kaspersky

Kaspersky Scan Engine для Linux

Руководство по эксплуатации

Версия программы: 2.0

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Дата редакции документа: 04.02.2021

https://www.kaspersky.ru
https://help.kaspersky.com/ru
https://support.kaspersky.ru

kaspersky

Содержание

kaspersky

О Kaspersky Scan Engine

Kaspersky Scan Engine – это серверное защитное решение, которое обеспечивает антивирусную защиту, сканирование HTTP-трафика и проверку репутации файлов и веб-адресов для сторонних клиентских решений.

Kaspersky Scan Engine обеспечивает комплексную защиту широкого ряда устройств от вредоносных программ, троянцев, червей, руткитов, шпионского и рекламного программного обеспечения (ПО). Его можно использовать с различными продуктами и службами, в том числе с приложениями для персональных компьютеров, серверными решениями, прокси-серверами и почтовыми шлюзами.

Решение Kaspersky Scan Engine основано на комплекте Kaspersky Anti-Virus Software Development Kit 8 Level 3 (KAV SDK) и на ядре Kaspersky Anti-Virus Engine, удостоившемся наград, и поэтому использует новейшие методы определения и удаления вредоносного ПО различных типов.

Вы можете запросить документацию KAV SDK либо купить KAV SDK вместе с документацией у вашего технического менеджера по работе с клиентами.

В этом разделе

Ключевые функции Kaspersky Scan Engine

Решение Kaspersky Scan Engine может работать в одном из двух режимов:

- Режим HTTP (см. раздел "Использование Kaspersky Scan Engine в режиме HTTP" на стр. 26)

  В этом режиме Kaspersky Scan Engine работает как REST-подобная служба, которая получает HTTP-запросы от клиентских приложений, сканирует объекты, переданные в этих запросах, и отправляет обратно HTTP-ответы с результатами сканирования.

- Режим ICAP (см. раздел "Использование Kaspersky Scan Engine в режиме ICAP" на стр. 50)

  Этот режим доступен только для операционных систем Linux.

  В этом режиме Kaspersky Scan Engine работает как ICAP-сервер, который сканирует HTTP-трафик, проходящий через прокси-сервер, и веб-адреса, запрашиваемые пользователями, а также блокирует веб-страницы, содержащие вредоносный контент.

kaspersky

Решение Kaspersky Scan Engine также включает в себя графический пользовательский интерфейс, который вам позволяет с легкостью настраивать поведение Kaspersky Scan Engine, просматривать его служебные события и результаты сканирования.

Сценарии использования:

Защита от угроз

Kaspersky Scan Engine может сканировать файлы и участки оперативной памяти, используя антивирусную базу данных "Лаборатории Касперского" и усовершенствованный эвристический модуль. Поддерживается сканирование сжатых исполняемых файлов, архивов, макросов Microsoft Office, электронных писем и почтовых баз.

Веб-фильтрация

Kaspersky Scan Engine может сканировать веб-адреса, явно заданные для проверки (в режиме HTTP), либо веб-адреса, которые запрашивают пользователи через прокси-сервер (в режиме ICAP). В режиме ICAP решение Kaspersky Scan Engine может подставлять заданную пользователем HTML-страницу вместо вредоносных веб-страниц.

Проверка репутации файлов и веб-адресов

Kaspersky Scan Engine может получать информацию о проверенных файлах и веб-адресах из Kaspersky Security Network (KSN).

Графический пользовательский интерфейс

Графический пользовательский интерфейс дает возможность настроить Kaspersky Scan Engine, проверить статус файла ключа или кода активации Kaspersky Scan Engine, просмотреть служебные события и результаты сканирования.

Ключевые функции:

- Удостоенная наград антивирусная технология "Лаборатории Касперского" обеспечивает лучшие в своем классе уровни обнаружения вредоносных программ и может мгновенно реагировать на возникающие угрозы.
- Kaspersky Security Network предоставляет информацию о репутации файлов и интернет-ресурсов, что позволяет приложениям "Лаборатории Касперского" быстрее реагировать на угрозы, не дожидаясь обновления баз, и уменьшает вероятность ложного срабатывания.
- Блокирует доступ к вредоносным, фишинговым и рекламным веб-адресам.
- Определяет повторно упакованные объекты и объекты, упакованные при помощи «серых» архиваторов (часто используемых для сокрытия вредоносных программ от антивирусного ПО).
- Использует усовершенствованный эвристический анализатор и технологии обнаружения, основанные на машинном обучении.
- Очищает инфицированные файлы, архивы и закодированные объекты.
- Использует обновляемое антивирусное ядро: технологии обнаружения и логика обработки данных могут обновляться или изменяться посредством обычного обновления антивирусных баз данных.
- Kaspersky Scan Engine естественным образом поддерживает многопоточность и может выполнять несколько заданий одновременно. Вы можете настроить число сканирующих процессов и потоков для увеличения производительности Kaspersky Scan Engine.
- Дополнительный фильтрующий слой представлен компонентом Format Recognizer. Вы можете использовать этот компонент для распознавания файлов и игнорирования файлов определенных

форматов во время сканирования. Поддерживаются десятки форматов, в том числе исполняемые, офисные файлы, медиа-файлы и архивы.

- Графический пользовательский интерфейс для управления и мониторинга:
  - Позволяет настраивать и управлять приложением.
  - Позволяет отслеживать статус работы приложения, статус используемого файла ключа или кода активации, а также число проверенных и обнаруженных объектов.
  - Отображает на дашборде информацию обо всех проверенных объектах. Результаты проверки могут быть сохранены в формате CSV.
- Простота в установке и конфигурации. После установки не требуется разработка дополнительного ПО, решение запустится в течение минут.
- Составление отчетов:
  - Важные события приложения отсылаются в Syslog в формате CEF.
  - Все служебные события видны в дашборде.
- Возможности сопровождения продукта:
  - Антивирусные базы обновляются автоматически. В случае обнаружения поврежденных баз Kaspersky Scan Engine продолжает использовать старые неповрежденные.
  - Простота отслеживания работы продукта с помощью графического интерфейса.
  - Возможность использования онлайн-активации. При онлайн-активации лицензионная информация для ядра сканирования "Лаборатории Касперского" обновляется автоматически.
- Отказоустойчивая архитектура.
- В пакете распространения поставляется исходный код HTTP-клиента и ICAP-службы для возможности изменения.
- Подробная документация и поддержка кроссплатформенности прикладного программного интерфейса (API). Схожие прикладные программные интерфейсы для версий под Linux/UNIX и Windows.
- Возможность минимизировать внешний трафик путем создания локальных зеркал для антивирусных баз (нужны дополнительные программы).

Технологии обнаружения Kaspersky Scan Engine

В этом разделе описаны технологии обнаружения, реализованные в Kaspersky Scan Engine.

Анализ сигнатур

Этот метод обнаружения основывается на поиске определенной строки в сканируемых файлах. Сигнатурный анализ также включает обнаружение, основанное на хеше всего вредоносного файла. Традиционные сигнатуры позволяют обнаруживать определенные объекты с высокой точностью. Другие технологии, основанные на использовании сигнатур, такие как структурные эвристические сигнатуры и SmartHash, могут обнаруживать неизвестное и полиморфное вредоносное ПО.

Сигнатурный анализ позволяет обнаруживать определенные атаки с высокой точностью и малой вероятностью ложного срабатывания. Однако этот метод обнаружения неэффективен против полиморфных вредоносных программ и различных версий одного и того же вредоносного ПО. Для высокой

эффективности сигнатурного анализа также требуется частое обновление сигнатур.

Часто обновляемая обширная антивирусная база данных Kaspersky Scan Engine обеспечивает высочайший уровень защиты от известного вредоносного ПО, троянцев, червей, руткитов, шпионского и рекламного ПО.

Расширенная эвристика

При сканировании скрипта или исполняемого файла ядро Kaspersky Anti-Virus Engine эмулирует его запуск в безопасной искусственной среде. Если во время анализа поведения эмулируемого объекта обнаруживается подозрительное поведение, он считается вредоносным. Этот метод позволяет обнаруживать новое и неизвестное вредоносное ПО.

Компонент Kaspersky Scan Engine, представляющий собой эмулятор, эмулирует функциональную среду запуска для объекта, в том числе функции и различные подсистемы целевой операционной системы. Реальные функции и подсистемы во время эмуляции не используются.

Технологии машинного обучения

SmartHash – это запатентованный алгоритм "Лаборатории Касперского" для построения интеллектуальных хешей, учитывающих локализацию. Хеши, учитывающие локализацию, – это статические характеристики файлов, которые могут быть извлечены и разбиты на группы. Значения SmartHash можно вычислить для каждого файла, при этом различные файлы могут иметь одинаковое значение SmartHash, когда они функционируют подобным образом. Поэтому конкретное значение SmartHash идентифицирует целый кластер подобных файлов и позволяет эффективно обнаруживать неизвестные вредоносные программы на основе уже известных семейств. Технология SmartHash использует несколько уровней точности, что позволяет обнаруживать даже сильно полиморфные вредоносные программы. Вместе с этим она позволяет снизить вероятность ложного срабатывания.

Преимущества технологии SmartHash:

- Хорошо справляется с новыми, избегающими обнаружение и полиморфными вредоносными программами.
- Обнаружение в течение нескольких минут.
- Работа без подключения и с подключением к интернету.
- Гибкая модель с несколькими уровнями схожести, что позволяет обнаруживать чистые и вредоносные файлы.
- Устойчивая технология: математическая модель обновляется с помощью машинного обучения и постоянно пересматривается экспертами. Использование технологии SmartHash приводит к минимуму ложных срабатываний и высокому уровню обнаружения.

Помимо использования для обнаружения вредоносных программ, использование SmartHash онлайн улучшает возможности "Лаборатории Касперского" составлять белые списки. Значение SmartHash, вычисленное на стороне клиента, можно сравнить с миллиардами известных чистых файлов в базе данных "Лаборатории Касперского" посредством глобальной сети Kaspersky Security Network.

"Лаборатория Касперского" использует машинное обучение для повышения качества обнаружения существующих технологий сканирования. Машинное обучение развертывается для автоматического анализа журналов запуска во внутренних песочницах. Во внутренних поведенческих системах-песочницах запускаются как известные вредоносные файлы, так и неизвестные файлы. Некоторые из этих песочниц имитируют пользовательские системы, на которых запущены стандартные продукты. Наиболее мощные песочницы используют возможности выборочного протоколирования, позволяя очень тонко настраивать обнаружение.

Роботы обрабатывают журналы песочниц по одной строке. Журналы выполнения с записями от новых вредоносных образцов изучаются с помощью машинного обучения, чтобы найти новые индикаторы

обнаружения. Эти новые индикаторы обогащают математические модели методов обнаружения, не основанных на сигнатурах, равно как и эвристические поведенческие записи, создаваемые экспертами "Лаборатории Касперского".

Обработка сжатых исполняемых файлов и архивов

Kaspersky Scan Engine включает в себя технологию, позволяющую обнаруживать вирусы и другие объекты внутри внутри сжатых исполняемых файлов и архивов. С помощью этой технологии можно безопасно вылечить или удалить инфицированные архивы и сжатые исполняемые файлы.

Kaspersky Scan Engine поддерживает примерно 4000 различных форматов сжатых исполняемых файлов и архивов.

Лечение архивов

Эта технология предназначена для лечения архивов. С помощью этой технологии успешно вылечиваются или удаляются инфицированные объекты внутри архивов (в зависимости от пользовательских настроек). Вам не нужно использовать другие архиваторы.

В настоящее время Kaspersky Anti-Virus Engine удаляет вирусы из архивов следующих форматов: ARJ, CAB, RAR и ZIP.

Kaspersky Security Network

Kaspersky Security Network (KSN) – это инфраструктура облачных служб, которая обеспечивает доступ к онлайновой базе знаний "Лаборатории Касперского", содержащей информацию о репутации файлов, веб-ресурсов и программ. Использование данных из Kaspersky Security Network обеспечивает более быстрое реагирование на угрозы, улучшает производительность некоторых компонентов защиты и уменьшает вероятность ложных срабатываний.

KSN может блокировать новое вредоносное ПО через несколько секунд после его появления с помощью использования автоматических правил, которые сгенерированы на основе данных, переданных пользователями "Лаборатории Касперского".

"Лаборатория Касперского" располагает серверы KSN в вычислительных центрах по всему миру, тем самым обеспечивая минимальное время отклика для облачных проверок. База данных KSN содержит терабайты информации; она постоянно обновляется аналитиками по безопасности, а также автоматическими методами.

При использовании KSN вы передаете в "Лабораторию Касперского" информацию об установленной копии Kaspersky Scan Engine и обнаруженных объектах. Эта информация не содержит персональной или конфиденциальной информации пользователя. "Лаборатория Касперского" защищает полученную информацию в соответствии с требованиями законодательства. Полный перечень информации, передаваемой в "Лабораторию Касперского" при использовании KSN, приведен в разделе «Данные, передаваемые в "Лабораторию Касперского" при проверке репутации файлов и веб-адресов (на стр. 66)».

Kaspersky Scan Engine соответствует требованиям Общего регламента по защите данных (GDPR).

Обнаружение вредоносных и фишинговых веб-адресов

В Kaspersky Scan Engine входит автономная база данных вредоносных и фишинговых веб-адресов. Кроме того, вы можете проверять репутации сканируемых веб-адресов в Kaspersky Security Network.

kaspersky

Архитектура Kaspersky Scan Engine

Kaspersky Scan Engine представляет собой реализацию HTTP-демона и ICAP-плагина, которые входят в Kaspersky Anti-Virus SDK.

Когда решение Kaspersky Scan Engine запущено как HTTP-демон, оно работает в режиме HTTP. Когда оно запущено как ICAP-плагин, оно работает в режиме ICAP.

Режимы Kaspersky Scan Engine характеризуются следующим:

- Режим HTTP (см. раздел "Использование Kaspersky Scan Engine в режиме HTTP" на стр. 26)

  В данном режиме Kaspersky Scan Engine работает как REST-подобная служба, которая получает HTTP-запросы от клиентских приложений, сканирует файлы и веб-адреса, переданные в этих запросах, и отправляет обратно HTTP-ответы с результатами сканирования.

- Режим ICAP (см. раздел "Использование Kaspersky Scan Engine в режиме ICAP" на стр. 50)

  > Этот режим доступен только для операционных систем семейства Linux.

  В данном режиме Kaspersky Scan Engine работает как ICAP-сервер, который сканирует HTTP-трафик, проходящий через прокси-сервер, сканирует веб-адреса, по которым попытались перейти пользователи, и блокирует веб-страницы с вредоносным контентом.

Kaspersky Scan Engine состоит из следующих компонентов:

- Служба, обрабатывающая клиентские запросы

  Эти службы разные в режимах HTTP и ICAP.

- Kaspersky Scan Engine GUI

  Графический интерфейс, доступный через браузер. Его функционал реализован в исполняемом файле klScanEngineUI.

- Kaspersky Anti-Virus Engine

  Исполняемый файл, который сканирует переданные ему объекты.

Режим HTTP

При работе в режиме HTTP решение Kaspersky Scan Engine состоит из HTTP-службы kavhttpd, ядра Kaspersky Anti-Virus Engine и графического интерфейса Kaspersky Scan Engine.

Когда вы используете Kaspersky Scan Engine в режиме HTTP, взаимодействие между компонентами происходит в следующем порядке:

1. Файлы и веб-адреса для сканирования посылаются в kavhttpd в HTTP-запросах.

   Вы можете переслать объекты в kavhttpd двумя способами:

   - Используя HTTP-клиент, подобный включенному в комплект поставки;
   - Посылая HTTP-запросы вручную (см. раздел "Совершение запросов в режиме HTTP" на стр. 38).

2. Служба kavhttpd посылает объекты ядру Kaspersky Anti-Virus Engine.
3. Kaspersky Anti-Virus Engine сканирует объекты.

Если вы используете компонент проверки репутации файлов и веб-адресов, объекты также отправляются в KSN для проверки репутации.

4. После выполнения сканирования Kaspersky Anti-Virus Engine возвращает результат службе kavhttpd.
5. Служба kavhttpd посылает результаты сканирования HTTP-клиенту либо другому приложению, которое послало объекты на сканирование.

