

?????????????? ?? ?????????????? ? ?????????????? ??????????????? Sandbox ? ?????/KEDR/NDR 7.0-7.1

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

Версия платформы: KATA / KEDR / NDR 7.0 - 7.1

Источник: [Установка компонента Sandbox](#)

Официальная документация: Справка [Kaspersky Anti Targeted Attack Platform 7.1](#)

Введение

Компонент Sandbox в платформе Kaspersky Anti Targeted Attack (KATA) предназначен для глубокого анализа поведения подозрительных файлов и URL в изолированной среде. Он позволяет выявлять целевые атаки, вредоносные программы и скрытые угрозы, которые не обнаруживаются традиционными средствами защиты.

Установка Sandbox — ответственный процесс, требующий точного соблюдения системных требований и последовательной настройки. В данной статье подробно описаны все этапы: от подготовки виртуальной машины до подключения к ****Central Node**** и настройки пользовательских шаблонов.

⚠ **Перед началом** обязательно ознакомьтесь с [официальными требованиями](#).

1. Подготовка виртуальной машины

Подготовка

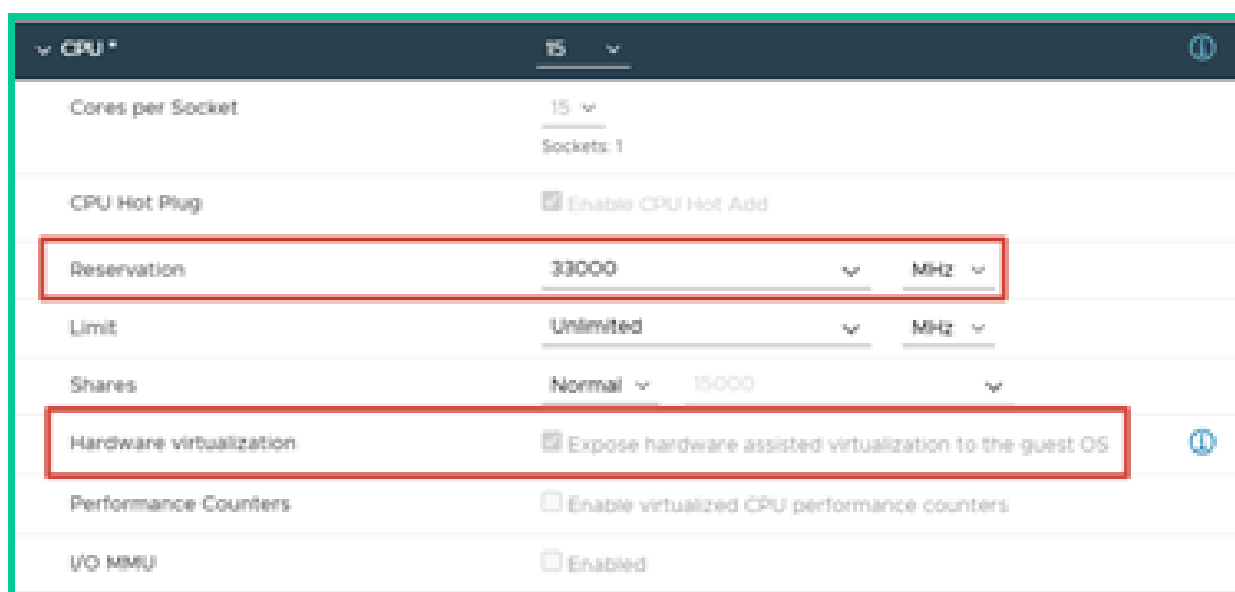
Sandbox должен быть развёрнут на виртуальной машине с особыми настройками. Ниже — ключевые требования.

ПАРМЕТРЫ	ТРЕБОВАНИЕ
Процессор	Только Intel с поддержкой Hyper-Threading
Вложенная виртуализация	Обязательно включена (Для платформ виртуализации)
Latency Sensitivity	Установлено в High (Для платформ виртуализации)
Оперативная память	Полностью зарезервирована
Процессор	Частота полностью зарезервирована
Прошивка	UEFI (с отключённым Secure Boot)

1.2. Настройка VMware vSphere

Шаг 1: Включение вложенной виртуализации

Перейдите в настройки виртуальной машины → **CPU** → включите опцию:

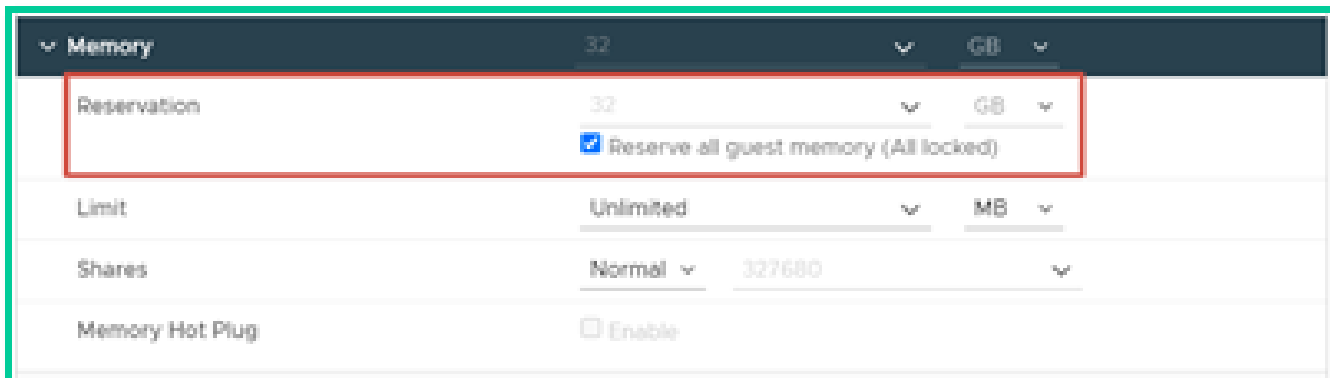


 **Рис. 1. Expose hardware assisted virtualization to the guest OS**

Шаг 2: Резервирование ресурсов

- Память:

В разделе **Memory** → поставьте галочку:



□ Рис. 2. Reserve all guest memory (All locked)

- Процессор:

В **CPU Reservation** укажите значение (см. Рисунок 1) по формуле:

Примечание: Параметр «**Reservation**» рассчитывается в зависимости от частоты процессора ESXi-хоста, на котором разворачивается Sandbox, по следующей формуле:

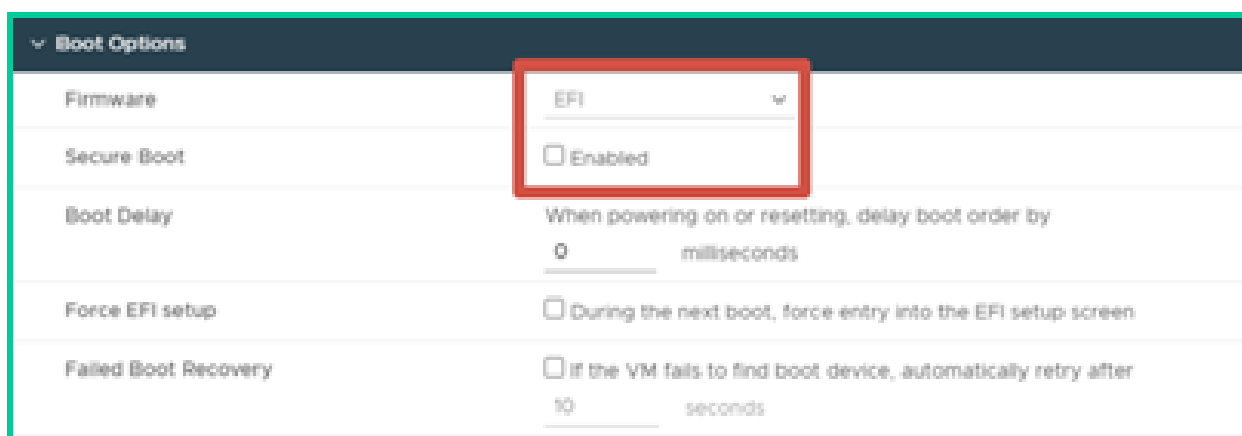
$$15 * <\text{значение частоты в МГц}>$$

□ **Пример:**

Для CPU 2,2 ГГц (2200 МГц) и 1 ядра: $15 \times 2200 = 33\ 000$ МГц

Шаг 3: Настройка прошивки UEFI

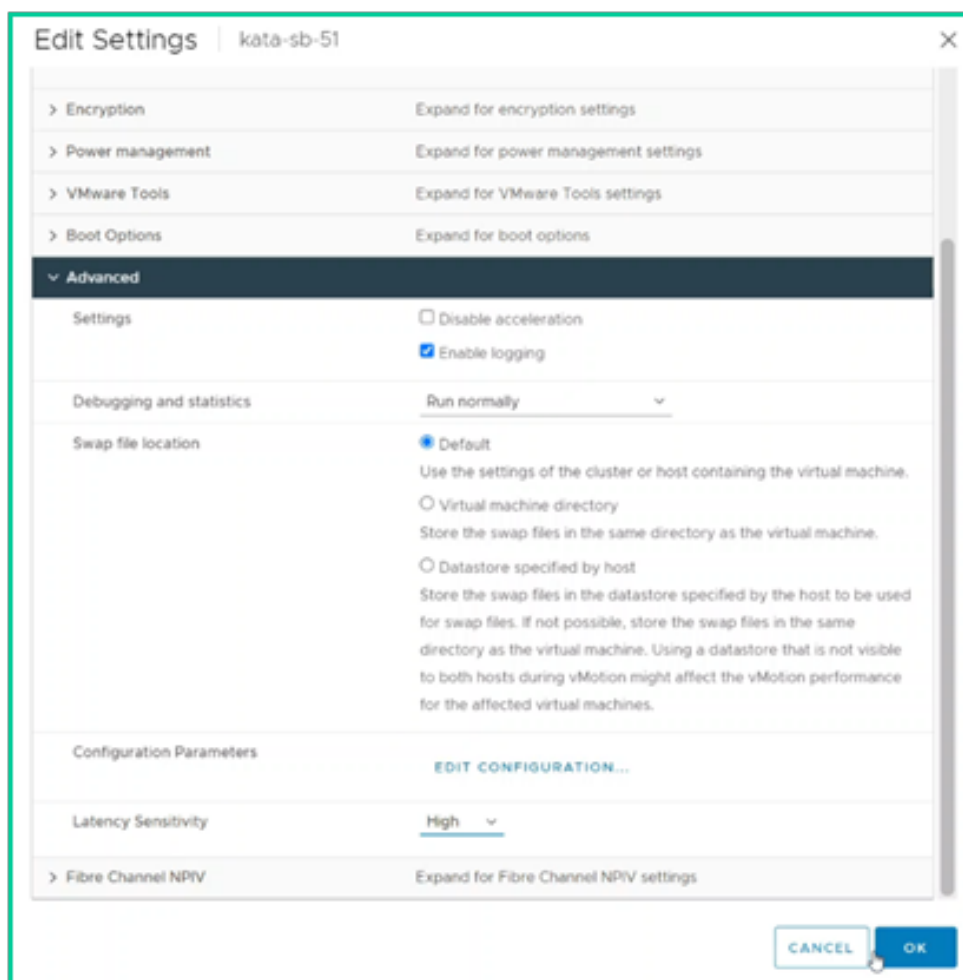
1. Перейдите в **VM Options** → **Boot Options** → **Firmware**.
2. Выберите **UEFI**.
3. Обязательно **отключите Secure Boot**.



