?????????? ?? ????????? ? ????????? ?????????? ?entral Node ? ?????? " ????????????????? ?????? ???????" ????/NDR 8.0

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

> Официальная документация по данному разделу приведена в **Онлайн-справке** на продукт. Далее по разделам:
>
> - Аппаратные и программные требования
> - Архитектура приложения
> - Распределенное решение и мультитенантность
> - Руководство по масштабированию
> - Установка и первоначальная настройка приложения

? ????????? Central Node ? ?????? "**?????????????? ?????? ???????**"

> **Версия решения:** 8.0
> **Тип установки:** Central Node (на одном сервере)

?? **??????????:** ? ?????? ??????? ??????????? ??????? ????????? ?????????? Central Node ??????????? ? ???? ??????????? ??????? ???????????? ???? ???? ??? ?????????????? ?????? ???????.
?????????????? ?????? ??????? ????????? ???????????? ????????? ????? ??????? ?????? ? ?????? ????? ????????, ??????????? ? ??????.
???? ????????? ???????????? ?????? ??? ?????????????? ??????? ???????. ???????? ???? ??????? ????? ????????? ??????????. ?? ?????? ?????????? ? ????? ?????????? Sandbox.

> ?? **??????????:** ????????? ???????????? ? ??????? ??????? ?????????? ????? ? [?????? ????????????](#).

?????: ??????? ???????? ??? ??????? ???????????? ????????????? ????? KATA+NDR. ????? ????????? ????? ???????? ????????????? ????? ?????????? ??????? ??????? ???????? ?????????? ??? ?????????. ?????????????? ??????? ?? ???????????. ????????? ???????? ?????? ? ??????? ????? ?????.

---

1. Подготовка

1.1. ???????? ?????????

Решение поддерживает три архитектуры:

Вариант	Описание
Standalone	Central Node + Sensor на одном сервере. Подходит для пилотных внедрений, тестовых сред и организаций с небольшой ИТ-инфраструктурой.

1.2. ?????????? ? ????????????

Компонент	Требование
Режим загрузки	Обязательно **UEFI**
Процессор	Минимум 24+ потоков (логических ядер), поддержка **BMI2, AVX, AVX2**
ОЗУ	Минимум **64 ГБ**
Диски	• 1 диск — для ОС и компонентов
Жёсткие диски	Только **SAS HDD 10K rpm и выше (рекомендуется использовать SSD)**
RAID	Только **аппаратный RAID**. Программный RAID **не поддерживается**

? ????? ?????????? ?????

Сценарий	Минимальный объём
KATA и/или NDR	2–2,4 ТБ

1.3. ????????? ?????????????

Решение **не поддерживает Microsoft Hyper-V**. Поддерживаются:

- **VMware ESXi 6.7.0 или 7.0**
- **KVM**
- **ПК СВ "Брест" 3.3**
- **"РЕД Виртуализация" 7.3**
- **zVirt Node 4.2**

Решение **не поддерживает** **Microsoft Hyper-V.**

> □□ **Примечание по KVM:**
>
> - ОС: **Debian GNU/Linux 12**
> - Эмулятор: **QEMU version 8.0.2**

????????????? ?????????? ??? ???????? ????????????

Платформа	Особенности
VMware ESXi	Виртуальная машина требует на **10% больше CPU**, чем физический сервер. Тип виртуального диска: **Thick Provision**
ПК СВ "Брест" / "РЕД Виртуализация"	При использовании **KATA+NDR** увеличьте минимальное количество логических ядер на **20%**

> □□ **Примечание:**
> Если вы хотите устранить уязвимости типа **Spectre и Meltdown** на уровне гипервизора, необходимо дополнительно увеличить количество логических ядер **в 1,5 раза** относительно уже увеличенного значения.

1.4. ???????? ?????????? ? RAID

Подсистема	Назначение	Рекомендуемый RAID
Первая	ОС, контейнеры, базы (кроме ТАА)	RAID 1 или RAID 10
Вторая	База ТАА и журналы	RAID 10

> **Рекомендации:**
>
> - Минимум **2000 ГБ** на первой подсистеме
> - Используйте **аппаратный RAID-контроллер** с кэшем и BBU

1.5. ?????????? ? ??????????

Центральный процессор **должен поддерживать наборы инструкций**:

- **BMI2**
- **AVX**
- **AVX2**

> **Проверка поддержки:**
>
> - Выполните в терминале команду: **cat /proc/cpuinfo | grep flags**
> - Убедитесь, что в выводе присутствуют: **avx avx2 bmi2**
> - Либо выполните следующую команду:
>
> ```
> grep -E 'avx|avx2|bmi2' /proc/cpuinfo
> ```

1.6. ????? ? ??????? ?????????? / KSN

Перед установкой приложения подготовьте IT-инфраструктуру вашей организации к установке компонентов Kaspersky Anti Targeted Attack Platform: Подготовка IT-инфраструктуры к установке компонентов приложения:

1. Для обеспечения безопасности сети от анализируемых объектов запретите доступ в локальную сеть сервера Sandbox управляющему сетевому интерфейсу и интерфейсу для доступа обрабатываемых объектов.
2. Произведите подготовку IT-инфраструктуры организации, согласно таблице.
3. Открыт доступ до серверов обновления и KSN согласно таблице ниже:

