kaspersky

Kaspersky Research Sandbox

Руководство Администратора

kaspersky

О продукте

Kaspersky Research Sandbox 2.0 (далее-Kaspersky Research Sandbox) - это усовершенствованная автоматизированная система анализа вредоносных программ, предназначенная для анализа поведения файлов и обнаружения угроз. Он предлагает гибридный подход, сочетающий разведку угроз, собранную из петабайт статистических данных, поведенческий анализ и надежные технологии борьбы с уклонением и античеловеческим моделированием, такие как автоматический кликер, прокрутка документов и имитационные процессы. Kaspersky Research Sandbox предназначен для ускорения реагирования на инциденты и криминалистической деятельности и может использоваться в качестве локальной системы для автоматической обработки файлов.

Kaspersky Research Sandbox позволяет создавать и настраивать пользовательские среды, а также использовать их для выполнения объектов. Он предоставляет больше возможностей для отображения своей операционной среды. Виртуальные машины Kaspersky Research Sandbox также могут быть подключены к внутренней сети организации. В результате он позволяет выявить вредоносное ПО, предназначенное для работы только в определенной инфраструктуре, и возможность понять его намерения.

После загрузки файла в выбранную среду Kaspersky Research Sandbox исполняет ваш файл, а затем отображает различные результаты, включая графическое представление. Результаты исполнения файла могут быть загружены в виде архивов (все результаты или данные из определенных разделов) для дальнейшего анализа. Кроме того, во время исполнения файла снимаются скриншоты при каждом изменении среды исполнения файла. Вы можете просмотреть скриншоты в своем браузере или загрузить их все в виде архива.

Kaspersky Research Sandbox предоставляет два интерфейса для реализации этого сценария:

- Веб-интерфейс для ручной подачи файлов и анализа результатов

  Вы можете работать с Kaspersky Research Sandbox online с помощью любого из поддерживаемых браузеров. После входа в систему вы можете загружать и выполнять файлы в песочнице.

- RESTful API для автоматизации и интеграции

  Вы можете управлять задачами выполнения файлов и получать результаты выполнения.

Предоставляются следующие предустановленные среды (конфигурации виртуальных машин):

- Операционные системы:
  - Microsoft Windows XP x86
  - Microsoft Windows 7 x86
  - Microsoft Windows 7 x64

    - Microsoft Windows 10 x64
- Мобильные операционные системы:
    - Android ARM
    - Android x86
- Дополнительное ПО:
    - Microsoft Office
    - Adobe Acrobat Reader
    - Браузеры (Microsoft Edge, Microsoft Internet Explorer, Mozilla Firefox)
    - 7-Zip
    - Microsoft .NET Framework
    - Oracle Java

Требования к аппаратному и программному обеспечению

Kaspersky Research Sandbox поставляется предварительно установленным и настроенным на оборудовании заказчика.

Общие требования

- Минимальная установка на одном физическом сервере
- Монитор, поддерживающий разрешение дисплея 1366x768

Конфигурация зависит от требуемой производительности и может быть масштабирована.

Требования к сети

- 2 или более различных канала (настоятельно рекомендуется для обеспечения отказоустойчивости)
- Сетевой канал, используемый для доступа в Интернет исполняемых объектов, должен быть изолирован от локальной сети вашей организации: исполняемый файл может генерировать вредоносную активность, которая может повлиять на ваши локальные сетевые ресурсы
- 100 Мбит / с для каждого канала

- Интернет-провайдер должен быть готов к вредоносным действиям в интернет - трафике
- Исходящий IP-адрес должен меняться каждый день/неделю и быть взят из широкого спектра IP-адресов

Требования к протоколам и портам

Исходящие соединения:

Откройте порт 443 (HTTPS) для Kaspersky Private Security Network

Откройте порт 80 (HTTP) для обновленных компонентов (необязательно)

Входящие соединения:

Откройте порт 443 (HTTPS) для пользователей (веб - интерфейс и Restful API)
Откройте 22 (SSH) порта для администраторов Kaspersky Research Sandbox

Интеграция с Kaspersky Private Security Network

Kaspersky Research Sandbox поддерживает интеграцию с Kaspersky Private Security Network 3.1.

Освобождение места на жестком диске

Выполнение файла может завершиться неудачей, если на жестком диске недостаточно свободного места. При необходимости вы можете освободить место на жестком диске, удалив ненужные результаты выполнения файлов и экспортированные архивы шаблонов/

Процесс установки

Подготовка к установке

Для процесса установки вы должны иметь под рукой следующую информацию.

Лицензионное соглашение с конечным пользователем (EULA)

Лицензионное соглашение KRS входит в комплект поставки и должно быть подписано клиентом по электронной почте.

Требования к оборудованию

Рекомендуемые:
Технические характеристики сервера: 2 x Intel Xeon E5 (40 lCPU), 192 ГБ оперативной памяти, 4 x 1 ТБ HDD RAID 10, 2 x 1 Гбит / с NIC (с возможностью расширения хранилища данных)
Количество слотов: не менее 40:

Технические характеристики сервера: 12 процессоров Intel, 32 ГБ оперативной памяти, 2 x 500+ ГБ HDD RAID 1, 1 Гбит / с
Количество слотов NIC: 6
KRS не гарантирует правильную работу на виртуальных машинах! Экземпляры для тестирования могут пытаться использовать только виртуальные машины:

Требования и настройки гипервизора:

- Хост-машина должна иметь процессор Intel
- KRS VM должна иметь включенную аппаратную виртуализацию, в VMware эта настройка называется CPU – Expose hardware-assisted virtualization to guest OS
- Виртуальная машина KRS должна иметь настроенное резервирование распределения ресурсов
- Виртуальная машина RMS должна быть связана только с одним узлом NUMA, в VMware этот параметр называется numa.node Affinity VM & RMS configuration:
- 12 логических ядер процессора
- 16 ГБ оперативной памяти
- Жесткий диск :300 ГБ
- Количество слотов: 6

Параметры сети

Важно: Вы должны отключить любое использование Wi-Fi, Bluetooth или NFC-соединений на главном компьютере RMS.

Наиболее вероятный случай с клиентами заключается в том, что вам понадобится один вредоносный интерфейс и один шлюз.
Все необходимые восходящие линии интерфейса должны быть подключены к соответствующим сетям VLAN.
Если вы хотите использовать интерфейс в качестве вредоносного интерфейса, вы должны иметь и восходящую линию связи на нем, в идеале в VLAN, отличной от интерфейса управления VLAN.
Для каждого интерфейса (управляющего или вредоносного) вы должны знать его сетевой IP-адрес и сетевую маску.
Для интерфейса управления вы также должны знать IP-адрес шлюза по умолчанию.
Интерфейс управления может получить эти настройки от DHCP, если он настроен.

Для каждого вредоносного интерфейса вы должны знать следующее:

1. Если вам нужен какой-то канал вредоносного ПО в KRS для доступа в Интернет с помощью этого интерфейса вредоносного ПО: шлюз (- ы), который позволяет получить доступ в Интернет.
2. Если вам нужен какой-то вредоносный канал в KRS для доступа к локальной/доменной сети с помощью этого вредоносного интерфейса:
    a. Если вам нужен маршрут локальной/доменной сети(-ы), возможно, вы используете дополнительный шлюз(-ы), вы должны знать сетевой IP-адрес/префикс маршрутизатора (например 10.70.29.0/24) и опционально шлюз. В большинстве случаев он доступен, это соответствует IP-адресу подсети вредоносного интерфейса и префиксу (маске сети).
    б. Если вам нужно разрешить локальные/доменные адреса и присоединить виртуальные компьютеры к домену, вы должны знать IP-адреса контроллеров домена /серверов имен локальных сетей и соответствующие доменные зоны.
    В противном случае корневые DNS-серверы будут использоваться для разрешения через интернет-шлюз (см.)

Источник обновления антивирусных баз

Вы можете настроить KRS для получения обновлений одним из следующих способов:
1. KRS загружает AV-базы непосредственно из общедоступного источника обновлений Kaspersky. Это возможно в том случае, если шлюз по умолчанию интерфейса управления разрешает доступ в Интернет, а его DNS-серверы разрешают доменные имена Интернета. Этот случай маловероятен.
2. То же самое, что и 1, но с использованием HTTP-прокси, с базовой аутентификацией опционально. У вас должен быть адрес/порт HTTP-прокси и, возможно, учетные данные. Он должен быть доступен из интерфейса управления.
3. KRS загружает AV-базы с локального зеркала источника обновления в сети клиента. У вас должен быть зеркальный адрес/порт и, возможно, учетные данные. Он должен быть доступен из интерфейса управления.
Вы должны иметь зеркало, настроенное и настроенное для синхронизации обновлений из источника Kaspersky, обычно с помощью утилиты Kaspersky Update Utility и некоторого HTTPServer, обслуживающего каталог обновлений. Этот случай наиболее вероятен.
4. То же самое, что и 3, но с использованием HTTP-прокси для доступа к локальному зеркалу.

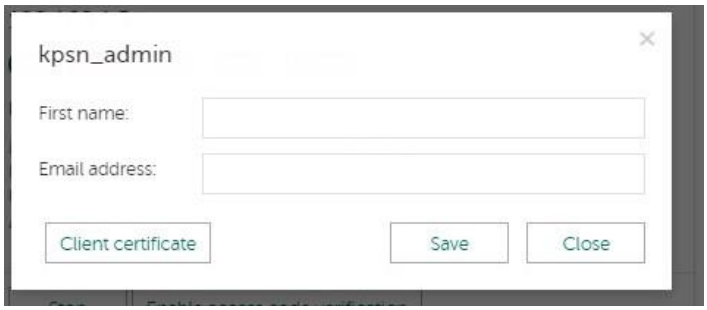
Пожалуйста, используйте следующий URL-адрес источника обновления для всех новых установок:
http://opsb.kaspersky-labs.com/ced2f99465a90733c5c2e9f2196b671512154b1a/

Интеграция с KPSN

KRS интегрируется с KPSN,установленным локально в сети заказчика.
URL-адрес KPSN HTTPS API должен быть доступен из интерфейса управления. Если он содержит доменное имя, он должен разрешаться на DNS-серверах интерфейса управления.
Обычно это выглядит так: https://kpsn.example.com:80/api/
Аутентификация клиента SSL/TLS должна быть настроена в KPSN. Необходимо получить следующие файлы в формате PEM: kpsn_client
.crt – KPSN SSL/TLS клиентский сертификат kpsn_client.key – KPSN SSL/TLS клиентский ключ kpsn_server.crt – KPSN SSL/TLS серверный сертификат, который является доверенным
Чтобы получить эти файлы из вашей установки KPSN, вам необходимо выполнить следующие действия:
1. Переключите KPSN в режим HTTPS (Инструкция доступна в руководстве KPSN PoC guide)
2. Переименуйте загруженный SSL-сертификат сервера в kpsn_server.crt. Если вы потеряли загруженный SSL-сертификат сервера, выполните следующие действия:
a. Откройте HTTPS-сертификат в веб-браузере.

b. Экспортируйте его в kpsn_server.crt [WIP]

3. Введите в веб-интерфейсе KPSN: Перейдите в kpsn_admin → Мой профиль → Сертификат клиента



4. Переименуйте загруженные файлы:
    a. kpsn_admin_cert.pem -> vpn_client.crt
    b. kpsn_admin_key.pem -> kpsn_client.key

Вам нужно будет загрузить эти 3 файла на машину KRS в каталог /home/krs admin/ позже в разделе 3.2 шаги консоли управления.