□ Рис. 3. Выбор UEFI и отключение Secure Boot

Шаг 4: Установка высокой чувствительности к задержкам

- Перейдите в **VM Options** → **Latency Sensitivity**.
- Установите значение **High**.



□ **Рис. 4.** Настройка **Latency Sensitivity** в **High**

□ На этом этапе подготовка виртуальной машины завершена.

2. Установка компонента Sandbox

Установка

2.1. Запуск установщика

1. Примонтируйте ISO-образ Sandbox к виртуальной машине.
2. Запустите VM.

3. В меню загрузки выберите:

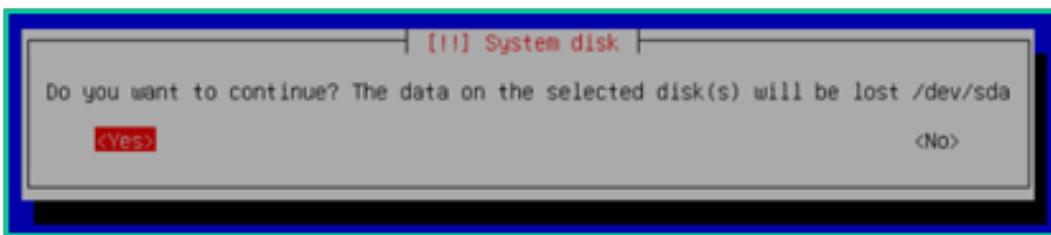


□ Рис. 5. Меню установки — выбор "Installation KATA Sandbox"

2.2. Пошаговая установка

Установка проходит в текстовом интерфейсе. Действуйте по шагам:

1. Язык: Выберите русский или английский → нажмите **Enter**.
2. Лицензия: Примите условия (нажмите **TAB**, выберите "**Я принимаю**").
3. Политика конфиденциальности: Аналогично — примите.
4. Диск: Выберите диск → нажмите **Enter**.
5. Очистка диска: Подтвердите — выберите **Yes**.



□ Рис. 6. Подтверждение очистки диска

2.3. Настройка учётных данных и сети

1. Минимальная длина пароля: По умолчанию — **12 символов** (рекомендуется оставить).
2. Пароль **admin**: Задайте надёжный пароль.

3. Управляющий интерфейс (Management Interface):

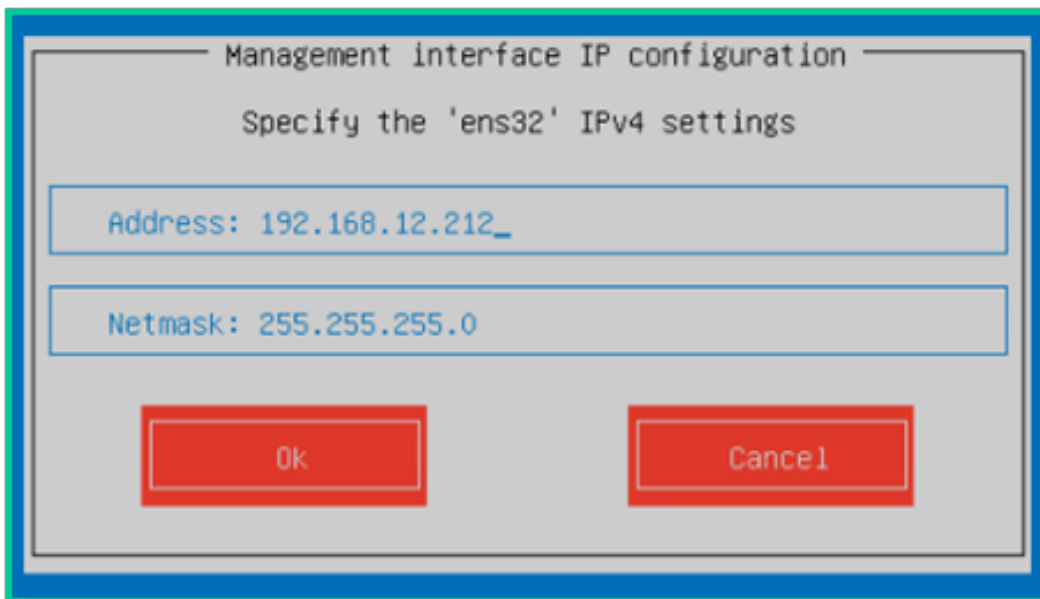
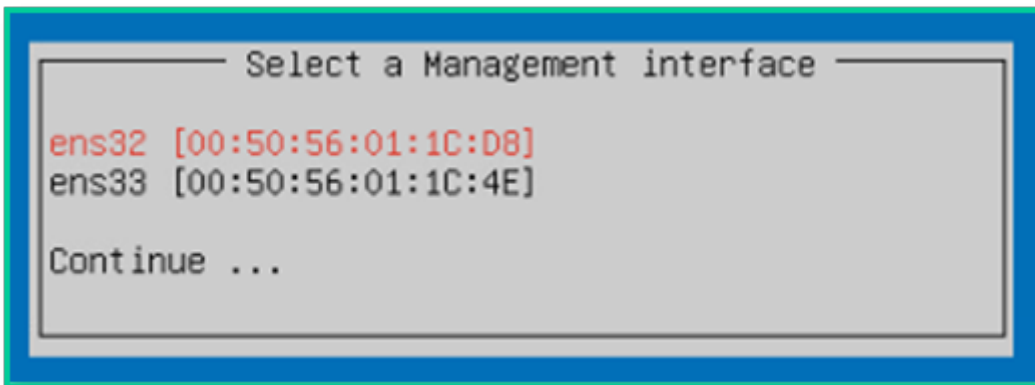
- Выберите сетевой адаптер.
- Назначьте:
 - IP-адрес
 - Маску подсети
 - Шлюз

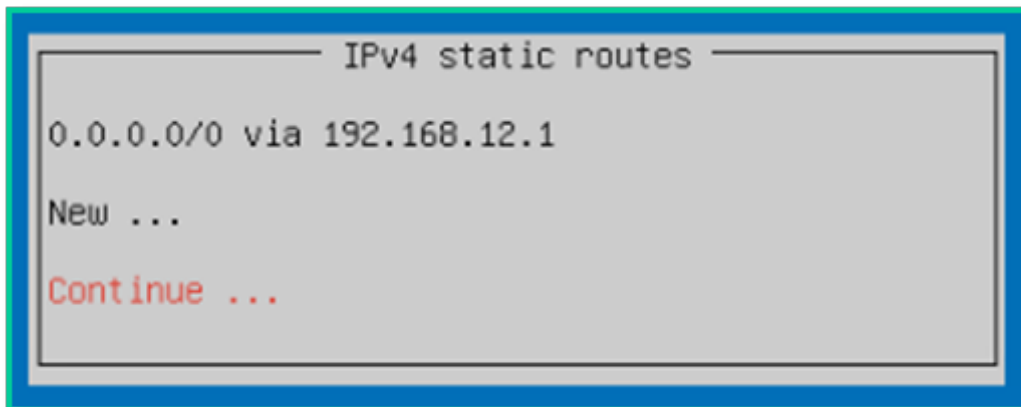
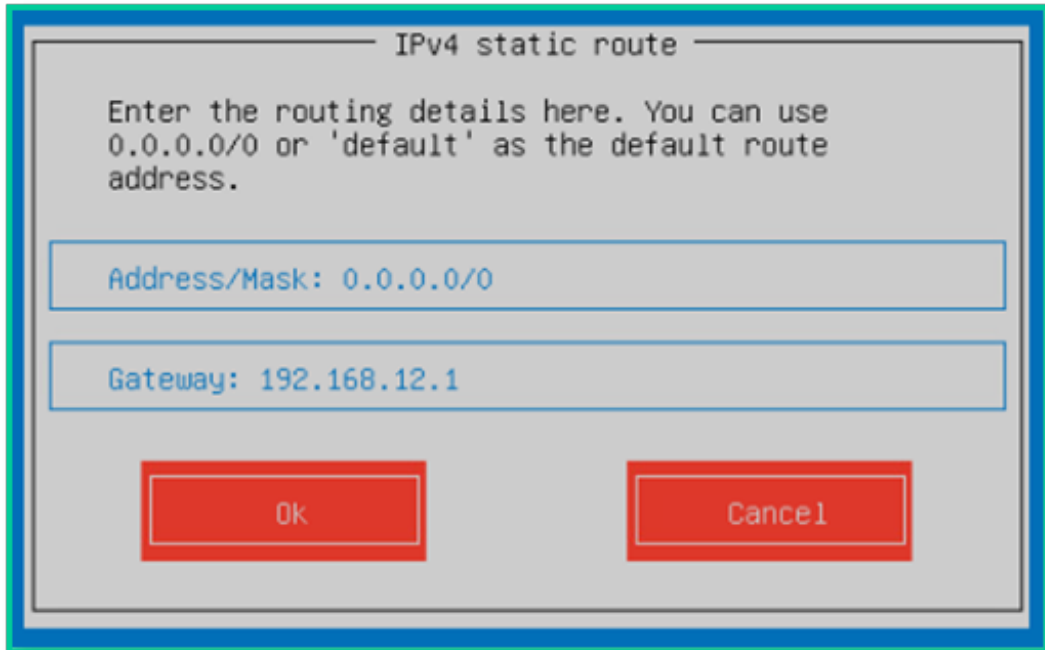
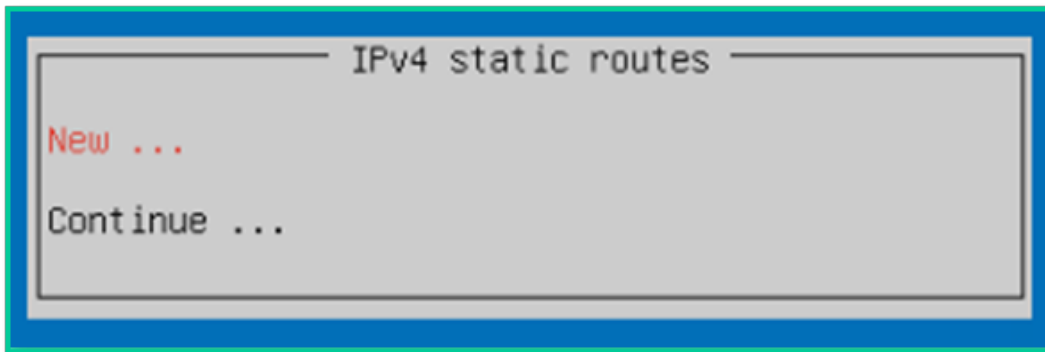
4. FQDN-имя сервера: Укажите полное доменное имя (например, `sandbox.corp.local`). (**Важно:** имя должно быть задано в нижнем регистре, так же, как и на DNS-сервере).

