?????????? ?? ????????? ? ????????? ?????????? ?entral Node ? ????/KEDR/NDR 7.0-7.1

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 ? ?????????? Sensor ? ????????????? ?????????

> **Версия решения:** 7.1
> **Тип установки:** Central Node + Sensor (на одном сервере)

?????: ?????????? ???????

> ⚠ **Очень важно:**
> Точный и надёжный расчёт аппаратных ресурсов (сайзинг) возможен **только после заполнения официального опросника** от Kaspersky.

> Данные, предоставленные без опросника, являются **предварительными** и могут привести к нестабильной работе системы.
> Окончательные рекомендации по ресурсам (CPU, ОЗУ, дисковое пространство) должны быть предоставлены **официальным партнёром или вендором Kaspersky**.

> **Важно:** Подробнее о принципе работы решения Kaspersky Anti Targeted Attack Platform описано в онлайн-документации.

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.
Кластер	Распределённая отказоустойчивая система. Минимум 4 сервера: 2 storage + 2 processing.
Распределенное решение и мультитенантность	Primary CN (PCN) + Secondary CN (SCN) в филиалах. Централизованное управление.

> **Рекомендация:**
>
> - Смена архитектуры (например, с Standalone на Cluster или Распределенное решение) возможна только через переустановку.
> - Для кластера и распределённого решения требуется предварительный сайзинг на основе заполненного опросника и анализа от вендора.

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

Компонент	Требование
Режим загрузки	Обязательно **UEFI**

Компонент	Требование
Процессор	Минимум 10+ потоков (логических ядер), поддержка **BMI2, AVX, AVX2**
ОЗУ	Минимум **64 ГБ**
Диски	• 1 диск — для ОС и компонентов • 2 диска — **обязательно при использовании KEDR** (второй — для ТАА)
Жёсткие диски	Только **SAS HDD 10K rpm и выше**
RAID	Только **аппаратный RAID**. Программный RAID **не поддерживается**

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

Сценарий	Минимальный объём
KATA и/или NDR	2–2,4 ТБ
Только KEDR	1 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**

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

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

VMware ESXi

- Виртуальная машина требует на 10% больше CPU, чем физический сервер

- Тип виртуального диска: **Thick Provision**

?? ?? "?????" / "??? ?????????????"

- При использовании **KEDR или KATA+KEDR** 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
> - Минимум **2400 ГБ** на второй подсистеме
> - Используйте **аппаратный RAID-контроллер** с кэшем и BBU

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

Центральный процессор **должен поддерживать наборы инструкций**:

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

> ❓ **Проверка поддержки:**

```
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. Убедитесь, что серверы, а также компьютер, предназначенный для работы с веб-интерфейсом приложения, и компьютеры, на которых устанавливается компонент Endpoint Agent, удовлетворяют аппаратным и программным требованиям.
2. Для обеспечения безопасности сети от анализируемых объектов запретите доступ в локальную сеть сервера Sandbox управляющему сетевому интерфейсу и интерфейсу для доступа обрабатываемых объектов.
3. Произведите подготовку IT-инфраструктуры организации, согласно таблице.
4. 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

На рисунках ниже показана схема сетевого взаимодействия между компонентами приложения и системами, необходимыми для работы приложения. Стрелки на схеме указывают направление соединения: каждая стрелка проведена от объекта, который инициирует соединение, к объекту, который отвечает на вызов.

□□ Показать схему архитектуры

Процесс сканирования

Рис. 1 — Схема сетевого взаимодействия между компонентами приложения и системами, которые необходимы для работы приложения. Central Node развернут со встроенным Sensor

Процесс сканирования

Рис. 2 — Схема сетевого взаимодействия между компонентами приложения и системами, которые необходимы для работы приложения. Sensor развернут на отдельном от Central Node сервере

Процесс сканирования

Рис. 3 — Принцип работы приложения в режиме распределенного решения

2. Установка

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

1. Установите **Central Node и Sensor**
2. Установите **Sandbox**
3. Добавьте **образы виртуальных машин** в Sandbox
4. (Опционально) Установите **выделенный Sensor**
5. (Опционально) Установите **агенты Kaspersky Endpoint Agents**

> **□□ Сценарии:**
>
> - **Пилот:** Central Node + Sensor на одном сервере, Sandbox — на другом
> - **Промышленный:** кластер или распределённая архитектура

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

Скачайте образ:

```
kata-cn-7.1.0.530-inst.x86_64_en-ru-zh.iso
```

- **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 7.1.0.530
```

> **Скриншот 2:**
>
> Схема

??? 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**
- Если используется **KEDR**, появится предложение выделить второй диск под **TAA**
- Если вы хотите использовать систему хранения данных SAN, для хранения телеметрии **TAA**, выполните одно из следующих действий:
  - Если SAN подключена к физическому или виртуальному серверу, на этом шаге установки выберите SAN, отображаемую как локальный диск, в качестве диска для хранения данных.
  - Если SAN доступна через сетевой интерфейс, выполните следующие действия:
    1. На этом шаге установки выберите **Do not allocate a separate disk for TAA**.
    2. Обратитесь в Техническую поддержку за инструкцией по изменению точки монтирования второй дисковой подсистемы.
    3. Выполните оставшиеся шаги мастера установки компонента Central Node со встроенным Sensor на сервере.
    4. В режиме Technical Support Mode измените точку монтирования в соответствии с полученной инструкцией.

> **Скриншот 7:**
>
> Схема 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: ???????? ??????????

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

> 🖼 **Скриншот 16:**
>
> 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:**
>
> СхемаСхема

? ?????????? Endpoint Agents

> □ Указывается **не количество хостов**, а **количество эффективных агентов**, по которым рассчитывается нагрузка и выделяется дисковое пространство.

Тип хоста	Коэффициент
Windows-хост	×1
Linux/Mac-хост	×3
Сервер (Windows/Linux)	×20

Формула:

```
K = Σ(Windows) + Σ(Linux × 3) + Σ(Серверы × 20)
```

Пример:

- 800 Windows
- 100 Linux
- 200 Windows Server
- 100 Linux Server
  → `K = 800 + (100×3) + (300×20) = 7100`

> □ Если **KEDR не используется** → укажите `0`.

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

> □ Указывается **среднее количество писем в секунду (PPS)**.

Формула:

```
PPS = M / (H × 3600)
```

- `M` — писем в день
- `H` — часов в рабочем дне

Пример:
10 000 писем/день, 8 часов → `10000 / 28800 ≈ 0.35`

> □ Если **KATA не используется** → укажите `0`.

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

Укажите **суммарный объём трафика (Мбит/с)** с CN и всех Sensor.

Пример:

- CN: 500 Mbps
- Sensor: 1.5 Gbps = 1500 Mbps
  → Укажите: **2000**

> Если **NDR не используется** → укажите `0`.

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

> ⚠ Если вы установили Central Node **не в виде отказоустойчивого кластера**, вам необходимо рассчитать объём диска для параметров **База событий, ГБ** и **Хранилище, ГБ** по следующей формуле:

```
A = F - R, ГБ
```

Где:

- `A` — объём, используемый для базы событий и хранилища
- `F` — объём жёсткого диска, на котором будет храниться база событий TAA
- `R` — зарезервированное количество свободного пространства (ГБ) на второй дисковой подсистеме, соответствующее количеству подключенных хостов с компонентом Endpoint Agent

> **Примечание:**
> Если количество подключенных к Central Node хостов находится в диапазоне между значениями, используйте в расчётах **большее число**.

? ???????: ????????????????? ?????????? ?????????? ???????????

Количество хостов с Endpoint Agent	Зарезервированное пространство (ГБ)
1000	1000
3000	1200
5000	1400
10 000	1900
15 000	2400

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

Объём дискового пространства, необходимого для хранения данных телеметрии на сервере Central Node, рассчитывается по следующей формуле:

```
S = 150 ГБ + (K / 15000) × ((400 + 460 × d) / 0.65)
```

Где:

- `S` — объём требуемого дискового пространства (в ГБ)
- `K` — количество хостов с Kaspersky Endpoint Agent или Kaspersky Endpoint Security для Windows
- `d` — срок хранения данных в днях
- `150 ГБ` — базовый объём, требуемый для хранения

> ⚠ **Если включена функция проверки цепочек событий (NDR), применяется изменённая формула:**
>
> ```
> S = 150 ГБ + (K / 15000) × ((600 + 460 × d) / 0.65)
> ```

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

Допустим, в инфраструктуре **5000 хостов** и срок хранения данных — **30 дней**. Рассчитаем объём дискового пространства:

1. **Вычисляем сумму в числителе:**
   ```
   400 + 460 × 30 = 400 + 13 800 = 14 200
   ```
2. **Делим на коэффициент хранения:**
   ```
   14 200 / 0.65 ≈ 21 846.15 ГБ
   ```
3. **Определяем долю хостов:**
   ```
   5000 / 15000 = 0.33333
   ```
4. **Умножаем:**
   ```
   0.33333 × 21 846.15 ≈ 7282.05 ГБ
   ```

5. **Прибавляем базовые 150 ГБ:**

```
S = 150 + 7282.05 ≈ 7432.05 ГБ ≈ 7.43 ТБ
```

 Итог:
Для 5000 хостов с 30-дневным хранением данных требуется **≈7.43 ТБ** дискового пространства.

> **Примечание:**
> Если включена функция **проверки цепочек событий (NDR)**, объём увеличится до **≈7.53 ТБ**.

? ?????????????? ????? ??? ???????? ?????????? NDR

Если используется анализ SPAN-трафика, рассчитайте дополнительный объём:

```
S_NDR = (N_NDR × 0.02 + T_SPAN × 10) × d
```

Где:

- `N_NDR` — количество агентов NDR
- `T_SPAN` — объём SPAN-трафика в Гбит/с
- `d` — срок хранения (дней)

Пример:

- `N_NDR = 2000`
- `T_SPAN = 2 Гбит/с`
- `d = 30`

```
S_NDR = (2000 × 0.02 + 2 × 10) × 30 = (40 + 20) × 30 = 1800 ГБ = 1.8 ТБ
```

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

```
S_total = S + S_NDR
```

Пример:

```
S_total = 7.43 ТБ + 1.8 ТБ = 9.23 ТБ
```

 Итого требуется: ≈9.23 ТБ

> ⚠ **Максимальный объём на одной подсистеме — 15 ТБ.**
> При превышении рассмотрите кластерную архитектуру.

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

Рекомендуется указать **до 100 ГБ** — для файлов, полученных через задачу «Получить файл».

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:**
>
> Схема

? ??? ???????

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

> **?????!**
>
> ??? ?????????? Central Node ????? ???????? ?????? ????? ???-?????????. ????????????? ??????????? ??? ????????? ??? ?????? ??????.

> □□ **Скриншот 22:**
>
> Схема

? ????????

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

> □□ **Скриншот 23:**
>
> Схема

? 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

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

- 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**, **выделенного Sensor** и настройки/подключению **Endpoint Agents**.

Revision #52
Created 19 August 2025 07:50:43 by Николай
Updated 29 March 2026 16:54:32 by Николай