2.6. TLS-сертификаты интерфейса

Если вы хотите, чтобы HTTPS-соединение KRIS Web UI и API было безопасным ("зеленым" в браузере клиента), следующие файлы в формате PEM должны быть получены из центра сертификации PKI клиента:

- front_server.crt – SSL/TLS public certificate for server frontend
- front_server.key – SSL/TLS key for server frontend

Вам нужно будет загрузить эти 2 файла на машину KRS в каталог /home/krs admin/ позже в разделе 3.2 шаги консоли управления.

В противном случае, вы можете использовать самозаверяющие сертификаты, которые будут сгенерированы в процессе установки.

2.7 Загрузочный файл и инсталляция

Если вы хотите запустить установку непосредственно на хост-компьютере, вам следует создать установочный USB-накопитель. Этот процесс подробно описан здесь: Руководство по установке RHEL7, Глава 3.2. Создание установочного USB-носителя, но вам необходимо использовать USB-жесткий диск размером не менее 40 ГБ. Возможно, использование Rufus на Windows будет более полезным и простым. Вставьте загрузочный носитель в ваш сервер.

Если вы хотите использовать консоль дистанционного управления KVM для установки на вашем хост-компьютере, вы можете:

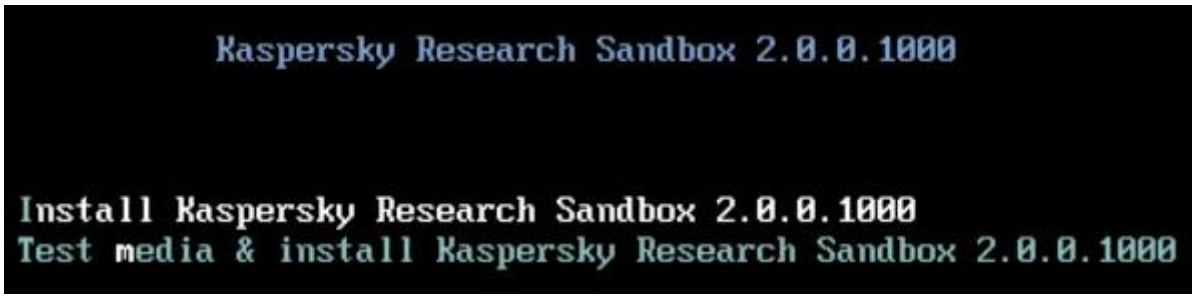
- создать установочный USB-накопитель, как описано выше, или прикрепите ISO-файл в качестве виртуального носителя и загрузите его.Дополнительные сведения см. в документации, прилагаемой к вашему серверу.
- Примечание: использование виртуальных носителей может значительно замедлить процесс установки (см. 3.1.7 Завершение начальной установки)

3. Процесс установки

3.1. Этапы загрузки и начальной установки

Включите питание на вашем сервере. Вам нужно нажать определенную клавишу или комбинацию клавиш для загрузки с носителя или настроить BIOS вашей системы для загрузки с носителя. Дополнительные сведения см. в документации, прилагаемой к вашему серверу.

Как только ваша система завершит загрузку загрузочного носителя, появится меню загрузки. Меню загрузки содержит несколько вариантов загрузки. Если в течение 60 секунд не будет нажата ни одна клавиша, будет запущена опция загрузки по умолчанию (выделенная белым цветом). Чтобы выбрать значение по умолчанию, либо дождитесь окончания таймера, либо нажмите клавишу Enter.

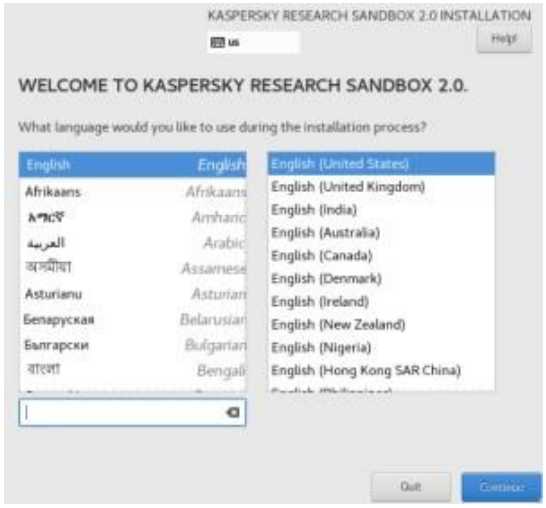


- Установите Kaspersky Research Sandbox
  Выберите этот параметр, чтобы установить KRS в вашу компьютерную систему с помощью графической программы установки.

- Протестируйте этот носитель и установите Kaspersky Research Sandbox
  Этот параметр используется по умолчанию. Перед запуском программы установки запускается утилита для проверки целостности установочного носителя.

  После завершения загрузки системы запускается графический установщик (Anaconda) и отображается экран приветствия:

После завершения загрузки системы запускается графический установщик (Anaconda) и отображается экран приветствия:



Выберите английский язык и регион Английский (Соединенные Штаты) и нажмите кнопку Продолжить.

Далее будет показан экран Сводки установки. Это центральный экран для установки параметров конфигурации:

Установщик позволяет настроить вашу установку, открывая и настраивая subscreens в произвольном порядке, однако более полезно сначала настроить сеть и имя хоста, а затем все остальное.

Ничего не будет записано на диск, пока вы не нажмете кнопку «Начать установку».

3.1.1. Имя хоста и сеть

Пожалуйста, сначала внимательно прочтите глоссарий и предварительные условия, приведенные выше.

Этот экран очень похож на экран CentOS 7 / RHEL 7. Пожалуйста, обратитесь к Руководству по установке RHEL 7, глава 8.12. Сеть и имя хоста для получения полных инструкций по настройке сети для более сложных случаев.

Вы должны настроить один и только один интерфейс управления. Другие интерфейсы должны быть отключены (даже если вы знаете, что будете использовать его в качестве вредоносного интерфейса). Интерфейсы вредоносных программ будут настроены позже в консоли управления.

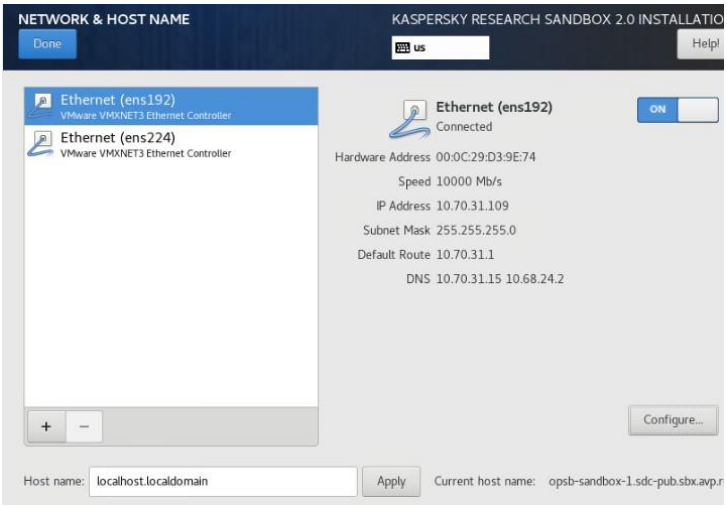
Вы должны выбрать интерфейс, предназначенный для интерфейса управления, и настроить его, нажав кнопку Configure.

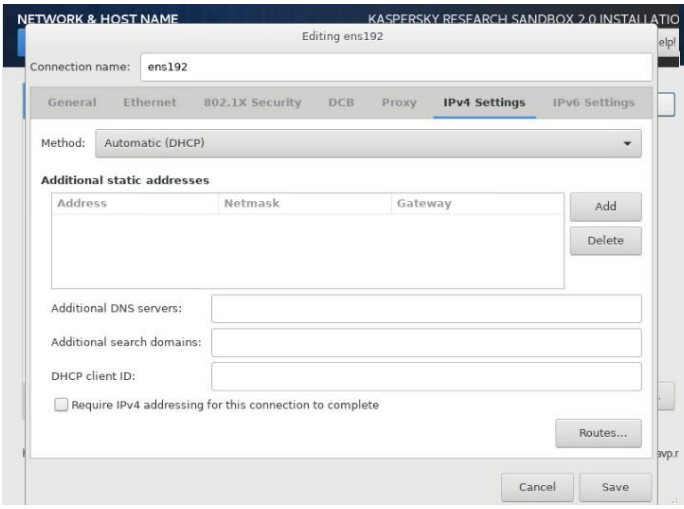
Затем перейдите на вкладку Настройки IPv4 и выберите метод:

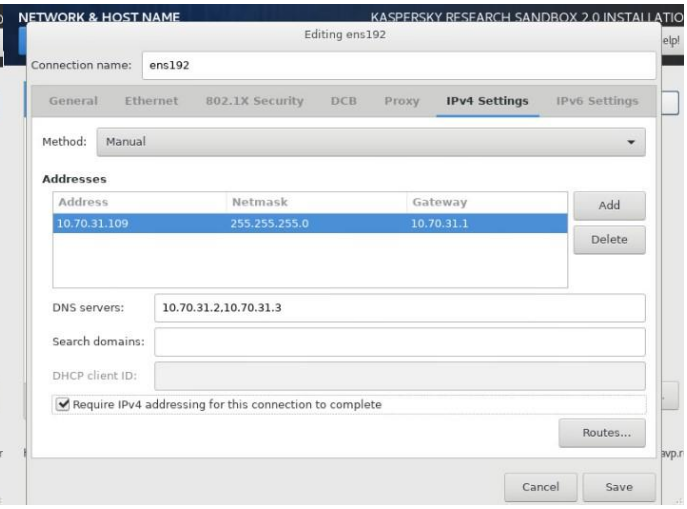
- Автоматический (DHCP) – если у вас есть DHCP в сети клиентов, вы можете использовать автоматически назначенные значения.
- Ручное управление и настройка IP, маски сети, шлюза и DNS вручную.

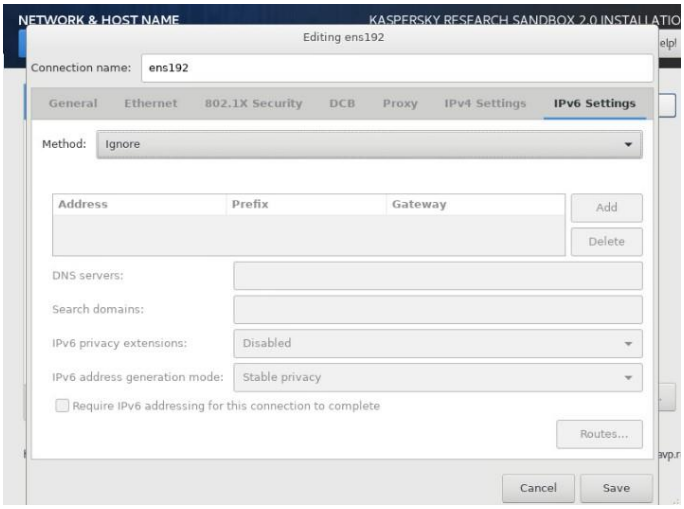
Затем перейдите на вкладку Настройки IPv6 и выберите метод: Игнорировать Вы также должны ввести имя хоста на главном экране сети и применить его.