5. DNS-серверы:

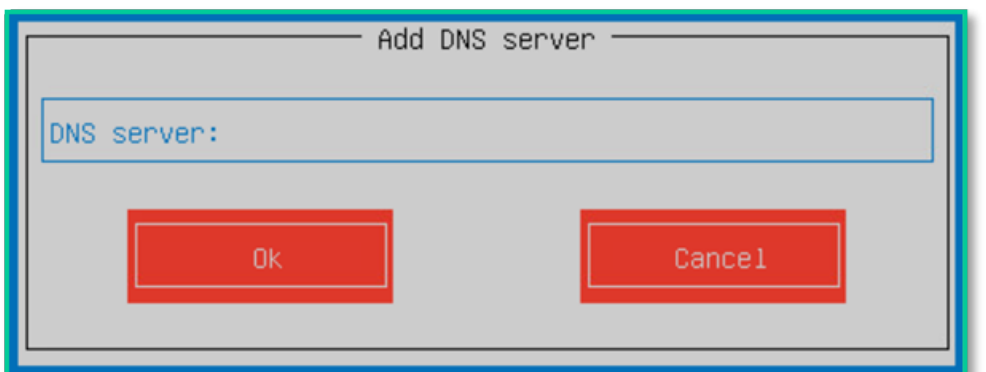
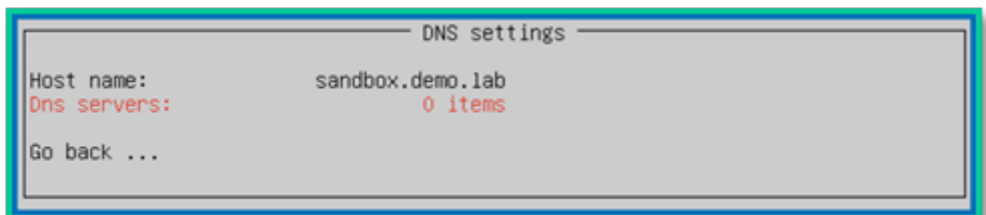
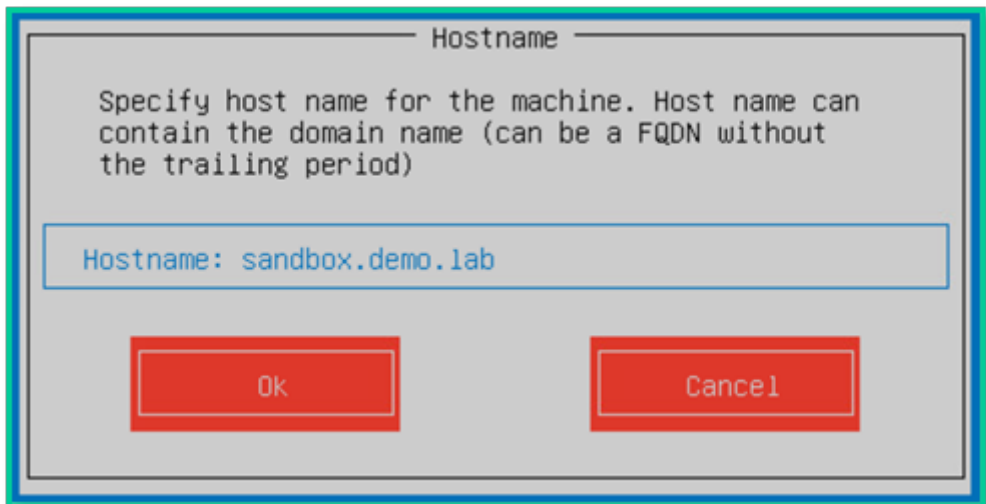
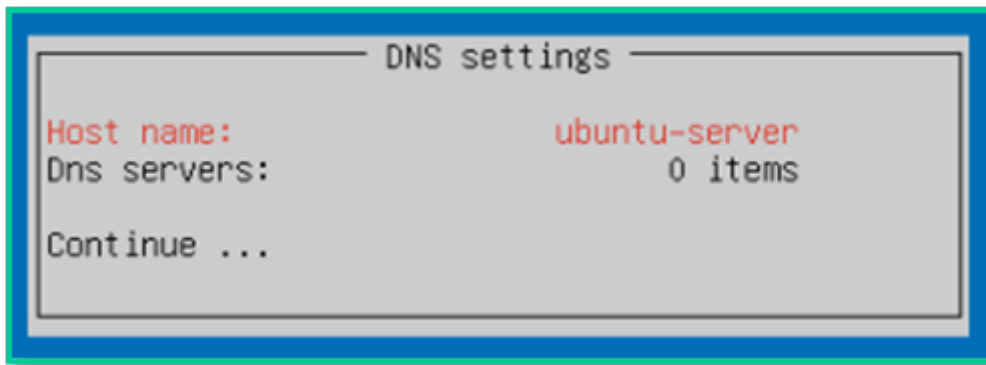
- Добавьте основной и резервный DNS.

6. Шлюз по умолчанию*: Укажите IP-адрес шлюза.





□ **Рис. 7.** Настройка IP, маски и шлюза



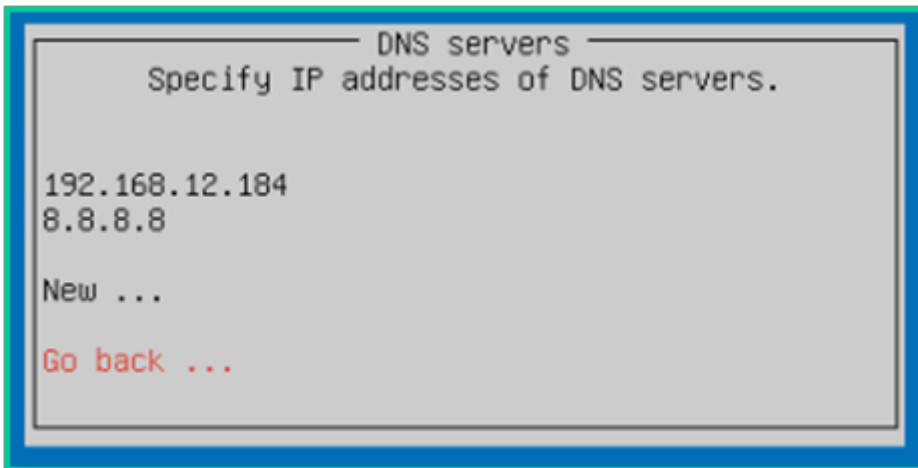
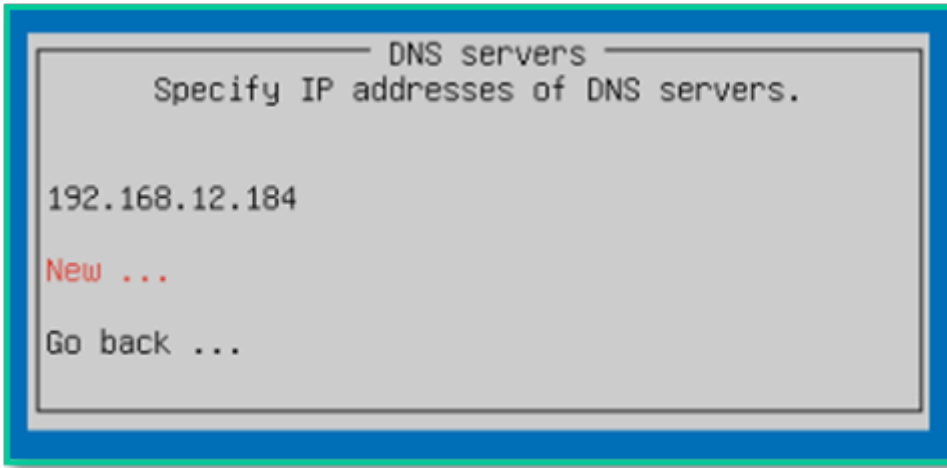
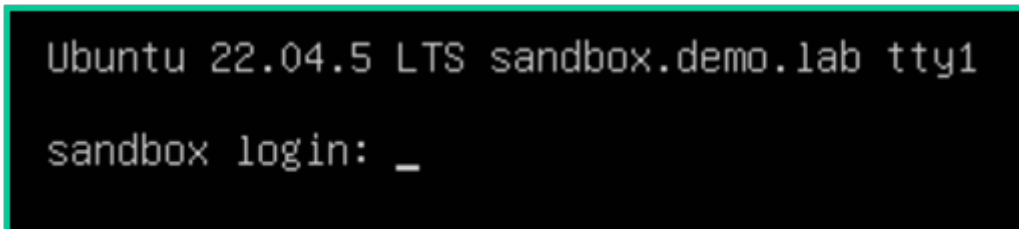