   Если вы используете графический интерфейс Kaspersky Scan Engine, результаты сканирования отображаются на странице **Scan results**.

Нижеследующий рисунок отображает взаимодействие между компонентами Kaspersky Scan Engine.

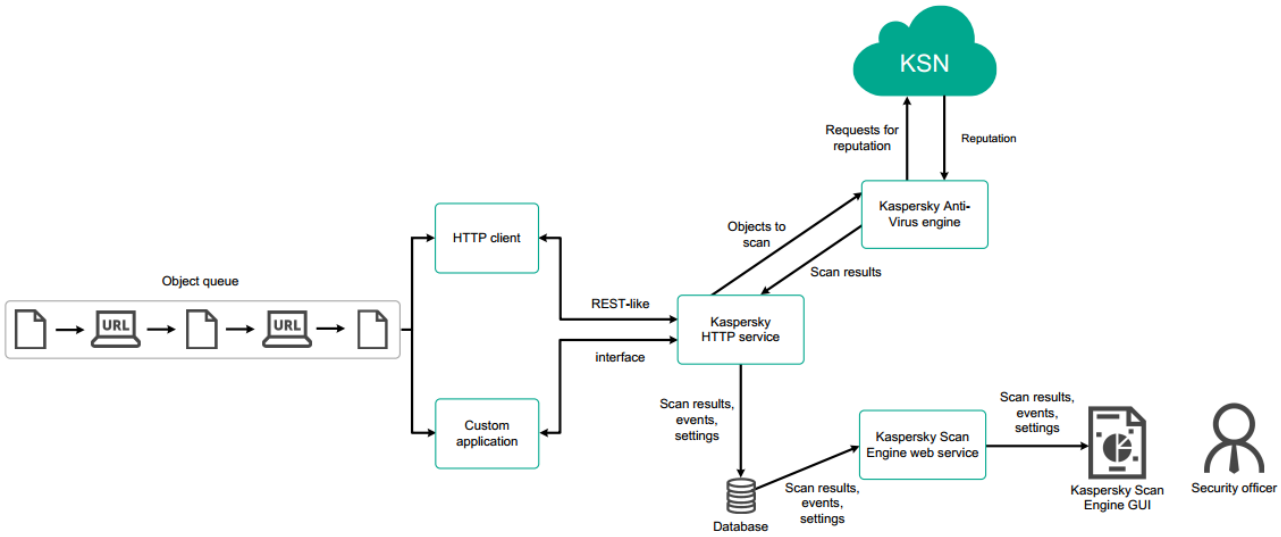

Рисунок 1. Взаимодействие между HTTP-клиентами и Kaspersky Scan Engine в режиме HTTP

Режим ICAP

При работе в режиме ICAP решение Kaspersky Scan Engine состоит из ICAP-сервера kavicapd, ядра Kaspersky Anti-Virus Engine и графического интерфейса Kaspersky Scan Engine.

Когда вы используете Kaspersky Scan Engine в режиме ICAP, взаимодействие между компонентами происходит в следующем порядке:

1. ICAP-клиент (например, прокси-сервер) посылает ICAP-запросы службе kavicapd.
2. Служба kavicapd отправляет файлы ядру Kaspersky Anti-Virus Engine на сканирование.
3. Kaspersky Anti-Virus Engine сканирует содержимое HTTP-сообщений и веб-адреса, содержащиеся в этих ICAP-запросах.

   Если вы используете компонент проверки репутации файлов и веб-адресов, содержимое HTTP-сообщений и веб-адреса также отправляются в KSN для проверки репутации.
4. После сканирования ядро Kaspersky Anti-Virus Engine возвращает результаты службе kavicapd.
5. Служба kavicapd отправляет ICAP-ответы с результатами сканирования ICAP-клиенту.

   Если вы используете графический интерфейс Kaspersky Scan Engine, результаты сканирования отображаются на странице **Scan results**.

Kaspersky Scan Engine может работать одновременно с несколькими ICAP-клиентами.

Нижеследующий рисунок показывает пример взаимодействия между прокси-сервером и Kaspersky Scan Engine в режиме ICAP.

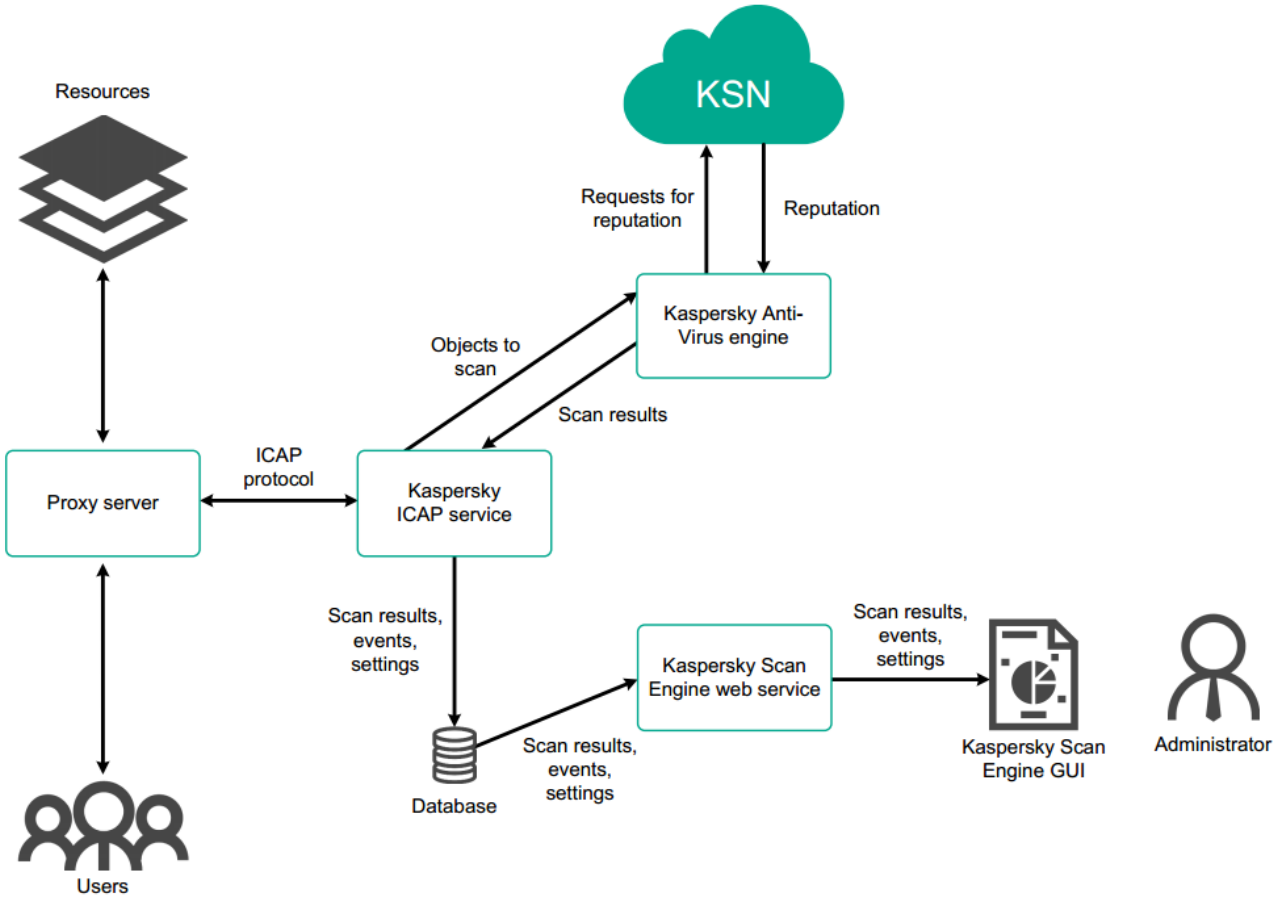

Рисунок 2. Взаимодействие прокси-сервера и Kaspersky Scan Engine в режиме ICAP

Системные требования

В этом разделе описаны системные требования Kaspersky Scan Engine.

Поддерживаемые операционные системы

Kaspersky Scan Engine работает на 64-битной версии Linux® или на 64-битной версии Microsoft® Windows®.

Требования к установленному ПО

Графический интерфейс Kaspersky Scan Engine может быть доступен с помощью следующих браузеров:

- Google Chrome™ 60 и более поздние версии
- Microsoft Internet Explorer® 11 и более поздние версии
- Mozilla™ Firefox™ 55 и более поздние версии
- Microsoft Edge 38 и более поздние версии

Графический интерфейс Kaspersky Scan Engine работает при установленной СУБД PostgreSQL 10.7 или более поздней версии.

Пакет распространения Kaspersky Scan Engine не содержит исходного кода библиотек Boost и OpenSSL. Если вы хотите адаптировать HTTP-службу или ICAP-службу под свои нужды, отредактировав и пересобрав исходный код из пакета распространения Kaspersky Scan Engine, загрузите код библиотек Boost и OpenSSL с официальных сайтов и используйте в своей системе. Если вы внесете изменения в исходный код HTTP-службы или ICAP-службы и захотите использовать графический интерфейс Kaspersky Scan Engine, получите одобрение на изменения от вашего технического менеджера по работе с клиентами, чтобы HTTP-служба или ICAP-служба по-прежнему работала с графическим интерфейсом Kaspersky Scan Engine.

Для сборки HTTPD-службы и ICAP-службы используйте следующее ПО:

- Boost 1.72.0
- OpenSSL (последнюю версию)
- GCC 7.3 или более позднюю версию
- Библиотеки PostgreSQL. Рекомендуется установить пакет libpqxx-devel.

Требования к аппаратуре

Kaspersky Scan Engine требует 1 ГБ свободного места на диске. Если вы планируете использовать графический интерфейс Kaspersky Scan Engine, вам нужно также выделить место для базы данных PostgreSQL, которая хранит служебные события. База данных PostgreSQL может храниться на том же компьютере, где установлено решение Kaspersky Scan Engine, либо на другом компьютере. Размер базы данных зависит от количества событий и может достигать нескольких гигабайт. В базе данных хранятся события, произошедшие за последние полгода.

В нижеследующей таблице приведены минимальные требования к процессору и ОЗУ для работы Kaspersky Scan Engine в зависимости от используемой операционной системы.

Операционная система	Требования к ОЗУ и процессору
64-битная Linux	1 ГБ ОЗУ 1 ГГц либо более быстрый 64-битный (x64) процессор
64-битная Windows 7 и более поздняя версия 64-битная Windows Server 2008 R2 и более поздняя версия	1 ГБ ОЗУ 1 ГГц либо более быстрый 64-битный (x64) процессор

Содержимое пакета распространения (Linux)

Пакет распространения Kaspersky Scan Engine для Linux содержит следующие папки и файлы:

Таблица 1. Содержимое пакета распространения (Linux)

Путь	Описание
`/bin/appinfo.kli`	Файл с информацией о приложении.
`/bin/bases/`	Директория, содержащая файлы антивирусной базы.

Путь	Описание
/bin/httpdkavlog.ini	Конфигурационный файл, который содержит настройки журналирования службы kavhttpd.
/bin/icapdkavlog.conf	Конфигурационный файл, который содержит настройки журналирования службы kavicapd.
/bin/kavhttpd	Исполняемый файл службы kavhttpd.
/bin/kavhttp_client	Исполняемый файл клиента kavhttpd.
/bin/kavhttpd.sh	Скрипт для запуска службы kavhttpd.
/bin/kavicapd	Исполняемый файл службы kavicapd.
/bin/kavicapd.sh	Скрипт для запуска службы kavicapd.
/bin/klScanEngineUI	Исполняемый файл графического интерфейса Kaspersky Scan Engine.
/bin/libssp.so.0	Вспомогательная библиотека.
/doc/About data provision - gateway set.txt	Файл, который описывает процедуру предоставления данных, когда вы отправляете статистическую информацию KSN в Kaspersky Scan Engine для Linux.
/doc/About data provision - online activation.txt	Файл, который описывает процедуру предоставления данных для режима лицензирования онлайн.
/doc/About data provision.txt	Файл, который описывает процедуру предоставления данных для проверки репутации файлов и веб-адресов.
/doc/Doc_data/	Директория, которая содержит документацию Kaspersky Scan Engine.
/doc/Kaspersky_Scan_Engine.htm	Главная страница документации Kaspersky Scan Engine.
/doc/ksn_license.txt	Пользовательское соглашение для Kaspersky Security Network (KSN).
/doc/legal_notices.txt	Информация о стороннем коде.
/doc/license.txt	Пользовательское соглашение для Kaspersky Scan Engine.
/doc/version_history.txt	Изменения в документации для Kaspersky Scan Engine.
/etc/init.d/kavhttpd	Скрипт инициализации для службы kavhttpd.
/etc/init.d/kavicapd	Скрипт инициализации для службы kavicapd.
/etc/init.d/klScanEngineUI	Скрипт инициализации для графического интерфейса Kaspersky Scan Engine.
/etc/kavhttpd.service	Файл systemd для службы kavhttpd.
/etc/kavicapd.service	Файл systemd для службы kavicapd.

Путь	Описание
/etc/kavhttpd.xml	Конфигурационный файл для режима HTTP.
/etc/kavicapd.xml	Конфигурационный файл для режима ICAP.
/etc/klScanEngineUI.service	Файл systemd для службы klScanEngineUI
/etc/klScanEngineUI.xml	Конфигурационный файл для графического интерфейса Kaspersky Scan Engine.
/httpsrv/etc/kavaccess	Файл, который содержит зашифрованные учетные данные для графического интерфейса Kaspersky Scan Engine.
/httpsrv/templates/	Директория, которая содержит шаблоны для графического интерфейса Kaspersky Scan Engine.
/icap_data/kavicapd_gui_rules.conf	Конфигурационный файл, который содержит правила для службы kavicapd.
/icap_data/templates/detect_req /icap_data/templates/macro_req	Шаблоны, которые используются в режиме модификации запросов (REQMOD).
/icap_data/templates/detect_resp /icap_data/templates/macro_resp	Шаблоны, которые используются в режиме модификации ответов (RESPMOD).
/icap_data/scripts/send_syslog	Скрипт, который выводит в терминал информацию о просканированных объектах и перенаправляет ее в утилиту журналирования.
/include/	Директория, которая содержит заголовочные файлы KAV SDK для разработки приложений.
/install	Скрипт установки.
/gcc version	Используемая версия GCC.
/lib/	Директория, которая содержит библиотеки KAV SDK для разработки приложений.
/platform	Используемая версия библиотеки GLIBC.
/ppl/	Директория, которая содержит плагины KAV SDK.
/ReleaseNotes.pdf	Примечания к выпуску.
/samples/kavhttp/	Директория, которая содержит исходный код службы kavhttpd и образец клиента для нее.
/samples/kavicap/	Директория, которая содержит исходный код службы kavicapd.
/samples/tables.sql	Файл, содержащий SQL-запросы, которые необходимо выполнить после установки Kaspersky Scan Engine вручную.
/tools/kav_encrypt	Утилита для шифрования учетный данных прокси-серверов и базы данных Kaspersky Scan Engine.
/tools/kavsigner	Утилита для подписи приложений.

Путь	Описание
/tools/kl_access_util	Утилита для восстановления пароля от учетной записи admin в графическом интерфейсе Kaspersky Scan Engine.
/tools/libssp.so.0	Вспомогательная библиотека.
/tools/openssl	Утилита OpenSSL.
/tools/openssl.cnf	Конфигурационный файл для OpenSSL.
/tools/integrity_check	Утилита для проверки целостности компонентов программы
/tools/integrity_check.xml	Файл манифеста для утилиты проверки целостности
/uninstall	Скрипт удаления.
/version	Версия Kaspersky Scan Engine.