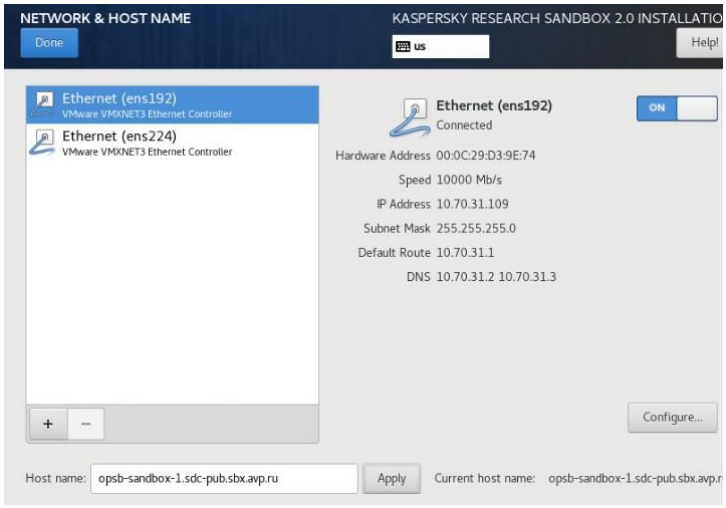
Примеры скриншотов для справочной конфигурации:

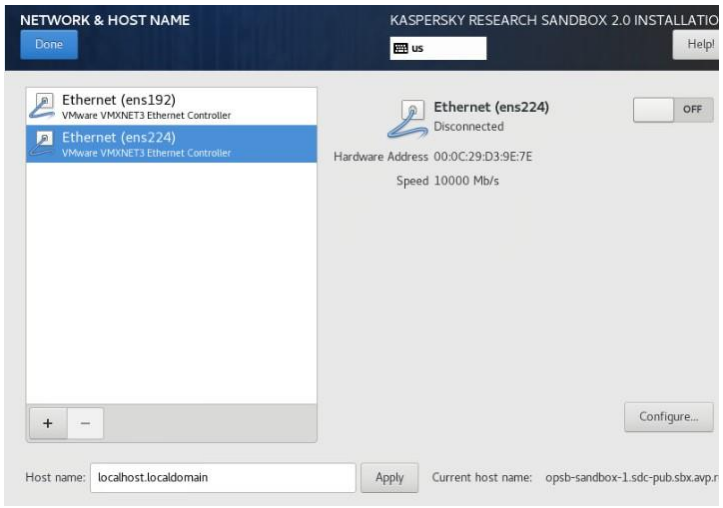

NETWORK & HOST NAME
Done
KASPERSKY RESEARCH SANDBOX 2.0 INSTALLATIO
us
Help!
Ethernet (ens192)
VMware VMXNET3 Ethernet Controller
Ethernet (ens224)
VMware VMXNET3 Ethernet Controller
Ethernet (ens192)
Connected
ON
Hardware Address 00:0C:29:D3:9E:74
Speed 10000 Mb/s
IP Address 10.70.31.109
Subnet Mask 255.255.255.0
Default Route 10.70.31.1
DNS 10.70.31.15 10.68.24.2
Configure...
Host name: localhost.localdomain
Apply
Current host name: opsb-sandbox-1.sdc-pub.sbx.avp.r


NETWORK & HOST NAME
KASPERSKY RESEARCH SANDBOX 2.0 INSTALLATIO
Editing ens192
Connection name: ens192
General
Ethernet
802.1X Security
DCB
Proxy
IPv4 Settings
IPv6 Settings
Method: Automatic (DHCP)
Additional static addresses
Address
Netmask
Gateway
Add
Delete
Additional DNS servers:
Additional search domains:
DHCP client ID:
Require IPv4 addressing for this connection to complete
Routes...
Cancel
Save


NETWORK & HOST NAME
KASPERSKY RESEARCH SANDBOX 2.0 INSTALLATIO
Editing ens192
Connection name: ens192
General
Ethernet
802.1X Security
DCB
Proxy
IPv4 Settings
IPv6 Settings
Method: Manual
Addresses
Address
Netmask
Gateway
10.70.31.109
255.255.255.0
10.70.31.1
Add
Delete
DNS servers: 10.70.31.2,10.70.31.3
Search domains:
DHCP client ID:
Require IPv4 addressing for this connection to complete
Routes...
Cancel
Save

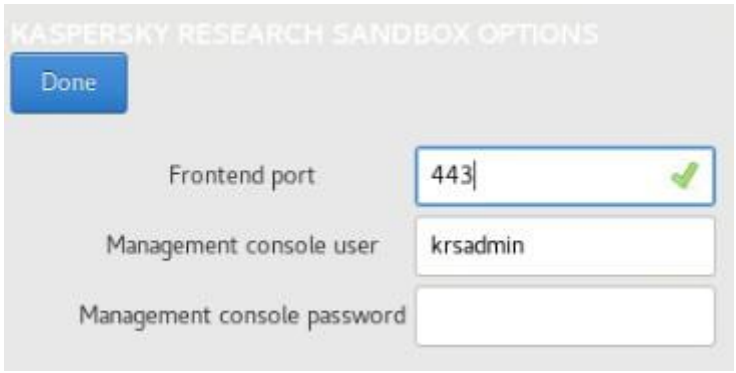

NETWORK & HOST NAME
KASPERSKY RESEARCH SANDBOX 2.0 INSTALLATIO
Editing ens192
Connection name: ens192
General
Ethernet
802.1X Security
DCB
Proxy
IPv4 Settings
IPv6 Settings
Method: Ignore
Address
Prefix
Gateway
Add
Delete
DNS servers:
Search domains:
IPv6 privacy extensions: Disabled
IPv6 address generation mode: Stable privacy
Require IPv6 addressing for this connection to complete
Routes...
Cancel
Save





После внесения изменений нажмите кнопку Готово, чтобы вернуться на экран Итогов установки.

3.1.2. Настройки KRS



Frontend порт: TCP-порт, на котором будут доступны KRS Web UI и API. Значение по умолчанию-443, но вы можете установить его на какое-то другое значение в диапазоне 165535. Следующие значения портов не допускаются: 22, 25, 111, 5432, 8443, 44999, 8181-8187

Пользователь консоли управления: Он показан только для справки и не поддается изменению.

Пароль консоли управления: Пароль пользователя rsadmin для последующего доступа к консоли управления.
Доступ к консоли управления обычно осуществляется через SSH, так что это также SSH user/password.

После внесения изменений нажмите кнопку «Готово», чтобы вернуться на экран Сводки установки.

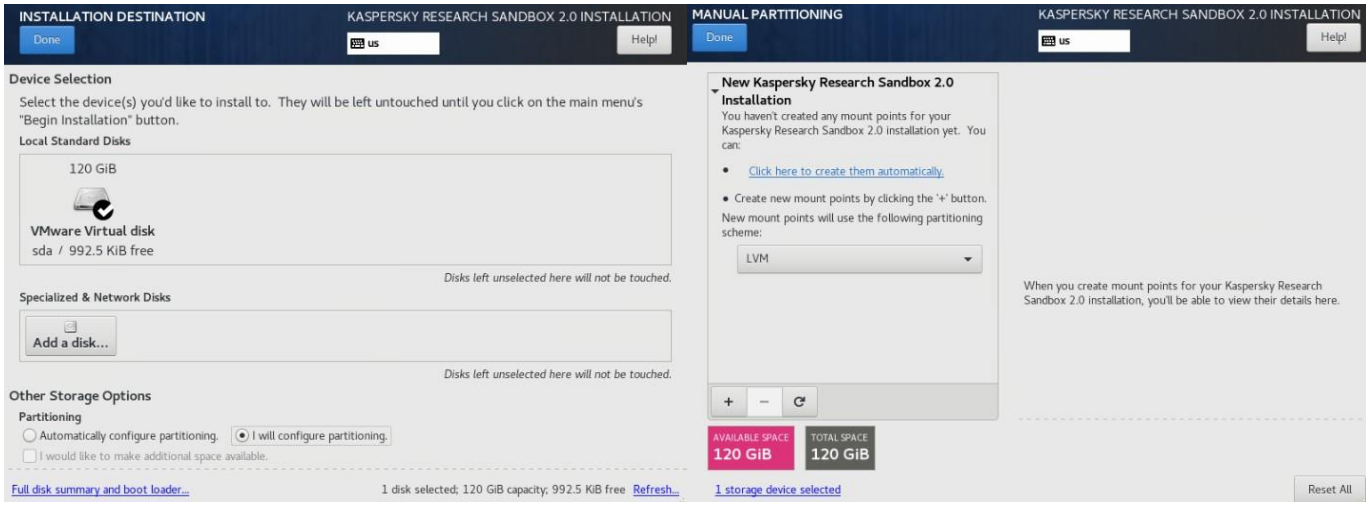
3.1.3 Местоположение инсталляции

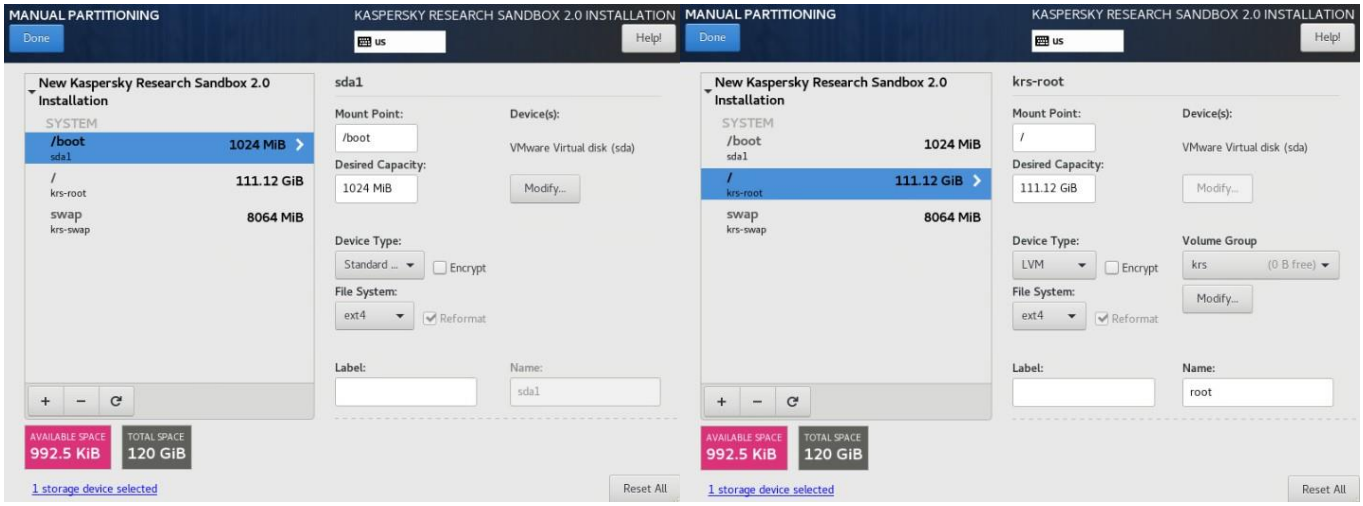
Этот экран очень похож на экран CentOS 7 / RHEL 7. Пожалуйста, обратитесь к Руководству по установке RHEL 7, глава 8.14. Место установки для получения полных инструкций по разделению для более сложных случаев.