Рис. 8. Настройка FQDN и DNS-серверов



? ?????????? ??????????. ?????????? URL ??????????:

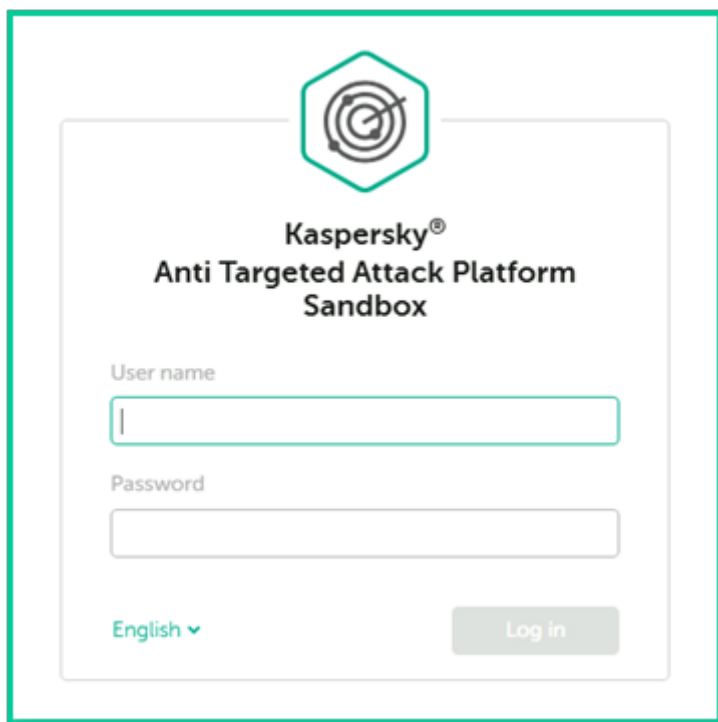
Management URL: https://<IP>:8443/

3. Первый вход и базовая настройка

Базовая настройка

3.1. Вход в веб-интерфейс

1. Откройте браузер.
2. Перейдите по адресу: **https://<IP_Sandbox>:8443/**
3. Войдите под учётной записью:
 - Логин: **`admin`**
 - Пароль: **заданный при установке.**



□□ **Рис. 9.** Страница входа в веб-интерфейс Sandbox

3.2. Настройка даты и времени

1. Перейдите в раздел "**Дата и время**".
2. Установите:
 - Часовой пояс
 - Текущее время
3. Рекомендуется настроить синхронизацию с NTP-сервером.

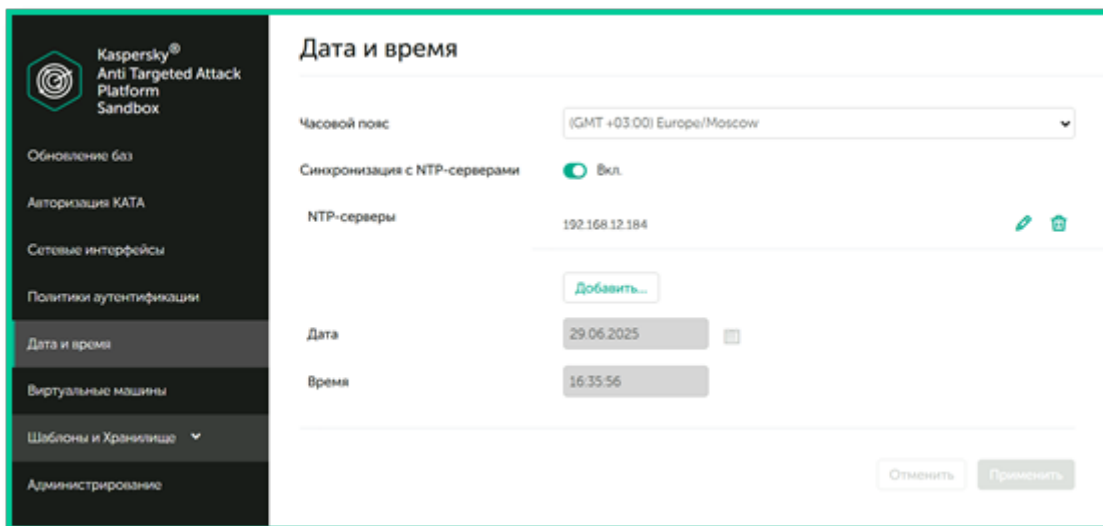
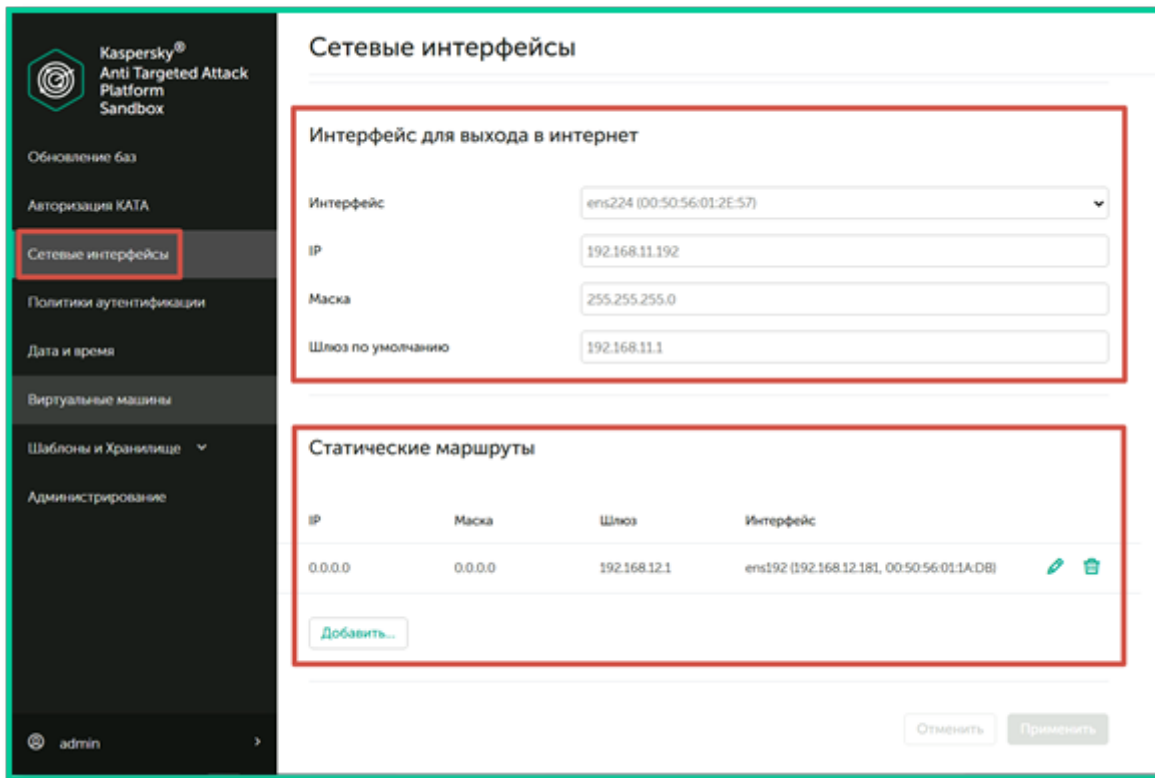


Рис. 10. Настройка времени и NTP

4. Настройка Malware Interface

4.1. Настройка интерфейса

1. Перейдите в "**Сетевые интерфейсы**".
2. Найдите "**Интерфейс для выхода в интернет**".
3. Укажите:
 - IP-адрес
 - Маску
 - Шлюз



□ □ **Рис. 11.** Настройка Malware Interface

4.2. Обновление баз

“ **Важно!** Перед подключением к Central Node выполните обновление баз.

1. Перейдите в "**Обновление баз**".
2. Убедитесь, что Malware Interface имеет доступ в интернет.
3. Нажмите "**Обновить**".
4. Дождитесь статуса: "**Успешно**".