Server	URL
Updates	• antiapt.kaspersky-labs.com • antiapt.k.kaspersky-labs.com • antiapt.s.kaspersky-labs.com • activation-v2.kaspersky.com
KSN	• https://ksn-crypto-file-geo.kaspersky-labs.com • https://ksn-crypto-stat-geo.kaspersky-labs.com • https://ksn-crypto-url-geo.kaspersky-labs.com • https://ksn-crypto-verdict-geo.kaspersky-labs.com • https://ksn-crypto-kas-geo.kaspersky-labs.com • https://ksn-crypto-a-stat-geo.kaspersky-labs.com • https://ksn-crypto-hash-geo.kaspersky-labs.com • https://ksn-his-geo.kaspersky-labs.com • https://ksn-file-geo.kaspersky-labs.com • https://ksn-verdict-geo.kaspersky-labs.com • https://ksn-url-geo.kaspersky-labs.com • https://ksn-kas-geo.kaspersky-labs.com • https://ksn-a-stat-geo.kaspersky-labs.com • https://ksn-info-geo.kaspersky-labs.com • https://ksn-cinfo-geo.kaspersky-labs.com • https://dc1.ksn.kaspersky-labs.com • https://dc1-file.ksn.kaspersky-labs.com • https://dc1-kas.ksn.kaspersky-labs.com • https://dc1-st.ksn.kaspersky-labs.com

2. Установка

2.1. ????? ??????????????????

1. Установите **Central Node в режиме "Ретроспективный анализ трафика"**
2. Установите **Sandbox**
3. Добавьте **образы виртуальных машин** в Sandbox

> **Сценарии:**

> - **Пилот:** Central Node + Sensor на одном сервере, Sandbox — на другом

2.2. ???????? ? ?????? ??????

Скачайте образ:

- **Физический сервер:** запишите на USB/DVD и загрузитесь.
- **Виртуальный сервер:** подключите ISO к ВМ.

> ⚠ **Важно:**
> При установке на виртуальной платформе **обязательно выберите UEFI** в настройках:
> `Options → Boot Options → Firmware → UEFI`.

> □□ **Скриншот 1:**
>
> Схема

2.3. ??????? ?????????

??? 1: ????????

Выберите:

`Install KATA 8.0.0.1`

> □□ **Скриншот 2:**

??? 2: ????

Выберите язык (например, **русский**) → **Enter**

> **Скриншот 3:**
>
> Схема

??? 3: ???????????? ??????????

- Нажмите **Tab**, выберите **«Я Принимаю»**
- Нажмите **Enter**

> **Скриншот 4:**
>
> СхемаСхема

??? 4: ???????? ??????????????????

- Выберите **«Я Принимаю»** → **Enter**

> **Скриншот 5:**

> СхемаСхема

??? 5: ????? ???? ???????

Роль	Описание
`single`	Central Node + Sensor на одном сервере
`sensor`	Только Sensor (выделенный)
`storage`	Сервер хранения для кластера
`processing`	Обрабатывающий сервер (включает Sensor)

> ⚠ После установки сменить роль **невозможно**.

> **Скриншот 6:**
>
> Схема

??? 6: ????? ?????

- Подтвердите очистку диска → **Yes** → **Enter**

> **Скриншот 7:**
>
> Схема Схема

? ?????? ??????? ???? ?? ????????????? ??????????? ???????????

??? 7: ????????? ???? ???????? (???? ?????????)

> ? ????????? ??????????? **?????? ??? ?????????? ?????????.**

Для **не-кластерной установки** просто нажмите **Enter** (оставьте `198.18.0.0/16`)

>

> **Скриншот 8:**
>
> Схема

> **Скриншот 9:**
>
> Схема

??? 8: ????? ???????? ??????????

Выберите интерфейс для **Management Interface**

> **Скриншот 10:**
>
> Схема

??? 9: ????????? IP-??????

- **DHCP** — автоматически
- **Static** — вручную (IP, Mask, Gateway)

> **Скриншот 11:**
>
> СхемаСхемаСхема

??? 10: ??????? ?????? `admin`

- Пароль: **минимум 12 символов**
- Подтвердите пароль → OK

> **Скриншот 12:**
>
> СхемаСхема

??? 11: ???? NDR

Выберите язык (например, **русский**) → Enter

> **Скриншот 13:**
>
> Схема

??? 12: DNS-???????

> ⚠ **Обязательно!** Даже в изолированной сети укажите фиктивный DNS (например, `1.1.1.1`)

> **Скриншот 14:**
>
> СхемаСхема

??? 13: NTP-???????

