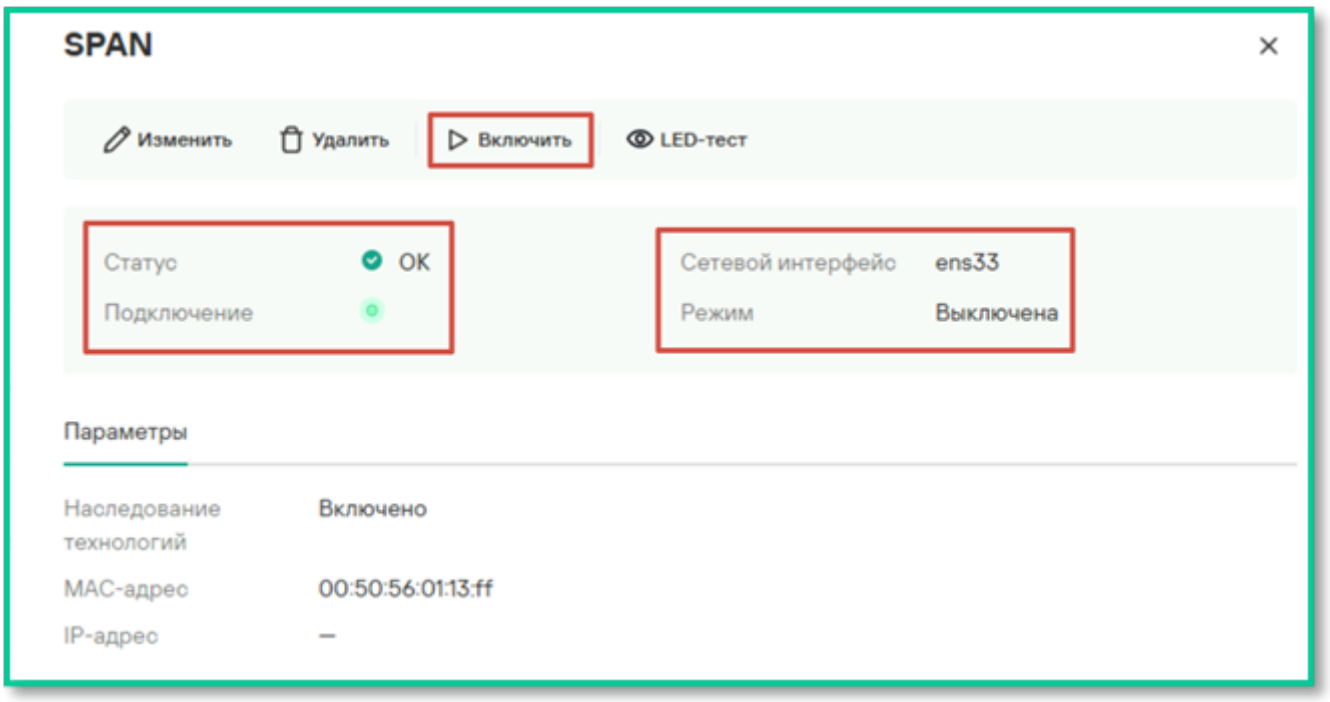
Внимание: Эта настройка одинакова для **Central Node** и **Sensor**.

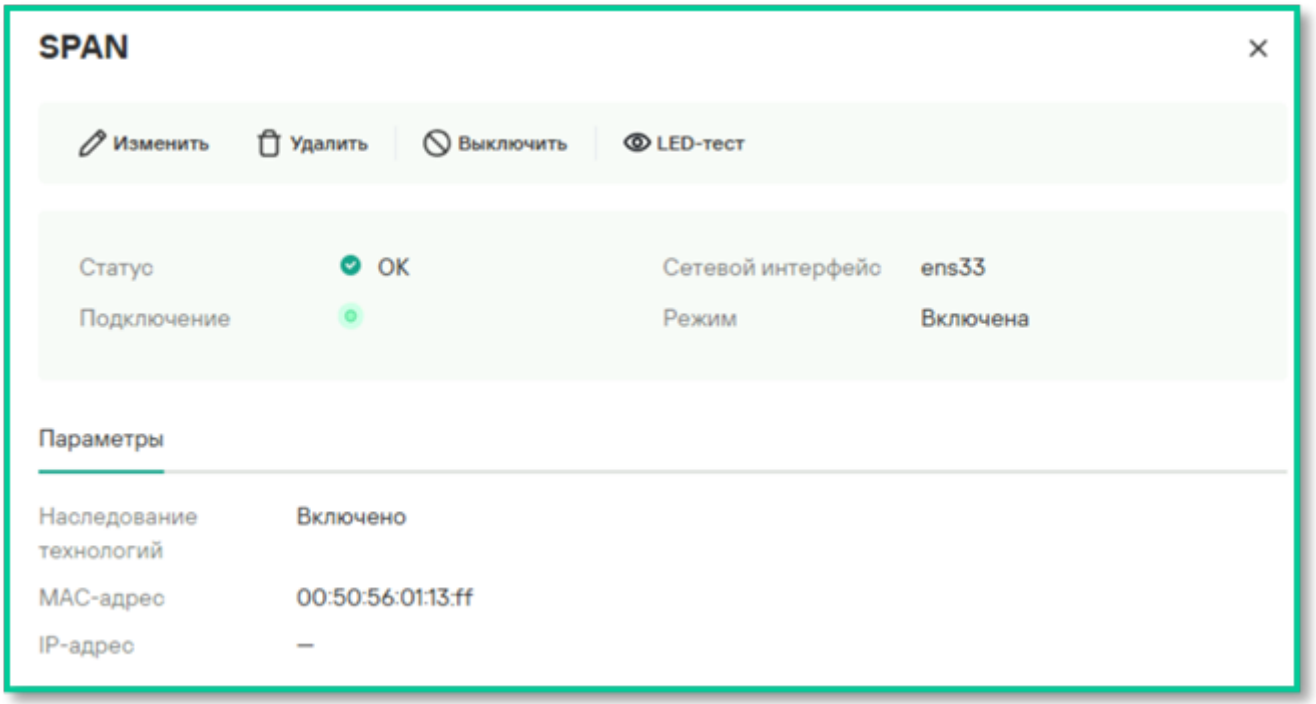
2.5. Включение обработки трафика

1. После создания точки мониторинга откроется её экран.

2. Убедитесь, что в разделе **«Режим»** указано состояние **«Выключен»**.

3. Нажмите кнопку **«Включить»**.





Скриншот 7: Окно точки мониторинга с кнопкой "**Включить**"

Режим обработки SPAN-трафика перейдёт в **активное состояние**.