Содержимое пакета распространения (Windows)

Пакет распространения Kaspersky Scan Engine для Windows содержит следующие папки и файлы:

Таблица 2. Содержимое пакета распространения (Windows)

Путь	Описание
\bin\appinfo.kli	Файл с информацией о приложении.
\bin\kavehost.exe	Исполняемый файл службы kavehost.
\bin\kavhttp_client.exe	Исполняемый файл клиента kavhttpd.
\bin\klScanEngineUI.exe	Исполняемый файл графического интерфейса Kaspersky Scan Engine.
\bin\klScanEngineUI.xml	Конфигурационный файл для графического интерфейса Kaspersky Scan Engine.
\bin\kavhttpd.exe	Скрипт инициализации для службы kavhttpd.
\bin\kavhttpd.xml	Конфигурационный файл для режима HTTP режима.
\bin\httpdkavlog.ini	Конфигурационный файл, который содержит настройки журналирования службы kavhttpd.
\bin\bases\	Папка, содержащая файлы антивирусной базы.
\bin\ossl\	Библиотека OpenSSL.
\bin\x86\	32-образы библиотек, которые используются эмуляторами.
\bin*.dll	Динамические библиотеки, используемые Kaspersky Scan Engine.
\bin*.ppl	Исполняемые модули Kaspersky Scan Engine.
\doc\Doc_data\	Папка, которая содержит документацию Kaspersky Scan Engine.

Путь	Описание
\doc\About data provision.txt	Файл, который описывает процедуру предоставления данных для проверки репутации файлов и веб-адресов.
\doc\About data provision extended.txt	Файл, который описывает процедуру предоставления данных, когда вы отправляете статистическую информацию KSN в Kaspersky Scan Engine для Windows.
\doc\About data provision - online activation.txt	Файл, который описывает процедуру предоставления данных для режима лицензирования онлайн.
\doc\Kaspersky_Scan_Engine.html	Главная страница документации Kaspersky Scan Engine.
\doc\legal_notices.txt	Информация о стороннем коде.
\doc\license.txt	Пользовательское соглашение для Kaspersky Scan Engine.
\doc\ksn_license.txt	Пользовательское соглашение для Kaspersky Security Network (KSN).
\doc\version_history.txt	Изменения в документации для Kaspersky Scan Engine.
\httpsrv\etc\kavaccess	Файл, который содержит зашифрованные учетные данные для графического интерфейса Kaspersky Scan Engine.
\httpsrv\templates\	Папка, которая содержит шаблоны для графического интерфейса Kaspersky Scan Engine.
\include\	Папка, которая содержит заголовочные файлы KAV SDK для разработки приложений.
\runtime\	Библиотеки Universal C Runtime (UCRT) C++ Runtime.
\samples\kavhttp\	Папка, которая содержит исходный код службы kavhttpd и образец клиента для нее.
\samples\tables.sql	Файл, содержащий SQL-запросы, которые необходимо выполнить после ручной установки Kaspersky Scan Engine.
\tools\kav_encrypt.exe	Утилита для шифрования учетных данных прокси-серверов и базы данных Kaspersky Scan Engine.
\tools\kavsigner.exe	Утилита для подписи приложений.
\tools\kl_access_util.exe	Утилита для восстановления пароля от учетной записи admin в графическом интерфейсе Kaspersky Scan Engine.
\tools\openssl.exe	Утилита OpenSSL.

Путь	Описание
\tools\openssl.cnf	Конфигурационный файл для OpenSSL.
\tools\msvcp80.dll \tools\msvcr80.dll \tools\Microsoft.VC80.CRT	Компоненты Microsoft Visual C++ Redistributable.
\install.exe	Инсталлятор.
\kl_control.bat	Скрипт для управления службами kavhttpd и klScanEngineUI.
\uninstall.exe	Деинсталлятор.
\ReleaseNotes.pdf	Примечания к выпуску.
\version	Версия Kaspersky Scan Engine.

kaspersky

Установка Kaspersky Scan Engine

Этот раздел содержит информацию о том, как установить Kaspersky Scan Engine.

В этом разделе

Подготовка к установке графического интерфейса Kaspersky Scan Engine

Графический интерфейс Kaspersky Scan Engine использует объектно-реляционную систему управления базами данных (СУБД) PostgreSQL для хранения статистики сканирования, результатов сканирования, служебных событий и статуса службы. По этой причине, если вы хотите использовать графический интерфейс Kaspersky Scan Engine, вам нужно вначале установить PostgreSQL.

Вы можете использовать одну из двух интеграционных схем:

- Установите Kaspersky Scan Engine на том же компьютере, что и PostgreSQL.
- Установите Kaspersky Scan Engine на другом компьютере, с которого есть доступ к компьютеру с PostgreSQL.

In this section

Установка и настройка PostgreSQL (Linux)

Графический интерфейс Kaspersky Scan Engine требует установленной СУБД PostgreSQL 10.7 или более поздней версии. Приведенная ниже процедура описывает установку и настройку PostgreSQL 10.7. Для более поздней версии СУБД процедура может отличаться от данной.

► *Чтобы установить и настроить PostgreSQL:*

1. Загрузите и установите PostgreSQL.

   Вы можете установить PostgreSQL одним из следующих способов:

   - Установите пакет, загруженный с веб-сайта PostgreSQL.

     Зайдите на сайт https://www.postgresql.org/download/ https://www.postgresql.org/download/, чтобы ознакомиться со списком поддерживаемых операционных систем и инструкциями по установке

для каждой из них.

- Установите PostgreSQL из исходного кода.

  Зайдите на сайт https://www.postgresql.org/docs/10/installation.html, чтобы ознакомиться с инструкциями по установке.

2. Откройте конфигурационный файл `postgresql.conf`. Расположение этого файла зависит от используемой операционной системы:

   - В дистрибутивах Linux, основанных на Debian, файл `postgresql.conf` находится в директории `/etc/postgresql/10/main/`.
   - В дистрибутивах Linux, основанных на Red Hat, файл `postgresql.conf` находится в директории /var/lib/pgsql/data/.

   Если вы используете иную операционную систему, расположение файла `postgresql.conf` может быть другим.

3. Укажите IP-адрес, который решение Kaspersky Scan Engine должно использовать для соединения с PostgreSQL, в настройке `listen_addresses` конфигурационного файла `postgresql.conf`.
4. Укажите порт, который СУБД PostgreSQL должна прослушивать в ожидании соединений от Kaspersky Scan Engine, в настройке `port` конфигурационного файла `postgresql.conf`.
5. Сохраните и закройте `postgresql.conf`.
6. Откройте конфигурационный файл `pg_hba.conf` на редактирование. Этот файл расположен в той же директории, что и файл `postgresql.conf`.
7. Укажите, что СУБД PostgreSQL должна принимать пароли, зашифрованные по алгоритму MD5, для аутентификации всех ее клиентов:

   a. Найдите следующую строку в файле `pg_hba.conf`:

   ```
   host        all   all   127.0.0.1/32   peer
   ```

   b. Отредактируйте эту строку следующим образом:

   ```
   host        all   all   127.0.0.1/32   md5
   ```

   > Если конфигурационный файл `pg_hba.conf` не содержит указанную строку `host all all 127.0.0.1/32 peer`, отредактируйте вместо нее строку `host all all 127.0.0.1/32 ident`.

8. Если PostgreSQL и Kaspersky Scan Engine установлены на разных компьютерах, добавьте следующую строку в файл `pg_hba.conf`:

   ```
   host        all   all   %IP%/32   md5
   ```

   Здесь `%IP%` – IP-адрес компьютера, на котором установлено решение Kaspersky Scan Engine.

9. Сохраните и закройте файл `pg_hba.conf`.
10. Перезапустите PostgreSQL, выполнив следующую команду:

    ```
    service postgresql restart
    ```

11. Задайте пароль для пользователя PostgreSQL, существующего по умолчанию.

При установке PostgreSQL создает суперпользователя `postgres`. По умолчанию для этого пользователя пароль не задан.

Чтобы задать пароль для пользователя `postgres`:

a. Из командной строки сделайте пользователя `postgres` текущим следующим образом:

```
su postgres
```

b. Из-под учетной записи `postgres` запустите утилиту psql, выполнив следующую команду в командной строке:

```
psql
```

c. В psql измените пароль пользователя `postgres` с помощью следующей команды:

```
alter user postgres with password '%PASSWORD%';
```

Здесь `%PASSWORD%` – это новый пароль пользователя `postgres`.

d. Закройте утилиту psql, выполнив следующую команду в psql:

```
\q
```

Теперь вы можете установить графический интерфейс Kaspersky Scan Engine.

Чтобы установить графический интерфейс Kaspersky Scan Engine, вам нужен пользователь PostgreSQL с правами на создание новых баз данных и пользователей. Для этого вы можете использовать пользователя `postgres` или создано нового.

После установки PostgreSQL и задания пароля для пользователя postgres вы можете перейти к действиям, описанным в разделе Установка с использованием скрипта (Linux) (на стр. 22).

Все данные хранятся в базе данных `kavebase`. Kaspersky Scan Engine не использует другие базы данных.

Установка и настройка PostgreSQL (Windows)

В том разделе описана установка и настройка СУБД PostgreSQL в операционной системе семейства Windows.

► *Чтобы установить и настроить PostgreSQL:*

1. Загрузите и установите PostgreSQL.

   Зайдите на сайт https://www.enterprisedb.com/downloads/postgres-postgresql-downloads https://www.postgresql.org/download/, чтобы ознакомиться со списком поддерживаемых операционных систем и загрузить установщик.

2. Откройте конфигурационный файл `postgresql.conf` на редактирование. Этот файл расположен в папке `%postgresql_dir%\data`. Здесь `%postgresql_dir%` – это папка, куда установлена СУБД PostgreSQL (например, `C:\Program Files\PostgreSQL\11`).

3. Укажите IP-адрес, который решение Kaspersky Scan Engine должно использовать для соединения с PostgreSQL, в настройке `listen_addresses` конфигурационного файла `postgresql.conf`.

4. Укажите порт, который СУБД PostgreSQL должна прослушивать в ожидании соединений от Kaspersky Scan Engine, в настройке `port` конфигурационного файла `postgresql.conf`.
5. Сохраните и закройте `postgresql.conf`.
6. Откройте конфигурационный файл `pg_hba.conf` на редактирование. Этот файл расположен в той же папке, что и файл `postgresql.conf`.
7. Убедитесь, что PostgreSQL принимает пароли, зашифрованные по алгоритму MD5, для аутентификации всех ее клиентов. Для этого найдите следующую строку в файле `pg_hba.conf`:

   ```
   host        all   all   127.0.0.1/32   md5
   ```

   Если метод аутентификации, указанный в этой строке, отличается от `md5`, замените его на `md5`.
8. Если PostgreSQL и Kaspersky Scan Engine установлены на разных компьютерах, добавьте следующую строку в файл `pg_hba.conf`:

   ```
   host        all   all   %IP%/32   md5
   ```

   Здесь `%IP%` – IP-адрес компьютера, на котором установлено решение Kaspersky Scan Engine.
9. Сохраните и закройте файл `pg_hba.conf`.
10. Перезапустите PostgreSQL, выполнив следующие команды:

```
sc stop postgresql-x64-11
sc start postgresql-x64-11
```

Теперь вы можете установить графический интерфейс Kaspersky Scan Engine.

Чтобы установить графический интерфейс Kaspersky Scan Engine, вам нужен пользователь PostgreSQL с правами на создание новых баз данных и пользователей. Для этого вы можете использовать пользователя `postgres` или создать нового.

После установки PostgreSQL вы можете перейти к действиям, описанным в разделе Установка с использованием (Windows) (см. раздел "Установка с использованием инсталлятора (Windows)" на стр. 24).

Все данные хранятся в базе данных `kavebase`. Kaspersky Scan Engine не использует другие базы данных.

Установка с использованием скрипта (Linux)

Этот раздел объясняет как установить Kaspersky Scan Engine используя скрипт установки.

Если вы хотите использовать графический интерфейс Kaspersky Scan Engine, вам нужно установить СУБД PostgreSQL на компьютер, к которому у Kaspersky Scan Engine есть доступ. Графический интерфейс Kaspersky Scan Engine не будет работать без доступа к PostgreSQL.

► *Чтобы установить Scan Engine, используя скрипт установки:*

1. Убедитесь, что у вас есть права администратора.
2. Запустите скрипт `install`.
3. Ознакомьтесь с Пользовательским соглашением (End User License Agreement, EULA) для Kaspersky Scan Engine.

   Если вы согласны с условиями Пользовательского соглашения, примите его. Если вы не согласны с условиями Пользовательского соглашения, прекратите установку.
4. Если вы хотите использовать графический интерфейс Kaspersky Scan Engine, выполните следующие действия:

   a. Выполните действия, описанные в разделе "Подготовка к установке графического интерфейса Kaspersky Scan Engine" (на стр. 19).

   b. Укажите IP-адрес и порт для соединения с PostgreSQL.

   c. Введите учетные данные пользователя, у которого есть права на создание баз данных и пользователей. Учетные данные этого пользователя нигде не записываются.

      С помощью этой учетной записи Kaspersky Scan Engine создаст новую базу данных, которая будет называться kavebase и нового пользователя PostgreSQL с именем scanengine. В базе kavebase Kaspersky Scan Engine будет хранить данные. Учетная запись scanengine будет использоваться для внесения изменения в эту базу данных.
5. Выберите режим, в котором будет работать Kaspersky Scan Engine.

   Доступны следующие режимы:

   - режим HTTP;
   - режим ICAP.
6. Если вы выбрали режим HTTP, укажите IP-адрес и порт или UNIX-сокет, которые Kaspersky Scan Engine будет использовать для получения запросов на сканирование объектов.
7. Если вы выбрали режим ICAP, укажите порт, трафик с которого будет сканироваться решением Kaspersky Scan Engine.
8. Укажите, должно ли решение Kaspersky Scan Engine использовать Kaspersky Security Network (KSN).
9. Если вы хотите использовать KSN, ознакомьтесь с Пользовательским соглашением для KSN и Политикой конфиденциальности (Privacy Policy).

   Если вы согласны с условиями Пользовательского соглашения и Политики конфиденциальности, примите их.

   Участие в Kaspersky Security Network добровольное. Отказ от участия в Kaspersky Security Network не прерывает процесс установки Kaspersky Scan Engine. Если вы не примете условия Пользовательского соглашения и Политики конфиденциальности, вы не сможете использовать KSN, но установка продолжится.

   Вы сможете включить KSN позже, используя графический интерфейс Kaspersky Scan Engine или конфигурационные файлы.

   Для сохранения сертифицированной конфигурации программы использование Глобального KSN должно быть выключено.
10. Если вы хотите использовать графический интерфейс Kaspersky Scan Engine, при необходимости укажите порт, на котором будет доступен.
11. Укажите, будет ли Kaspersky Scan Engine использовать прокси-сервер.
12. Если вы хотите использовать прокси-сервер, укажите настройки прокси.

13. Укажите директорию, где будут храниться временные файлы.

    Установочный скрипт создаст в ней поддиректорию `scanengine`, в которой будут создаваться временные файлы.

14. Укажите режим лицензирования, который будет использоваться в Kaspersky Scan Engine.

    - Если вы хотите использовать режим лицензирования оффлайн, укажите файл ключа.
    - Если вы хотите использовать режим лицензирования онлайн, укажите код активации.

15. Проверьте указанные вами параметры и при необходимости откорректируйте их.

После того, как вы укажете все необходимые данные, скрипт `install` установит Kaspersky Scan Engine и запустит его. Информация об установке будет выведена на терминал.

Установка с использованием инсталлятора (Windows)

В этом разделе описана установка Kaspersky Scan Engine с использованием инсталлятора.

Если вы хотите использовать графический интерфейс Kaspersky Scan Engine, вам нужно установить СУБД PostgreSQL на компьютер, к которому у Kaspersky Scan Engine есть доступ. Графический интерфейс Kaspersky Scan Engine не будет работать без доступа к PostgreSQL.

► *Чтобы установить Kaspersky Scan Engine, используя инсталлятор:*

1. Распакуйте архив пакета распространения в пустую папку на вашем компьютере.
2. Убедитесь, что у вас есть права администратора.
3. Запустите файл `install.exe`.
4. Ознакомьтесь с Пользовательским соглашением (End User License Agreement, EULA) для Kaspersky Scan Engine.

   Если вы согласны с условиями Пользовательского соглашения, примите его. Если вы не согласны с условиями Пользовательского соглашения, установка будет завершена.

5. Если вы хотите использовать графический интерфейс Kaspersky Scan Engine, выполните следующие действия:

   a. Выполните действия, описанные в разделе "Установка и настройка PostgreSQL (Windows)" (на стр. 21).

   b. Укажите IP-адрес и порт для соединения с PostgreSQL.

   c. Введите учетные данные пользователя, у которого есть права на создание баз данных и пользователей. Учетные данные этого пользователя нигде не записываются.