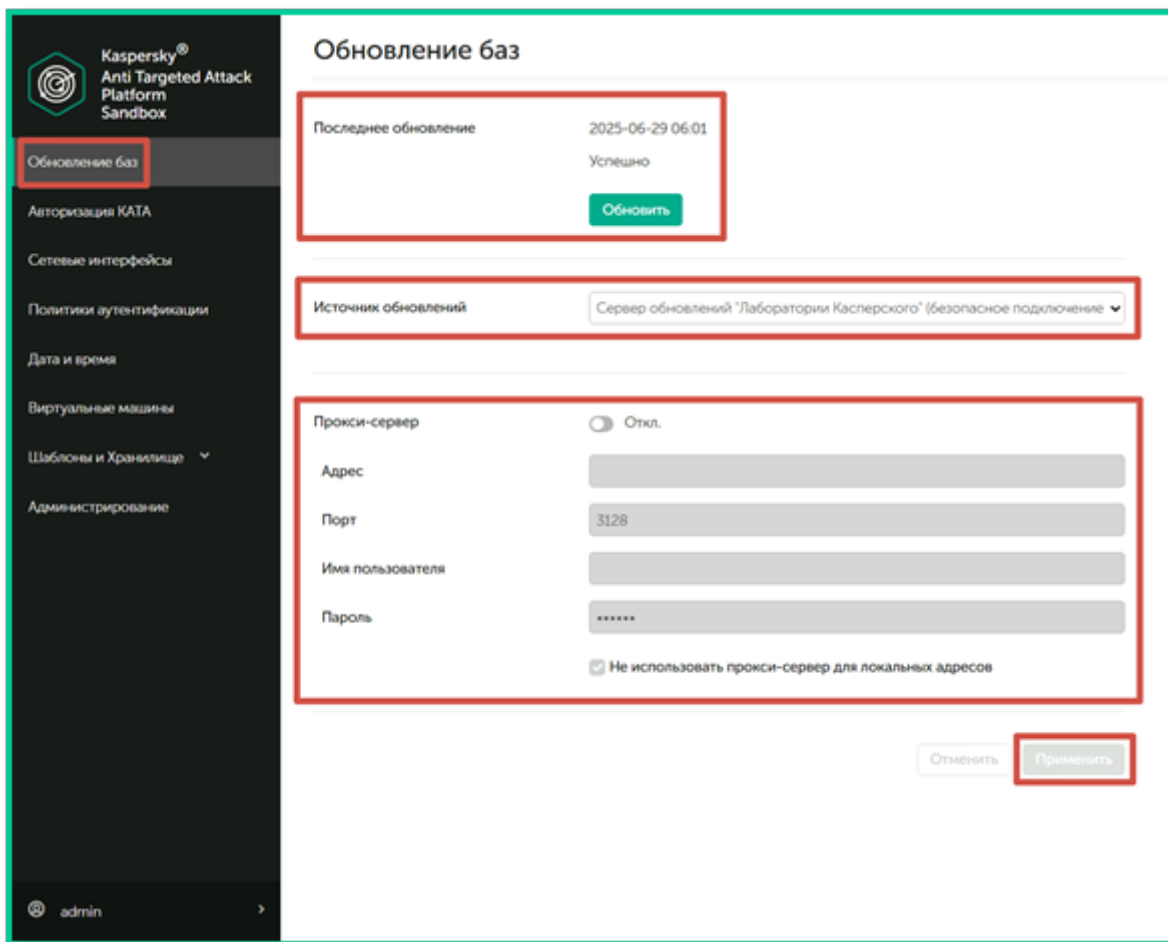


Рис. 13. Статус успешного обновления баз

5. Загрузка и настройка шаблонов ОС

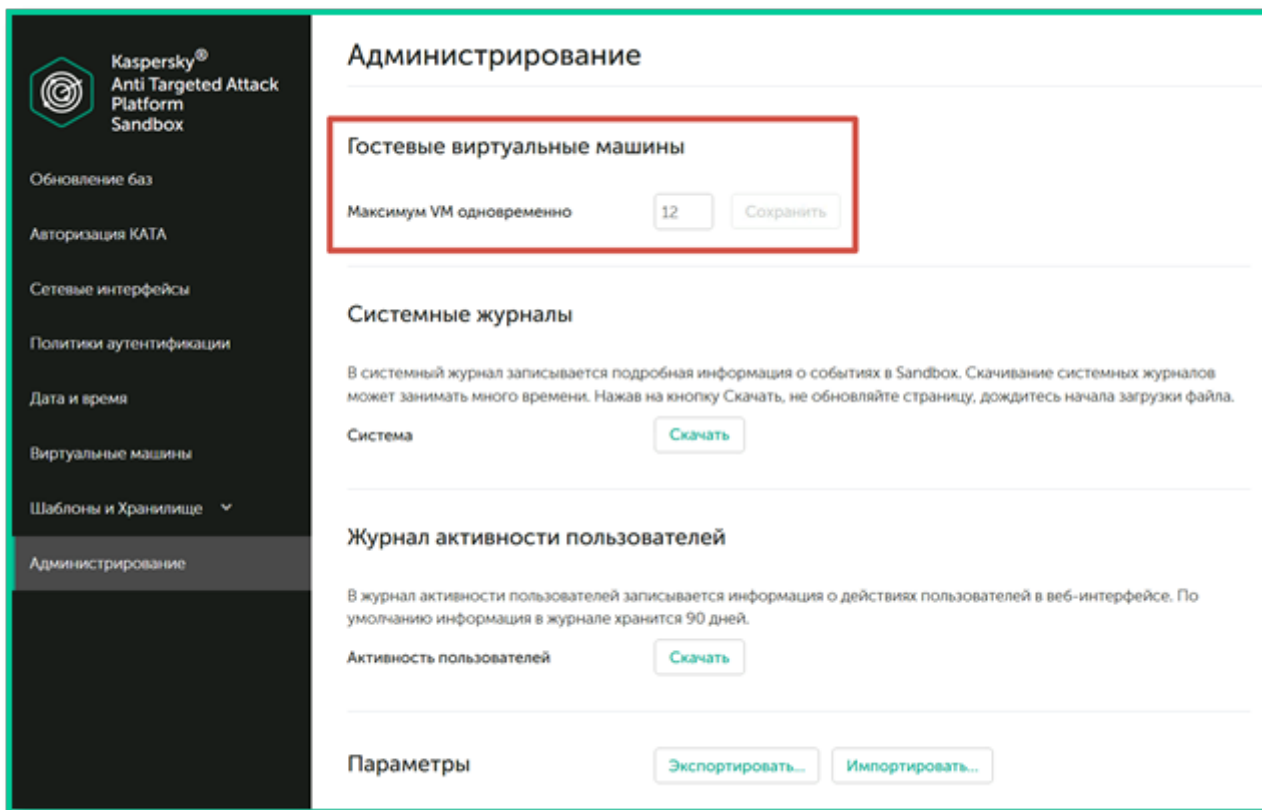
5.1. Ограничение количества VM

Перед загрузкой шаблонов установите лимит:

- **Виртуальный сервер:** до 12 VM
- **Физический сервер:** до 48 VM (В зависимости от характеристик оборудования, это значение можно увеличить до 72 или 144).

Путь:


`Администрирование → Гостевые виртуальные машины`



□ **Рис. 14.** Настройка лимита VM

5.2. Загрузка предустановленных шаблонов

1. Перейдите в "**Шаблоны и хранилища**" → "**Шаблоны**".
2. Нажмите "**Добавить**" → выберите ISO-образ ОС.
3. Дождитесь статуса: "**Готова к установке**".
4. Перейдите в "**Виртуальные машины**" → "**Создать VM**".
5. Выберите шаблон → нажмите "**Сохранить**".
6. Примите лицензионное соглашение.
7. Нажмите "**Установить готовые VM**".
8. Дождитесь статуса: "**Включено**".



Kaspersky®
Anti Targeted Attack
Platform
Sandbox

Шаблоны

Доступно 267.67 ГБ из 293.74 ГБ

Шаблоны используются для создания виртуальных машин, в которых приложение будет запускать объекты для проверки. В комплекте поставки есть предустановленные образы, для которых не нужно создавать шаблон. Если вы хотите их использовать, импортируйте образы на этой странице.

Создано ↑	Тип	Имя	Состояние	Размер	ВМ	Действия
Создайте или импортируйте шаблон						
<div style="border: 1px solid #ccc; border-radius: 5px; padding: 5px; display: inline-block;"> Добавить ▾ </div>						

⊙

admin

>

Шаблоны

Доступно: 267,8 ГБ из 293,74 ГБ

Добавить ▾

Шаблоны используются для создания виртуальных машин, в которых приложение будет запускать объекты для сканирования. В дистрибутив входят предустановленные образы, для которых не нужно создавать шаблон. Если вы хотите их использовать, импортируйте образы на этой странице.

Созданный ↑	Тип	Имя	Статус	Размер	ВМ	Действия	Описание
2025-06-04 10:46:13	По умолчанию	sandbox-images-win1...	Загрузка 0%	12 ГБ	–	–	–

Шаблоны

Доступно 267.67 ГБ из 293.74 ГБ

Шаблоны используются для создания виртуальных машин, в которых приложение будет запускать объекты для проверки. В комплекте поставки есть предустановленные образы, для которых не нужно создавать шаблон. Если вы хотите их использовать, импортируйте образы на этой странице.

Создано ↑	Тип	Имя	Состояние	Размер	ВМ	Действия
2025-02-07 19:01:31	Default	sandbox-images-c...	Готова к установке	992 MB	–	

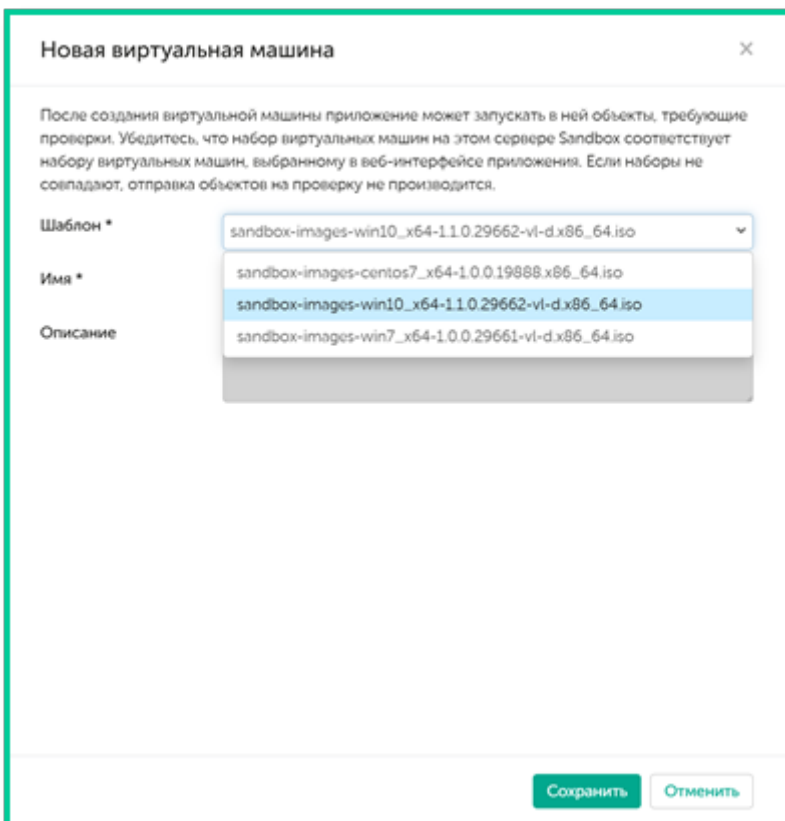
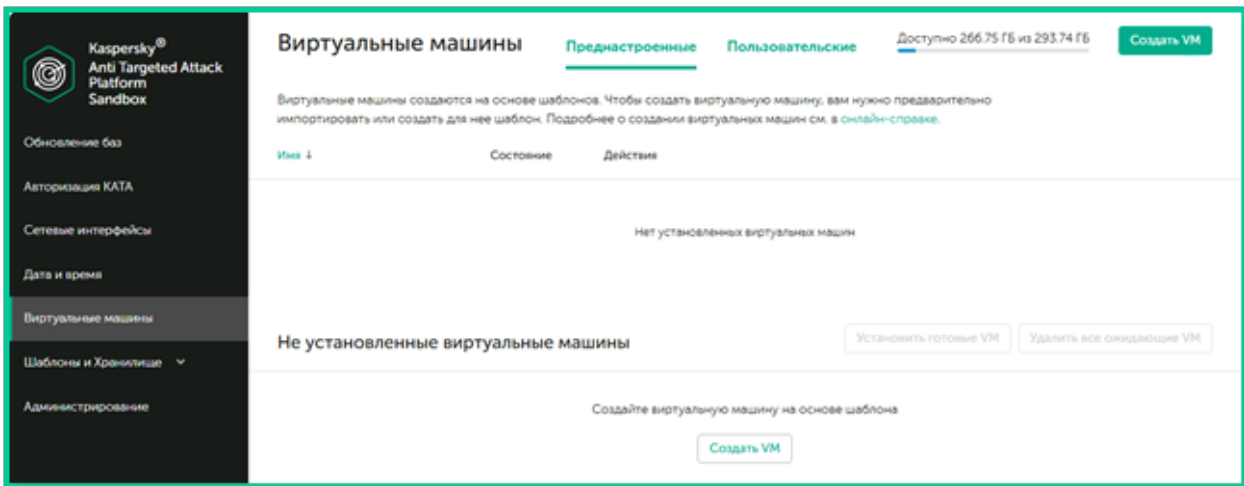
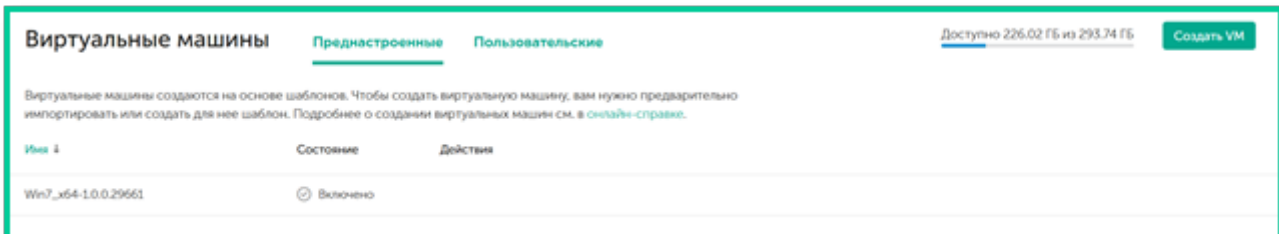
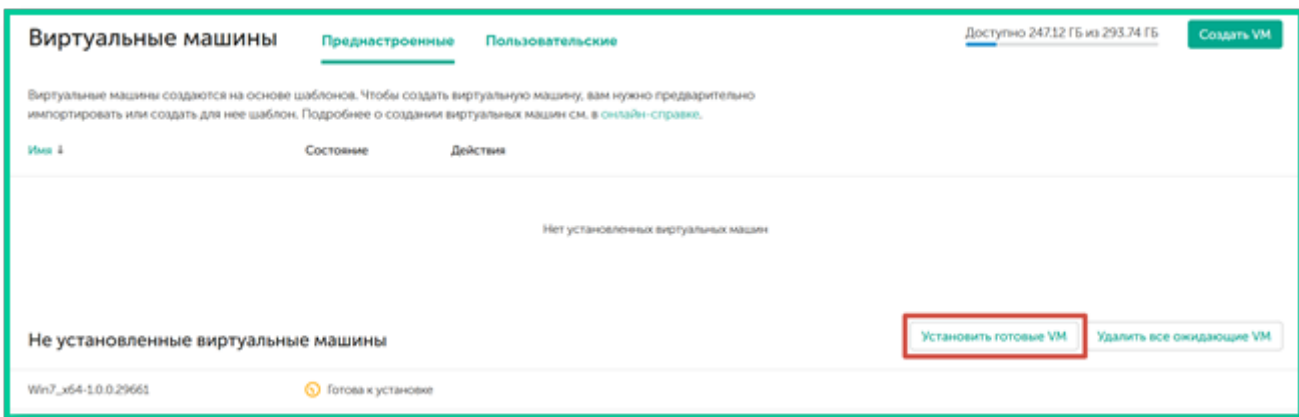
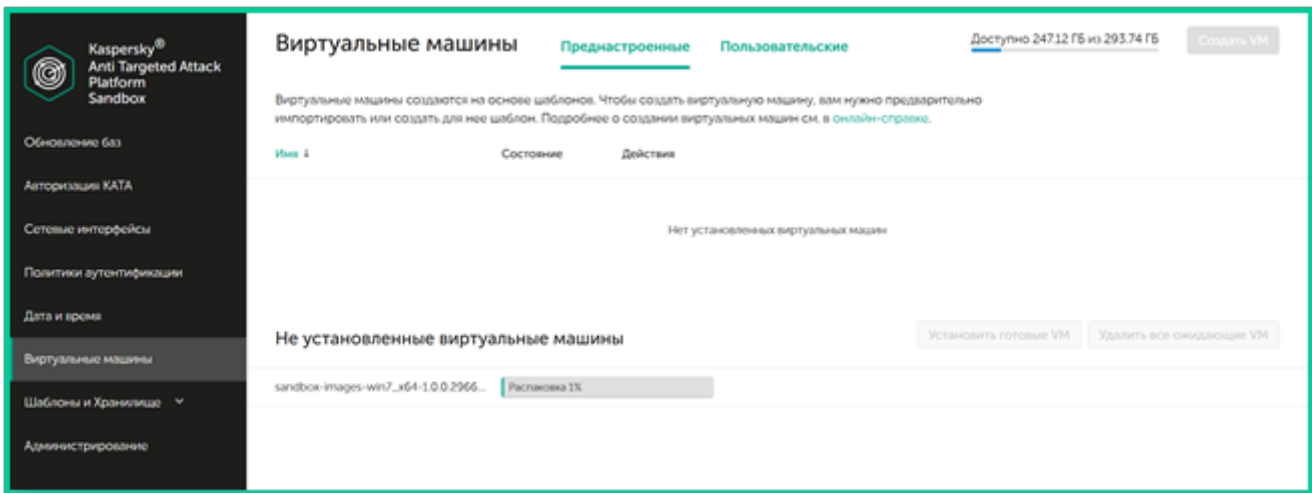


Рис. 15. Создание VM из шаблона



□□ **Рис. 16.** Статус "Включено" после установки

5.3. Создание пользовательских шаблонов

Поддерживаемые ОС:

- Windows XP SP3+
- Windows 7
- Windows 8.1 (64-bit)
- Windows 10 (64-bit, до версии 1909)

Требования к ОС:

- Отключить экранную заставку.
- Схема питания: "**Всегда включено**".
- Отключить **автообновления** и **брандмауэр Windows**.
- Для Windows 7: требуется поддержка хеш-алгоритма **SHA-2**; Для поддержки этого хеш-алгоритма установите обновление **Security Update for Windows 7 for x64-based Systems (KB3033929)**. Для **32-битных** операционных систем Windows 7 также требуется установить обновление **KB3033929**.
- Для использования Windows 7 необходимо в настройках операционной системы включить использование TLS 1.1 и TLS 1.2. Для этого в Windows 7 в разделе Панель управления → Свойства браузера → Дополнительно установите флажок Использовать TLS 1.1 и Использовать TLS 1.2.
- Не устанавливайте **KB4474419** (может вызвать сбой во время развертывания виртуальной машины.).
- Для Windows 8.1/10: отключить **Fast Boot**, включить функцию автоматического входа в систему (**авто логин**).

Ограничения, действующие при установке программного обеспечения:

- К одному шаблону одновременно можно подключить только один образ. После того как шаблон будет сохранен, вы можете отключить один образ и подключить другой.
- Не поддерживаются версии Microsoft Office выше 2016.
- Для пользовательских образов операционных систем полностью поддерживаются следующие локализации: русский, английский, упрощенный китайский (simplified), арабский, испанский (Mexico).
- Для операционной системы Windows XP поддерживаются только русский и английский языки.
- Лицензионные ключи для активации операционных систем и программного обеспечения не предоставляются.
- Настоятельно не рекомендуется устанавливать программное обеспечение следующих типов:
 - Программное обеспечение, внедряющее свой код в другой запущенный процесс.
 - Драйверы для защиты.
 - Антивирусные приложения, включая Защитник Windows.
- Не гарантируется обнаружение вредоносной активности файлов, которые запускаются с помощью узкоспециального программного обеспечения.

Kaspersky Anti Targeted Attack Platform не уведомляет о проблемах с установленным программным обеспечением в операционной системе.

Процесс создания шаблона

1. Перейдите в "**Хранилище**" → загрузите ISO-образ ОС.
2. Перейдите в "**Шаблоны**" → "Создать шаблон".
3. Укажите:
 - Имя
 - Описание
 - Образ ОС (из хранилища)
4. Нажмите "**Продолжить**".
5. На этапе "**Настройка шаблона**" установите ОС и ПО.
6. При необходимости: нажмите "**Подключить ISO**" → выберите образ с ПО.