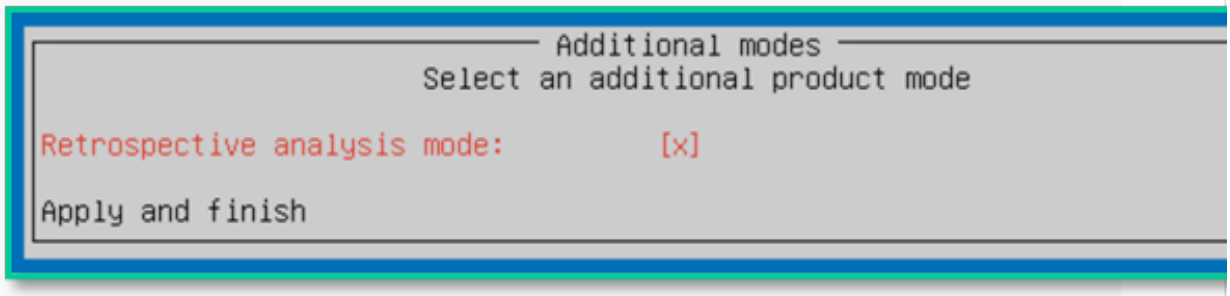
- Нажмите **Add**
- Введите адрес (например, `pool.ntp.org`)
- Нажмите **Continue**

> **Скриншот 15:**
>
> СхемаСхема

??? 14: ????????? ?????? ???????????????? ??????? ???????

Для ретроспективного анализа трафика, на этом шаге требуется включить режим ретроспективного анализа трафика. В этом режиме для компонента действует ряд ограничений, вы можете ознакомиться с ними в разделе *Ретроспективный анализ трафика*.

> **Скриншот 16:**



??? 15: ???????? ??????????

Процесс займёт **5–20 минут**. Не перезагружайте сервер.

> ◫ **Скриншот 17:**
>
> Схема

---

3. Настройка

3.1. ?????? ? ???-??????????

После завершения установки подождите **пару минут** — идёт запуск контейнеров и инициализация сервисов.

> ⚠ Не пытайтесь входить сразу — возможна ошибка авторизации.

Откройте в браузере:

`https://<IP-адрес-сервера>:8443`

Войдите под:

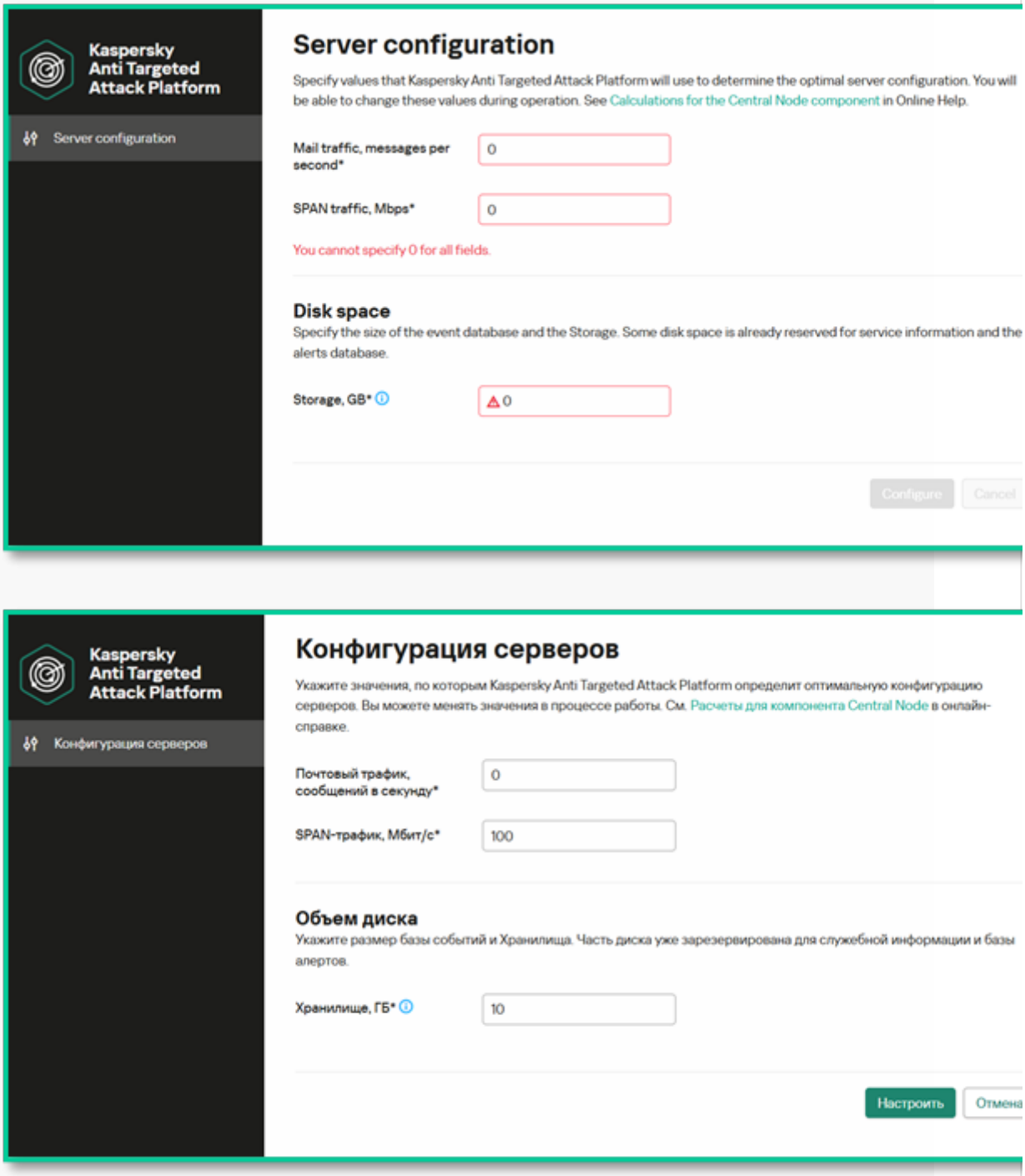
- **Логин:** `admin`
- **Пароль:** заданный при установке

> ◫ **Скриншот 17:**
>
> Схема

3.2. ???????????? ????????