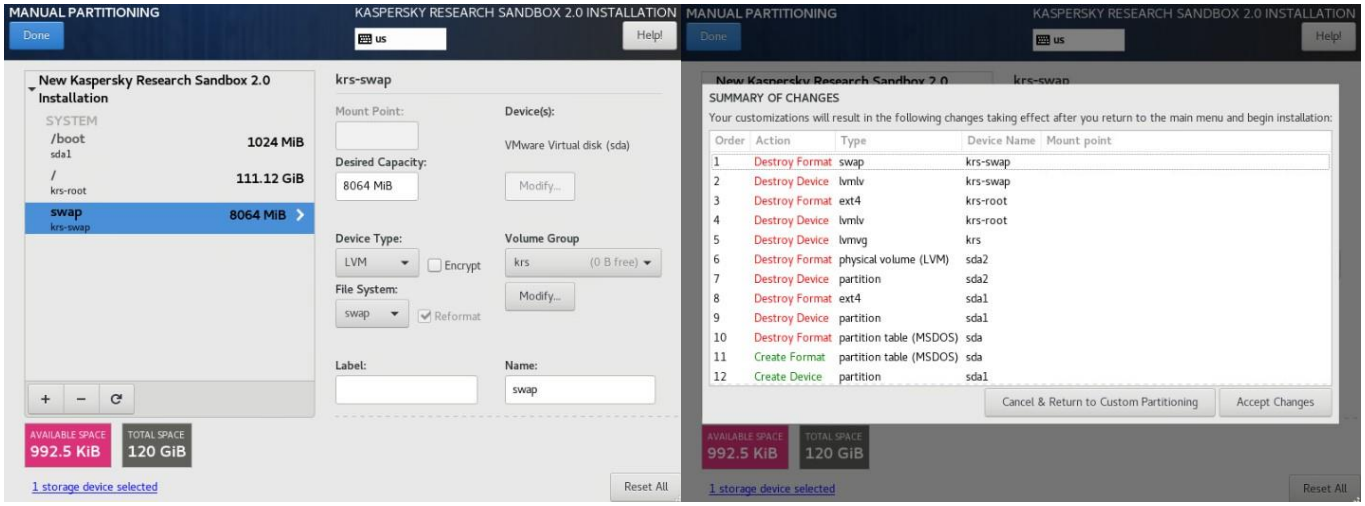
Вы должны настроить таблицу разделов вручную и создать следующие разделы LVM с файловой системой ext4:

- /home – Он не нужен, удалите его.
- /boot – 1024 MiB swap – Для аппаратных серверов с оперативной памятью > 100 ГБ установите значение ниже 10 ГБ. Для виртуальных машин достаточно 1-2 ГБ свопа.
- / (root) – Все остальное доступное пространство. Он должен быть не менее 300 ГБ.

Примеры скриншотов для справки:







После внесения изменений нажмите кнопку Готово, чтобы вернуться на экран Сводки установки.

3.1.4 Начало первичной установки

Когда все будет настроено на экране Сводки установки, нажмите кнопку Начать установку в правом нижнем углу.

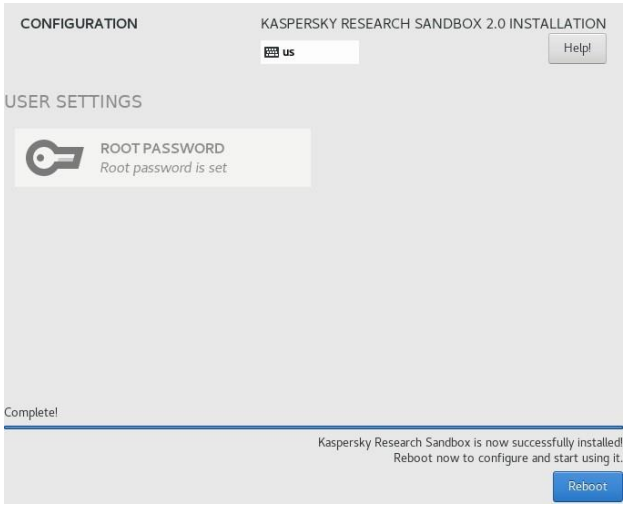
Установка началась. Он разделит диск, установит все необходимые пакеты и установит настроенные параметры. (Если сервер поддерживает EFI, то используется загрузчик GRUB. Если сервер работает только в BIOS, то используется загрузчик EXTLINUX/SYSLINUX.) Вы увидите второй экран, называемый Конфигурацией.

3.1.5 Итог первичной установки

После того как все шаги будут настроены, дождитесь завершения процесса установки.

Процесс установки может занять значительное количество времени (от 30 минут до ~8 часов, зависит от полосы пропускания подключения к установочному носителю), особенно если вы используете пульт дистанционного управления KVM консолью с загрузкой виртуального носителя.

Самый длинный шаг установки - это настройка аддонов, поскольку он копирует большие образы виртуальных машин с смонтированного загрузочного носителя ISO. Пожалуйста, не закрывайте окно KVM и просто ждите его завершения.



После завершения установки нажмите кнопку Перезагрузка. Извлеките установочный носитель во время перезагрузки.

Настройте загрузку с локального жесткого диска в BIOS (если это не используется по умолчанию).

Выберите CentOS Linux в загрузчике и дождитесь его загрузки. Вам будет предложено войти в систему.

3.2 Консоль управления

После загрузки вы должны войти на сервер, используя следующие учетные данные:

Логин: `krsadmin`

Пароль: пароль, который вы ввели на шаге настройки KRS. Он не будет показан по соображениям безопасности.

Вы также можете войти в систему удаленно через SSH (если настроенный интерфейс управления доступен в сети), используя следующую команду:

```
ssh krs admin@<hostname>
```

Замените `@<hostname>` вашим фактическим именем хоста.

Вам будет предложено продолжить установку в консоли управления. Он используется для интерактивной настройки установленных KRS. Следуйте подсказкам из следующей таблицы, чтобы ответить на все ее вопросы.
Ответ требует ввода буквы Y или N, соответствующей Да или Нет. По умолчанию используется заглавная буква (вы можете просто нажать enter, чтобы принять ее без ввода).

Вы также можете использовать ту же консоль управления для последующей перенастройки KRS. Для этого войдите в систему как `krsadmin` и введите:

```
sudo /opt/kaspersky/sandbox/bin/sbsetup management-console
```

3.3 Доступ к веб-интерфейсу

По окончанию настройки, вы можете получить доступ к веб-интерфейсу KRS, открыв `https://<hostname>` в веб-браузере.

В случае, если 443 – не порт интерфейса вы должны открыть `https://<hostname>:<frontend_port>`

Введите логин и пароль администратора для веб-интерфейса, который был предоставлен в комплекте поставки

- Логин администратора по умолчанию: admin

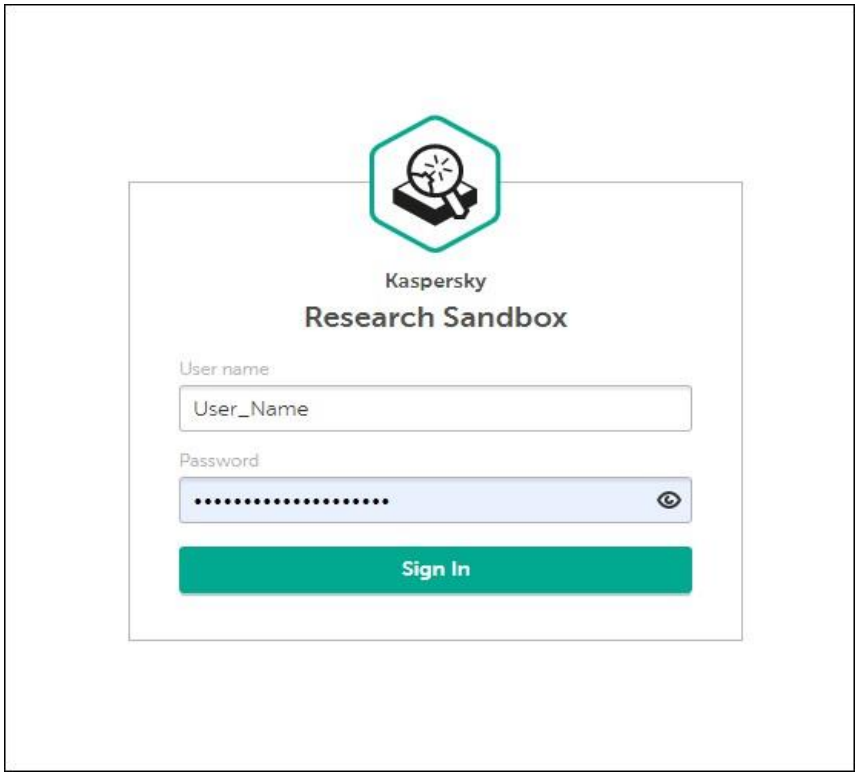
Затем обратитесь к интегрированной онлайн - справке по использованию KRS.

Администрирование Kaspersky Research Sandbox

Вход в Kaspersky Research Sandbox

В этом разделе объясняется, как войти в Kaspersky Research Sandbox. Когда вы входите в систему Kaspersky Research Sandbox впервые вы должны принять Лицензионное соглашение с конечным пользователем (EULA).

Чтобы войти в Kaspersky Research Sandbox:
1. В адресной строке браузера введите следующую ссылку: https://<адрес Kaspersky Research Sandbox >. Здесь <адрес Kaspersky Research Sandbox> - это имя хоста или IP-адрес компьютера, на котором установлена Kaspersky Research Sandbox.
2. Введите имя пользователя и пароль, полученные от администратора Kaspersky Research Sandbox.
3. Нажмите кнопку **Sign in**.



Вход в Kaspersky Research Sandbox может завершиться неудачно по одной из следующих причин:

- Имя пользователя или пароль неверны.
- Ваша учетная запись пользователя заблокирована.

Количество попыток аутентификации на веб-портале не ограничено.

После успешного входа в Kaspersky Research Sandbox можно выполнять файлы, просматривать и экспортировать результаты выполнения, а также создавать пользовательские образы для последующего использования в качестве среды выполнения файлов.

Выход из Kaspersky Research Sandbox

Когда вы закончите работу с Kaspersky Research Sandbox, вы должны выйти из приложения.

Чтобы выйти из Kaspersky Research Sandbox,

В окне браузера откройте меню учетная запись и нажмите кнопку **Sign out**.
После того как вы вышли из системы, в окне браузера появится страница входа.

Интерфейс Kaspersky Research Sandbox

В этом разделе описаны основные элементы интерфейса Kaspersky Research Sandbox.

Страница Sandbox

На странице Песочницы Kaspersky Research Sandbox вы можете загрузить вредоносный или, возможно, зараженный файл, чтобы выполнить его в безопасной среде Kaspersky Research Sandbox.