2.6. Проверка поступления трафика

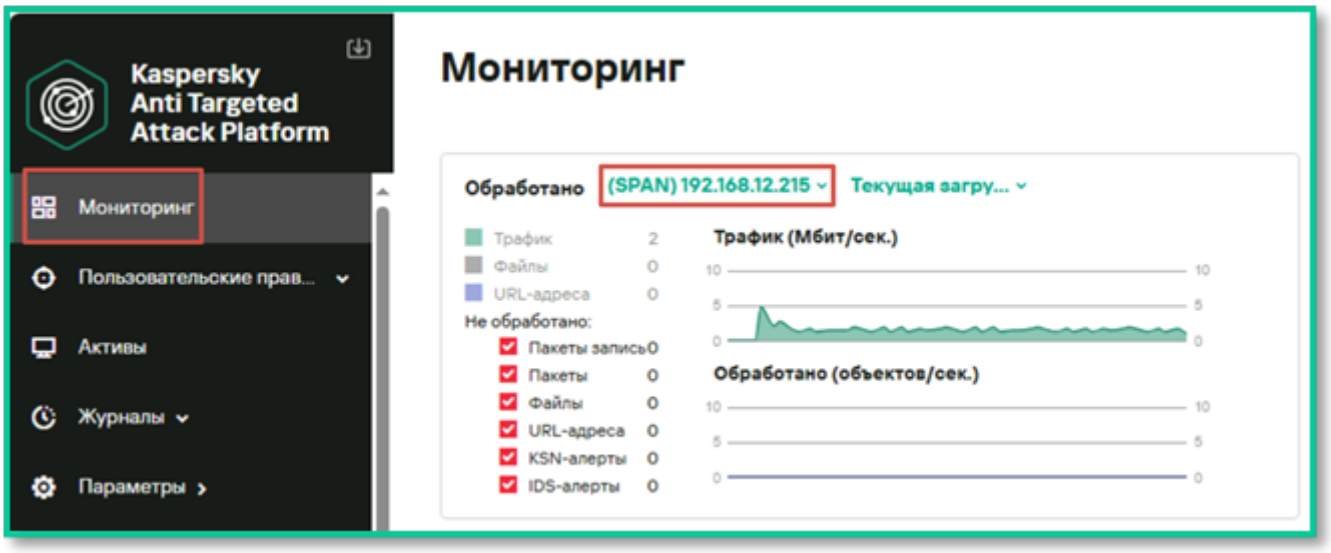
1. Перейдите: **Мониторинг → Обработано**.

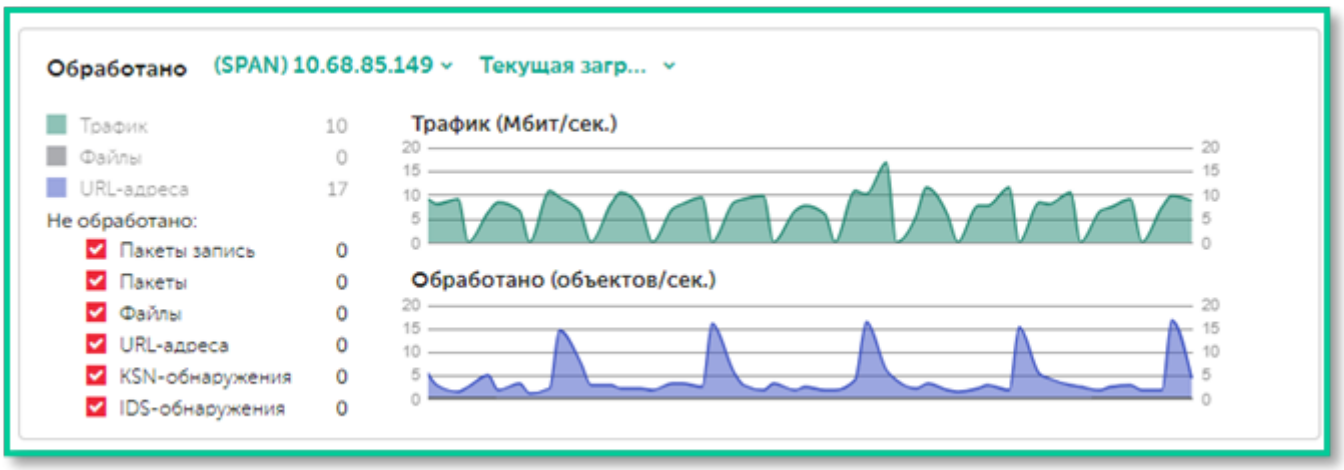
2. Выберите источник: **SPAN**.

3. Укажите тип отображения:

- **Текущая загрузка**

- **Выбранный период** (настраивается в правом верхнем углу)





Скриншот 8: График нагрузки по SPAN-трафику

Если SPAN-трафик подаётся на интерфейс, вы увидите график по нагрузке.

> **Примечание:**
> Данные по обнаруженным аномалиям и угрозам будут отображаться в веб-

> интерфейсе **только под учётной записью «Офицера безопасности»**.

3. Подключение и настройка внешнего хранилища

3.1. Настройка внешнего хранилища на Central Node

?????: ????????? ???????? ?????? ??????? ?? ??????? ?????????.

1. На узле с Central Node подключите диск **≥100 ГБ**.

2. Подключитесь по SSH и выполните:

```
sudo -i
  fdisk -l  # убедитесь, что диск виден (например, /dev/sdb)
```

```
Disk /dev/sda: 300 GiB, 322122547200 bytes, 629145600 sectors
Disk model: Virtual disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 08FA7C51-6950-4FAC-9662-241B90EDB311

Device         Start       End   Sectors   Size Type
/dev/sda1       2048   1026047   1024000   500M BIOS boot
/dev/sda2    1026048 252684287 251658240   120G EFI System
/dev/sda3  252684288 629143551 376459264 179.5G Linux filesystem


Disk /dev/sdb: 100 GiB, 107374182400 bytes, 209715200 sectors
Disk model: Virtual disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
root@1.srv.node1.node.dyn.katasensor:~#
```