После входа откроется **веб-интерфейс для управления масштабированием**. Вам будет доступен раздел «**Конфигурация серверов**», где необходимо указать параметры, определяющие нагрузку и объём хранилища.

> **Скриншот 18:**



? ???????? ?????? (KATA)

> ⚠ **ВАЖНО:** ? ???? **???????? ??????**, ????????? ? ??????? **?????? ?? ?????????.**

? SPAN-?????? (NDR)

- Укажите **объём трафика (Мбит/с)** поданного на CN.
- ? ???? **SPAN-??????**, ????/? ??????? ??????????? ?????????? ??????? ?? SPAN-??????.
- ? ???? ???? ??????????? ????? ????? **SPAN-???????**, ??????? ????????????? ?? **Central Node/RAM**.

3.3. ????? ?????

? ???? «**?????????**» ????? ??????? ????? ????????? ???????????, ??????????? ??? ???????? ??????, ??????????? ????? ??? ????????? ??? ??????? ??????????? Cental Node ? Sandbox. ????????????? ???????? ?? ?????? 100 ??.

3.4. ?????? ???????????

1. Нажмите **«Настроить»**
2. Нажмите **«Запустить»**
3. Дождитесь завершения (10–20 минут)

> 🖼 **Скриншот 19:**
>
> Схема

> 🖼 **Скриншот 20:**
>
> СхемаСхемаСхема

> ⚠ **ВАЖНО!** После успешного завершения система предложит войти заново. После завершения конфигурации подождите **5-20 минут** — идёт запуск контейнеров и инициализация сервисов.

3.5. ????????? ?????????

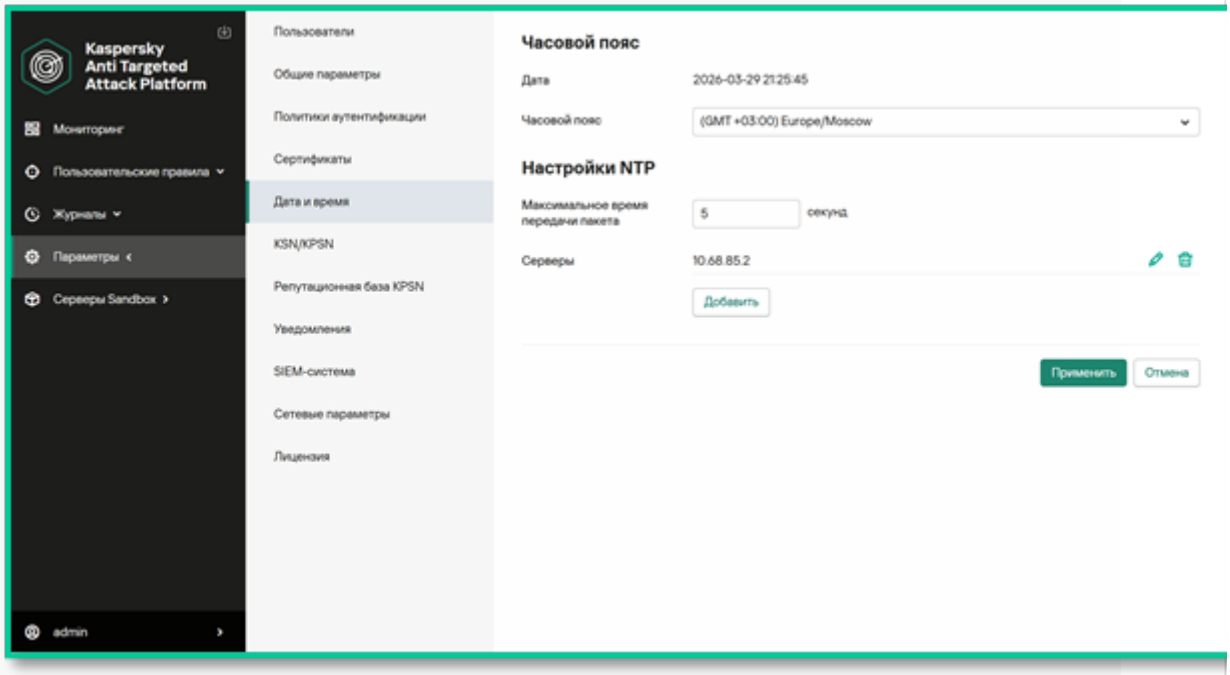
После успешной конфигурации:

? ???????? ???????

- **Параметры → Дата и время**
- Убедитесь в правильности часового пояса и NTP

> ⚠ Время должно быть одинаковым на всех компонентах: CN, Sensor, Sandbox.