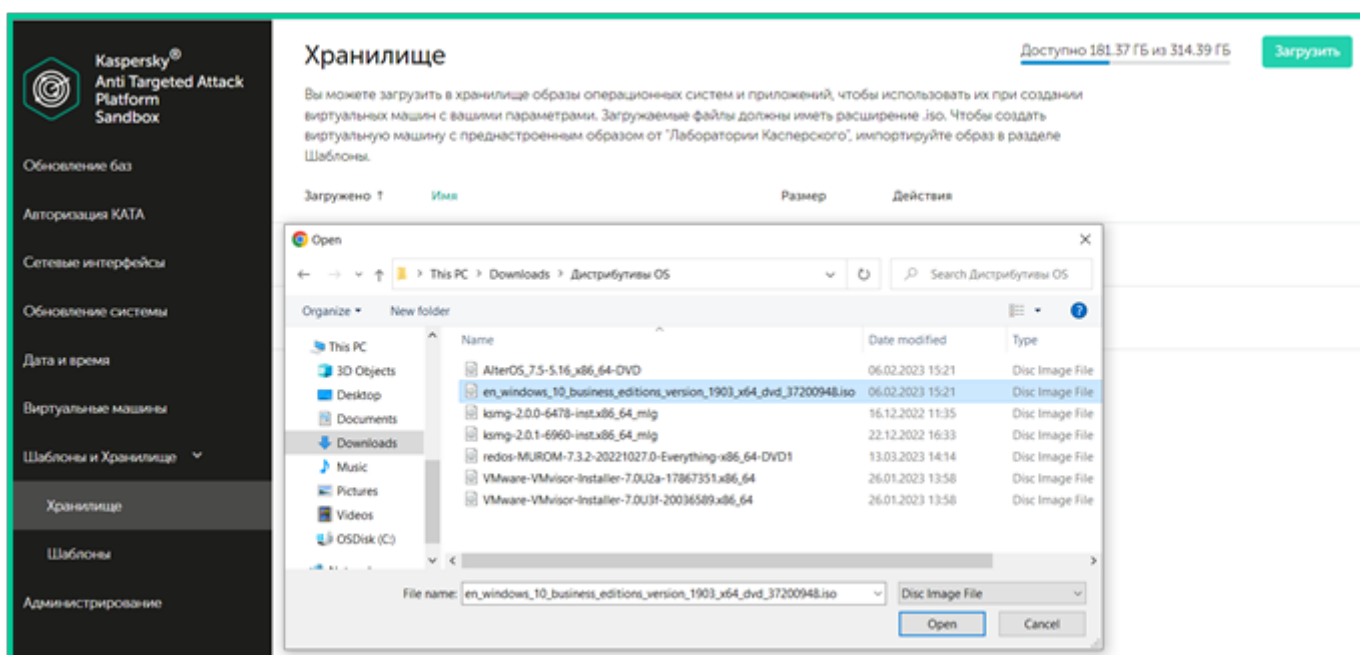


Рис. 17. Создание нового шаблона





Шаблоны > Создать шаблон

Подготовка образа
Выбор имени и образа

Настройка шаблона
Установка и настройка ОС. Вы можете остановить и продолжить настройку в любое время

Имя * Win10_customvm

Описание * Win10_customvm

Образ ОС * 
SW_DVD5_Office_Professional_Plus_2016_64Bit_Russi...
en_windows_10_business_editions_version_1903_x64...
 Загрузить образ

Продолжить



Шаблоны > Создать шаблон

Подготовка образа
Выбор имени и образа


Настройка шаблона
Установка и настройка ОС. Вы можете остановить и продолжить настройку в любое время

Имя * Win10_customvm

Описание * Win10_customvm

Образ ОС * 
SW_DVD5_Office_Professional_Plus_2016_64Bit_Russi...
en_windows_10_business_editions_version_1903_x64...
 Загрузить образ

Продолжить

 Рис. 18. Подключение ISO с ПО

6. Решение проблемы с отсутствием интернета

Если для сервера, на котором устанавливается виртуальная машина с пользовательским образом, **не настроен доступ в интернет**, для корректного завершения установки виртуальной машины вам нужно **загрузить отладочные символы Microsoft**.

Пример ошибки из журнала установки:

Касперский®
Anti Targeted Attack
Platform
Sandbox

Обновление баз
Авторизация KATA
Сетевые интерфейсы

Виртуальные машины

Преднастроенные Пользовательские

Виртуальные машины создаются на основе шаблонов. Чтобы создать виртуальную машину, вам нужно предварительно импортировать или создать для нее шаблон. Подробнее о создании виртуальных машин см. в онлайн-справке.

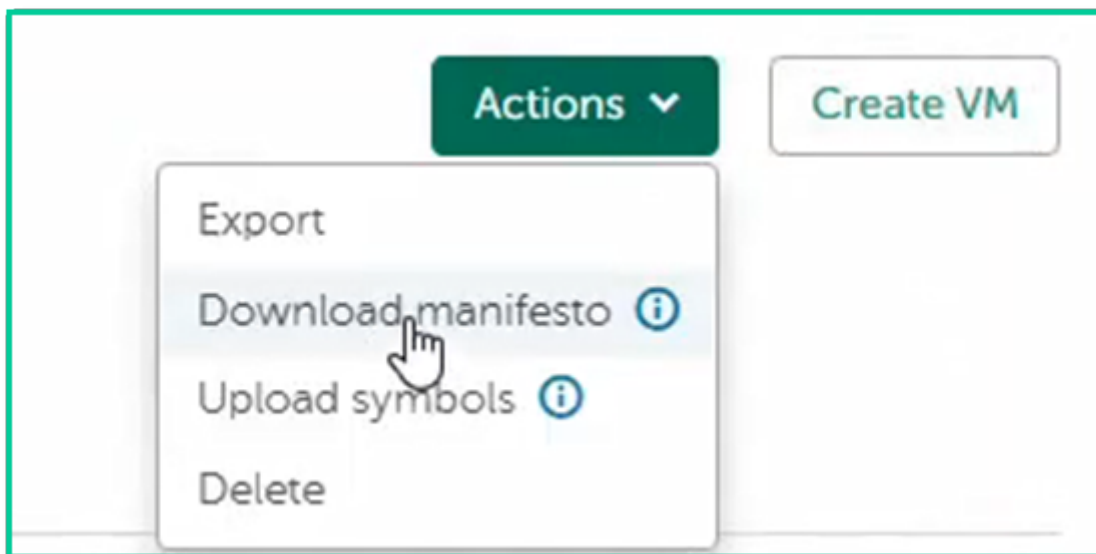
Создано	Имя	Состояние	Действия	Описание
2023-11-09 13:21:17	Win10_1809	Сбой		-

*File "/opt/kaspersky/python3-venv/lib/python3.10/site-packages/KL/snapshot/vm_steps.py", line 390, in inner
raise err_cls(str(err)) from err*

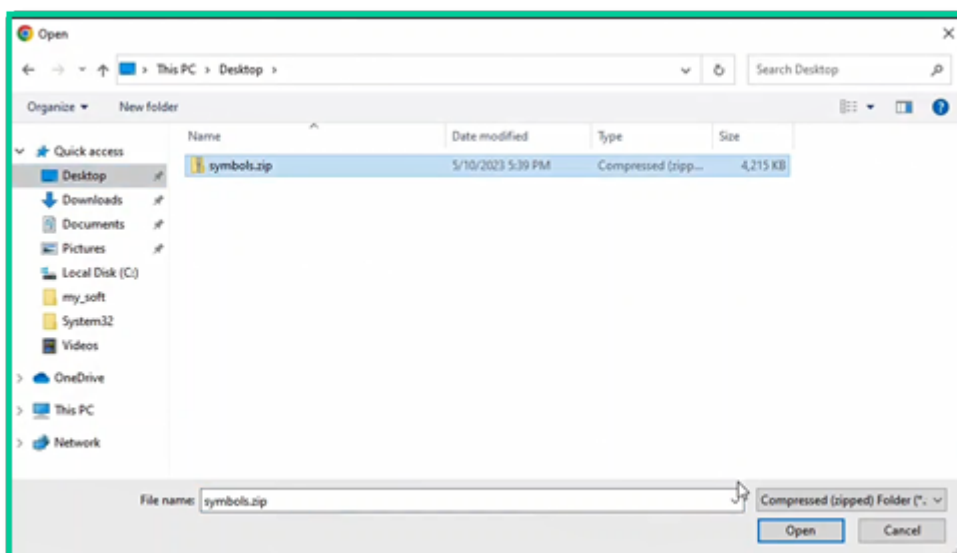
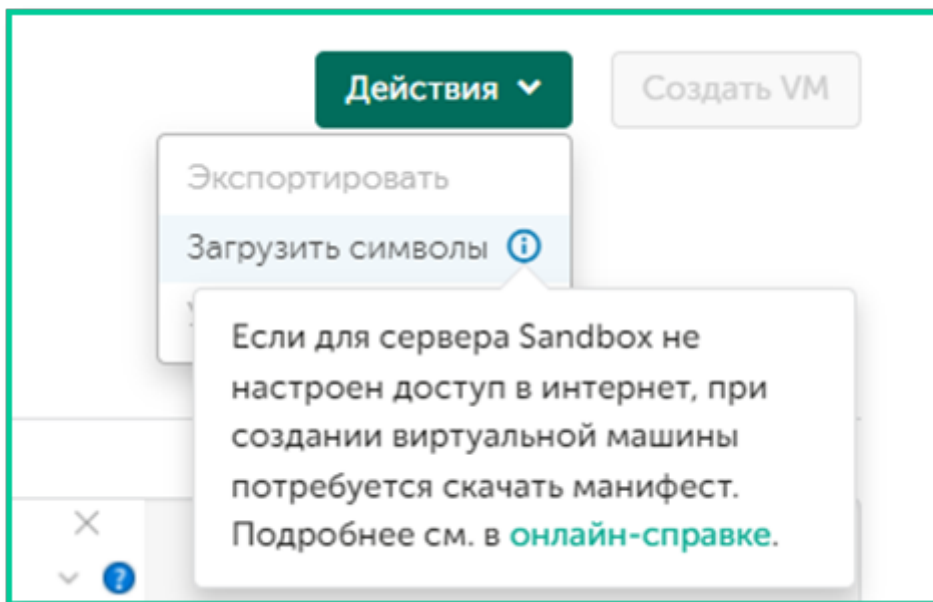
[M <:common.exceptions.InstallKmExpErr: Offline kmbuild failed. Probably no symbols

Решение: загрузка отладочных символов

1. В разделе "**Шаблоны**" нажмите "**Скачать манифест**".
2. Распакуйте архив.
3. Запустите ``sbsymtool.ps1`` от имени администратора в **PowerShell**.
4. Скрипт загрузит символы Microsoft.
5. Вернитесь в Sandbox → "**Шаблоны**" → "**Загрузить символы**".
6. Выберите полученный архив → нажмите "**Open**".
7. Повторите установку VM.



□ Рис. 19. Кнопка "Скачать манифест"



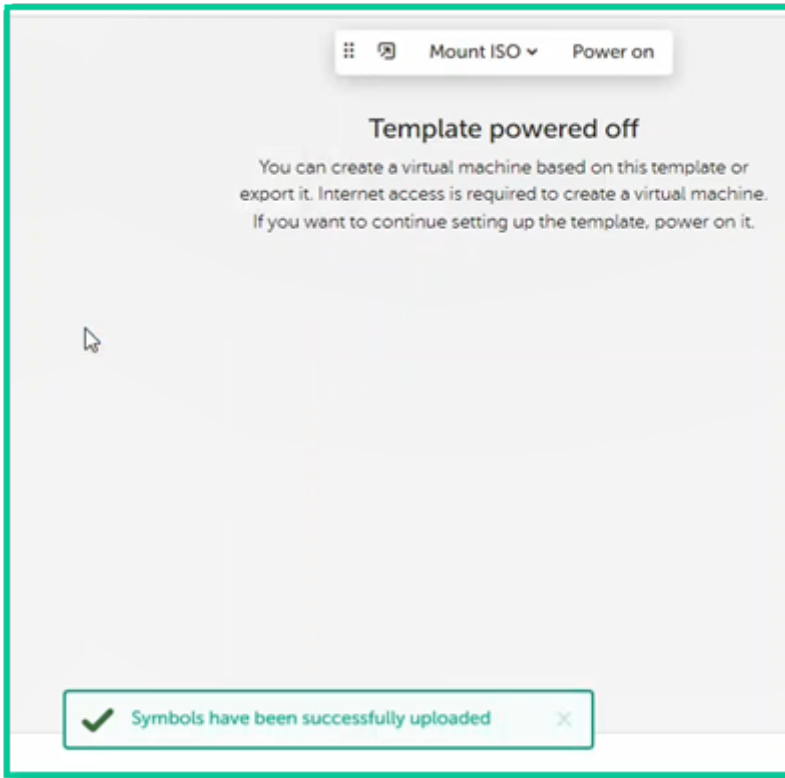


Рис. 20. Загрузка архива с символами

7. Подключение к Central Node

7.1. Добавление Sandbox в Central Node

1. В **Central Node** перейдите в "Серверы Sandbox" → "Добавить".
2. Укажите IP-адрес Sandbox.
3. Нажмите "Получить отпечаток сертификата".
4. Сравните отпечаток с тем, что указан в **Sandbox** → "Авторизация KATA".
5. Укажите имя сервера.
6. Поставьте галочку "**Включить**" → нажмите "Добавить".



Подключение сервера Sandbox

IP: 192.168.12.181

Отпечаток сертификата: E3:11:57:AA:76:F6:84:28:2A:72:54:1F:F6:B8:90:F1:89:B0:0C:C3:4D:CB:AB:D0:4C:83:76:1C:50:F1:79:0E

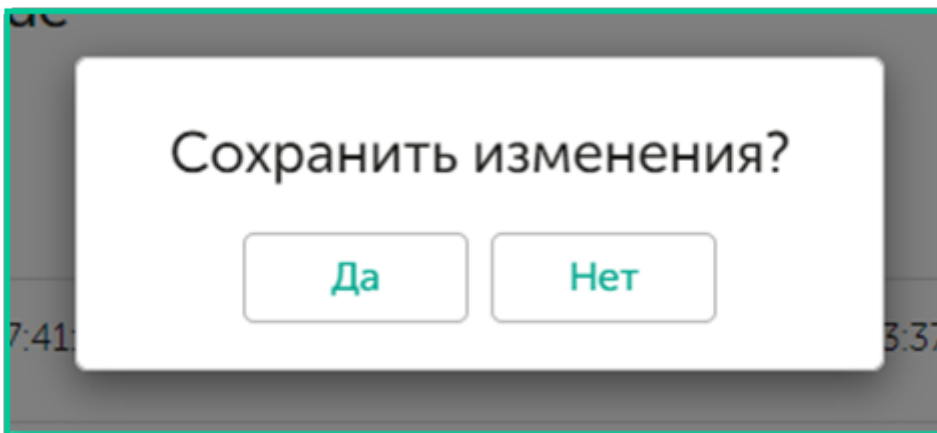
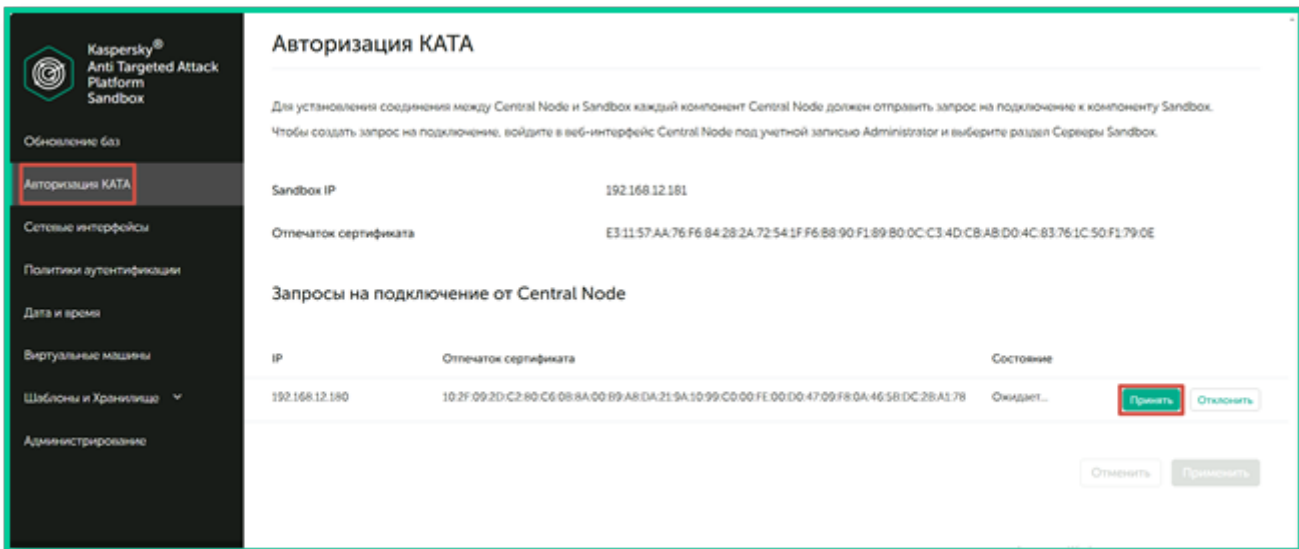
Имя: sandbox

Включить

Рис. 21. Добавление Sandbox в Central Node

7.2. Подтверждение на стороне Sandbox

1. Откройте веб-интерфейс Sandbox.
2. Перейдите в "**Авторизация КАТА**".
3. Найдите запрос от Central Node → нажмите "**Принять**".
4. Нажмите "**Применить**" → подтвердите.
5. Запрос перейдёт в статус "**Принят**".



□ □ **Рис. 22.** Подтверждение подключения в Sandbox

□ **Важно:** После подключения требуется **5-10 минут** на подготовку. Предупреждение в интерфейсе исчезнет автоматически.

8. Настройка набора ОС

1. В **Central Node** перейдите в "**Параметры**" → "**Набор ОС**".
2. Выберите:
 - **Стандартные ОС:** Windows 7, Windows 10
 - **При необходимости:** CentOS, Astra Linux
 - **Пользовательские ОС:** активируйте нужные
3. Нажмите "**Сохранить**".

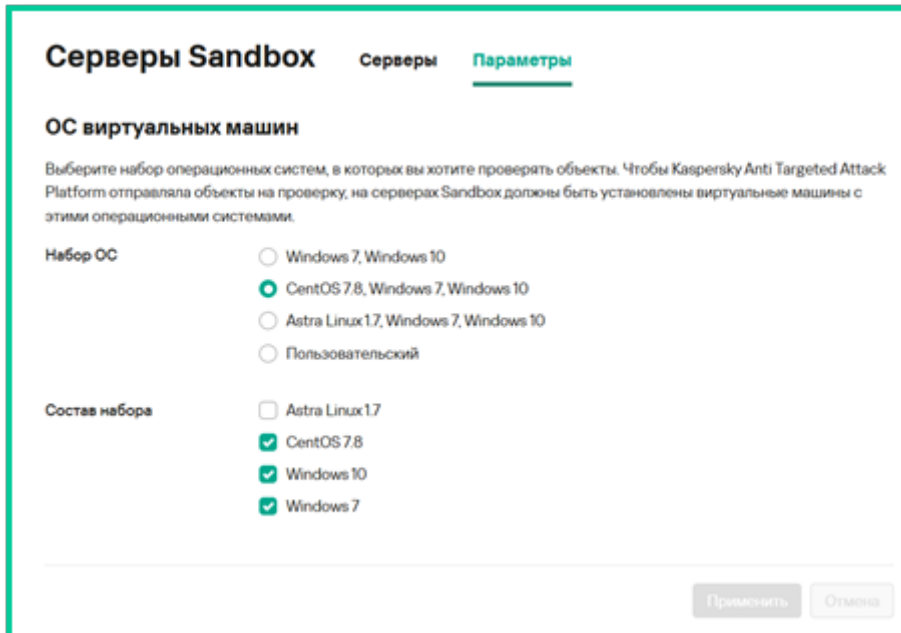


Рис. 23. Настройка набора ОС в Central Node

4. Проверьте статус в разделе "**Серверы Sandbox**".

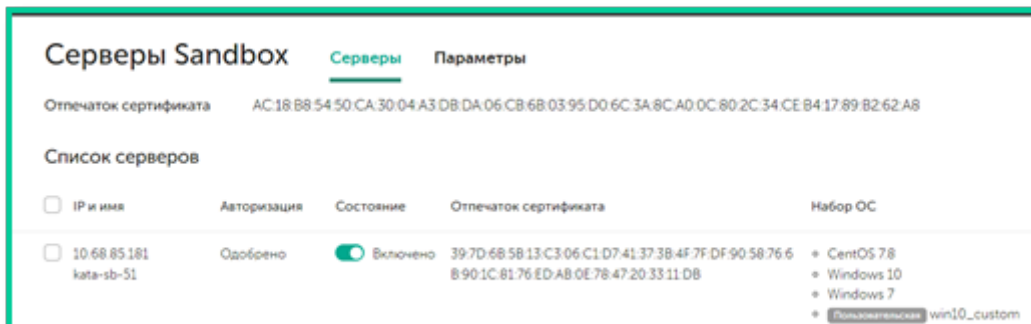


Рис. 24. Статус подключённых образов ОС

Заключение

Установка и настройка компонента **Sandbox** завершена. Компонент готов к анализу подозрительных объектов. Теперь можно:

- Настроить **политики проверки файлов и ссылок**. (Применимо только для пользовательских образов)
- Мониторить поведение угроз в изолированной среде.

Полезные ссылки

- [Работа с шаблонами виртуальных машин](#)
- [Создание виртуальной машины](#)
- [Официальная документация KATA 7.1](#)

Revision #25

Created 22 August 2025 08:35:10 by Николай

Updated 17 April 2026 11:03:31 by Николай