При необходимости можно выбрать требуемую среду выполнения (операционную систему) и другие параметры выполнения файла.

После того как файл будет выполнен и проанализирован Kaspersky, результаты отображаются в таблице результатов последнего выполнения файла. Вы можете открыть результаты выполнения файлов других пользователей по прямой ссылке.

В таблице отображается следующая информация для каждого исполненного файла:

Zone — Зона исполняемого файла:

Clean — Выполнение задачи завершено; объект не является вредоносным.

Malware — Выполнение задачи завершено; объект является вредоносным.

Adware and other — Выполнение задачи завершено; объект может быть классифицирован как «не вирус».

Not categorized — Задача исполнения выполнена; информация об объекте отсутствует.

Created — Дата и время начала исполнения объекта.

Status— Состояние задачи исполнения объекта:

In progress — Выполняется задача исполнения.

Completed — Процесс загрузки и исполнения успешно завершен.

<Error message> — Ошибка произошла во время исполнения объекта. Для получения более подробной информации об ошибках задачи обратитесь к разделу Ошибки выполнения задачи.

Для исполненного файла можно выполнить следующие действия:

View details— Открывает страницу результатов выполнения для выбранного объекта.

Export all results — Открывает раскрывающееся меню, в котором можно выбрать формат файла, в который вы хотите экспортировать результаты расследования: STIX, JSON archive, CSV archive, PDF и PCAP. Вы также можете выбрать пункт **Загрузить** отчет об отладке, чтобы загрузить архив, содержащий отчет об отладке. Этот пункт доступен только в том случае, если при создании задачи выполнения файла был установлен флажок **Создать отладочный отчет**.

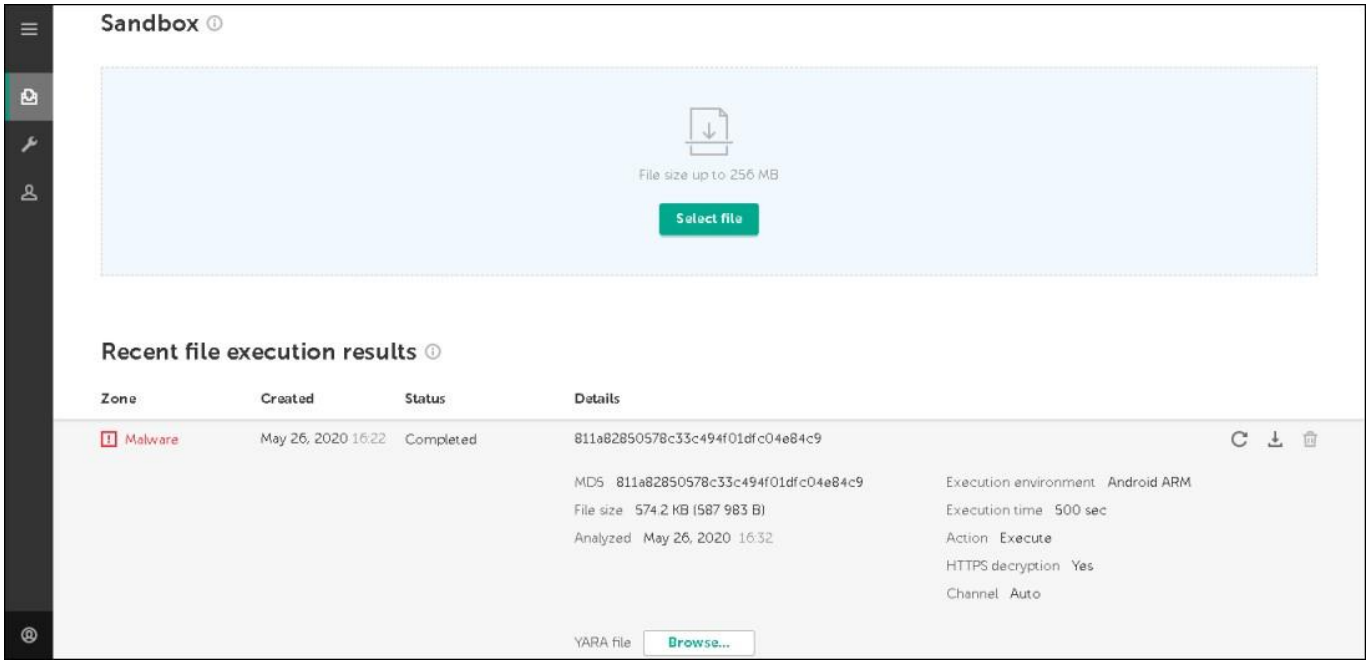
Если анализ объекта выполняется, ссылки Просмотр сведений и Экспорт всех результатов не отображаются.

Rescan— Повторяет выполнение выбранного объекта. Вы можете изменить параметры выполнения для выбранного объекта.

Delete — Удаляет результаты выполнения объекта.

Browse — Выбор файла YARA.

Если администратор Kaspersky Research Sandbox удалил результаты выполнения задач с жесткого диска сервера во время технического обслуживания Kaspersky Research Sandbox, информация об этих задачах по-прежнему отображается в таблице **Результат исполнения последних файлов**, но вы не можете просмотреть или экспортировать результаты выполнения этой задачи. Кроме того, вы не можете повторить выполнение файла, нажав кнопку **Повторное сканирование**. Соответствующие кнопки недоступны. Чтобы повторить выполнение, вам нужно снова загрузить файл.



Вкладка Шаблоны

На вкладке Шаблоны можно просматривать шаблоны для создания пользовательских сред выполнения и управлять ими.

Для каждого шаблона отображается следующая информация:

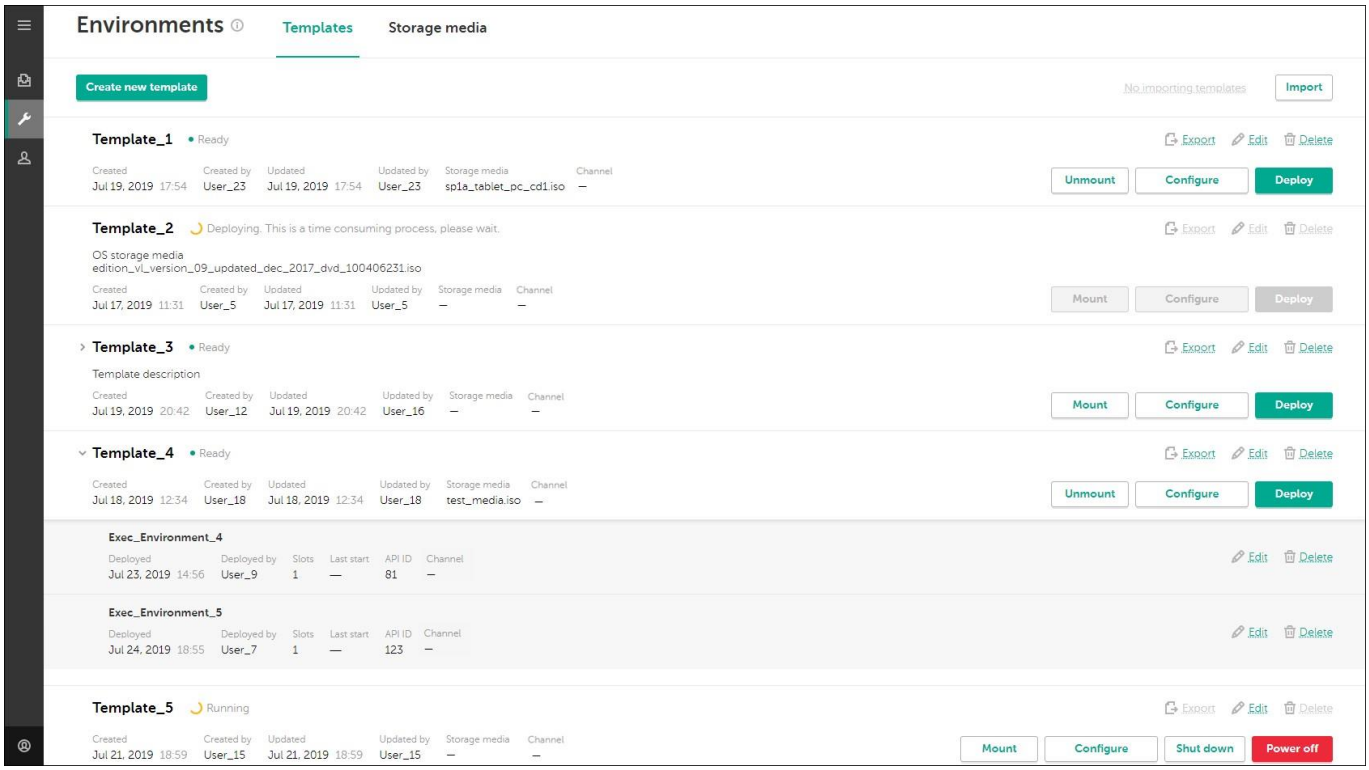
- Имя шаблона.
- Метка, указывающая состояние шаблона.
- Описание шаблона (если имеется). Вы можете отредактировать описание в любое время.
- **Created** — Дата и время создания шаблона.
- **Created by** — Логин пользователя, создавшего шаблон.
- **Updated** — Дата и время обновления шаблона.
- **Updated by** — Логин пользователя, обновившего шаблон.
- **Storage media** (если имеется)—носитель информации, используемый для шаблона.
- **Channel** — Сетевой канал, используемый для доступа в Интернет. Kaspersky Research Sandbox отображает канал, указанный при создании или редактировании шаблона. Если сетевой канал не выбран, отображается символ —.

При настройке и развертывании шаблона для среды выполнения отображается следующая информация:

Title — Пользовательское название среды.
Description — Пользовательское описание среды.
Deployed — Дата и время развертывания шаблона в песочнице Kaspersky Research.
Deployed by — Логин пользователя, развернувшего шаблон.

Slots — Количество слотов (максимальное количество задач выполнения файлов, которые могут одновременно выполняться в пользовательской среде).
Last start — дата и время последнего использования пользовательской среды в задаче выполнения файла.
API ID — Пользовательский идентификатор среды, используемый в качестве значения параметра exec_env в API песочницы Kaspersky Research.
Channel — Сетевой канал, используемый для доступа в Интернет. Kaspersky Research Sandbox отображает канал, указанный в начале процесса развертывания. Если сетевой канал не выбран, отображается символ—.

Вы можете редактировать и удалять пользовательские среды выполнения.
Для шаблонов доступны следующие действия:
Export — Вы можете загрузить выбранный шаблон в виде архива .tar.
Edit — Вы можете редактировать заголовок и описание выбранного шаблона.
Delete — Вы можете удалить выбранный шаблон.
Mount — Вы можете монтировать выбранный шаблон.
Configure — Вы можете настроить выбранный шаблон.
Deploy — Вы можете развернуть выбранный шаблон.
Также на вкладке Шаблоны можно создавать или импортировать шаблоны в Kaspersky Research Sandbox, а также просматривать и останавливать активные процессы импорта.