> **Скриншот 21:**



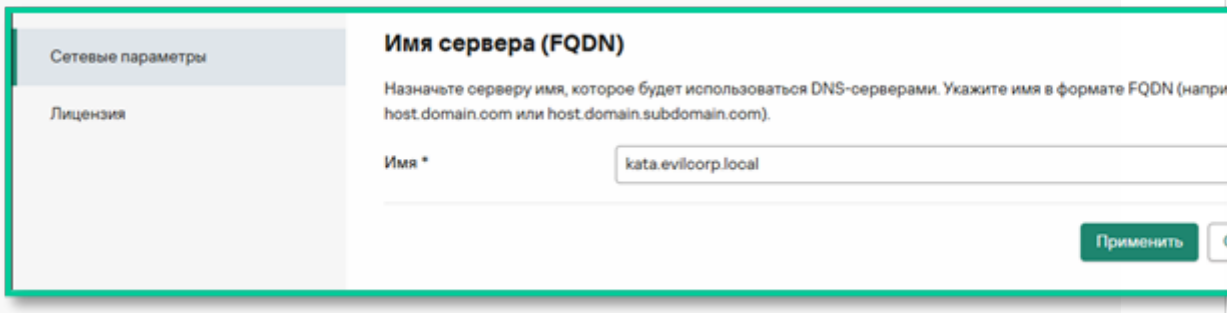
? ??? ???????

- **Параметры → Сетевые параметры → Имя сервера**
- Укажите имя в **нижнем регистре**, совпадающее с DNS (если планируется интеграция с AD)

> ?????!

> ??? ?????????? Central Node ????? ???????? ?????? ????? ???-?????????. ????????????? ??????????? ??? ????????? ??? ?????? ??????.

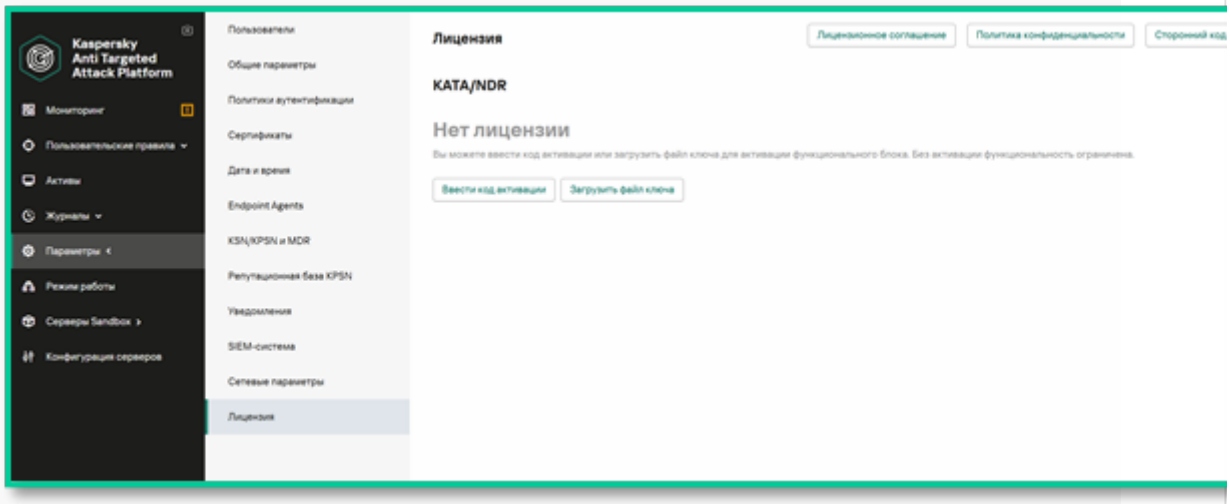
> “ ◫ **Скриншот 22:**



? ????????

- **Параметры → Лицензия**
- Загрузите файл ключа или введите код активации (KATA, NDR, KEDR)

> “ ◫ **Скриншот 23:**



? KSN

- **Параметры → KSN/KPSN и MDR**
- Примите соглашение и включите KSN

> **Скриншот 24:**
>
> СхемаСхема

? ?????????? ???

- **Параметры → Общие параметры → Обновление баз**
- Выберите источник и запустите обновление

> Обновление должно завершиться со статусом **успешно**

> **Скриншот 25:**
>
> Схема

? ???????? ??????? ?????? ??????? ???????????

- **Параметры → Пользователи → Добавить**
- Роль: **Старший сотрудник службы безопасности**
- Укажите имя, пароль (дважды), включите учётную запись

> Эта учётная запись будет использоваться для работы с инцидентами.

> **Скриншот 26:**
>
> СхемаСхема

?????: ????? ??? ??? ?????????? ? ?????? ??????????, ???????? KATA ??? KATA/NDR ?????? ???? ??????????? ????????? ? ??????????? ?? ???????????? ???????????.

> **??????????:**
> o ???????? KATA ???????? ?? ?????? ????????? IT-?????????????? ?????????? ????????? ??????? ??????????.
> o NDR ?????????????? ?????? ?????????? ???? ???????????, ?????????? ????? ???? ? ???????????????? ???????.

> Процесс первоначальной установки и настройки на данном этапе завершен.

---

4. Настройка подключения источников

1. API

????????? KATA ???????????? ?????????? ?? ?????????? ??????? ?? ????????? REST API.

????? ???????????? ??????????, ?????????? ????????? ????????? ????????:

? ?????? ?????????? ???? ??????? ?????? ?? ?????, ??? ??? ???? ?????????? ?????????? ?? ?????? ? ?????? ????????????. ?????? ?????????? ????? ????????? ???? ??????? ?? ?????? ??????

- Руководство по настройке API KATA, KEDR, NDR до 7.1.3

????????? ? ?????? ???????????? ????? ???????????? ? ?????? ???????????? **KATA API** **?** **NDR API**.

????????????? ????????? ???????? ???????????? ???????? ????????????? ????? ?????????? ?? ?????? ??????? ?? API

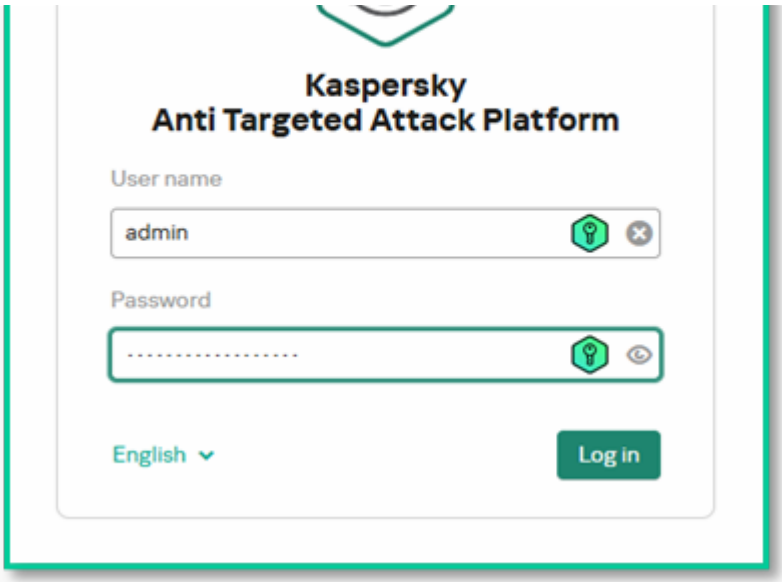
???????????? ?? “**SSH**” ? “**Central Node**”, ??????? ? “**Technical Support Mode**” ? ????????? ????????? ???????:

- ??????? ? root – “**sudo su**”.
- ?????????? ????????????? ???????? “API-????????”

```
sudo su
console-settings-updater set --merge /kata/configuration/product/kata_scanner '{"ksmg":
{"max_tasks_per_client": 500}}'
```

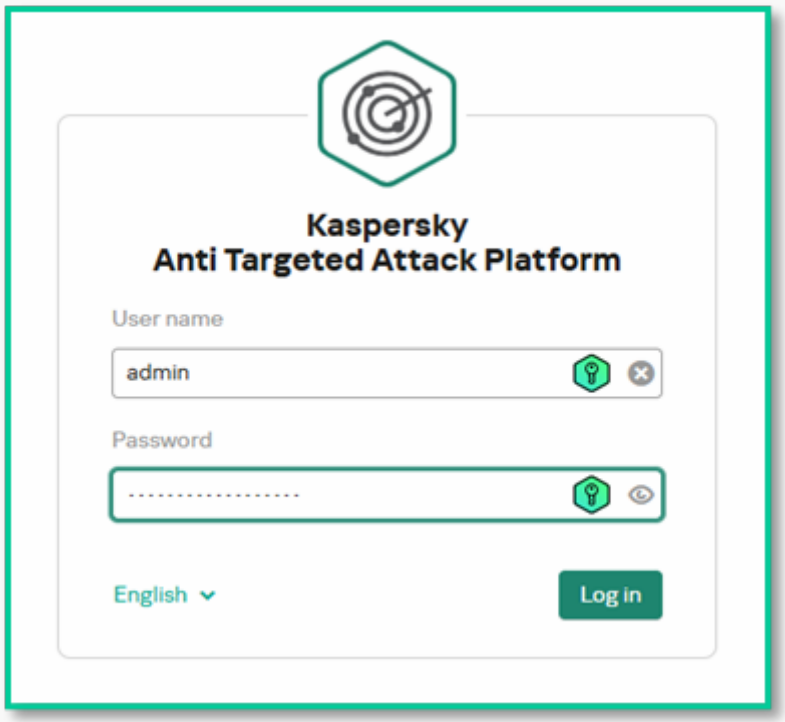
???????? ? ???-????????? “**Central Node**” ? ????????????? ??? ?? “**admin**”.

Скриншот 27:



????????? ? ?????? “**??????? ???????**” ? ?????????? ????? “**???????????? ????????? ????????**” ? ????????? “**????????**”.

Скриншот 28:



2. SPAN

?????? ????? ????????? ??????? ????????? Central Node ??? ??????? ????? ???????, ????????? ? ??????????? ??? ???????? ???????? ????.

?????: ??? ????????? ??????? ???????? ??????? ??????????? ?????? ???? ???????? ????????????? ?????????.
??? Central Node ?????????? ? ?????? Retrospective analysis mode, ????? ???????????? ?????? ???? ?????? ????.

??????????: ? ?????? KATA 6.0 ????????? ??????????? ??????, ???????? ? ???????? ????? ?????? ???????? ???????. ? ?????? ????????? ???? ?????????? ?????? ?? ?????, ?????? ????????? ?????? SPAN. ???????? ?? ??????? ??????????? ????? ???????????? ? ?????? ????????????.

Процесс настройки и подключения SPAN в ?????? ?????????? ???? ??????? ?????? ?? ?????, ??? ??? ???? ??????????? ?????????? ?? ?????? ? ?????? ????????????. ?????? ?????????? ?????

????????? ???? ??????? ?? ?????? ?????? - Настройка приёма SPAN-трафика на Central Node и Sensor

---

3. SIEM

Kaspersky Anti Targeted Attack Platform ????? ??????????? ?????????? ? **???????? ???????????? ? ???-??????????** ?????????? ? **????????????** ? **SIEM-???????**, ??????? ??? ???????????? ? ????? ???????????, ?? ????????? **Syslog**.

??????? ????????? ? ??????????? SPAN ? ?????? ?????????? ???? ??????? ?????? ?? ?????, ??? ??? ???? ??????????? ?????????? ?? ?????? ? ?????? ????????????. ?????? ?????????? ?????

????????? ???? ??????? ?? ?????? ?????? - Cheat Sheet по интеграциям KATA с KUMA

????????? ?? ????????? ??????? ??????????? ????? ???????????? ? ?????? ????????????.

? ??????? ?????? ?????? **Network Detection and Response** (**NDR**), ??????? ???????? ?????? ????????? **Kaspersky Anti Targeted Attack Platform** (**KATA**), ???????? ?????? ? ????????, ????????? ? ???? ????????????, ?????????????? ????? ????????? **???????????**.

????????? ?? ????????? ??????? ??????????? ????? ???????????? ? ?????? ????????????

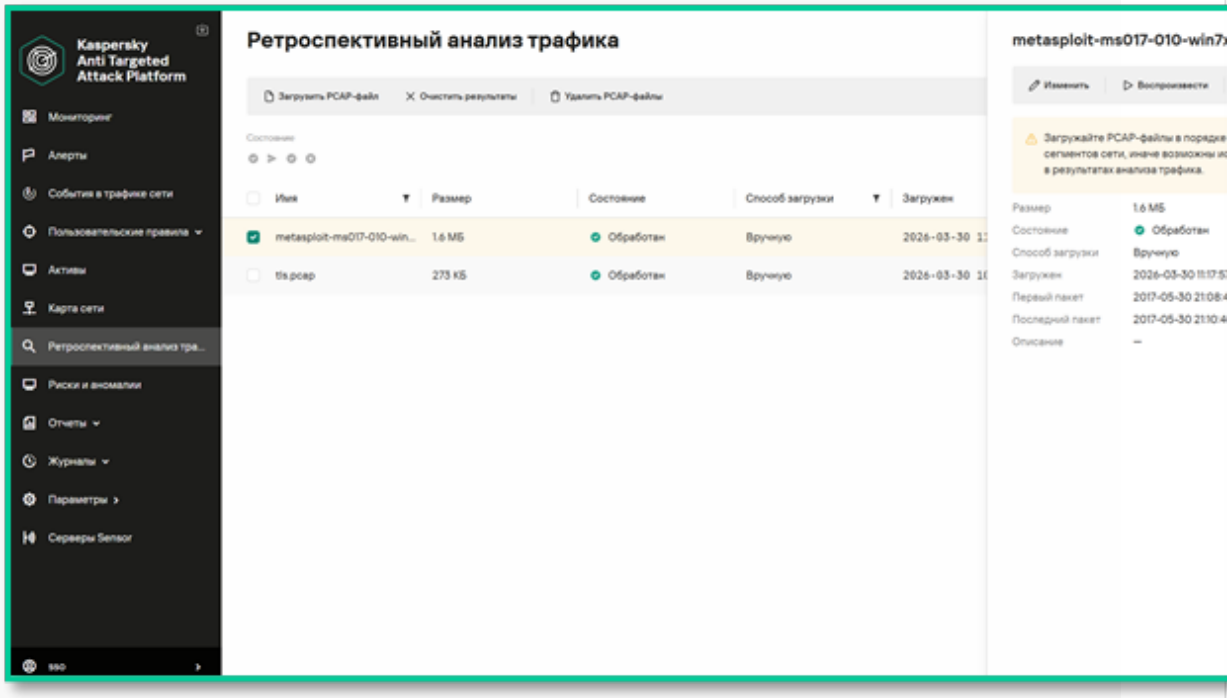
---

4. ???????? PCAP-????? ???????

1. В окне веб-интерфейса из под уз "**Офицера безопасности**" приложения выберите раздел "**Ретроспективный анализ трафика**".
   Откроется таблица PCAP-файлов.
2. Нажмите на кнопку "**Загрузить PCAP-файл**".
   Откроется окно выбора файлов.
3. Выберите PCAP-файл, который вы хотите загрузить, и нажмите на кнопку "**Open**".
   Вы можете выбрать несколько файлов.