      С помощью этой учетной записи Kaspersky Scan Engine создаст новую базу данных, которая будет называться kavebase и нового пользователя PostgreSQL с именем scanengine. В базе kavebase Kaspersky Scan Engine будет хранить данные. Учетная запись scanengine будет использоваться для внесения изменения в эту базу данных.

6. Укажите IP-адрес и порт, которые Kaspersky Scan Engine будет использовать, чтобы получать запросы на сканирование объектов.
7. Укажите, должен ли Kaspersky Scan Engine использовать Kaspersky Security Network (KSN).
8. Если вы хотите использовать KSN, ознакомьтесь с Пользовательским соглашением для KSN и Политикой конфиденциальности (Privacy Policy).

Если вы согласны с условиями Пользовательского соглашения и Политики конфиденциальности, примите их. Если вы не примете условия Пользовательского соглашения и Политики конфиденциальности, вы не сможете использовать KSN, но установка продолжиться. Вы сможете включить KSN позже, используя графический интерфейс Kaspersky Scan Engine или конфигурационные файлы.

9. Если вы хотите использовать графический интерфейс Kaspersky Scan Engine, укажите порт, на котором будет доступен.
10. Укажите, будет ли Kaspersky Scan Engine использовать прокси-сервер.
11. Если вы хотите использовать прокси-сервер, укажите настройки прокси.
12. Укажите директорию, где будут храниться временные файлы.

    Установочный скрипт создаст в ней поддиректорию scanengine, в которой будут создаваться временные файлы.
13. Укажите режим лицензирования, который будет использоваться в Kaspersky Scan Engine.
    - Если вы хотите использовать режим лицензирования оффлайн, укажите файл ключа.
    - Если вы хотите использовать режим лицензирования онлайн, укажите код активации.
14. Проверьте указанные вами параметры и при необходимости откорректируйте их.

После того, как вы укажете все необходимые данные, скрипт `install` установит Kaspersky Scan Engine и запустит его. Решение Kaspersky Scan Engine будет установлено в папку `C:\Program Files\Kaspersky Lab\ScanEngine`. Информация об установке будет выведена на консоль.

kaspersky

Использование Kaspersky Scan Engine в режиме HTTP

Этот раздел содержит информацию о том, как использовать Kaspersky Scan Engine в режиме HTTP.

В этом разделе

Kaspersky Scan Engine и режим HTTP

Протокол HTTP является стандартным протоколом для передачи данных в архитектуре "клиент-сервер". В режиме HTTP решение Kaspersky Scan Engine выступает как REST-подобная служба, которая получает от клиентов HTTP-запросы в формате JSON. Служба сканирует объекты, посланные в этих запросах, и отправляет обратно HTTP-ответы с результатами сканирования.

Пакет распространения Kaspersky Scan Engine включает в себя образец HTTP-клиента и его исходный код.

Способы передачи данных

Поддерживаются два способа передачи данных между клиентами и Kaspersky Scan Engine:

- TCP-соединение
- UNIX-сокет

  Этот режим доступен только для операционных систем Linux.

Режимы сканирования

Kaspersky Scan Engine поддерживает следующие режимы сканирования:

- `scanfile`

  В этом режиме клиент посылает решению Kaspersky Scan Engine путь до файла, который нужно просканировать.

- `scanmemory`

  В этом режиме клиент посылает решению Kaspersky Scan Engine содержимое файла, который нужно просканировать.

- `checkurl`

  В этом режиме клиент посылает решению Kaspersky Scan Engine веб-адрес, который нужно проверить.

Дополнительную информацию о режимах сканирования вы можете найти в разделе "Совершение запросов в режиме HTTP (на стр. 38)".

Настройка Kaspersky Scan Engine в режиме HTTP

Этот раздел содержит информацию о том, как настроить Kaspersky Scan Engine в режиме HTTP, не используя графический интерфейс.

Конфигурационный файл для режима HTTP

Конфигурационный файл для режима HTTP (далее также конфигурационный файл) представляет собой XML-файл, который определяет параметры Kaspersky Scan Engine.

Конфигурационный файл для режима HTTP (Linux)

В пакете распространения для Linux (см. раздел "Содержимое пакета распространения (Linux)" на стр. 13) конфигурационный файл расположен в директории `/etc/kavhttpd.xml`.

После установки Kaspersky Scan Engine (см. раздел "Установка с использованием скрипта (Linux)" на стр. 22), скопируйте файл `kavhttpd.xml` в желательную для вас директорию:

- Если вы скопируете `kavhttpd.xml` в директорию `/etc/`, Kaspersky Scan Engine автоматически найдет его и применит указанные в нем параметры после перезагрузки службы.
- Если вы скопируете `kavhttpd.xml` в другую директорию, вам нужно указать путь до него в переменной `CONFILE` скрипта инициализации (см. раздел "Запуск Kaspersky Scan Engine с помощью скрипта инициализации (Linux)" на стр. 36), например:

  `CONFILE=/opt/kaspersky/ScanEngine/etc/kavhttpd.xml`.

  После этого нужно перезагрузить службу.

Конфигурационный файл для режима HTTP (Windows)

В пакете распространения для Windows (см. раздел "Содержимое пакета распространения (Linux)" на стр. 13) конфигурационный файл расположен по пути `bin\kavhttpd.xml`.

Параметры конфигурационного файла для режима HTTP

Большинство элементов конфигурационного файла имеют значения по умолчанию, которые используются, если элемент не указан явно. Не указывайте в элементах конфигурационного файла пустые значения, если возможность этого не указана в данной документации.

ServerSettings

Следующие элементы определяют параметры Kaspersky Scan Engine:

- `MaxIncomingConnectionsNum` – максимальное количество TCP-соединений между Kaspersky Scan Engine и клиентами. Значение этого элемента должно быть целым положительным числом.

  Kaspersky Scan Engine может одновременно обработать количество соединений, указанное в элементе `MaxHTTPSessionsNum` (см. ниже). Остальные соединения образуют очередь.

  Значение по умолчанию – `100`.

- `MaxHTTPSessionsNum` – максимальное количество одновременных TCP-соединений между Kaspersky Scan Engine и клиентами. Значение этого элемента должно быть целым положительным числом.

  Значение по умолчанию – `10`. Если вы укажете в этом элементе `0`, будет использовано значение по умолчанию.

- `MaxTCPFileSize` – максимальный допустимый размер HTTP-сообщения, которое клиент может послать в Kaspersky Scan Engine (в байтах). Значение этого элемента должно быть целым положительным числом.

  Рекомендуется выделять по крайней мере 100 КБ для заголовков сообщения.

  Значение по умолчанию – `104857600` (100 МБ). Если вы укажете в этом элементе `0`, будет использовано значение по умолчанию.

- `ConnectionString` – IP-адрес и порт или путь к UNIX-сокету, которые используются клиентами для соединения с Kaspersky Scan Engine. Значение этого элемента должно быть строкой. Обязательный параметр.

  Значение по умолчанию – `/tmp/.kavhttpd` в Linux и `127.0.0.1:9999` в Windows. Указывайте IP-адрес и порт в следующем формате: `ip_addr:port`.

- `SessionTimeout` – таймаут на соединение с клиентом, сканирование и ответ (в миллисекундах). Значение этого элемента должно быть целым положительным числом.

  Значение по умолчанию – `1000`. Если вы укажете в этом элементе 0, будет использовано значение по умолчанию.

- `Flags` – параметры инициализации Kaspersky Scan Engine. Параметры определяются комбинацией флагов, разделенных вертикальными чертами (`|`).

  Значение этого элемента должно быть строкой.

  Поддерживаемые флаги:

  - `KAV_SHT_ENGINE_KLAV`

    Включает антивирусный движок KLAV.

    > Если вы указали этот флаг, указывать флаг `KAV_SHT_ENGINE_KLAVEMU` не обязательно. Движок KLAV автоматически включает эмулятор KLAV.

  - `KAV_SHT_ENGINE_KLAVEMU`

    Включает глубинный эвристический анализ (эмулятор KLAV). Укажите этот флаг, если вы хотите использовать эвристику.

  - `KAV_SHT_ENGINE_WMUF`

    Включает обнаружение вредоносных веб-адресов.

  - `KAV_SHT_ENGINE_APUF`

    Включает обнаружение фишинговых веб-адресов.

  - `KAV_SHT_ENGINE_KSN`

    Включает проверку репутации файлов и веб-адресов в Kaspersky Security Network (KSN).

Прежде чем указывать этот флаг, убедитесь, что ваша лицензия позволяет вам использовать эту функциональность и что вы прочитали и приняли условия EULA для KSN.

- `KAV_SHT_ENGINE_STATISTIC_MAIL`

  Включает передачу статистики в KSN в операционной системе Linux.

  Прежде чем указывать этот флаг, убедитесь, что ваша лицензия позволяет вам использовать эту функциональность.

- `KAV_SHT_ENGINE_STATISTIC`

  Включает передачу статистики в KSN в операционной системе Windows.

  Прежде чем указывать этот флаг, убедитесь, что ваша лицензия позволяет вам использовать эту функциональность.

Обратите внимание, что, указывая флаг `KAV_SHT_ENGINE_KSN`, флаг `KAV_SHT_ENGINE_STATISTIC_MAIL` или флаг `KAV_SHT_ENGINE_STATISTIC`, вы соглашаетесь передавать данные, описанные в соответствующем файле `About data provision*.txt`, в "Лабораторию Касперского". Дополнительную информацию о передаче данных в "Лабораторию Касперского" вы можете найти в разделе "О предоставлении данных (на стр. 67)".

KSNSettings

Следующие элементы определяют параметры KSN:

- `UrlCheckTimeoutMs` – таймаут на ожидание ответа от KSN при проверке репутации веб-адресов (в миллисекундах). Значение этого элемента должно быть целым положительным числом.

  Значение по умолчанию – `20000`.

  Обратите внимание, что этот элемент устанавливает таймаут только на проверки репутации в KSN. Этот таймаут не включает в себя время, необходимое для отправки запроса, и время получения ответа от KSN. Таймаут может быть превышен, если KSN определит, что веб-адрес опасен.

- `ObjectCheckOnDemandTimeoutMs` – таймаут на ожидание ответа от KSN при проверке репутации файлов (в миллисекундах). Значение этого элемента должно быть целым положительным числом.

  Значение по умолчанию – `10000`.

> Обратите внимание, что этот элемент устанавливает таймаут только на проверки репутации в KSN. Этот таймаут не включает в себя время, необходимое для отправки запроса, и время получения ответа от KSN. Таймаут может быть превышен, если KSN определит, что файл опасен.

- `CacheSizeKb` – Размер кеша ответов от KSN (в килобайтах). Kaspersky Scan Engine использует этот кеш, чтобы хранить информацию о репутации объектов, полученную от KSN.

  Значение этого элемента должно быть целым положительным числом. Если вы укажете в этом элементе `0`, KSN не будет использоваться. Максимальное допустимое значение – `262143`. Значение по умолчанию – `30720`.

KAVScanningSettings

Следующие элементы определяют параметры библиотеки KAV SDK, которая является частью Kaspersky Scan Engine:

- `ScannersCount` – количество сканирующих процессов. Максимальное допустимое значение – `256`. Значение этого элемента должно быть целым положительным числом.

  Значение по умолчанию – `16`.

- `ThreadsCount` – количество одновременно работающих сканирующих программных потоков. Максимальное допустимое значение – `256`. Значение этого элемента должно быть целым положительным числом.

  Значение по умолчанию – `16`.

- `QueueLen` – максимальная длина очереди сканирования. Значение этого элемента должно быть целым положительным числом.

  Значение по умолчанию – `1024`.

- `Flags` – режим сканирования.

  Режим сканирования определяется комбинацией флагов, разделенных вертикальными чертами (|). Значение этого элемента должно быть строкой.

  Поддерживаемые флаги:

  - `KAV_O_M_PACKED`

    Включает сканирование упакованных исполняемых файлов.

  - `KAV_O_M_ARCHIVED`

    Включает сканирование архивов.

  - `KAV_O_M_MAILBASES`

    Включает сканирование почтовых баз.

  - `KAV_O_M_MAILPLAIN`

    Включает сканирование электронной почты.

  - `KAV_O_M_HEURISTIC_LEVEL_SHALLOW`

    Включает эвристический анализ с уровнем детализации `shallow` (**Low** в графическом интерфейсе).

- `KAV_O_M_HEURISTIC_LEVEL_MEDIUM`

  Включает эвристический анализ с уровнем детализации `medium` (**Medium** в графическом интерфейсе).

- `KAV_O_M_HEURISTIC_LEVEL_DETAIL`

  Включает эвристический анализ с уровнем детализации `detailed` (**High** в графическом интерфейсе).

- `KAV_O_M_MSOFFICE_MACRO`

  Включает обнаружение макросов в файлах Microsoft Office.

Элемент `Flags` может быть пустым. В этом случае используется значение `0`.

Значение по умолчанию – `KAV_O_M_PACKED | KAV_O_M_ARCHIVED | KAV_O_M_MAILBASES | KAV_O_M_MAILPLAIN | KAV_O_M_HEURISTIC_LEVEL_DETAIL`.

- `Mode` – режим лечения и удаления зараженных объектов. Обязательный параметр.

  Значение этого элемента должно быть строкой.

  Поддерживаемые флаги:

  - `KAV_SKIP`

    Если во время сканирования объекта Kaspersky Scan Engine найдет угрозу, рекламную программу или легальную программу, которая может быть использована злоумышленником для нанесения вреда вашим данным, он не предпримет никаких действий над этим объектом.

    Вы должны указать это значение, если вы хотите сканировать объекты в оперативной памяти (см. раздел "Пример HTTP запроса на сканирование части оперативной памяти" на стр. 41).

  - `KAV_DELETE`

    Если во время сканирования объекта Kaspersky Scan Engine найдет угрозу, рекламную программу или легальную программу, которая может быть использована злоумышленником для нанесения вреда вашим данным, он попробует удалить этот объект. Если удаление невозможно, Kaspersky Scan Engine перейдет к сканированию следующего объекта.

  - `KAV_CLEAN_DELETE`

    Если во время сканирования объекта Kaspersky Scan Engine найдет угрозу, рекламную программу или легальную программу, которая может быть использована злоумышленником для нанесения вреда вашим данным, он попробует вылечить этот объект. Если лечение невозможно, Kaspersky Scan Engine попробует удалить объект. Если удаление также невозможно, Kaspersky Scan Engine перейдет к сканированию следующего объекта.

  - `KAV_CLEAN_SKIP`

    Если во время сканирования объекта Kaspersky Scan Engine найдет угрозу, рекламную программу или легальную программу, которая может быть использована злоумышленником для нанесения вреда вашим данным, он попробует вылечить этот объект. Если лечение невозможно, Kaspersky Scan Engine перейдет к сканированию следующего объекта.

  Значение по умолчанию – `KAV_SKIP`.

DirectorySettings

Следующие элементы определяют настройки для директорий библиотеки KAV SDK, которая является частью Kaspersky Scan Engine:

- `BasesPath` – директория, в которой находится база данных. Значение этого элемента должно быть строкой.

  Обязательный параметр.

  > Обратите внимание, что если вы работаете в Windows, вам нужно указать абсолютный путь.

- `TempPath` – директория, в которой находятся файлы, создаваемые во время работы Kaspersky Scan Engine. Путь до директории должен быть абсолютным. Значение этого элемента должно быть строкой.

  Обязательный параметр.

  > Не удаляйте файлы из этой директории.

- `LicensePath` – директория, в которой находятся файлы, относящиеся к лицензированию. Значение этого элемента должно быть строкой.

  KAV SDK ищет эти файлы в следующих директориях:

  - В директории, указанной в `LicensePath`.
  - В директории, которая содержит исполняемый файл `kavhttpd`.
  - В директории `%service_dir%/ppl` (только для операционных систем Linux).

  Обязательный параметр.

- `LicensingMode` – режим лицензирования.

  Возможные значения:

  - `1` – режим лицензирования оффлайн;
  - `2` – режим лицензирования онлайн.

  Значение по умолчанию – `1`.

- `ScanningPaths` – пути до директорий, в которых разрешено сканирование по TCP-сокету, когда клиент посылает запрос на сканирование с удаленного компьютера. Этот параметр позволяет предотвратить ситуацию, когда удаленный клиент по ошибке запрашивает сканирование всей файловой системы на компьютере, на котором установлено решение Kaspersky Scan Engine.