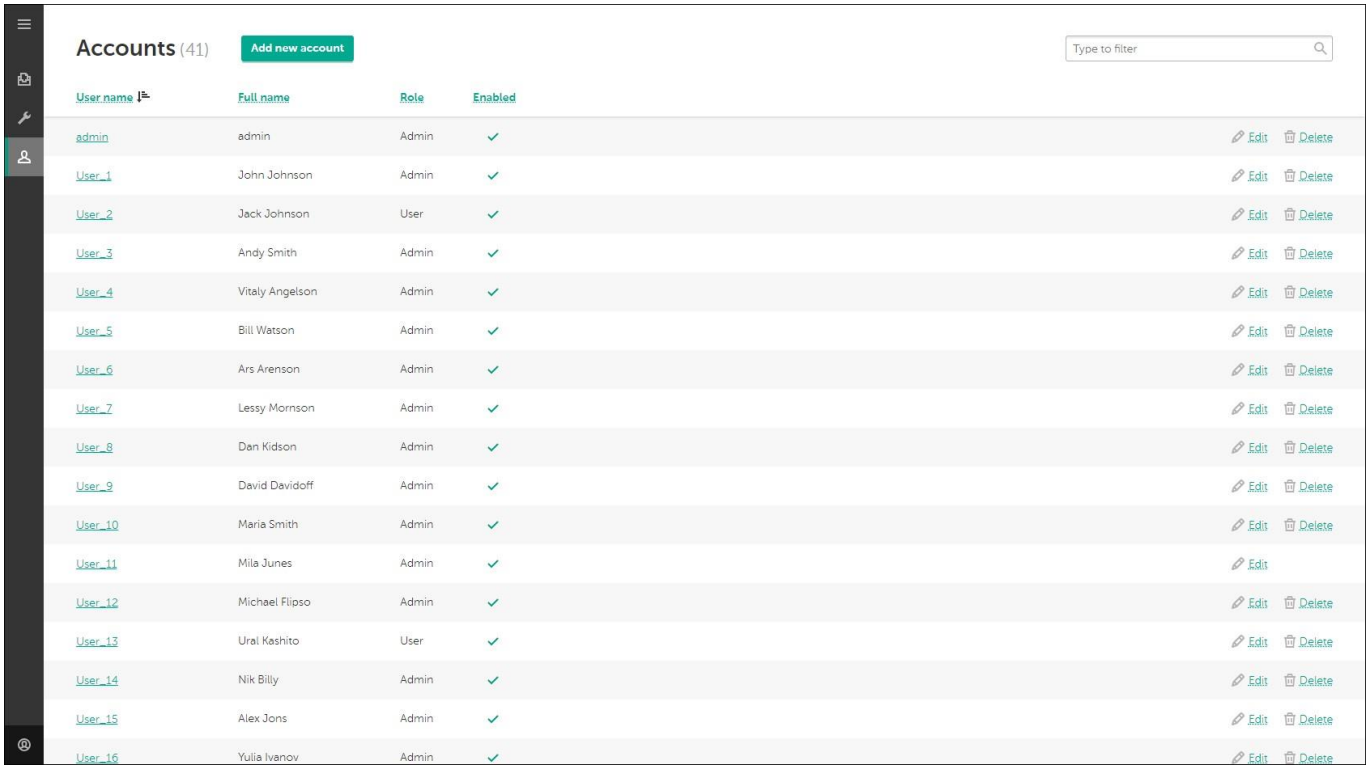


Страница аккаунтов

Страница **Accounts** доступна только для пользователей Kaspersky Research Sandbox с правами администратора (`Role=Admin`).

На странице **Accounts** вы можете управлять учетными записями своей компании. Вы можете добавлять новые учетные записи, изменять настройки для определенных учетных записей или удалять их.

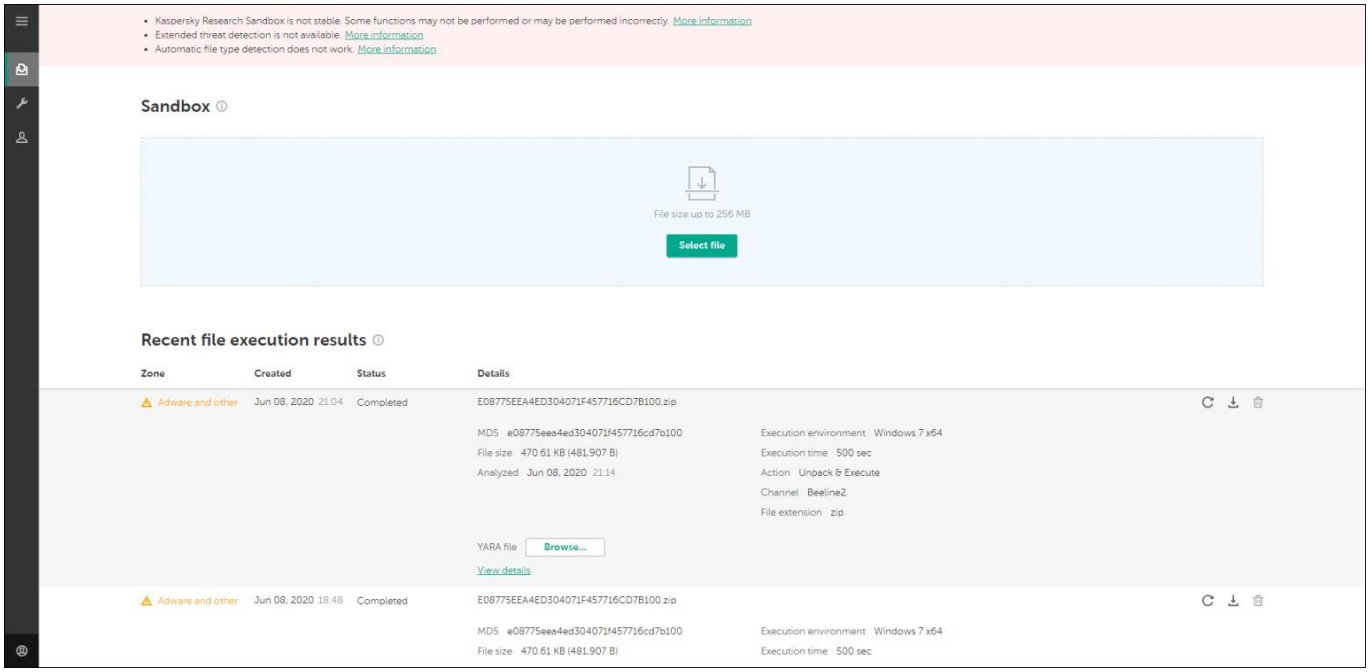
Вы можете искать конкретную учетную запись или сортировать элементы в таблице по имени пользователя (login), полному имени, роли или по полю **Enabled** в порядке убывания или возрастания.



Мониторинг сообщений

Сообщения мониторинга песочницы Kaspersky Research могут появляться в верхней части страницы. Сообщение отображается во всех разделах (**Sandbox**, **Environments** или **Accounts**) до тех пор, пока проблема не будет решена.

Для получения более подробной информации о сообщениях мониторинга обратитесь к разделу **Диагностика.**



Запуск исполнения файла

Перед выполнением файла в Kaspersky Research Sandbox необходимо загрузить его и выбрать параметры выполнения.

Чтобы выполнить файл в песочнице Kaspersky Research Sandbox:

1. На странице **Sandbox** Kaspersky Research Sandbox выберите объект, который вы хотите выполнить, выполнив одно из следующих действий:

   - Нажмите кнопку **Select File** и выберите нужный объект в открывшемся окне.
   - Перетащите нужный объект в зону перетаскивания. Зона перетаскивания отображается, когда вы начинаете перетаскивать объект.

   При выборе объекта отображаются его имя файла и размер (в мегабайтах).

   Максимальный размер объекта, который может быть загружен, составляет 256 МБ.

2. В раскрывающемся списке File execution environment выберите операционную систему, которую вы хотите использовать в качестве среды выполнения.

Доступны следующие предопределенные операционные системы:

- Microsoft Windows XP SP3 x86
- Microsoft Windows 7 x86
- Microsoft Windows 7 x64
- Microsoft Windows 10 x64
- Android ARM
- Android x86

По умолчанию выбрана операционная система Microsoft Windows 7 x64.

Если вы успешно развернули пользовательские среды выполнения, они также будут отображаться в списке доступных сред в разделе **Custom environments**.

3. В поле **File execution time (sec)** укажите время выполнения объекта (в секундах) с помощью ползунка.

Вы можете указать время выполнения от 30 до 500 секунд. Значение по умолчанию-100 секунд. Загруженный объект будет выполняться только в выбранной среде в течение указанного времени выполнения. Указанное время не включает в себя время, необходимое для анализа и отображения результатов.

4. При необходимости нажмите кнопку **Browse** в поле **Choose YARA file**, чтобы выбрать файл, содержащий правила YARA.

5. При необходимости перейдите по ссылке **Advanced options** и укажите следующие параметры:

- В поле **File extension** укажите расширение файла для объекта, который должен быть выполнен.

Для корректной обработки файлов, не являющихся изображениями в формате portable executable (PE), необходимо явно указать расширение файла в имени файла или в поле **File extension** в разделе **Advanced options**.

Большинство символов можно использовать для указания расширения файла, за исключением зарезервированных символов (<, >, :, ", /, \, |, ?, *, и космос). Точка перед расширением файла уже добавлена в поле.

Вы можете ввести до 10 символов, чтобы указать расширение файла.

Если расширение файла не указано, Kaspersky Research Sandbox попытается определить его автоматически, и файл будет выполнен с расширением, определенным Kaspersky Research Sandbox.

- Если вы хотите указать имя сетевого канала, который объект будет использовать для доступа в Интернет, выберите один из следующих вариантов:
    1. **Auto** — Выберите этот параметр, чтобы автоматически определить сетевой канал.
    2. **Tarpit** — Выберите этот параметр, чтобы эмулировать доступность сети без доступа в Интернет.

  Другие параметры в списке задаются во время установки Kaspersky Research Sandbox. Для получения более подробной информации о доступных опциях обратитесь к своему администратору. Этот параметр нельзя изменить, если во время развертывания шаблона был указан сетевой канал.

- Если вы хотите расшифровать HTTPS-трафик, генерируемый объектом во время выполнения, установите флажок **Decrypt HTTPS**.

  Этот флажок недоступен, если в качестве среды выполнения файлов выбрана Microsoft Windows XP SP3 x86.

  Если вы выбрали пользовательскую среду с установленной операционной системой Microsoft Windows XP SP3 x86, флажок **Decrypt HTTPS** отображается и доступен для выбора в веб-интерфейсе. Однако HTTPS-трафик не будет расшифрован во время выполнения файла.