Скриншот 9: Пример вывода команд

```
mke2fs -t ext4 -L DATA -m 0 /dev/sdb
```

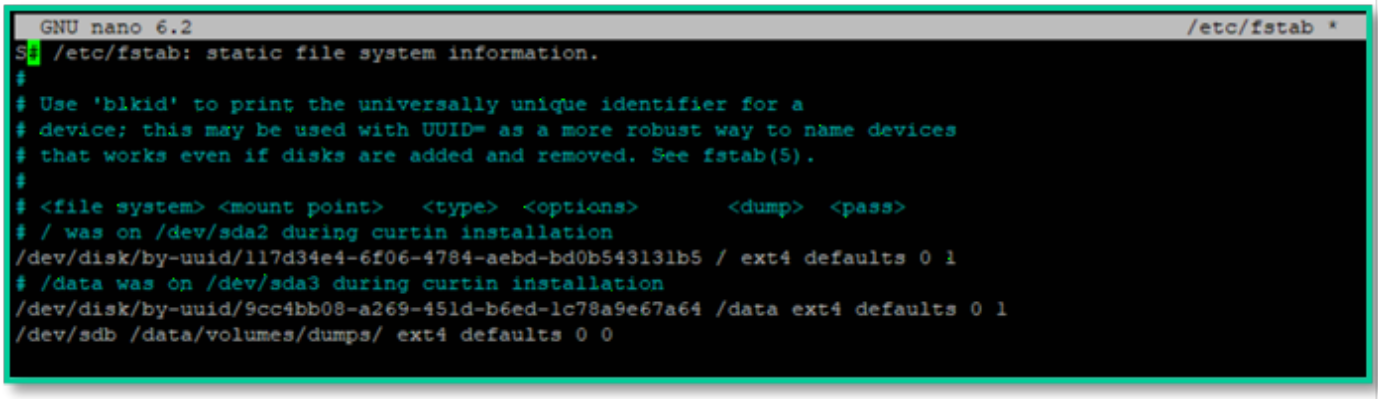
```
root@1.srv.node1.node.dyn.katasensor:~# mke2fs -t ext4 -L DATA -m 0 /dev/sdb
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 40370787-efla-429c-a677-8a6e47594a04
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done

root@1.srv.node1.node.dyn.katasensor:~#
```

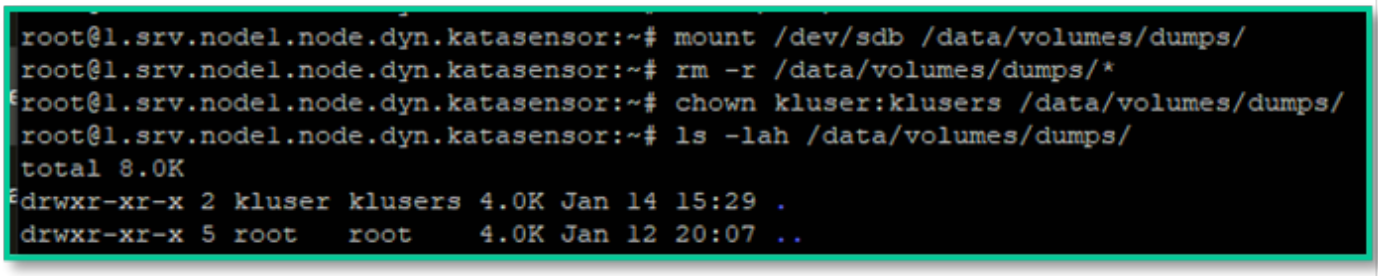
Скриншот 10: Пример вывода команд

```
echo "/dev/sdb /data/volumes/dumps/ ext4 defaults 0 0" >> /etc/fstab
```



Скриншот 11: Пример вывода команд

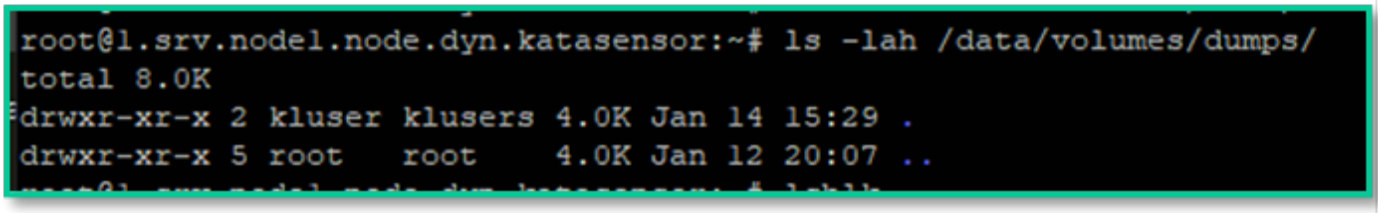
```
mount
  rm -rf /data/volumes/dumps/*
  chown kluser:klusers /data/volumes/dumps/
```

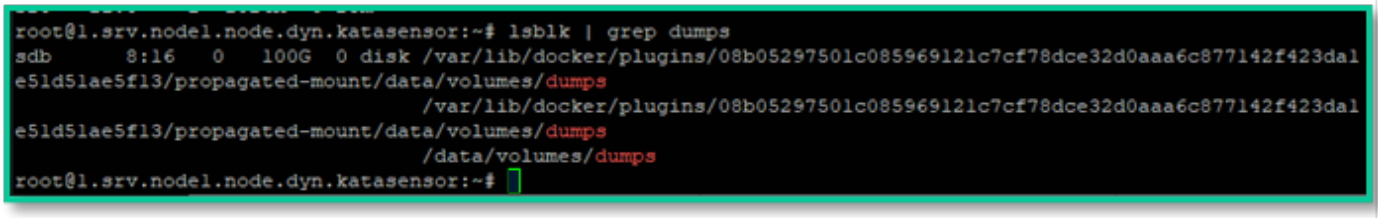


Скриншот 12: Пример вывода команд

3. Убедитесь, что напротив имени подключенного диска в столбце **MOUNTPOINTS** отображается значение **/data/volumes/dumps**.

```
chown kluser:klusers /data/volumes/dumps/
  ls -lah /data/volumes/dumps/
  lsblk
```





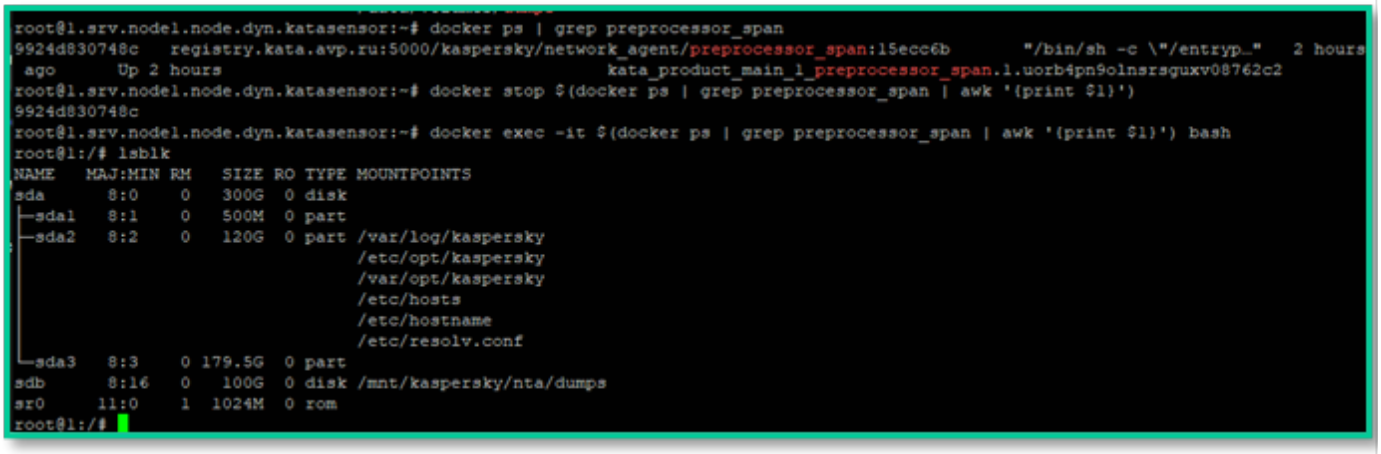
Скриншот 13: Пример вывода команд

4. Перезапустить работу контейнера **preprocessor_span**:

```
docker service update kata_product_main_1_preprocessor_span --force
  docker ps | grep preprocessor_span
```

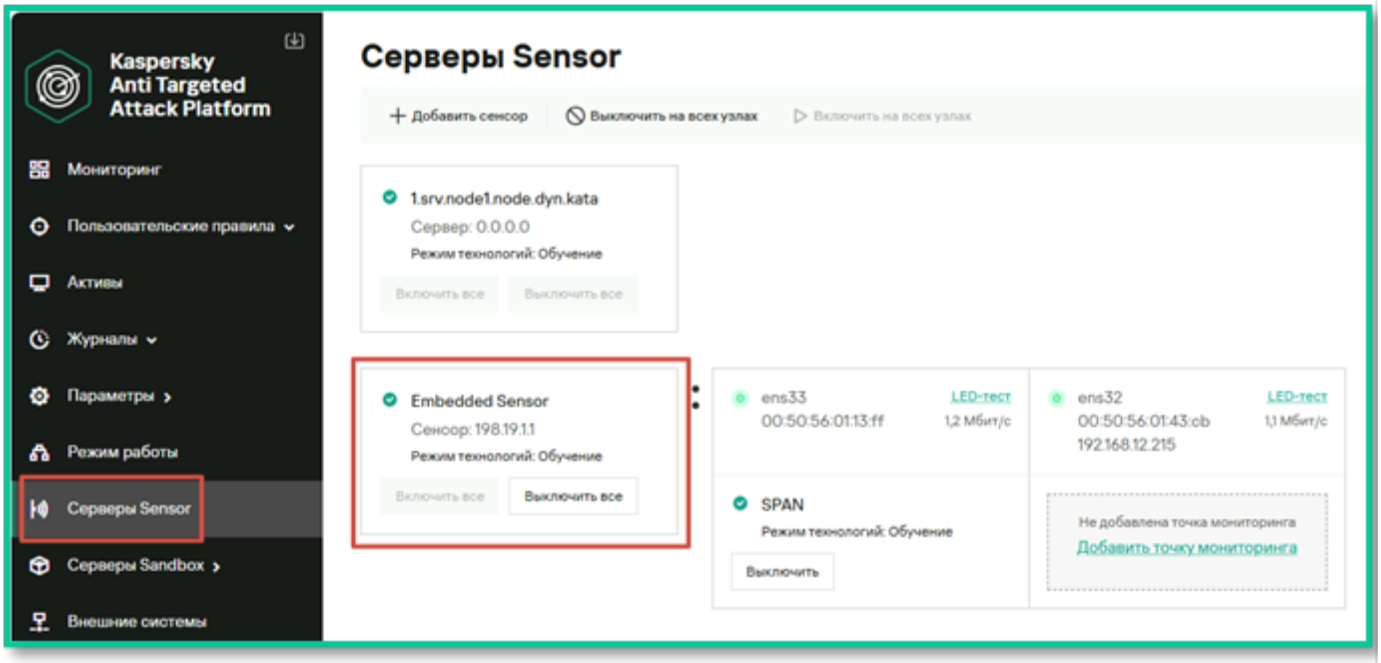
5. Убедитесь, что напротив имени подключенного диска в столбце **MOUNTPOINTS** отображается значение **/mnt/kaspersky/nta/dumps**.

```
docker exec -it $(docker ps | grep preprocessor_span | awk '{print $1}') bash
  lsblk
```



Скриншот 14: Пример вывода команд

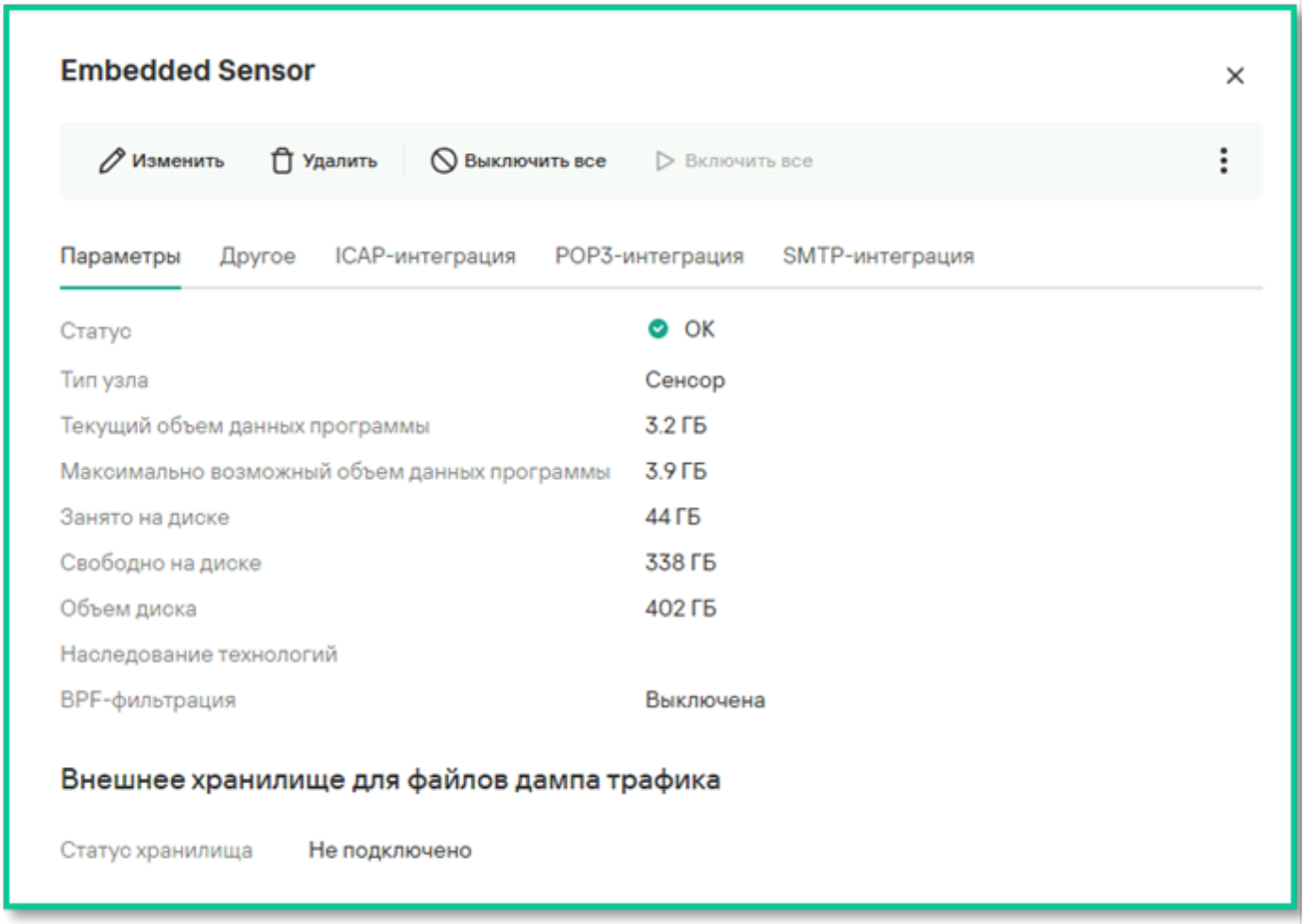
6. Войдите в веб-интерфейс приложения под учетной записью '**admin**'.

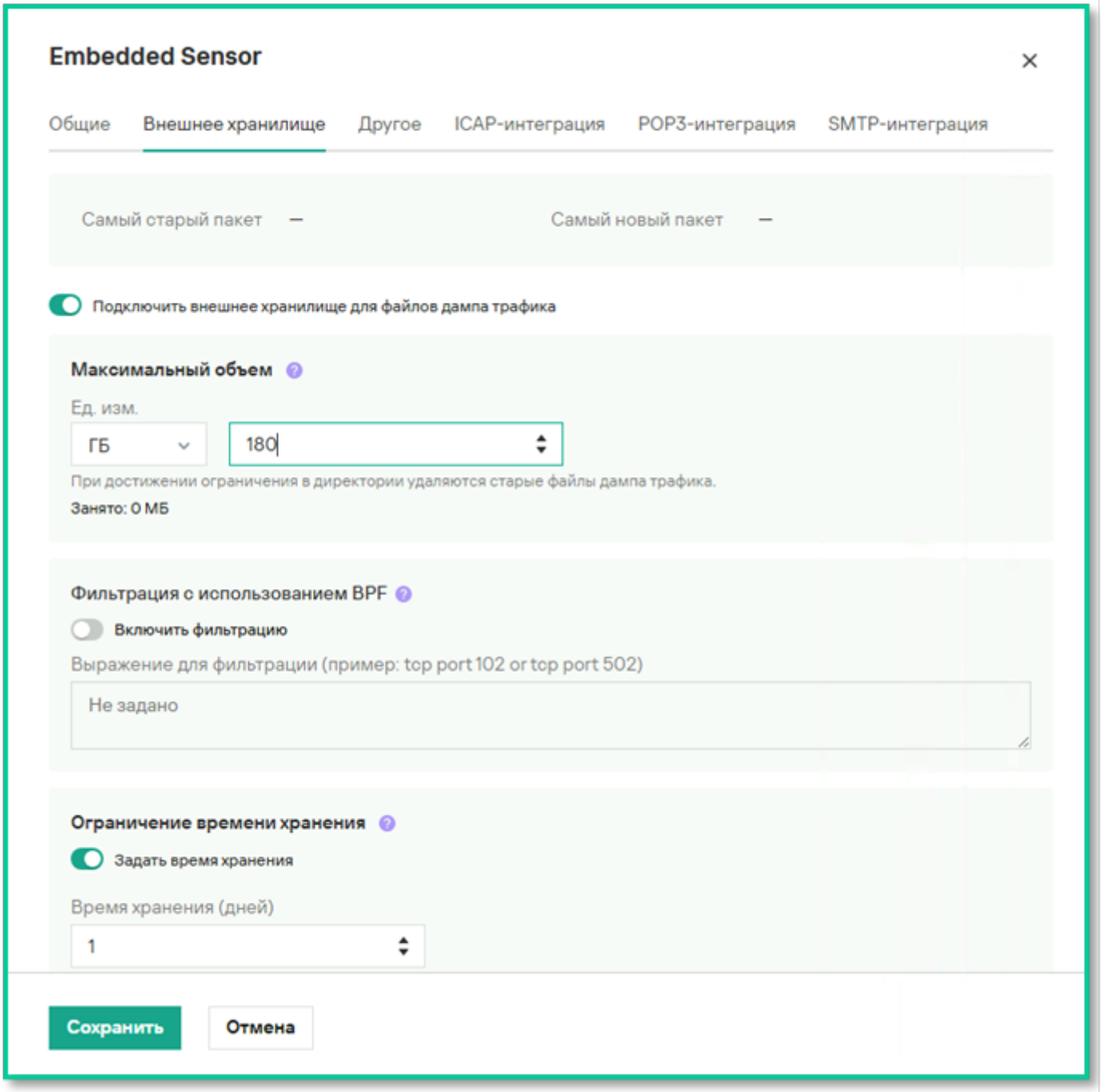


Скриншот 15: Раздел "**Серверы Sensor**"

7. В веб-интерфейсе: **Серверы Sensor → Изменить → Внешнее хранилище**

5. Включите: **«Подключить внешнее хранилище для файлов дампа трафика»**


Embedded Sensor
Изменить
Удалить
Выключить все
Включить все
Параметры
Другое
ICAP-интеграция
POP3-интеграция
SMTP-интеграция
Статус
OK
Тип узла
Сенсор
Текущий объем данных программы
3.2 ГБ
Максимально возможный объем данных программы
3.9 ГБ
Занято на диске
44 ГБ
Свободно на диске
338 ГБ
Объем диска
402 ГБ
Наследование технологий
BPF-фильтрация
Выключена
Внешнее хранилище для файлов дампа трафика
Статус хранилища
Не подключено



Скриншот 16: Раздел "**Серверы Sensor**"

6. Укажите:

   - Максимальный объём (в ГБ)

   - Ограничение времени хранения (в днях)

   - BPF-фильтр (например: `tcp port 102 or tcp port 502`)

7. Нажмите **«Сохранить»**.

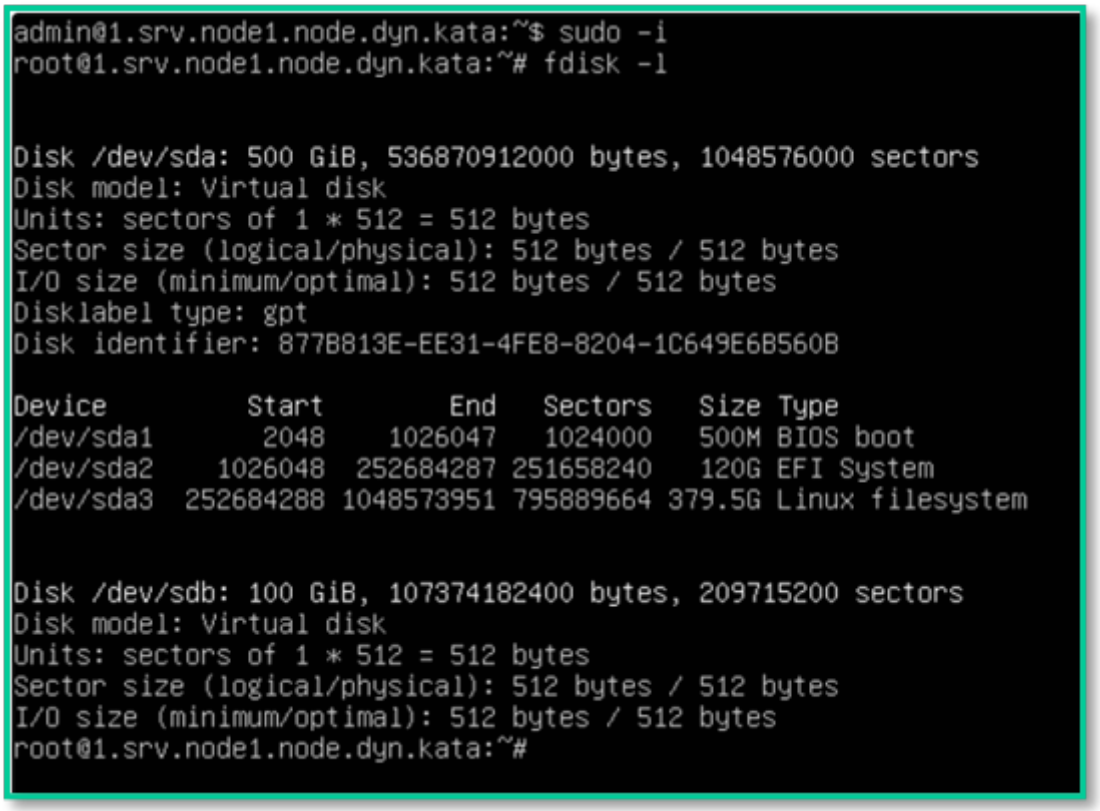
> **Примечание:**
> Сырой трафик записывается в `**/mnt/kaspersky/nta/dumps**`, но **просматривается и выгружается из `/data/volumes/dumps`**.

3.2. Настройка внешнего хранилища на Sensor

1. На узле с Sensor подключите диск **≥100 ГБ**.

2. Подключитесь по SSH и выполните:

```
sudo -i
  fdisk -l  # убедитесь, что диск виден (например, /dev/sdb)
```



Скриншот 17: Пример вывода команд

```
mke2fs -t ext4 -L DATA -m 0 /dev/sdb
```

```
root@1.srv.node1.node.dyn.kata:~# mke2fs -t ext4 -L DATA -m 0 /dev/sdb
mke2fs 1.46.5 (30-Dec-2021)
/dev/sdb contains a ext4 file system labelled 'DATA'
        created on Sun Jan 12 17:31:20 2025
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: f1aa89a8-9e97-467e-a278-0d7b4a11f6b7
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done

root@1.srv.node1.node.dyn.kata:~#
```

Скриншот 18: Пример вывода команд

```
echo "/dev/sdb /data/volumes/dumps/ ext4 defaults 0 0" >> /etc/fstab
```

```
 GNU nano 6.2                                                    /etc/fstab *
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/117d34e4-6f06-4784-aebd-bd0b543131b5 / ext4 defaults 0 1
# /data was on /dev/sda3 during curtin installation
/dev/disk/by-uuid/9cc4bb08-a269-451d-b6ed-1c78a9e67a64 /data ext4 defaults 0 1
/dev/sdb /data/volumes/dumps/ ext4 defaults 0 0
```

Скриншот 19: Пример вывода команд

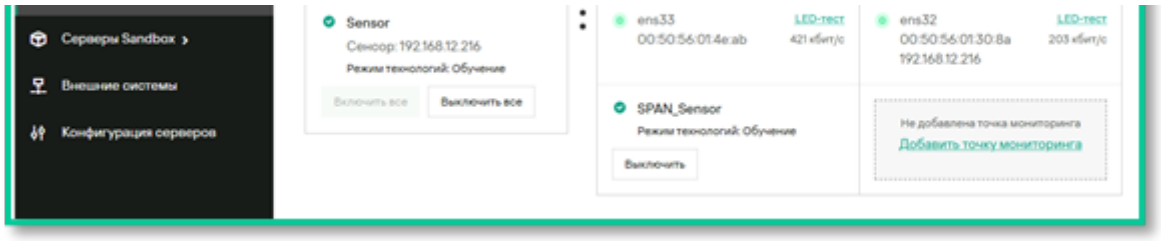
3. Закройте текстовый редактор и выполните команду:

```
rm -r /data/volumes/dumps/*
```

```
de=700,uid=1000,gid=1000,inode64)
tmpfs on /var/lib/docker/plugins/dce8a3c7c037692e84e9a2f9dc814bfe3445cb7d33bd9c4299c01a590c86599c/pr
opagated-mount/run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=6584360k,nr_inodes=1646090,mo
de=700,uid=1000,gid=1000,inode64)
root@1.srv.node1.node.dyn.kata:~# rm -r /data/volumes/dumps/*
root@1.srv.node1.node.dyn.kata:~# _
```

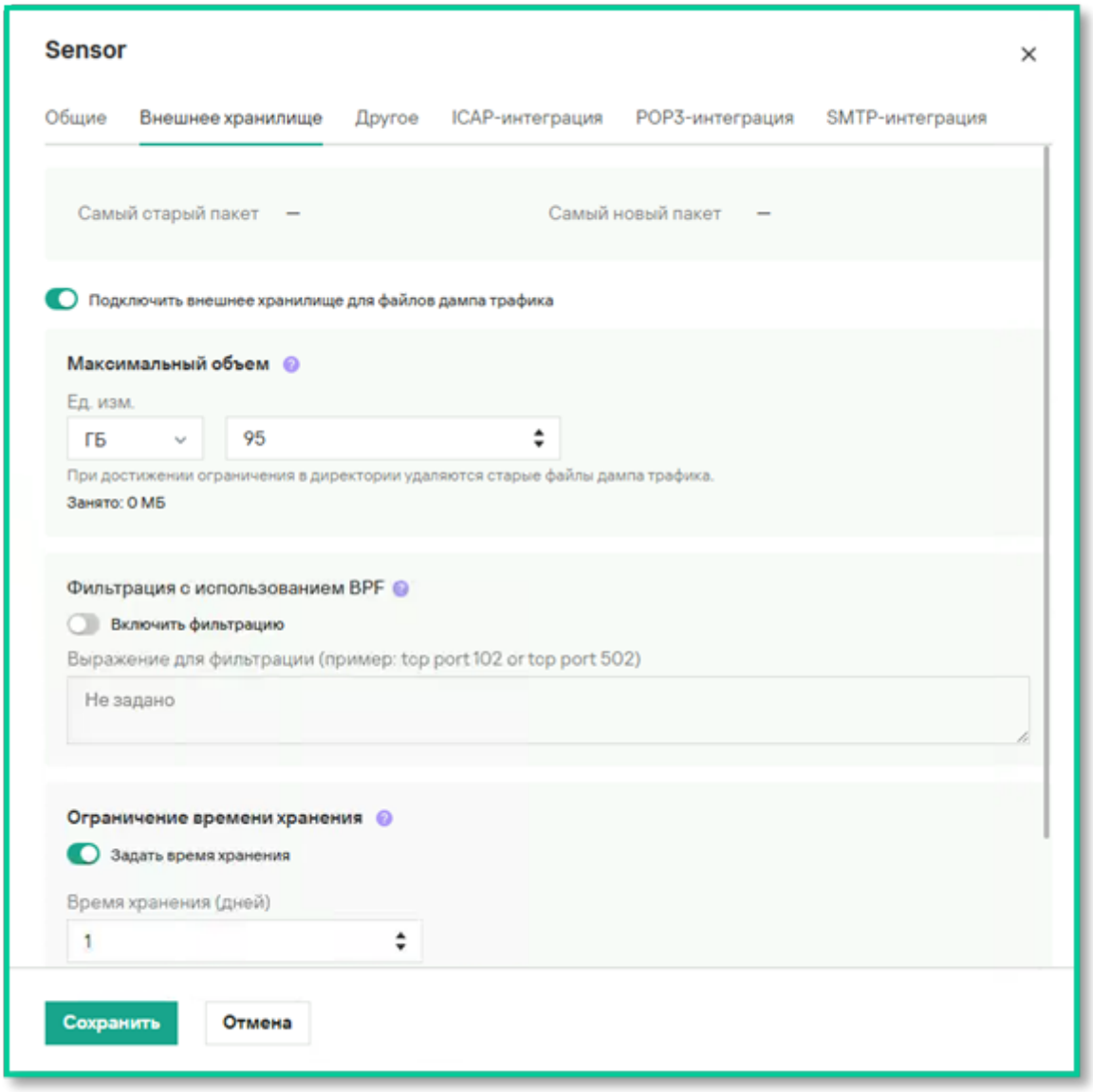
Скриншот 20: Пример вывода команд

6. Войдите в веб-интерфейс приложения под учетной записью '**admin**'.



Скриншот 21: Раздел "**Серверы Sensor**"

7. В веб-интерфейсе: **Серверы Sensor → Изменить → Внешнее хранилище**



Скриншот 22: Раздел "**Серверы Sensor**"

5. Включите: **«Подключить внешнее хранилище для файлов дампа трафика»**

6. Укажите:

- Максимальный объём (в ГБ)

- Ограничение времени хранения (в днях)

- BPF-фильтр (например: `tcp port 102 or tcp port 502`)

7. Нажмите **«Сохранить»**.

> **Примечание:**
> Сырой трафик записывается в `**/mnt/kaspersky/nta/dumps**`, но просматривается и выгружается из `**/data/volumes/dumps**`.

---

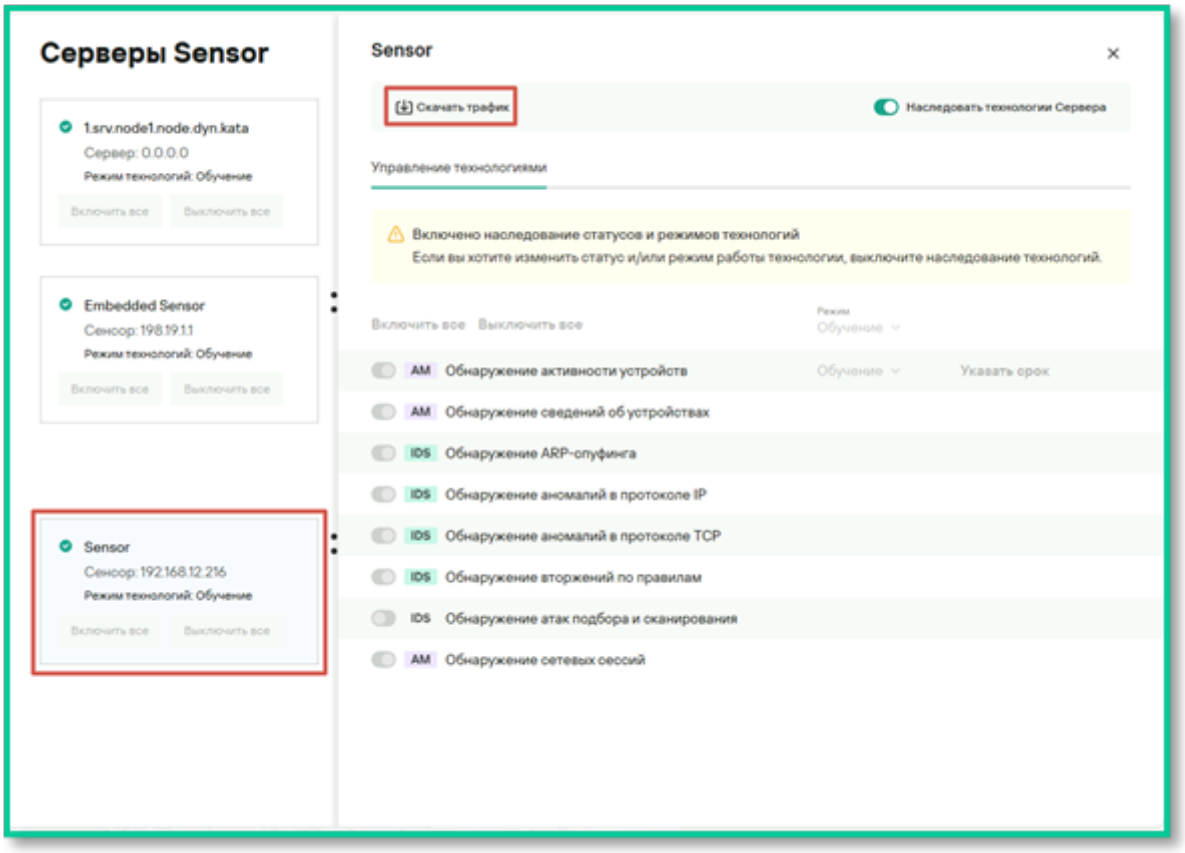
4. Проверка работы выгрузки дампов трафика

4.1. Выгрузка дампов трафика

? ????: ??????? ???? ??????? ??? ???????.

1. Авторизуйтесь под УЗ **«Офицера безопасности»**.

2. Перейдите: **Серверы Sensor → Выбрать Sensor → Скачать трафик**.



Скриншот 23: Раздел "**Серверы Sensor**"

3. Укажите:

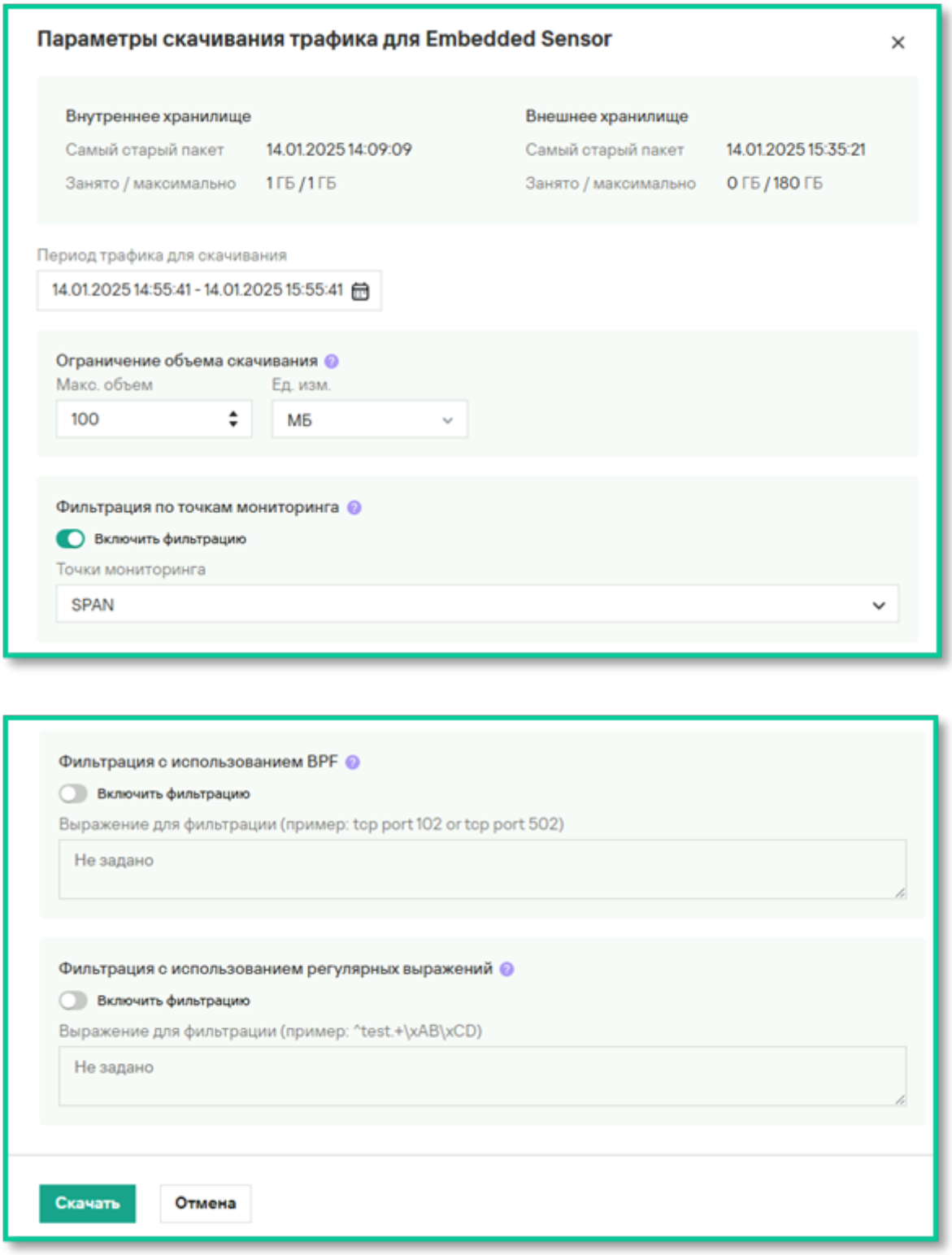
- Период

- Максимальный размер дампа

- Точки мониторинга

- BPF-фильтр

- Регулярное выражение (например: `^test.+xABxCD`)



Скриншот 24: Раздел "**Серверы Sensor**"

4. Нажмите **«Скачать»** → файл в формате **PCAP** начнёт загрузку.

Полезные ссылки

- Официальная документация Kaspersky
- Настройка SPAN-трафика (онлайн)
- Распределённое решение и мультитенантность
- Kaspersky на YouTube
- Kaspersky на Rutube
- Полная инструкция по NDR и Sensor

? Настройка приёма SPAN-трафика завершена!

Теперь Central Node и/или Sensor:

- Принимает зеркалированный трафик
- Анализирует выбранные протоколы
- Отображает статистику в реальном времени
- Готов к детектированию угроз во внутренней сети
- При необходимости — записывает и позволяет выгружать дампы

Revision #35
Created 21 October 2025 12:32:15 by Николай
Updated 6 February 2026 11:30:14 by Кирилл