  - `ScanningPath` – путь до директории, в которой разрешено сканирование по TCP-сокету.

    Возможные значения:

    - Абсолютный путь до директории

      Позволяет сканировать файлы, расположенные внутри этой директории и всех ее поддиректорий.

      Директория должны быть расположена на том же компьютере, что и Kaspersky Scan Engine, или на смонтированном внешнем жестком диске.

      Путь должен начинаться с корневой директории файловой системы компьютера, на котором установлен Kaspersky Scan Engine.

Служба kavhttpd должна иметь права на чтение файлов в этой директории и всех ее поддиректориях.

- Абсолютный путь до файла.

  Позволяет сканировать определенный файл.

  Файл должен быть расположен на том же компьютере, что и Kaspersky Scan Engine, или на смонтированном внешнем жестком диске.

  Путь должен начинаться с корневой директории файловой системы компьютера, на котором установлен Kaspersky Scan Engine.

  Служба kavhttpd должна иметь права на чтение этого файла.

- `/` (косая черта)

  Позволяет сканировать все файлы файловой системы.

  > Этот режим доступен только для операционных систем Linux.

Каждое значение должно быть указано внутри отдельного элемента <`ScanningPath`>.

UseHTTPProxy и HTTPProxy

Следующие элементы определяют настройки прокси-сервера для библиотеки KAV SDK, которая является частью Kaspersky Scan Engine.

> В текущей версии библиотеки KAV SDK поддерживаются только HTTP-прокси.

- `UseHTTPProxy` – определяет, использует ли Kaspersky Scan Engine прокси при соединении с интернетом. Этот параметр может иметь значение `0` или `1`.

  Значение по умолчанию – `0` (прокси не используется). Чтобы начать использовать прокси, поменяйте значение на `1`.

- `HTTPProxy` – параметры прокси.

  - `url` – адрес прокси-сервера. Значение этого элемента должно быть строкой.

    Адрес прокси-сервера может быть IPv4-адресом, IPv6-адресом или доменным именем. Не указывайте протокол (`http://` или `https://`) в этом элементе.

    Если элемент `UseHTTPProxy` имеет значение `1`, этот параметр указывать обязательно.

  - `port` – порт прокси-сервера.

    Значение по умолчанию – `3128`.

  - `user` – зашифрованное имя пользователя для аутентификациии. Имя пользователя должно быть зашифровано с помощью утилиты `kav_encrypt`. Значение этого элемента должно быть строкой.

    Если элемент `UseHTTPProxy` имеет значение `1`, этот параметр указывать обязательно.

  - `pass` – зашифрованный пароль для аутентификациии. Пароль должно быть зашифровано с помощью утилиты `kav_encrypt`. Значение этого элемента должно быть строкой.

Если элемент `UseHTTPProxy` имеет значение `1`, этот параметр указывать обязательно.

UpdateSettings

Следующие элементы определяют параметры обновления Kaspersky Scan Engine:

- `DisableBackup` – определяет, включена ли функция резервного копирования антивирусной базы. Этот параметр может иметь значение `0` или `1`.

  Если этот параметр имеет значение `1`, резервное копирование антивирусной базы отключено.

  Значение по умолчанию – `0`.

- `UpdatePeriodMinutes` – интервал между автоматическими обновлениями (в минутах). Значение этого элемента должно быть целым положительным числом.

  Максимальное возможное значение – `44640`.

  Если этот параметр имеет значение `0`, автоматические обновления отключены.

  Значение по умолчанию – `0`.

- `UseOnlyCustomSources` – определяет, используются ли источники обновления по умолчанию. Этот параметр может иметь значение `0` или `1`.

  Если этот параметр имеет значение `1`, используются только дополнительные источники обновления.

  Значение по умолчанию – `0`.

- `UpdateSources` – адреса дополнительных источников обновления.

  - `Source` – адрес дополнительного источника обновления. Значение этого элемента должно быть строкой.

  Каждый источник обновления должен быть указан внутри отдельного элемента `<Source>`.

FormatRecognizerSettings

Следующие элементы определяют параметры компонента Format Recognizer:

- `FormatsToSkipScanning` – определяет, какие форматы файлов решение Kaspersky Scan Engine не должно сканировать.

  Чтобы выключить этот компонент, удалите элемент `FormatRecognizerSettings` или оставьте его пустым.

Структура конфигурационного файла

Ниже приведен пример конфигурационного файла:

```
<Configuration>

    <ServerSettings>
        <ConnectionString>/tmp/.kavhttpd</ConnectionString>
        <MaxIncomingConnectionsNum>100</MaxIncomingConnectionsNum>
        <MaxHTTPSessionsNum>50</MaxHTTPSessionsNum>
        <MaxTCPFileSize>100</MaxTCPFileSize>
        <SessionTimeout>1000</SessionTimeout>
```

```
            <Flags>KAV_SHT_ENGINE_KSN | KAV_SHT_ENGINE_APUF</Flags>
      </ServerSettings>

      <KSNSettings>
            <UrlCheckTimeoutMs>20000</UrlCheckTimeoutMs>

      <ObjectCheckOnDemandTimeoutMs>10000</ObjectCheckOnDemandTimeoutMs>
            <CacheSizeKb>30720</CacheSizeKb>
      </KSNSettings>

      <KAVScanningSettings>
            <ScannersCount>16</ScannersCount>
            <ThreadsCount>32</ThreadsCount>
            <QueueLen>1028</QueueLen>
            <Flags>KAV_O_M_PACKED | KAV_O_M_ARCHIVED | KAV_O_M_MAILBASES |
KAV_O_M_MAILPLAIN | KAV_O_M_HEURISTIC_LEVEL_DETAIL</Flags>
            <Mode>KAV_SKIP</Mode>
      </KAVScanningSettings>

      <DirectorySettings>
            <BasesPath>/home/bases</BasesPath>
            <TempPath>/home/temp</TempPath>
            <LicensePath>/home/license</LicensePath>
            <LicensingMode>1</LicensingMode>
            <ScanningPaths>
                  <ScanningPath></ScanningPath>
            </ScanningPaths>
      </DirectorySettings>

      <UseHTTPProxy>1</UseHTTPProxy>

      <HTTPProxy>
            <url>myproxy.mycompany.com</url>
            <port>3128</port>
            <user>proxyuser</user>
            <pass>proxypass</pass>
      </HTTPProxy>

      <UpdateSettings>
            <DisableBackup>0</DisableBackup>
            <UpdatePeriodMinutes>0</UpdatePeriodMinutes>
            <UseOnlyCustomSources>0</UseOnlyCustomSources>
            <UpdateSources>
                  <Source>[update source]</Source>
            </UpdateSources>
      </UpdateSettings>

      <FormatRecognizerSettings>
            <FormatsToSkipScanning>
                  <KAV_FF_GENERAL_TXT/>
```

```
                <KAV_FF_GENERAL_CSV/>
                <KAV_FF_AUDIO_WMA/>
            </FormatsToSkipScanning>
        </FormatRecognizerSettings>

    </Configuration>
```

Запуск Kaspersky Scan Engine в режиме HTTP

Этот раздел содержит информацию о том, как запустить Kaspersky Scan Engine в режиме HTTP.

Запуск Kaspersky Scan Engine с помощью скрипта инициализации (Linux)

С помощью скрипта инициализации вы можете управлять решением Kaspersky Scan Engine. Скрипт находится в директории `/etc/init.d/kavhttpd` пакета распространения (см. раздел "Содержимое пакета распространения (Linux)" на стр. 13).

Автоматический запуск Kaspersky Scan Engine

► *Чтобы настроить автоматический запуск Kaspersky Scan Engine при старте операционной системы:*

1. Если вы используете Security-Enhanced Linux (SELinux) в принудительном (`enforcing`) режиме, измените режим:
   a. Откройте файл `/etc/selinux/config` для редактирования.
   b. Найдите строку, которая содержит переменную `SELINUX`:

      ```
      SELINUX=enforcing
      ```

   c. Измените значение переменной `SELINUX` на `permissive` или `disabled`, например:

      ```
      SELINUX=permissive
      ```

   d. Сохраните и закройте файл `/etc/selinux/config`.
2. Скопируйте скрипт инициализации в директорию, в которой хранятся скрипты инициализации. Расположение этой директории зависит от операционной системы, которую вы используете, но обычно это `/etc/init.d`.
3. При необходимости отредактируйте скрипт инициализации.
4. Добавьте службу `kavhttpd` в список служб, которые загружаются автоматически при старте операционной системы. То, как вы можете это сделать, зависит от операционной системы, которую вы используете.

5. Убедитесь, что служба `kavhttpd` была успешно добавлена в список служб, которые загружаются автоматически при старте операционной системы. То, как вы можете это сделать, зависит от операционной системы, которую вы используете.
6. Перезапустите операционную систему, чтобы изменения вступили в силу.

Запуск Kaspersky Scan Engine

Чтобы запустить Kaspersky Scan Engine, вызовите скрипт инициализации с параметром `start`, как показано ниже:

```
/etc/init.d/kavhttpd start
Starting kavhttpd:  [  OK  ]
```

Остановка Kaspersky Scan Engine

Чтобы остановить Kaspersky Scan Engine, вызовите скрипт инициализации с параметром `stop`, как показано ниже:

```
/etc/init.d/kavhttpd stop
Stopping kavhttpd:  [  OK  ]
```

Перезапуск Kaspersky Scan Engine

Чтобы перезапустить Kaspersky Scan Engine, вызовите скрипт инициализации с параметром `restart`, как показано ниже:

```
/etc/init.d/kavhttpd restart
Stopping kavhttpd:  [  OK  ]
Starting kavhttpd:  [  OK  ]
```

Перезагрузка антивирусной базы

Чтобы перезагрузить антивирусную базу, вызовите скрипт инициализации с параметром `reloaddb` как показано ниже:

```
/etc/init.d/kavhttpd reloaddb
Reload databases kavhttpd:  [  OK  ]
```

Обновление антивирусной базы

Чтобы обновить антивирусную базу, вызовите скрипт инициализации с параметром `updatedb`, как показано ниже:

```
/etc/init.d/kavhttpd updatedb
Update databases kavhttpd:  [  OK  ]
```

Получение статуса Kaspersky Scan Engine

Чтобы получить статус Kaspersky Scan Engine, вызовите скрипт инициализации с параметром `status`, как показано ниже:

```
/etc/init.d/kavhttpd status
kavhttpd (pid 12892) is running...
```

Запуск Kaspersky Scan Engine в качестве службы (Windows)

После установки Kaspersky Scan Engine автоматически регистрируется в операционной системе как служба Windows. Вы можете запустить ее из командной строки, используя следующую команду:

```
net start "Kaspersky ScanEngine"
```

Совершение запросов в режиме HTTP

Этот раздел содержит информацию о том, как совершать запросы в режиме HTTP с использованием протокола KAV версии 3.

Формат POST-запроса на сканирование

POST-запросы на сканирование объекта имеют следующий формат:

```
* Заголовки запроса *

* Тело запроса *
{
    "timeout": %ТАЙМАУТ%,
    "omitCleanSubobjectResults": %ПРОПУСКАТЬ ЛИ ЧИСТЫЕ ПОДОБЪЕКТЫ%,
    "url": "%ВЕБ-АДРЕС%",
    "requestHeaders": "%ЗАГОЛОВКИ ИСХОДНОГО ЗАПРОСА%",
    "responseHeaders": "%ЗАГОЛОВКИ ИСХОДНОГО ОТВЕТА%",
    "object": "%ОБЪЕКТ%"
}
```

Здесь:

- `timeout` – таймаут на сканирование объекта (в миллисекундах). Это поле не является обязательным.
- `omitCleanSubobjectResults` – переменная логического типа, которая определяет, будут ли включены в массив `subObjectsScanResults` вложенные подобъекты с результатом сканирования `CLEAN`. Если у `omitCleanSubobjectResults` указано значение `true`, такие подобъекты не будут включены в массив. Если указано значение `false`, то такие подобъекты включаются в массив. Это поле не является обязательным.
- `url` – веб-адрес, который будет использован как контекст для запроса на сканирование. Это поле не является обязательным.
- `requestHeaders` – заголовки HTTP-запроса, извлеченные из HTTP-трафика. Указывайте это поле для увеличения точности сканирования объектов. Это поле не является обязательным.
- `responseHeaders` – заголовки HTTP-ответа, извлеченные из HTTP-трафика. Указывайте это поле для увеличения точности сканирования объектов. Это поле не является обязательным.

- `object` – абсолютный путь до файла, который нужно просканировать (если запрос послан к `/api/v3.0/scanfile`) или строка, закодированная по алгоритму Base64 (если запрос послан к `/api/v3.0/scanmemory`). Это поле является обязательным для заполнения.

Специальные символы в теле запроса должны быть экранированны как указано в Standard ECMA-404 (The JSON Interchange Syntax): https://www.ecma-international.org/publications/standards/Ecma-404.htm.

Формат ответа на POST-запрос на сканирование

Если POST-запрос был успешно обработан, тело ответа будет содержать JSON-объект со следующими полями:

```
{
    "object": "%ОБЪЕКТ%",
    "scanResult": "%РЕЗУЛЬТАТ СКАНИРОВАНИЯ%",
    "detectionName": "%ОБНАРУЖЕННЫЙ ОБЪЕКТ%",
    "containsOfficeMacro": "%ОБНАРУЖЕН ЛИ МАКРОС%",
    "subObjectsScanResults": [
    {
        "object": "%ПОДОБЪЕКТ%",
        "scanResult": "%РЕЗУЛЬТАТ СКАНИРОВАНИЯ ПОДОБЪЕКТА%",
        "detectionName": "%ОБНАРУЖЕННЫЙ ОБЪЕКТ%",
        "containsOfficeMacro": "%ОБНАРУЖЕН ЛИ МАКРОС%"
    },
    …
    {
        "object": "%ПОДОБЪЕКТ%",
        "scanResult": "%РЕЗУЛЬТАТ СКАНИРОВАНИЯ ПОДОБЪЕКТА%",
        "detectionName": "%ОБНАРУЖЕННЫЙ ОБЪЕКТТ%",
        "containsOfficeMacro": "%ОБНАРУЖЕН ЛИ МАКРОС%"
    }
    ]
}
```

Здесь:

- `object` – абсолютный путь до просканированного файла (если запрос был послан к `/api/v3.0/scanfile`) или строка "`memory`" (если запрос был послан к `/api/v3.0/scanmemory`)..
- `scanResult` – результата сканирования. Он может иметь следующие значения:
  - `CLEAN`
  - `DETECT`
  - `DISINFECTED`
  - `DELETED`
  - `NON_SCANNED`
  - `SERVER_ERROR`

- `detectionName` – категория обнаруженного объекта в классификации "Лаборатории Касперского".
- `containsOfficeMacro` – переменная логического типа, которая имеет значение `true`, если в просканированном объекте был обнаружен макрос, и `false` в противоположном случае.
- `subObjectsScanResults` – массив, состоящий из результатов сканирования подобъектов, вложенных в просканированный объект. Это поле и все вложенные в него поля будут добавлены в ответ, только если просканированный объект включает вложенные подобъекты.
  - `subObjectsScanResults/object` – путь до вложенного подобъекта. Обратите внимание, что путь к подобъекту отделен от пути к родительскому объекту двумя косыми чертами (`//`), например:

    `/home/user/archive.tar//folder/subobject`
  - `subObjectsScanResults/scanResult` – результат сканирования вложенного подобъекта.
  - `subObjectsScanResults/detectionName` – категория обнаруженного объекта в классификации "Лаборатории Касперского".
  - `subObjectsScanResults/containsOfficeMacro` – переменная логического типа, которая имеет значение `true`, если в просканированном подобъекте был обнаружен макрос, и `false` в противоположном случае.

Если POST-запрос был обработан с ошибкой, тело ответа будет содержать JSON-объект с единственным полем `error`:

```
{
    "error": "%СООБЩЕНИЕ ОБ ОШИБКЕ%"
}
```

Здесь поле `error` содержит описание ошибки, которая произошла во время обработки запроса.

Пример HTTP-запроса на сканирование локального файла

Ниже приведен пример HTTP-запроса на сканирование локального файла:

```
POST /api/v3.0/scanfile HTTP/1.0
Content-Type: application/octet-stream
Content-Length: 22

{
    "timeout": "10000",
    "object": "\/home\/user\/eicar"
}
```

Вы можете найти описание всех полей HTTP-запроса на сканирование в разделе "Формат POST-запроса на сканирование (на стр. 38)".

Ниже приведен пример ответа на запрос:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 15:46:29 GMT
Content-Length: 75

{
    "object": "\/home\/user\/eicar",
    "scanResult": "DETECT",
    "detectionName": "EICAR-Test-File"
}
```

Вы можете найти описание всех полей HTTP-ответа в разделе "Формат ответа на POST-запрос на сканирование (на стр. 39)".

Пример HTTP-запроса на сканирование части оперативной памяти

Ниже приведен пример HTTP-запроса на сканирование объекта в оперативной памяти:

```
POST /api/v3.0/scanmemory HTTP/1.0
Content-Type: application/octet-stream
Content-Length: 105

{
    "timeout": "10000",
    "object":
"WDVPIVAlQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFOVElWSVJVUy1UR
VNULUZJTEUhJEgrSCo="
}
```

Вы можете найти описание всех полей HTTP-запроса на сканирование в разделе "Формат POST-запроса на сканирование (на стр. 38)".

Ниже приведен пример ответа на запрос:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 16:08:12 GMT
Content-Length: 72

{
    "object": "memory",
    "scanResult": "DETECT",
    "detectionName": "EICAR-Test-File"
}
```

Вы можете найти описание всех полей HTTP-ответа в разделе "Формат ответа на POST-запрос на сканирование (на стр. 39)".

Пример HTTP-запроса на проверку веб-адреса

Ниже приведен пример HTTP-запроса на проверку веб-адреса:

```
POST /api/v3.0/checkurl HTTP/1.0
Content-Type: application/octet-stream
Content-Length: 50

{
    "timeout": "10000",
    "url": "http:\/\/bug.qainfo.ru\/TesT\/Aphish_w"
}
```

Ниже приведен пример ответа на запрос:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 16:15:44 GMT
Content-Length: 104

{
    "url": "http:\/\/bug.qainfo.ru\/TesT\/Aphish_w",
    "scanResult": "DETECT",
    "detectionName": "PHISHING_URL"
}
```

Здесь:

- `url` – проверенный веб-адрес.

- `scanResult` – результат сканирования веб-адреса. Результат сканирования может иметь следующие значения:
  - `CLEAN`
  - `DETECT`
  - `DISINFECTED`
  - `DELETED`
  - `NON_SCANNED`
  - `SERVER_ERROR`
- `detectionName` – категория обнаруженного объекта в классификации "Лаборатории Касперского". Категория может иметь следующие значения:
  - `PHISHING_URL`
  - `MALICIOUS_URL`
  - `ADWARE_URL`
  - `RISKWARE_URL`

Пример HTTP-запроса на получение даты выпуска текущей антивирусной базы

Запрос на получение даты выпуска текущей антивирусной базы обычно посылается, чтобы убедиться, что база успешно обновилась до последней версии.

Ниже приведен пример HTTP-запроса на получение даты выпуска текущей антивирусной базы:

```
GET /api/v3.0/basesdate HTTP/1.0
```

Ниже приведен пример ответа на запрос:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 19:03:18 GMT
Content-Length: 50

{
    "databaseVersion": "30.01.2019 18:38 GMT"
}
```

Дата указана в следующем формате: `ДД.ММ.ГГГГ чч:мм GMT`.

kaspersky

Пример HTTP-запроса на получение текущей версии Kaspersky Scan Engine

Ниже приведен пример HTTP-запроса на получение версии библиотеки KAV SDK, на которой основана текущая версия Kaspersky Scan Engine:

```
GET /api/v3.0/version HTTP/1.0
```

Ниже приведен пример ответа на запрос:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 19:05:51 GMT
Content-Length: 36

{
    "KAVSDKVersion": "8.8.2.58"
}
```

Версия KAV SDK указана в следующем формате:
`МажорнаяВерсия.МинорнаяВерсия.НомерСборки.Ревизия`.

Пример HTTP-запроса на получение лицензионной информации

Ниже приведен пример HTTP-запроса на получение лицензионной информации:

```
GET /api/v3.0/licenseinfo HTTP/1.0
```

Ниже приведен пример ответа, который будет возвращен, если вы используете режим лицензирования оффлайн:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 19:04:30 GMT
Content-Length: 81

{
    "licenseName": "EXAMPLE.key",
    "licenseExpirationDate": "05.12.2020"
}
```

Здесь:

- `licenseName` – имя используемого файла ключа.
- `licenseExpirationDate` – дата, до которой действителен используемый файл ключа. Дата указана в следующем формате: `ДД.ММ.ГГГГ`.

Ниже приведен пример ответа, который будет возвращен, если вы используете режим лицензирования онлайн.

```
HTTP/1.0 200 OK
Date: Mon, 10 February 2014 12:25:21 GMT
Server: KAVHTTPD/1.0
Content-Length: 185
Connection: close
Content-Type: text/plain

{
    "activationCode": "EXMPL-*****-*****-12345",
    "licenseExpirationDate": "05.12.2020",
    "ticketExpired": "The license ticket has expired. Computer must be
connected to the Internet to update the license ticket."
}
```

Здесь:

- `activationCode` – используемый код активации.
- `licenseExpirationDate` – дата, до которой действителен используемый код активации. Дата указана в следующем формате: `ДД.ММ.ГГГГ`.
- `ticketExpired` – сообщение, которое будет включено в ответ, если истек срок действия лицензионного билета.

Пример HTTP-запроса на получение обобщенной статистики

Ниже приведен пример HTTP-запроса на получение обобщенной статистики:

```
GET /api/v3.0/getstatistics HTTP/1.0
```

Ниже приведен пример ответа на запрос:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 19:07:54 GMT
Content-Length: 314

{
    "statistics": {
         "total_requests": 3,
         "infected_requests": 3,
         "protected_requests": 3,
         "error_requests": 0,
         "engine_errors": 0,
         "processed_data": 204,
         "infected_data": 204,
         "processed_urls": 1,
         "infected_urls": 1
    }
}
```

Объект `statistics` содержит следующие поля:

- `total_requests` – количество запросов на проверку файлов, блоков RAM и веб-адресов.
- `infected_requests` – количество запросов, на которые решение Kaspersky Scan Engine вернуло результаты `DETECT`, `DISINFECTED` или `DELETED`.
- `protected_requests` – количество запросов, на которые решение Kaspersky Scan Engine вернуло результаты `DISINFECTED` or `DELETED`.
- `error_requests` – количество запросов, на которые решение Kaspersky Scan Engine вернуло результат `NOT_SCANNED` (ошибка сканирования связана со сканируемым объектом).
- `engine_errors` – количество запросов, на которые решение Kaspersky Scan Engine вернуло результат `SERVER_ERROR` (ошибка сканирования не связана со сканируемым объектом).
- `processed_data` – размер всех просканированных файлов в байтах.
- `infected_data` – размер всех данных, отправленных в HTTP-запросах, на которые решение Kaspersky Scan Engine вернуло результаты `DETECT`, `DISINFECTED` или `DELETED`.
- `processed_urls` – количество проверенных веб-адресов.
- `infected_urls` – количество веб-адресов, распознанных решением Kaspersky Scan Engine как `MALICIOUS_URL`, `PHISHING_URL`, `ADWARE_URL` или `RISKWARE_URL`.

Пример HTTP-запроса на удаление обобщенной статистики

Ниже приведен пример HTTP-запроса на удаление обобщенной статистики:

```
POST /api/v3.0/clearstatistics HTTP/1.0
Content-Type: application/octet-stream
Content-Length: 2

{}
```

Ниже приведен пример ответа на запрос:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 19:09:27 GMT
Content-Length: 27

{
    "error": "CLEARED"
}
```

Пример HTTP-запроса на обновление антивирусной базы

Этот запрос может быть выполнен, только если HTTP-клиент и Kaspersky Scan Engine установлены на одном компьютере. Если вы пошлете этот запрос на другой компьютер, Kaspersky Scan Engine вернет ошибку `405 Method Not Allowed`.

Ниже приведен пример HTTP-запроса на обновление антивирусной базы:

```
POST /api/v3.0/update/start HTTP/1.0
Content-Type: application/octet-stream
Content-Length: 2

{}
```

Ниже приведен пример ответа, который будет возвращен в случае, если обновление началось успешно:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 18:05:44 GMT
Content-Length: 26

{
    "status": "update started"
}
```

Ниже приведен пример ответа, который будет возвращен в случае, если запрос был послан, когда обновление уже началось:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 18:05:44 GMT
Content-Length: 35

{
    "status": "update already launched"
}
```

Ниже приведен пример ответа, который будет возвращен в случае, если во время запуска обновления произошла ошибка:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 18:05:44 GMT
Content-Length: 40

{
    "status": "error while launching update"
}
```

kaspersky

Пример HTTP-запроса на получение статуса обновления антивирусной базы

> Этот запрос может быть выполнен, только если HTTP-клиент и Kaspersky Scan Engine установлены на одном компьютере. Если вы пошлете этот запрос на другой компьютер, Kaspersky Scan Engine вернет ошибку `405 Method Not Allowed`.

Ниже приведен пример HTTP-запроса на получение статуса обновления антивирусной базы:

```
GET /api/v3.0/update/status HTTP/1.0
```

Ниже приведен пример ответа на запрос:

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/plain
Server: KAVHTTPD/1.0
X-KAV-ProtocolVersion: 3
Date: Wed, 30 Jan 2019 18:05:44 GMT
Content-Length: 116

{
    "status": "not started",
    "last_update_result": "success",
    "last_update_time": "21:03:53 30.01.2019"
}
```

kaspersky

Использование Kaspersky Scan Engine в режиме ICAP

В этом разделе описана работа Kaspersky Scan Engine в режиме ICAP.

Kaspersky Scan Engine в режиме ICAP

Протокол ICAP (Internet Content Adaptation Protocol) используется для коммуникации между прокси-серверами и поставщиками услуг. В режиме ICAP решение Kaspersky Scan Engine взаимодействует с прокси-серверами, совместимыми с протоколом ICAP. Kaspersky Scan Engine сканирует HTTP-трафик, который проходит через прокси-сервер, а также веб-адреса, запрашиваемые пользователями.

При запуске в режиме ICAP решение Kaspersky Scan Engine состоит из службы kavicapd, конфигурационных файлов и библиотек.

Ключевые функции:

- Веб-фильтрация

  Kaspersky Scan Engine позволяет сканировать веб-адреса, которые запрашивает пользователь через прокси-сервер. Эта функция доступна как для режима REQMOD (проверяются объекты, передаваемые от пользователя через прокси-сервер), так и для режима RESPMOD (проверяются объекты, передаваемые пользователю с прокси-сервера).

- Сканирование HTTP-трафика

  Kaspersky Scan Engine позволяет сканировать входящий и исходящий HTTP-трафик, который проходит через прокси-сервер. Эта функция доступна как для режима REQMOD (проверяются объекты, передаваемые от пользователя через прокси-сервер), так и для режима RESPMOD (проверяются объекты, передаваемые пользователю с прокси-сервера).

  Поддерживается сканирование составных объектов (объектов, включающих в себя несколько файлов).

- Поддержка кода состояния протокола HTTP `204 No Content`

  Служба kavicapd может быть настроена на возврат такого кода состояния, если сообщение, посланное клиентом, не требует модификации.

- Управление поведением службы kavicapd с помощью настройки правил службы.

- Режим сканирования по частям

  Режим позволяет сканировать файлы целиком и посылать их пользователю по блокам до окончания сканирования. Эта функция необходима, чтобы браузер пользователя не прерывал соединение с прокси-сервером после истечения таймаута.

  > Вы можете использовать эту функцию в Kaspersky Scan Engine, начиная с версии 1.0.1.51.

- Фильтрация объектов с помощью режима предварительной проверки

  В этом режиме ICAP-клиент посылает запрос ICAP-плагину, а ICAP-плагин выполняет предварительную проверку объекта с помощью правил исключений. Такие запросы позволяют не

сканировать те объекты, которые заведомо не являются вредоносными.

Вы можете использовать эту функцию в Kaspersky Scan Engine, начиная с версии 1.0.1.51.

Настройка Kaspersky Scan Engineв режиме ICAP

В этом разделе описано, как настроить Kaspersky Scan Engine в режиме ICAP вручную без использования графического интерфейса Kaspersky Scan Engine.

Конфигурационный файл режима ICAP

Конфигурационный файл режима ICAP `kavicapd.xml` состоит из нескольких секций, в которых перечислены основные настройки службы kavicapd и KAV SDK.

Подготовка конфигурационного файла режима ICAP после установки Kaspersky Scan Engine вручную

Если вы установили Kaspersky Scan Engine вручную, вам нужно скопировать конфигурационный файл туда, где служба kavicapd сможет его найти. По умолчанию конфигурационный файл находится в директории `%distr_kit%/etc/`.

После установки продукта скопируйте `kavicapd.xml` в одну из директорий по вашему усмотрению:

- Директория `/etc/`. Если вы копируете `kavicapd.xml` в эту директорию, Kaspersky Scan Engine находит и обрабатывает файл автоматически.
- Другая директория. Если вы копируете `kavicapd.xml` в другую директорию, вам нужно задать путь к ней во время запуска Kaspersky Scan Engine.

Параметры конфигурационного файла режима ICAP

Ниже перечислены секции конфигурационного файла kavicapd.xml. Пример конфигурационного файла находится в конце раздела.

Некоторые секции конфигурационного файла необязательны. Однако если секция присутствует в файле, все ее дочерние элементы должны находиться в файле. Элементы не должны содержать пустые значения.

Секция SDKSettings

Ниже перечислены параметры настройки KAV SDK.

- `ScannersCount` – Задает количество сканирующих процессов. Вы можете использовать до 256 таких процессов.

  Значение по умолчанию: `16`.

- `ThreadsCount` – Задает общее количество сканирующих потоков в каждом процессе. Вы можете использовать до 256 таких потоков.

Значение по умолчанию: `16`.

- `QueueLen` – Задает размер очереди сканирующей задачи.

  Значение по умолчанию: `1024`.

- `ScanTimeout` – Задает таймаут сканирования (в миллисекундах). Если значение этого параметра `0`, таймаут не используется.

  Значение по умолчанию: `10000` (10 секунд).

- `LicensePath` – Задает абсолютный путь к директории, где хранятся файлы с ID приложения, лицензией и ключом.

  Kaspersky Scan Engine ищет эти файлы в следующих директориях:

  - В директории, которая указана в качестве значения элемента `LicensePath`;
  - В директории, в которой находится исполняемый файл службы kavicapd;
  - В директории `%service_dir%/ppl`.

  Значение по умолчанию: `/opt/kaspersky/ScanEngine/bin`.

- `BasesPath` – Задает абсолютный путь к директории, где находятся антивирусные базы.

  Значение по умолчанию: `/opt/kaspersky/ScanEngine/bin/bases`.

- `TempPath` – Задает абсолютный путь к директории, где хранятся временные файлы, создаваемые во время запуска продукта.

  Значение по умолчанию: `/tmp/kavicapd`.

  Не удаляйте файлы из этой директории.

- `DiskUsageLimit` – Задает максимальный объем дискового пространства в килобайтах, который может быть выделен для распаковки объектов.

  Ограничение объема дискового пространства помогает защитить сервер от zip-бомб (вредоносных файлов архивов).

  Если значение этого параметра `0`, защита от zip-бомб отключена.

  Значение по умолчанию: `102400`.

- `ScanningMode` – Задает режим сканирования файла.

  Режим сканирования задается комбинацией флагов, разделенных вертикальной чертой (`|`).

  Параметр может принимать следующие значения:

  - `KAV_O_M_PACKED`

    Сканирует сжатые исполняемые файлы.

  - `KAV_O_M_ARCHIVED`

    Сканирует архивы.

  - `KAV_O_M_MAILBASES`

    Сканирует файлы, которые содержат почтовые базы.

- KAV_O_M_MAILPLAIN

  Сканирует сообщения электронной почты.

- KAV_O_M_HEURISTIC_LEVEL_SHALLOW

  Устанавливает уровень сканирования расширенного эвристического анализатора в значение shallow (уровень **Low** в графическом интерфейсе пользователя).

- KAV_O_M_HEURISTIC_LEVEL_MEDIUM

  Устанавливает уровень сканирования расширенного эвристического анализатора в значение medium (уровень **Medium** в графическом интерфейсе пользователя).

- KAV_O_M_HEURISTIC_LEVEL_DETAIL

  Устанавливает уровень сканирования расширенного эвристического анализатора в значение detail (уровень **High** в графическом интерфейсе пользователя).

- KAV_O_M_MSOFFICE_MACRO

  Сообщает пользователю, что файл Microsoft Office содержит макрос.

- KAV_O_M_PHISHING

  Включает защиту от фишинга.

Значение по умолчанию: KAV_O_M_PACKED | KAV_O_M_ARCHIVED | KAV_O_M_MAILPLAIN | KAV_O_M_MAILBASES | KAV_O_M_HEURISTIC_LEVEL_SHALLOW.

- LicensingMode – Задает режим лицензирования, который использует Kaspersky Scan Engine.

  Возможные значения:

  - 1 – Режим лицензирования оффлайн.
  - 2 – Режим лицензирования онлайн.

  Значение по умолчанию: 1.

Секция KSNSettings

Ниже перечислены параметры настройки Kaspersky Security Network (KSN).

Эта секция необязательна. Если она отсутствует в конфигурационном файле, KSN не используется.

Используя KSN, вы выражаете согласие на передачу "Лаборатории Касперского" данных, которые описаны в файле About data provision.txt. Более подробно о процедуре предоставления данных описано в разделе "О предоставлении данных (на стр. 67)".

- UseKSN – Параметр, который содержит значение логического типа, определяющее доступность KSN.

  Если значение параметра равно 1, сеть KSN включена, а флаг KAV_O_M_COMPOSITE_SCAN_KSN используется автоматически. Если значение параметра равно 0, сеть KSN отключена.

  Значение по умолчанию: 0.

- ObjectCheckOnDemandTimeoutMs – Задает таймаут сканирования для KSN в миллисекундах.

Недопустимое значение: `0`.

Значение по умолчанию: `10000` (10 секунд).

- `CacheSizeKb` – Задает максимальный объем кеша статуса KSN в килобайтах (КБ).

  Kaspersky Scan Engine использует кеширование, чтобы хранить результаты сканирования, полученные от KSN.

  Значение по умолчанию: `30720`.

Секция ProxySettings

Ниже перечислены параметры настройки прокси-сервера для Kaspersky Scan Engine. Kaspersky Scan Engine использует эти настройки, если у вас есть доступ к интернету.

Эта секция необязательна. Если она отсутствует в конфигурационном файле, Kaspersky Scan Engine не использует прокси-сервер при подключении к интернету.

- `UseProxy` – Параметр, который содержит значение логического типа, определяющее, использует ли Kaspersky Scan Engine прокси-сервер при подключении к интернету.

  Если значение параметра `1`, Kaspersky Scan Engine использует прокси-сервер. Если значение параметра `0`, Kaspersky Scan Engine не использует прокси-сервер.

  Значение по умолчанию: `0`.

- `Host` – Задает IP-адрес прокси-сервера (IPv4 или IPv6) или его доменное имя.

  Если прокси-сервер используется, этот параметр обязателен.

  Не указывайте протокол (`http://` или `https://`) в этом параметре.

- `Port` – Задает номер порта прокси-сервера.

  Значение по умолчанию: `3128`.

- `User` – Содержит в зашифрованном виде имя пользователя, которое используется для аутентификации на прокси-сервере. Имя пользователя зашифровано утилитой `kav_encrypt`.

  Если прокси-сервер используется, этот параметр обязателен.

  Если параметры `User` и `Pass` не заполнены, используется анонимный прокси-сервер.

- `Pass` – Содержит пароль, который используется при аутентификации на прокси-сервере. Пароль зашифрован утилитой `kav_encrypt`.

  Если этот параметр и параметр `User` не заполнены, используется анонимный прокси-сервер.

Секция UpdateSettings

Ниже перечислены настройки обновления Kaspersky Scan Engine.

Эта секция необязательна. Если она отсутствует в конфигурационном файле, обновление недоступно.

- `DisableBackup` – Параметр, который содержит значение логического типа, определяющее доступность резервной антивирусной базы.

  Если значение параметра равно `0`, резервная антивирусная база отключена. Если значение параметра равно `1`, резервная антивирусная база доступна.

  Значение по умолчанию: `0`.

- `UpdatePeriodMinutes` – Задает интервал в минутах между автоматическими обновлениями.

  Максимальное значение: `44640`.

  Если значение параметра равно `0`, автоматическое обновление отключено.

  Значение по умолчанию: `30`.

- `UseOnlyCustomSources` – Определяет, являются ли серверы обновлений "Лаборатории Касперского" источниками обновлений.

  Если значение параметра равно `1`, используются только клиентские источники обновлений. Если значение параметра равно `0`, серверы обновлений "Лаборатории Касперского" используются совместно с клиентскими.

  Значение по умолчанию: `0`.

- `UpdateSources` – Содержит клиентские источники обновлений.

  - `Source` задает клиентский источник обновления.

- `USRSignalAction` – Задает действие, которое должно быть выполнено при получении сигнала, указанного в параметре `USRSignalToHandle`.

  Возможные значения:

  - `reload`

    Перезагружает антивирусную базу без ее обновления. Предполагается, что файлы в папке с базами уже обновлены и должны быть перезагружены.

  - `update`

    Обновляет и перезагружает антивирусную базу.

  Значение по умолчанию: `update`.

- `USRSignalToHandle` – Задает сигнал, который должен быть получен для обновления или перезагрузки базы (действие указано в параметре `USRSignalAction`).

  Возможные значения:

  - `USR1`

    Будет обработан только сигнал `SIGUSR1`.

  - `USR2`

    Будет обработан только сигнал `SIGUSR2`.

  - `all`

    И `SIGUSR1`, и `SIGUSR2` должны быть обработаны.

  - `None`

    Сигналы не нужно обрабатывать (обновление антивирусной базы выполняется по заранее установленному расписанию).

Секция ICAPSettings

Ниже перечислены параметры настройки Kaspersky Scan Engine в режиме ICAP.

- `Port` – Определяет номер порта Kaspersky Scan Engine.

Значение по умолчанию: `1344`.

- `MaxIcapSessionsCount` – Задает максимальное число одновременных подключений к Kaspersky Scan Engine.
- `RAMUsageLimit` – Определяет максимальный объем системной памяти (в килобайтах), который выделен для Kaspersky Scan Engine.

  Эта величина позволяет контролировать использование памяти. Чрезмерное использование оперативной памяти может возникнуть, когда Kaspersky Scan Engine сканирует большие файлы или получает много результатов сканирования одновременно. Когда лимит `RAMUsageLimit` достигнут, Kaspersky Scan Engine заканчивает обработку объекта, который вызвал чрезмерное потребление памяти.

  Задайте в параметре `RAMUsageLimit` максимально возможное значение, но при этом оставьте достаточно системной памяти для правильного функционирования Kaspersky Scan Engine. Антивирусная база и библиотеки, которые использует Kaspersky Scan Engine, потребляют около 300 мегабайт, и эта величина удваивается во время перезагрузки базы. Kaspersky Scan Engine также требует ресурсы памяти для всех своих компонентов.

  > Не устанавливайте в параметр `RAMUsageLimit` значение, меньшее 7 МБ. Это минимальный объем памяти, который обеспечивает правильное функционирование продукта.

  Если значение параметра равно `0`, объем системной памяти, который может быть выделена для Kaspersky Scan Engine, не ограничен.

  Значение по умолчанию: `0`.

  > Если значение параметра равно `0`, памяти может не хватить. Если Kaspersky Scan Engine использует слишком много системной памяти, операционная система может остановить службу.

- `Exclusions`

  Задает правила для режима запроса предварительной проверки объекта (REQMOD). Эта функция позволяет ICAP-клиенту отправлять ICAP-плагину запросы на предварительный просмотр, после чего ICAP-плагин может не сканировать объекты, которые заведомо не являются вредоносными.

  Возможные параметры:

  - `ContentSize`

    Правило исключения для размера объекта, измеряемое в килобайтах, который указан в поле `Content-Length` заголовка HTTP. Если значение `Content-Length` больше или равно значению `ContentSize`, ICAP-плагин не сканирует объект. Вы можете использовать не более одного элемента `ContentSize`.

    Вы можете не указывать этот параметр.

  - `ContentType`

    Правило исключения для типа объекта, который указан в поле `Content-Type` заголовка HTTP. Если поле `Content-Type` содержит значение, которое указано в `ContentType`, ICAP-плагин не сканирует объект. Вы можете использовать несколько элементов `ContentType`: ICAP-плагин учтет их все.

Вы можете не указывать этот параметр.

- `RequestURL`

  Правило исключения для веб-адреса, на который отправляется запрос. Веб-адрес содержится в поле `Host` (из заголовка HTTP) и в поле `URI` (из стартовой строки HTTP). Если параметр `URL` содержит запрошенный веб-адрес, ICAP-плагин не сканирует объект. Перед сравнением запрошенного веб-адреса со значением правила исключения из параметра `RequestURL`, ICAP-плагин применяет правила нормализации к этому веб-адресу.

  Параметр `RequestURL` может содержать маски.

  Вы можете указать символ `*` для обозначения доменов, начиная с третьего уровня и выше. Например, `*.domain.com`: обозначает все поддомены домена `domain.com`. Символ `*` можно использовать в качестве подстановки для любой последовательности символов.

  В поле `URI` вы можете указать символы `*` и `?`, которые используются как в качестве подстановки для любой последовательности символов, так и для одного символа. Например, `domain.com/test/page=*`: это значение значение включает все страницы, которые содержат путь `/test/page=` (к примеру, `domain.com/test/page=123`).

  Вы можете использовать несколько элементов `RequestURL`: ICAP-плагин учтет их все.

  Вы можете не указывать этот параметр.

Если для объекта выполняется хотя бы одно из описанных правил, ICAP-плагин возвращает код `204` независимо от значения параметра `Allow204` файла `kavicapd.xml`. Если ни одно из правил не выполняется, ICAP-плагин возвращает код `100` и ждет, когда ICAP-клиент отправит объект.

> Вы можете использовать этот параметр в Kaspersky Scan Engine, начиная с версии 1.0.1.51.

- `ScanMaxFileSize` – Задает максимальный размер файла в килобайтах, который Kaspersky Scan Engine может обработать.

  Если значение параметра равно `0`, Kaspersky Scan Engine сканирует файлы любого размера. Если при этом указано правило исключения `ContenSize`, значение параметра `ScanMaxFileSize` принимается равным значению из указанного правила.

  Значение по умолчанию: `0`.

- `Allow204` – Параметр, который содержит значение логического типа, устанавливающее, посылает ли Kaspersky Scan Engine код состояния HTTP `204 No Content` вместо измененных данных на прокси-сервер.

  Если значение параметра равно `1`, Kaspersky Scan Engine вместо измененных данных возвращает код состояния HTTP `204 No Content`. Если значение параметра равно `0`, Kaspersky Scan Engine возвращает измененные данные.

- `ScanInReqMode` – Задает типы содержимого, которые Kaspersky Scan Engine должен сканировать в режиме обработки исходящего трафика (REQMOD).

  Этот параметр необязателен. Если он отсутствует в конфигурационном файле, используется значение `All`.

Возможные значения:

- `Content`

  Kaspersky Scan Engine сканирует только тело HTTP-сообщения.

- `Url`

  Kaspersky Scan Engine сканирует только запрошенный веб-адрес.

- `All`

  Kaspersky Scan Engine сканирует и тело HTTP-сообщения, и запрошенный веб-адрес.

- Empty value

  Kaspersky Scan Engine не сканирует HTTP-сообщения в режиме обработки исходящего трафика (REQMOD).

Значение по умолчанию: `All`.

- `ScanInRespMode` – Задает типы содержимого, которые Kaspersky Scan Engine должен сканировать в режиме обработки входящего трафика (RESPMOD).

  Этот параметр необязателен. Если он отсутствует в конфигурационном файле, используется значение `All`.

  Возможные значения:

  - `Content`

    Kaspersky Scan Engine сканирует только тело HTTP-сообщения.

  - `Url`

    Kaspersky Scan Engine сканирует только запрошенный веб-адрес.

  - `All`

    Kaspersky Scan Engine сканирует и тело HTTP-сообщения, и запрошенный веб-адрес.

  - Empty value

    Kaspersky Scan Engine не сканирует HTTP-сообщения в режиме обработки входящего трафика (RESPMOD).

  Значение по умолчанию: `All`.

- `RulesFilePath` – Задает абсолютный путь к файлу, который содержит правила настройки службы kavicapd.

  Значение по умолчанию: `/opt/kaspersky/ScanEngine/icap_data/kavicapd_gui_rules.conf`.

- `CmdPath` – Задает абсолютный путь к папке, содержащей сценарии, которые будут выполнены при срабатывании соответствующих правил.

  Значение по умолчанию: `/opt/kaspersky/ScanEngine/icap_data/scripts`.

- `ResponsesPath` – Задает абсолютный путь к папке, содержащей шаблоны ответов, которые будут получены при срабатывании соответствующих правил.

  Значение по умолчанию: `/opt/kaspersky/ScanEngine/icap_data/templates`.

- `HTTPClientIpICAPHeader` – Задает имя поля заголовка, в котором указан IP-адрес HTTP-клиента.

  Этот параметр необязателен и может иметь пустое значение.

  > Вы можете использовать этот параметр в Kaspersky Scan Engine, начиная с версии 1.0.1.51.

- `HTTPUserNameICAPHeader` – Задает имя поля заголовка, в котором указано имя HTTP-клиента.

  Этот параметр необязателен и может иметь пустое значение.

  > Вы можете использовать этот параметр в Kaspersky Scan Engine, начиная с версии 1.0.1.51.

- `TransferBeforeScanEnding`

  Задает режим сканирования по частям для файлов, которые отправляются на прокси-сервер. Этот режим позволяет сканировать файлы целиком и отправлять их пользователю по блокам до окончания сканирования. Передача объекта по блокам начинается через столько секунд после начала получения объекта, сколько указано в атрибуте `Delay`. Обратите внимание, что передается не более одного блока в секунду. Такая передача объекта необходима для того, чтобы браузер пользователя не прерывал соединение с прокси-сервером после истечения таймаута.

  Вы можете указать одно из двух значений для этого параметра:

  - `0`

    Объект может быть отправлен только после окончания сканирования.

  - `1`

    Объект может быть отправлен до окончания сканирования.

  Значение по умолчанию: `0`.

  Параметр содержит следующие атрибуты:

  - `Delay` задает интервал (в секундах) между началом получения объекта конечным пользователем и началом отправки его первого блока.

    Этот атрибут необязателен. Диапазон возможных значений: от 1 до 3600.

    Значение по умолчанию: `10`.

  - `ChunkSize` задает размер передаваемых блоков объекта в период между началом получения объекта конечным пользователем и окончанием сканирования. Поскольку части объекта передаются со скоростью один блок за секунду, в `ChunkSize` указана максимальная скорость передачи (в килобайтах в секунду) до завершения сканирования. Если сканирование завершено и объект не является вредоносным, оставшаяся часть объекта передается без ограничения скорости.

    Этот атрибут необязателен. Диапазон возможных значений: от 1 до 1024.

    Значение по умолчанию: `4`.

Выбирайте подходящие значения для атрибутов `ChunkSize` и `Delay`. Так, не рекомендуется указывать слишком большое значение для `ChunkSize` и слишком маленькое для `Delay`. Если рекомендация не соблюдена, сканируемый объект может быть отправлен почти целиком (но без последнего блока) намного раньше окончания сканирования, а браузер пользователя прервет соединение с прокси-сервером.

Вы можете использовать этот параметр в Kaspersky Scan Engine, начиная с версии 1.0.1.51.

Структура конфигурационного файла

Ниже приведен пример конфигурационного файла режима ICAP.

```
<Configuration>

    <SDKSettings>
        <ScannersCount>16</ScannersCount>
        <ThreadsCount>16</ThreadsCount>
        <QueueLen>1024</QueueLen>
        <ScanTimeout>10000</ScanTimeout> <!-- 0 = unlimited -->
        <LicensePath>/opt/kaspersky/ScanEngine/bin</LicensePath>
        <BasesPath>/opt/kaspersky/ScanEngine/bin/bases</BasesPath>
        <TempPath>/tmp/kavicapd</TempPath>
        <LicensingMode>1</LicensingMode><!-- 1 = упрощенный режим
лицензирования ; 2 - онлайн режим лицензирования -->
        <DiskUsageLimit>102400</DiskUsageLimit> <!-- 0 = turn zip-bomb
protection off -->
        <ScanningMode>KAV_O_M_PACKED | KAV_O_M_ARCHIVED | KAV_O_M_MAILPLAIN
| KAV_O_M_MAILBASES | KAV_O_M_HEURISTIC_LEVEL_SHALLOW</ScanningMode>
    </SDKSettings>

    <KSNSettings>
        <UseKSN>0</UseKSN>

    <ObjectCheckOnDemandTimeoutMs>10000</ObjectCheckOnDemandTimeoutMs>
        <CacheSizeKb>30720</CacheSizeKb>
    </KSNSettings>

    <UpdateSettings>
        <DisableBackup>0</DisableBackup>
        <UpdatePeriodMinutes>30</UpdatePeriodMinutes>  <!-- 0 = turn update
off -->
        <UseOnlyCustomSources>0</UseOnlyCustomSources>
        <UpdateSources>
            <!-- <Source></Source> -->
        </UpdateSources>
    </UpdateSettings>
```

```
    <ProxySettings>
        <UseProxy>0</UseProxy>
        <Host>myproxy.mycompany.com</Host>
        <Port>3128</Port>
        <User>proxyuser</User>
        <Pass>proxypass</Pass>
    </ProxySettings>

    <ICAPSettings>
        <Port>1344</Port>
        <MaxIcapSessionsCount>100</MaxIcapSessionsCount>
        <Exclusions>
            <ContentSize>2048</ContentSize>
            <ContentType>video/mp4</ContentType>
            <RequestURL>example.com</RequestURL>
        </Exclusions>
        <ScanMaxFileSize>0</ScanMaxFileSize> <!-- 0 = unlimited -->
        <RAMUsageLimit>0</RAMUsageLimit> <!-- 0 = unlimited -->
        <Allow204>0</Allow204>
        <ScanInReqMode>All</ScanInReqMode>
        <ScanInRespMode>All</ScanInRespMode>

    <RulesFilePath>/opt/kaspersky/ScanEngine/icap_data/kavicapd_gui_rules.
conf</RulesFilePath>
        <CmdPath>/opt/kaspersky/ScanEngine/icap_data/scripts</CmdPath>

    <ResponsesPath>/opt/kaspersky/ScanEngine/icap_data/templates</Response
sPath>
        <HTTPClientIpICAPHeader>X-Client-IP</HTTPClientIpICAPHeader>

    <HTTPUserNameICAPHeader>X-Client-Username</HTTPUserNameICAPHeader>
        <TransferBeforeScanEnding Delay="10"
ChunkSize="4">0</TransferBeforeScanEnding>
    </ICAPSettings>

</Configuration>
```

Запуск Kaspersky Scan Engine в режиме ICAP

В этом разделе описано, как запустить Kaspersky Scan Engine в режиме ICAP.

kaspersky

Запуск Kaspersky Scan Engine в режиме ICAP с помощью скрипта инициализации

Вы можете запустить Kaspersky Scan Engine в режиме ICAP с помощью скрипта инициализации службы, который находится в директории `%service_dir%/etc/init.d`. Скрипт инициализации позволяет запускать службу вручную из командной строки или добавить ее в автозапуск.

Настройка скрипта инициализации

По умолчанию скрипт инициализации `kavicapd` ищет исполняемый файл `kavicapd` в директории `/opt/kaspersky/ScanEngine/bin`. Если вы хотите использовать службу kavicapd из другой директории, отредактируйте скрипт инициализации соответствующим образом. Значение `DAEMON_DIR` в скрипте `kavicapd` задает путь до исполняемого файла kavicapd.

► *Чтобы настроить скрипт инициализации kavicapd:*

1. Откройте скрипт `kavicapd.sh` на редактирование.
2. Задайте пути до плагинов и библиотек.
3. Откройте файл `/etc/init.d/kavicapd` на редактирование.
4. Найдите следующий код:

```
########## ICAP service configuration ##########
DAEMON_DIR="${SDKPATH}/bin"
DAEMON="${DAEMON_DIR}/kavicapd"
PIDFILE=/var/run/kavicapd.pid
CONFILE=/etc/kavicapd.xml
```

5. Если необходимо, присвойте переменной `DAEMON_DIR` значение пути к исполняемому файлу `kavicapd`.
6. Присвойте переменной `PIDFILE` значение пути к PID-файлу для `kavicapd`.

   Если PID-файла нет, его создаст процесс, инициируемый скриптом `kavicapd.sh`.
7. Присвойте переменной `CONFILE` значение пути к конфигурационному файлу режима ICAP.
8. Если вы установили Kaspersky Scan Engine вручную, укажите точный путь к файлу состояния службы kavicapd:
   a. Найдите следующую строку:

      `STATUS_FILE_PATH=/tmp/kavicapd`

   b. Присвойте переменной `STATUS_FILE_PATH` значение пути к директории, в которой будет находиться файл состояния службы kavicapd.

      Значение этой переменной должно совпадать со значением параметра `TempPath` конфигурационного файла режима ICAP.
9. Найдите следующую строку:

   `UPDATE_SIGNAL="USR1"`

10. Присвойте переменной UPDATE_SIGNAL знаение, соответствующее сигналу, который должен быть использован для обновления и перезагрузки антивирусной базы данных (команда updatedb).

    Используйте USR1 для задания сигнала SIGUSR1, а USR2 для SIGUSR2.

    Если служба kavicapd получает сигнал USR (SIGUSR1 или SIGUSR2), который не указан в параметре, служба останавливает работу (поведение по умолчанию для программ Linux). Учитывайте это поведение, когда задаете значение параметра.

11. Сохраните файлы и закройте редактор.

Запуск службы с помощью скрипта инициализации

Скрипт kavicapd.sh поддерживает следующие команды:

- start – Запускает службу kavicapd.

  После выполнения этой команды скрипт выводит [OK] на консоль и сразу передает управление консоли. Сама служба запускается в течение некоторого времени.

- stop – Останавливает службу kavicapd.
- restart – Перезапускает службу kavicapd (останавливает и снова запускает службу).

  После выполнения этой команды скрипт выводит [OK] на консоль и сразу передает управление консоли. Сама служба запускается в течение некоторого времени.

- updatedb – Посылает сигналы SIGUSR1 или SIGUSR2 (указанные в параметре UPDATE_SIGNAL скрипта инициализации) службе kavicapd.

  Служба kavicapd обрабатывает сигнал либо только перезагружая базу данных, либо обновляя и перезагружая ее (настройки заданы в конфигурационном файле режима ICAP).

- status – Показывает состояние службы kavicapd.

  Сообщение о состоянии содержит следующую информацию:

  - Версию KAV SDK;
  - Версию ICAP-службы;
  - Информацию об антивирусной базе данных;
  - Информацию о файле ключа или коде активации.

  Ниже приведен пример вывода команды status в упрощенном режиме лицензирования:

```
kavicapd (pid 1107) is running...
KAV SDK version:   KAV SDK v8.5.1.83
ICAPD version:     KL ICAP Service v1.0 (KAV SDK v8.5.1.83)
Database release date:  2015-Sep-14 07:46:00
Records in the database: 4308101
Key file name:     EXAMPLE.key
Key file expiration date:   2019-Jan-12 20:00:00
Days left:         590
```

Ниже приведен пример вывода команды `status` в режиме лицензирования онлайн.

```
kavicapd (pid 1107) is running...
KAV SDK version:   KAV SDK v8.5.1.83
ICAPD version:     KL ICAP Service v1.0 (KAV SDK v8.5.1.83)
Database release date:  2015-Sep-14 07:46:00
Records in the database: 4308101
Activation code:   EXMPL-*****-*****-12345
License expiration date:   2019-Jan-12 20:00:00
Days left:         590
```

Чтобы посмотреть список поддерживаемых команд, запустите скрипт без параметров.

```
[user@host ~]$ /etc/init.d/kavicapd
```

Автоматический запуск службы

Вы можете настроить автоматический запуск службы kavicapd.

► *Чтобы настроить автоматический запуск службы kavicapd:*

1. Скопируйте скрипт инициализации kavicapd.sh в директорию, которая содержит скрипты инициализации, запускаемые автоматически. Местоположение этой директории может меняться в зависимости от операционной системы.
2. Добавьте службу kavicapd в список служб, запускаемых автоматически. Точный метод может меняться в зависимости от операционной системы.
3. Проверьте, что служба была добавлена без ошибок.
4. Перезагрузите систему, чтобы изменения вступили в силу.

kaspersky

Проверка целостности компонентов программы

Программа Kaspersky Scan Engine содержит множество различных бинарных модулей в форме библиотек динамических ссылок, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов программы другими файлами, содержащими вредоносный код. Чтобы предотвратить такую замену модулей и файлов, в Kaspersky Scan Engine предусмотрена проверка целостности компонентов программы.

Программа проверяет модули и файлы на наличие несанкционированных изменений или повреждений. Если контрольная сумма модуля или файла программы является некорректной, он считается поврежденным.

Программа проверяет целостность файла манифеста, содержащего список файлов программы, целостность которых критична для корректной работы компонентов программы.

Целостность компонентов программы проверяется с помощью инструмента integrity_check_tool, расположенного в директории %ProductRoot%/tools/, где %ProductRoot% - директория установки программы Kaspersky Scan Engine. Эта же директория содержит файл манифеста – integrity_check.xml, защищенный криптографической сигнатурой "Лаборатории Касперского".

Для запуска инструмента проверки целостности необходима учетная запись с root -правами.

► *Чтобы проверить целостность компонентов приложения, выполните следующую команду:*

```
integrity_check [options]
```

По умолчанию инструмент проверки целостности использует файл манифеста integrity_check.xml, расположенный в директории %ProductRoot%/tools/.

► *Чтобы проверить целостность компонентов приложения, используя файл манифеста, расположенный в директории, отличной от директории по умолчанию, выполните следующую команду:*

```
integrity_check [options] %path%
```

где %path% - путь к файлу манифеста.

Если вы создаете исполняемые файлы для режима HTTP или режима ICAP из исходного кода, при закуске инструмента проверки целостности всегда будет возвращаться FAILED при проверке %ProductRoot%/bin/kavhttpd и %ProductRoot%/bin/kavhttp_client (режим HTTP) или %ProductRoot%/bin/kavicapd (режим ICAP).

Инструмент проверки целостности можно запустить со следующими дополнительными параметрами:

- `--help` – показать справку для параметров инструмента.
- `--verbose` – раскрыть вывод информации о выполненных действиях и результатах. Если вы не укажите этот параметр, будут отображаться только ошибки, объекты, не прошедшие проверку, и общая статистика проверки.
- `--version` – показать версию инструмента проверки целостности
- `--trace <имя файла>`, где `<имя файла>` – это имя файла, используемого для регистрации событий, происходящих во время сканирования.

Результат проверки каждого файла манифеста отображается рядом с именем файла манифеста в следующем формате:

- `SUCCEEDED` – целостность файлов подтверждена (код возврата `0`).
- `FAILED` – целостность файлов не подтверждена (код возврата отличен от `0`).

kaspersky

Удаление Kaspersky Scan Engine

В этом разделе описано, как удалить Kaspersky Scan Engine.

В этом разделе

Удаление с использованием деинсталлятора (Linux и Windows)

В этом разделе описано, как удалить Kaspersky Scan Engine с помощью исполняемого файла `uninstall` (Linux) или `uninstall.exe` (Windows).

Перед удалением Kaspersky Scan Engine убедитесь, что файлы из директории `%service_dir%` не задействованы ни в одном процессе.

► *Чтобы удалить Kaspersky Scan Engine:*

1. Убедитесь, что у вас есть права администратора.
2. Перейдите в директорию, отличную от `%service_dir%`, и запустите `uninstall` оттуда, например, с помощью командной строки.

   Если на компьютере запущен экземпляр Kaspersky Scan Engine, деинсталлятор остановит его.
3. Выберите, удалить базу с данными Kaspersky Scan Engine или нет.

   Если вы выбрали удаление, `uninstall` удалит следующее:

   - Базу, которая содержит данные Kaspersky Scan Engine;

     Установка PostgreSQL не будет удалена, равно как и пользователь базы данных PostgreSQL `scanengine`. Будет удалена только база данных Kaspersky Scan Engine `kavebase`. Если вы хотите переустановить Kaspersky Scan Engine, удалите пользователя базы данных `scanengine`.

     Чтобы удалить пользователя `scanengine` выполните следующую команду:

     ```
     DROP ROLE scanengine;
     ```
   - Директорию, в которую был установлен Kaspersky Scan Engine;
   - Директорию с временными файлами Kaspersky Scan Engine;
   - Службу Kaspersky Scan Engine (из списка служб).

kaspersky

Данные, передаваемые в "Лабораторию Касперского"

В этом разделе описаны данные, получаемые "Лабораторией Касперского" во время работы Kaspersky Scan Engine.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского".

"Лаборатория Касперского" использует полученную информацию только в обезличенном виде и в виде данных общей статистики. Данные общей статистики формируются автоматически из исходной полученной информации и не содержат персональных и иных конфиденциальных данных. Исходная полученная информация уничтожается по мере накопления (один раз в год). Данные общей статистики хранятся бессрочно.

В этом разделе

Данные, передаваемые в "Лабораторию Касперского" при проверке репутации файлов и веб-адресов

Когда вы используете функции проверки репутации файлов и веб-адресов, Kaspersky Scan Engine передает "Лаборатории Касперского" информацию об установленной копии Kaspersky Scan Engine и об обнаруженных объектах.

Следующая информация будет передана:

- Идентификатор Kaspersky Scan Engine;
- Полная версия Kaspersky Scan Engine: мажорная версия, минорная версия, сборка, редакция и пакет исправлений;
- Идентификатор обладателя лицензии;
- Хеш-суммы обрабатываемых файлов (MD5, SHA256);
- Версию KSN;
- Хеш-суммы имен обнаруженных объектов (MD5, SHA256);
- Нормализованный веб-адрес.

kaspersky

О предоставлении данных

В этом разделе приведена информация о предоставлении данных.

Следующие файлы в Kaspersky Scan Engine содержат информацию о процедуре предоставления данных, используемой Kaspersky Scan Engine:

- `%distr_kit%/doc/About data provision.txt` – Описывает процедуру предоставления данных для проверки репутации файлов и веб-адресов.
- `%distr_kit%/doc/About data provision - online licensing.txt` – Описывает процедуру предоставления данных для онлайн режима лицензирования.
- `%distr_kit%/doc/About data provision - gateway set.txt` – Описывает процедуру предоставления данных, когда вы отправляете статистическую информацию KSN в Kaspersky Scan Engine для Linux.
- `%distr_kit%/doc/About data provision extended.txt` – Описывает процедуру предоставления данных, когда вы отправляете статистическую информацию KSN в Kaspersky Scan Engine для Windows.

kaspersky

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в поддиректории `doc` директории установки программы.

kaspersky

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Safari – товарный знак Apple Inc., зарегистрированный в США и других странах.

Firefox и Mozilla – товарные знаки Mozilla Foundation.

Chrome, Google, Google Chrome – товарные знаки Google, Inc.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Internet Explorer, Microsoft, Microsoft Edge, Visual Studio, Win32, Windows, Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Red Hat – товарный знак Red Hat Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

kaspersky

АО "Лаборатория Касперского"

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг "IDC Worldwide Endpoint Security Revenue by Vendor"). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей ("IDC Endpoint Tracker 2014").

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

Продукты. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

Технологии. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

Достижения. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Сайт "Лаборатории Касперского": https://www.kaspersky.ru

Вирусная энциклопедия:	https://securelist.ru/
Kaspersky VirusDesk:	https://virusdesk.kaspersky.ru/ (для проверки подозрительных файлов и сайтов)
Сообщество пользователей "Лаборатории Касперского":	https://community.kaspersky.com