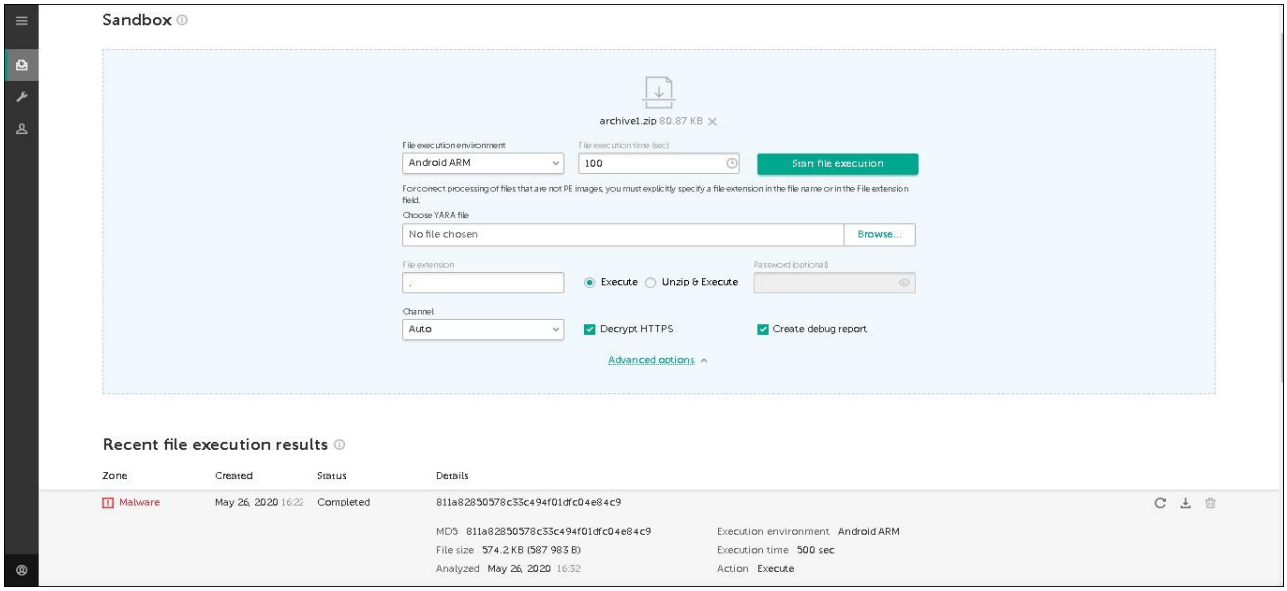
Расшифровка HTTPS-трафика может снизить вероятность обнаружения вредоносного ПО.

- Если вы хотите создать отладочный отчет для выполненного файла, который может быть использован для расследования инцидентов специалистами Kaspersky, установите флажок **Create debug report**. Диагностическая информация о том, как работает приложение, получается отдельно.

Включение этого параметра требует больше свободного места на диске для хранения результатов выполнения объекта.

По умолчанию этот флажок снят.

6. Нажмите кнопку **Start file execution**, чтобы начать процесс выполнения файла.
Kaspersky Research Sandbox будет отображать результаты выполнения объекта.
Если в процессе загрузки объекта возникает ошибка, вы можете попробовать загрузить объект снова или выбрать другой объект.
Если вы по какой-то причине завершите процесс загрузки, вы можете попробовать загрузить тот же объект позже или выбрать другой объект.
Запись, описывающая результаты выполнения, появляется в таблице **Recent file execution results**.
Вы можете начать анализировать результаты, когда процесс завершится и в поле **Status** появится сообщение *Completed*.
7. При необходимости нажмите кнопку **Rescan**, чтобы выполнить ранее загруженный и выполненный объект, и повторите шаги 2-6 этой процедуры.
Если файл будет выполнен снова через некоторое время, результаты могут отличаться от результатов, показанных в таблице **Recent file execution results** для того же файла, поскольку Kaspersky expert systems обновляет информацию об объектах в режиме реального времени.
Результаты выполнения зависят от ландшафта угроз.



Ошибки выполнения задачи

В этом разделе описываются ошибки, которые могут возникнуть во время выполнения объекта.

Обработка не удалась

Во время исполнения объекта произошла ошибка.

Попробуйте выполнить объект еще раз позже. Если проблема повторится, обратитесь к администратору Kaspersky Research Sandbox.

Неверный пароль

Не удалось распаковать архив из-за неправильного пароля.
Чтобы выполнить объект, щелкните ссылку **Rescan**, убедитесь, что в поле **Password** указан правильный пароль, а затем снова запустите выполнение объекта.

Недопустимый архив

Не удалось определить формат архива.
Чтобы выполнить объект, попробуйте снова сжать его в zip-архив или загрузить в распакованном виде.

Неверное количество архивных файлов

В архиве .zip обнаружено более одного объекта.
Чтобы выполнить объект, убедитесь, что вы заархивировали только один объект, и начните выполнение снова.

Недопустимый размер объекта

Не удалось выполнить объект, поскольку он является файлом нулевой длины или его размер превышает предельный размер.
Чтобы выполнить объект, убедитесь, что он содержит данные и его размер не превышает 256 мегабайт (МБ).

Перегрузка песочницы

Песочница Kaspersky Research в настоящее время перегружена.
Попробуйте выполнить объект еще раз позже. Если проблема повторится, обратитесь к администратору Kaspersky Research Sandbox.

Неизвестный тип файла

Не удалось автоматически определить тип объекта, объект не был выполнен.
Если вы знаете тип объекта, вручную введите расширение объекта в поле **File extension** в разделе **Advanced options** и запустите задачу выполнения.

Распаковка не удалась

Произошла ошибка при распаковке архива.
Чтобы выполнить объект, попробуйте снова сжать его в zip-архив или загрузить в распакованном виде.

Автоматически обнаруживаемые типы файлов

Kaspersky Research Sandbox автоматически определяет тип выполняемого файла, если вы не указали его вручную при создании задачи выполнения файла.

В таблице ниже приведены возможные типы файлов. Следующий список типов файлов не является фиксированным и может быть изменен во время обновления компонентов.

- APK - Файл пакета приложений для Android
- DOC - Документ Microsoft Word
- DOCM - Документ с поддержкой макросов Microsoft Word Open XML
- DOCX - Документ формата Microsoft Word Open XML
- DOTM - Шаблон файла Microsoft Word
- DOTX - Шаблон документа Microsoft Word Open XML
- JAR - Java Архивный файл
- JS - JavaScript файл
- JSE - Кодированный Fichier JavaScript
- LNK - используется Microsoft Windows для указания на исполняемый файл
- MSI - Пакет установщика Microsoft Windows
- PDF - Adobe Portable Document Format
- PE64_COM - Portable Executable format for executable for 64-bit operating systems
- PE64_CPL - Портативный исполняемый формат файлов панели управления для 64-битных операционных систем
- PE64_DLL - Портативный исполняемый формат для динамических библиотек (DLL) для 64-разрядных операционных систем
- PE64_EXE - Портативный исполняемый формат для исполняемых файлов для 64-битных операционных систем
- PE64_SRV - Портативный исполняемый формат для сервисов для 64-битных операционных систем
- PE_COM - Портативный исполняемый формат для исполняемых файлов для операционных систем MS-DOS и Windows
- PE_CPL - Портативный исполняемый формат для файлов панели управления

- PE_DLL - Портативный исполняемый формат для динамических библиотек (DLL)
- PE_EXE - Портативный исполняемый формат для исполняемых файлов для операционных систем MS-DOS и Windows
- PE_SRV - Портативный исполняемый формат для служб
- POTM - Шаблон презентации с поддержкой макросов Microsoft PowerPoint Open XML
- POTX - Шаблон презентации Microsoft PowerPoint Open XML
- PPAM - Файл надстройки, используемый Microsoft PowerPoint
- PPSM - Microsoft PowerPoint Open XML Macro-Enabled слайд-шоу
- PPSX - Microsoft PowerPoint Open XML слайд-шоу
- PPT - Microsoft PowerPoint презентация
- PPTM - Microsoft PowerPoint Open XML Macro-Enabled презентация
- PPTX - Microsoft PowerPoint Open XML презентация
- PUB - Документ Microsoft Publisher
- RTF – Формат файла Rich Text
- SWF – Файл фильма Shockwave Flash
- VBE - Кодированный файл скрипта VBScript
- VBS - Файл VBScript
- VDX - Рисунок Microsoft Visio
- WSF - Файл сценария Windows
- XLAM - Надстройка Microsoft Excel Open XML с поддержкой макросов
- XLS - Электронная таблица Microsoft Excel
- XLSB - Двоичная электронная таблица Microsoft Excel
- XLSM – Сводная таблица Microsoft Excel Open XML Macro-Enabled
- XLSX - Электронная таблица Microsoft Excel Open XML
- XLTM - Шаблон электронной таблицы Microsoft Excel Open XML с поддержкой макросов
- XLTX - Шаблон электронной таблицы Microsoft Excel Open XML

Сводный раздел

В разделе **Summary** представлена общая информация о результатах выполнения файла. Отображаются следующие круговые диаграммы:

Обнаружения

Общее количество объектов, которые были обнаружены во время выполнения файла, и доля объектов с вредоносными (красный), рекламными и другими (желтый), а также YARA обнаруживает статусы.

Имя круговой диаграммы кликабельно—вы можете нажать кнопку **Detects**, чтобы перейти к таблице **Sandbox detection names** на вкладке **Results**.

Подозрительная деятельность

Общее количество подозрительных действий, зарегистрированных в ходе выполнения объекта, и доля действий с Высоким (красным), Средним (желтым) и Низким (серым) уровнями.
Имя круговой диаграммы кликабельно—вы можете нажать кнопку **Suspicious activities**, чтобы перейти к таблице **Suspicious activities** на вкладке **Results**.

Извлеченные файлы

Общее количество файлов, которые были загружены или сброшены объектом в процессе выполнения, а также доля файлов со статусами Malware (извлеченные файлы, которые могут быть классифицированы как вредоносные, красным цветом), Adware и другие (извлеченные файлы, которые могут быть классифицированы как Не-вирус, желтым цветом), Clean (извлеченные файлы, которые могут быть классифицированы как не вредоносные, зеленым цветом) и Not categorized (информация об извлеченных файлах отсутствует, серым цветом).
Имя круговой диаграммы кликабельно—вы можете щелкнуть по **Extracted files**, чтобы перейти на вкладку **Extracted files**.

Сетевая деятельность

Общее количество зарегистрированных сетевых взаимодействий, выполняемых объектом в процессе выполнения, и доля сетевых взаимодействий со статусами Опасный (запросы к ресурсам с опасным статусом, красным цветом), Рекламный и прочие (запросы к ресурсам с Рекламным и иным статусом, желтым цветом), Хороший (запросы к ресурсам с хорошим статусом, зеленым цветом) и некатегоризированный (запросы к ресурсам с некатегоризированным статусом, серым цветом).
Имя круговой диаграммы является кликабельным—вы можете нажать кнопку **Network activities**, чтобы перейти на вкладку **Network activities**.

Когда вы позволяете указателю мыши остановиться на определенной точке круговой диаграммы, отображается количество обнаруженных объектов или действий с определенными статусами.
Статистическая информация представлена только для отображаемых результатов. Данные в экспортированных результатах и/или ответах API могут отличаться от данных, отображаемых в веб-интерфейсе.
Результаты выполнения файла можно загрузить в виде архива (сжатого), нажав на ссылку **Export all results**.

Кроме того, в разделе **Summary** вы можете просмотреть сведения о задаче выполнения:

Uploaded - Дата и время загрузки файла.
Analyzed- Дата и время завершения анализа файла.
Database update - Дата и время обновления антивирусных баз.
Execution environment - Выбранная среда (операционная система) для выполнения файла.