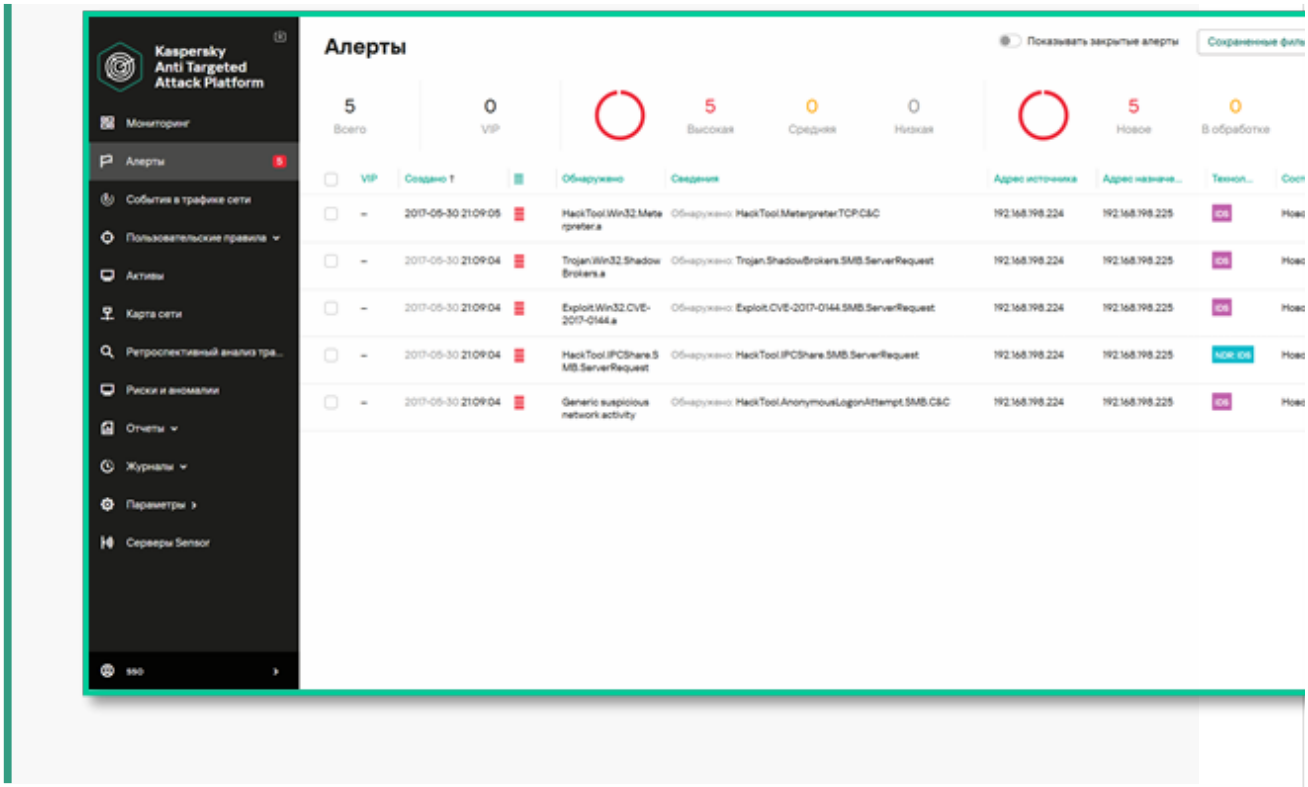
4. В таблице выберите файл с трафиком, который вы хотите воспроизвести. Откроется окно с информацией о PCAP-файле.
5. Нажмите на кнопку Воспроизвести report_status_in_progress. Воспроизведение трафика будет запущено.

> **Скриншот 29:**



После проигрывания PCAP-файла, результаты будут доступны в разделе "**Алерты**"

> **Скриншот 29:**



ВАЖНО: если включен автоматический анализ трафика, загрузка PCAP-файлов в Kaspersky Anti Targeted Attack Platform вручную недоступна.

5. ?????????? ???? Generic ??? ???????? PCAP-?????? ?? ??????? ??????? ? Kaspersky Anti Targeted Attack Platform.

Добавление коннектора типа Generic для загрузки PCAP-файлов из внешней системы в Kaspersky Anti Targeted Attack Platform.

Этот коннектор используется для соединения с внешней системой, из которой передаются PCAP-файлы.

6. ????????? ? ?????????? ???????????????? ??????? ???????

???? ?????????????? ?????? ??????? ???????, Kaspersky Anti Targeted Attack Platform ????????? ? ????????????? PCAP-????? ????????????? ?? ???? ?? ???????????. ??? ????????? ?????????, ??? PCAP-????? ????????? ? Kaspersky Anti Targeted Attack Platform ? ??????? ?????? ? ? ?????? ????????? ????, ????? ???????? ????????? ??????????? ???????.

??? ?????????? ?????????????? ??????? ??????? ???????? PCAP-?????? ? Kaspersky Anti Targeted Attack Platform ? ?????? ???????????????? ??????? ??????? ??????????.

?? **??????????:** ???? ?? ?????? ????????????? ????????? PCAP-?????? ?????? ??? ??????? ???????????, ??? ????????? ????????? PCAP-????? ? ??????? ?? ?????? ? ?????? ????????? ????, ????? ???????? ????????? ???????????? ???????.

? ???????? ??????

- Официальная документация Kaspersky
- Инструкция по интеграции с Active Directory
- Kaspersky на YouTube
- Kaspersky на Rutube

 Установка и настройка Central Node завершены!
Теперь можно приступать к установке **Sandbox**.

Revision #8
Created 31 March 2026 17:17:27 by Николай
Updated 1 April 2026 11:52:31 by Николай