Execution time - Заданное время выполнения файла, в секундах.

File extension - Указанное расширение файла.

HTTPS decryption – информация о том, был ли расшифрован HTTPS-трафик, генерируемый объектом, во время исполнения.

Channel - Имя сетевого канала, который использовался объектом для доступа в Интернет.

File size - Размер исполняемого файла в байтах.

File type - Автоматически определяется тип выполняемого файла.

Yara file – Файл с правилами YARA, который использовался во время анализа. Вы можете нажать на имя файла, чтобы загрузить файл YARA.

YARA scan status - Состояние сканирования файла с помощью правил YARA (например, Завершено или ошибка обработки).

YARA scan date - Дата и время сканирования файла по правилам YARA.

MD5 – MD5-хэш исполняемого файла. Этот пункт является кликабельным и ведет вас на веб-сайт Kaspersky Threat Intlligence Portal.

SHA-1 - SHA-1 хэш исполняемого файла. Этот пункт является кликабельным и ведет вас на веб-сайт Kaspersky Threat Intelligence Portal.

SHA-256 - SHA-256 хэш исполняемого файла. Этот пункт является кликабельным и ведет вас на веб-сайт Kaspersky Threat Intelligence Portal.

Диагностика

Общие шаги по устранению неполадок:

Войдите на сервер, используя следующие учетные данные:

Логин: `krsadmin`

Пароль: пароль, введенный ранее в разделе **Настройка KRS.** Он не будет показываться из соображений безопасности.

Переключитесь на root-пользователя (пароль тот же):

```
sudo su-
```

Затем выполните соответствующие действия для вашей проблемы.

Веб-интерфейс KRS не отвечает

Убедитесь, что служба активна в выводе следующей команды:

```
systemctl status opsb
```

Если служба неактивна, проверьте журналы в последнем файле opsb-error из:

```
less /var/log/kaspersky/opsb/opsb-error-*
```

Возможные ошибки:

Не удалось подключиться к KPSN

Проверьте, что KPSN доступен с хост-машины KRS:

```
curl https://kpsn.example.com:80/api/
```

Сбой обновления

Убедитесь, что источник обновления AV Bases доступен с хост-компьютера KRS:

```
curl http://opsb.kaspersky-labs.com/ced2f99465a90733c5c2e9f2196b671512154b1a/
```

Пароль администратора KRS Web UI был утерян

Войдите в консоль PostgreSQL:

```
sudo -u postgres psql opsb
```

Затем введите следующую команду для сброса пароля по умолчанию, который был задан с дистрибутивом:

```
update auth.users set password_hash =
'\x8cb697e76e8b018864ed11823911b27a4c3238ee3b12b0537126d7c6b10d61208878e2a1d5340ead7e
04ffa16167010e42c51a3b563c6b7 65a362e174ebb78f8', password_salt =
'\x172a8d81fccedb19e774cd0097f83e7101ac3c2e' где user_id = 1;
```

В веб-интерфейсе KRS появляется ошибка "KRS не стабилен".

Проверка локали системы

Выполните следующую команду:

```
localectl
```

Если локаль системы в выводе отличается от en_US.UTF-8, выполните следующую команду и перезагрузитесь:

```
localectl set-locale LANG=en_US.UTF-8
reboot now
```

Проверьте `last_check_timestamp` и ошибки в файле состояния

```
less /var/tmp/sbtest
```

Не удалось проверить репутацию файлов и URL-адресов

"Песочница Kaspersky Research не смогла проверить репутацию файлов и URL-адресов, потому что Kaspersky Private Security Network недоступна". при потере соединения с Kaspersky Private Security Network появляется сообщение об ошибке.

Проблемы

- Репутация файлов и URL-адресов не может быть дополнительно проверена по базам данных Kaspersky Private Security Network.
-

Рекомендации

- Создайте отладочный отчет для выполненного файла и отладочной информации приложения, а затем обратитесь к администратору Kaspersky Research Sandbox в вашей организации, чтобы сообщить ему об ошибке.

- Просмотр результатов выполнения файла (нажмите ссылку **View Details** в таблице **Recent file execution results**) после повторного подключения к Kaspersky Private Security Network. Вам не нужно повторять выполнение файла, чтобы просмотреть обновленные результаты.

Kaspersky Research Sandbox нестабильна

"Песочница Kaspersky Research" сейчас не стабильна. Некоторые функции могут не выполняться или выполняться неправильно." сообщение об ошибке появляется, если компонент, выполняющий выполнение файла, не функционирует. Доступность компонента проверяется каждые 30 минут.

Проблема также может возникнуть, если пользовательская среда выполнения настроена неправильно (например, установленное программное обеспечение не активировано или не выполняются другие необходимые операции).

Проблемы

- Загрузка и выполнение файлов недоступны.
- Повторное выполнение файла недоступно.
- Файл, который выполнялся в момент возникновения проблемы, может быть не выполнен или выполнен неправильно.

Рекомендации

- Повторите неудачное действие через некоторое время. Если вы снова получите сообщение об ошибке, создайте отладочный отчет для выполненного файла и отладочной информации приложения, а затем обратитесь к администратору Kaspersky Research Sandbox в вашей организации и сообщите ему об этом сообщении об ошибке.
- Если ошибка возникает при выполнении файла в пользовательской среде, рекомендуется удалить эту среду, правильно настроить новую и затем развернуть ее снова.

Расширенное обнаружение угроз недоступно

Сообщение об ошибке "Расширенное обнаружение угроз недоступно" появляется, если компонент, выполняющий обнаружение угроз, не функционирует. Доступность компонента проверяется при каждом выполнении файла, включая повторное выполнение файла.

Проблемы

Расширенное обнаружение угроз в исполняемом файле не выполняется.

Рекомендации

- Устраните причины проблемы и снова запустите файл.
- Выполните проверку исполняемого файла на вирусы с помощью антивирусных средств.

Автоматическое определение типа файла не работает

Сообщение об ошибке "Автоматическое определение типа файла не работает" появляется, если компонент, определяющий отдельные типы файлов, не работает. Доступность компонента проверяется при каждом выполнении файла, включая повторное выполнение объекта.

Проблемы

Для объектов без расширения файла в имени файла и без указанного пользователем расширения файла вероятность успешного выполнения объекта в песочнице снижается.

Рекомендации

- Перед выполнением объекта явно укажите расширение объектного файла.
- Устраните причины проблемы.

Антивирусные базы устарели

Сообщение об ошибке "Антивирусные базы устарели" появляется, если обновляемые компоненты, выполняющие обнаружение угроз, не обновлялись более 336 часов (14 дней).

Проблемы

Результаты выполнения файла содержат информацию об обнаруженных объектах на дату последнего обновления компонента обнаружения.

Рекомендации

- Обновите компоненты, выполняющие обнаружение угроз.
- Убедитесь, что антивирусные базы обновлены. Обратитесь к администратору Kaspersky Research Sandbox, чтобы проверить зеркало источника обновления базы данных, указанное при установке приложения.
- Повторите выполнение файлов, выполненных в течение последних 336 часов (14 дней) с момента возникновения проблемы.

Недостаточно свободного места на диске

Сообщение об ошибке "Недостаточно свободного места на диске" появляется, если на вашем компьютере доступно менее 10 ГБ для выполнения задач выполнения файлов.

Проблемы

- Загрузка и выполнение файлов недоступны.
- Повторное выполнение файла недоступно.

Файл, который выполнялся в момент возникновения проблемы, может быть не выполнен или выполнен неправильно.

Рекомендации

- Освободите место на жестком диске.
- Не повторяйте неудачное выполнение файла, чтобы сохранить диагностическую информацию для дальнейшего анализа сбоев. Просмотр результатов выполнения не влияет на диагностику.

Необходимые отладочные символы не найдены

Ошибка "*Template deploy error for custom image (ID: <custom image ID>). Required debug symbols are not found. See Help for details*." сообщение об ошибке появляется, если не удалось развернуть шаблон и создать пользовательскую среду выполнения.

Проблемы

- Необходимые файлы символов не найдены для пользовательского изображения.
- Шаблон не был развернут, и пользовательский образ (среда выполнения) не был создан.

Рекомендации

Сервер Kaspersky Research Sandbox подключен к Интернету в вашей сетевой инфраструктуре:

1. Проверьте подключение к Интернету на сервере, где установлена Kaspersky Research Sandbox.
2. Снова разверните шаблон.

Ограничения и предупреждения

Kaspersky Research Sandbox имеет несколько ограничений.

Ограничение в использовании представления совместимости Microsoft Internet Explorer

Представление совместимости Microsoft Internet Explorer не должно использоваться при работе с Kaspersky Research Sandbox.

Файлы не фильтруются по типу в проводнике файлов в Microsoft Edge

Microsoft Edge отображает файлы всех типов в проводнике во время загрузки ISO-файлов.

Ограничение для загрузочных носителей

Вы можете загрузиться только с носителя, содержащего одну из следующих операционных систем:

Windows XP SP3 (или более поздняя версия)

Windows 7

Windows 8.1 x64

Windows 10 x64 (не выше версии 1909 года)

Ограничения для пользовательской среды

Функциональные возможности пользовательской среды имеют следующие ограничения:

Поддерживаемые операционные системы: Windows XP SP3 (или более поздняя версия)

Windows 7

Windows 8.1 x64

Windows 10 x64 (не выше версии 1909 года)

Поддержка Microsoft Office:

Microsoft Office не выше версии 2016 года

Ограничение экспорта отчетов в PDF

Изображения могут быть недоступны при экспорте отчета в PDF в Microsoft Internet Explorer.

Неправильная печать в формате PDF в Microsoft Internet Explorer 11

Справка может быть неправильно напечатана в формате PDF в Microsoft Internet Explorer 11, если выбран параметр Печать всех.

Обращение в Службу технической поддержки

Если вы не можете найти решение своей проблемы в Справке, мы рекомендуем вам обратиться к администратору Kaspersky Research Sandbox.

Глоссарий

cURL utility

Утилита, которая может быть использована для выполнения файлов и получения отчетов о результатах с помощью Kaspersky Research Sandbox API.

MD5

Криптографическая хэш-функция, которая производит 128-битное хэш-значение. 128-битное хэш-значение представляется в виде последовательности из 32 шестнадцатеричных цифр.

Песочница

Изолированная безопасная среда, которая позволяет загружать и выполнять файлы.

SHA-1

Криптографическая хэш-функция, которая производит 160-битное хэш-значение. 160-битное хэш-значение представляется в виде последовательности из 40 шестнадцатеричных цифр.

SHA-256

Криптографическая хэш-функция, которая производит 256-битное хэш-значение. 256-битное хэш-значение представляется в виде последовательности из 64 шестнадцатеричных цифр.

Носитель информации

Файл образа диска (ISO) в формате ISO 9660 с программным обеспечением. В случае операционной системы это должен быть загрузочный образ.

Подозрительная деятельность

Группа причин, оцениваемых как необычные действия технологии обнаружения, недостаточные для полной генерации инцидента и, таким образом, перечисленные для информационных или дальнейших целей расследования.

Шаблон

Образ виртуальной машины. Пользователь может установить необходимое программное обеспечение на шаблон и развернуть его в песочнице в качестве пользовательской среды выполнения.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt.