Kaspersky Endpoint Security 12.0 для Linux

Краткое руководство по установке и первоначальной настройке через командную строку

Эта статья поможет вам выполнить установку и первоначальную настройку приложения Kaspersky Endpoint Security 12.0 для Linux через командную строку на отдельном устройстве в вашей инфраструктуре.

> В этой статье не рассматривается установка приложения Kaspersky Endpoint Security 12.0 для Linux в режиме Легкого агента, а также установка и первоначальная настройка приложения через Kaspersky Security Center. Подробнее о режимах работы приложения см. в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/93769.htm.

Также в этой статье вы найдете рекомендации по оптимизации работы приложения с целью снижения негативного влияния на производительность вашей инфраструктуры.

Подготовка к установке Kaspersky Endpoint Security 12.0 для Linux

Подготовка к установке состоит из следующих этапов:

1. Проверка соответствия целевого устройства (устройства, на которое вы будете производить установку) минимальным аппаратным требованиям для установки Kaspersky Endpoint Security 12.0 для Linux: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/261258.htm.

   Следует учитывать, что количество системных ресурсов, требуемых для Kaspersky Endpoint Security 12.0 для Linux, зависит от планируемой к использованию функциональности приложения и от той продуктивной нагрузки, которая имеется на данном конкретном устройстве. То есть если для сервера без нагрузки будет достаточно ресурсов, указанных в минимальных системных требованиях, то для нагруженного сервера может потребоваться значительно большее количество системных ресурсов.

2. Проверка соответствия целевого устройства минимальным программным требованиям для установки Kaspersky Endpoint Security 12.0 для Linux. В справке приведен список архитектур (32-бит, 64-бит и ARM 64-бит) и дистрибутивов ОС, поддерживаемых для установки Kaspersky Endpoint Security 12.0 для Linux: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/261283.htm.

   Если ваша ОС отсутствует в списке поддерживаемых, рекомендуем вам обратиться в Службу технической поддержки «Лаборатории Касперского» для уточнения возможности установки Kaspersky Endpoint Security 12.0 для Linux на вашу ОС.

   Отсутствие ОС в списке может означать, что приложение Kaspersky Endpoint Security 12.0 для Linux не проходило тестирование на совместимость с этой ОС на момент выхода релизной версии приложения. Такое бывает, если ОС устарела и снята с поддержки производителем ОС, или наоборот ОС слишком новая.

3. Проверка наличия на устройстве пакетов, необходимых для установки Kaspersky Endpoint Security 12.0 для Linux и подготовка ОС.

   Последовательность действий для проверки параметров ОС, необходимых для установки приложения, приведена в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/248502.htm.

   Обратите внимание на следующее:

   - Надо проверить, установлен ли интерпретатор языка perl версии 5.10 и выше. Это можно сделать, посмотрев на вывод команды perl -v. Пример:

     ```
     $ perl -v
     This is perl 5, version 30, subversion 0 (v5.30.0) built for x86_64-linux-gnu-thread-multi
     ...
     ```

   - Для RHEL-систем, например для РЕД ОС, надо проверить также наличие необходимых для установки пакетов perl-Getopt-Long и perl-File-Copy. Проверить это можно командами:

     - rpm -q perl-Getopt-Long
     - rpm -q perl-File-Copy

     Пример вывода команды rpm -q perl-Getopt-Long, если пакет установлен в системе:

     ```
     $ rpm -q perl-Getopt-Long
     perl-Getopt-Long-2.51-1.el7.noarch
     ```

Пример вывода команды rpm -q perl-Getopt-Long, если пакет не установлен в системе:

```
$ rpm -q perl-Getopt-Long
package perl-Getopt-Long is not installed
```

Perl и указанные пакеты необходимы для корректной работы скрипта первоначальной настройки, который запускается после установки пакета с Kaspersky Endpoint Security 12.0 для Linux.

4. Проверка наличия лицензионного ключа для активации Kaspersky Endpoint Security 12.0 для Linux.

   Набор доступных функций приложения Kaspersky Endpoint Security зависит от лицензии (см. таблицу в разделе справки: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/256558.htm).

   Подробнее о лицензировании Kaspersky Endpoint Security 12.0 для Linux см. в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/69238.htm.

   Добавлять лицензионный ключ можно с помощью кода активации или с помощью файла ключа.

   В случае процедуры активации приложения с помощью кода активации приложению понадобится доступ в интернет для подключения к серверам активации «Лаборатории Касперского».

   Если требуется, вы можете получить файл ключа на основе кода активации: https://support.kaspersky.ru/common/buy/7180.

   При первой установке Kaspersky Endpoint Security 12.0 для Linux в процессе выполнения скрипта первоначальной настройки вам будет предложено активировать приложение по пробной лицензии, срок действия которой составляет 30 дней.

Развертывание и первоначальная настройка Kaspersky Endpoint Security 12.0 для Linux

Установка приложения локально с помощью командной строки

Перед установкой надо определить архитектуру ОС (32-bit, 64-bit или ARM 64-bit) и тип пакетного менеджера, используемого в ОС.

Затем необходимо скопировать на целевое устройство пакет kesl (пакет, необходимый для установки приложения), и пакет kesl-gui (необязательный пакет для установки графического пользовательского интерфейса). Вам нужно выбрать пакеты в соответствии с архитектурой, типом менеджера пакетов и разрядностью ОС на целевом устройстве.

Если вы не планируете использовать на целевом устройстве графический пользовательский интерфейс, то пакет kesl-gui копировать не надо.

> Рекомендуем использовать последние сборки пакетов, содержащие исправления ошибок, обнаруженных с даты официального релиза устанавливаемой версии Kaspersky Endpoint Security. Скачать последнюю сборку с исправлениями можно из формы создания запроса в Службу технической поддержки «Лаборатории Касперского», см. подробнее: https://support.kaspersky.ru/corporate/faq-for-business-products#how-to-create-technical-support-request.

Описание установки пакетов kesl и kesl-gui для различных архитектур и пакетных менеджеров для разных дистрибутивов ОС Linux см. в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/233694.htm.

> Обратите внимание, что установка пакета kesl-gui без предварительной установки пакета kesl невозможна.

Первоначальная настройка Kaspersky Endpoint Security 12.0 для Linux после установки пакета

После установки следует выполнить скрипт первоначальной настройки Kaspersky Endpoint Security 12.0 для Linux.

Далее рассмотрим запуск скрипта первоначальной настройки в интерактивном режиме (см. подробнее в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/197897.htm). Сценарий первоначальной настройки приложения в автоматическом режиме с использованием файла автоответов autoinstall.ini в этой статье не рассматривается, см. описание в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/197909.htm.

Чтобы запустить скрипт первоначальной настройки Kaspersky Endpoint Security в интерактивном режиме, выполните следующую команду:

```
# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

> Скрипт первоначальной настройки требуется запускать с root-правами.

Обратите внимание на следующие важные шаги первоначальной настройки:

- На первом шаге скрипта на вопрос о том, собираетесь ли вы использовать приложение в режиме Легкого агента для защиты виртуальных сред, надо ответить n (No).
- На следующем шаге надо выбрать языковой стандарт. Этот параметр определяет язык, на котором будут отображаться Лицензионное соглашение и Политика конфиденциальности во время работы скрипта.
- Далее вам будет предложено прочитать и принять Лицензионное соглашение и Политику конфиденциальности.

  Если хотя бы одно из этих соглашений не будет принято, работа скрипта первоначальной настройки прервется, и вы не будете иметь возможность использовать приложение Kaspersky Endpoint Security 12.0 для Linux.
- Далее вам будет предложено принять или отклонить условия использования Kaspersky Security Network (подробнее см. в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/246794.htm).

  Использование Kaspersky Security Network является добровольным. Вы можете включить или выключить использование Kaspersky Security Network в любой момент после установки приложения.
- Следующий важный шаг скрипта первоначальной настройки – настройка параметров прокси-сервера для доступа приложения к сети интернет.

  Если доступ в интернет с целевого устройства осуществляется через прокси-сервер, необходимо настроить прокси-сервер, чтобы приложение могло выполнять обновление баз с публичных серверов обновления «Лаборатории Касперского».

  Подробнее о настройке прокси-сервера см. в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/197905.htm.
- Следующий важный шаг скрипта первоначальной настройки – первоначальное обновление баз приложения. Дистрибутив Kaspersky Endpoint Security 12.0 для Linux не содержит в себе антивирусные базы, необходимые для работы приложения.

  Приложение не будет активировано до момента успешного завершения задачи первоначального обновления баз.

  Вы можете выполнить обновление баз как во время работы скрипта первоначальной настройки, так и после завершения работы скрипта.

После завершения первоначальной настройки, обновления баз и добавления лицензионного ключа Kaspersky Endpoint Security 12.0 для Linux переходит в рабочее состояние с параметрами по умолчанию.

Вы можете проверить успешность установки и активации приложения командой:

```
# kesl-control --app-info
```

Пример вывода команды --app-info:

Некоторые задачи приложения могут быть недоступны из-за ограничений лицензии. Например, на скриншоте выше по этой причине недоступны задачи Container Monitoring (https://support.kaspersky.com/help/KES4Linux/12.0.0/ru-RU/210891.htm) и System Integrity Monitoring (https://support.kaspersky.com/help/KES4Linux/12.0.0/ru-RU/197992.htm).

Строка **Policy: Not Applied** означает, что приложение Kaspersky Endpoint Security 12.0 для Linux работает с локально настроенными параметрами, а не с параметрами из политики, распространяемыми централизованно через Kaspersky Security Center.

Оптимизация работы приложения

Этот раздел содержит рекомендации по настройке параметров приложения с целью снижения влияния на производительность бизнес-приложений, работающих на целевом устройстве. Также в этом разделе приведены рекомендации по настройке приложения для нескольких типовых серверных ролей.

Описание настройки параметров приведено для командной строки, так как после описанной выше установки приложение работает не под политикой Kaspersky Security Center.

> Настройку параметров приложения следует выполнять под учетной записью пользователя root или пользователя, которому была назначена роль администратора Kaspersky Endpoint Security 12.0 для Linux в процессе установки приложения.

Вы также можете настраивать параметры приложения централизованно с помощью политик и задач Kaspersky Security Center через Kaspersky Security Center Web Console (https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/245583.htm) или через Консоль администрирования (https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/245658.htm). В этой статье управление приложением с помощью Kaspersky Security Center не рассматривается.

Настройка задач Защита от веб-угроз и Защита от сетевых угроз

После завершения установки и первоначальной настройки приложения Kaspersky Endpoint Security 12.0 для Linux проанализируйте потребление ресурсов на устройстве и изменение производительности установленных приложений, используя встроенные средства ОС или данные системы мониторинга. Если анализ показывает значительное снижение производительности приложений и/или критичное для работы ОС или приложений потребление системных ресурсов, то рекомендуется выполнить дополнительную настройку параметров запущенных задач Защита от веб-угроз и Защита от сетевых угроз.

По умолчанию эти задачи выключены (задача Защита от веб-угроз включается при запуске приложения, только если в системе обнаружен установленный веб-браузер).

Рекомендуется учесть следующее:

- Если в системе настроены свои (или firewalld) сетевые правила с Drop политиками, то для корректной работы приложения надо добавить разрешающее правило для разрешения входящих соединений с локального хоста:

  ```
  iptables -A INPUT -i lo -j ACCEPT
  ```

- Если в процессе первоначальной настройки приложения вы не настроили параметры прокси-сервера и устройство не имеет прямого выхода в интернет, то для корректной работы задачи Защита от веб-угроз надо установить значение параметра CertificateVerificationPolicy=LocalCheck в параметрах проверки защищенных соединений (см. подробнее в справке: https://support.kaspersky.com/help/KES4Linux/12.0.0/ru-RU/198037.htm).

  Вы можете настроить параметр, выполнив команду:

  ```
  # kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
  ```

При таком значении параметра приложение не использует интернет для проверки и загрузки недостающих цепочек, необходимых для проверки сертификата.

Вы также можете настроить прокси-сервер, выполнив команду:

- если прокси-сервер использует аутентификацию:

```
# kesl-control --set-app-settings UseProxy=Yes ProxyServer=<имя пользователя>:<пароль>@<IP-адрес прокси-сервера>:<номер порта>
```

- если прокси-сервер не использует аутентификацию:

```
# kesl-control --set-app-settings UseProxy=Yes ProxyServer=<IP-адрес прокси-сервера>:<номер порта>
```

- Если вы используете задачу Защита от сетевых угроз, то установка параметра MonitorNetworkPorts=All гарантированно приведет к недоступности ресурсов по протоколу SMB.
- Совместная работа задач Защита от веб-угроз и Защита от сетевых угроз с Kubernetes требует дополнительной тонкой и трудоемкой настройки сетевых правил ОС, а в некоторых случаях и вовсе невозможна, например при использовании Kubernetes с CNI Cillium.

Настройка параметров и исключений задачи Защита от файловых угроз

Задача Защита от файловых угроз имеет ID=1 и включена по умолчанию после установки и активации приложения. Подробнее о задаче см. в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/197961.htm.

Задача Защита от файловых угроз перехватывает события о файловых операциях в системе и по умолчанию блокирует эти операции до окончания обработки события приложением. После окончания обработки приложение или разрешает операции, и блокировка файловой операции снимается, или приложение производит над проверяемым файлом действия, описанные в параметрах FirstAction, SecondAction задачи Защита от файловых угроз (подробнее о параметрах см. в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/234812.htm).

Существенное влияние на производительность системы может оказать включение проверки архивов (параметр ScanArchived задачи Защита от файловых угроз). Если проверка архивов включена, доступ к упакованному файлу «задерживается» до того, как он будет распакован во временную локацию и проверен. Под архивами здесь имеются в виду как традиционные архивы, так и упакованные объекты, например типа .jar.

По умолчанию проверка архивов выключена. и для оптимизации работы приложения включать ее не рекомендуется.

Для задачи Защита от файловых угроз есть несколько типов исключений:

- В параметрах задачи вы можете настраивать исключения по пути (в том числе можно задать тип монтирования), маске файла, типу угрозы и пути к процессу, совершающему файловые операции.

  Исключения этого типа работают так: файловая операция перехватывается и блокируется, затем, если приложение определяет, что операция производится в области, исключенной из проверки, то блокировка с файловой операции снимается, проверка объекта файловой операции не производится. Минимальные задержки в файловых операциях присутствуют.
- В общих параметрах приложения вы можете настраивать глобальные исключения.

Такие исключения можно задавать для точек монтирования в системе, типов точек монтирования в системе (Local, AllRemoteMounted, Mounted:NFS, Mounted:SMB, Mounted:Custom). Исключенные таким образом области вообще не отслеживаются приложением и, следовательно, не происходит никаких задержек в файловых операциях.

Рекомендуется добавлять в глобальные исключения примонтированные удаленные ресурсы с нестабильным или медленным соединением (например NFS, SMB).

О настройке исключений обоих типов для задачи Защита от файловых угроз см. в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/248490.htm.

Не снижают ли исключения степень защищенности устройства? Добавляя исключения, мы боремся за разумный баланс между защищенностью системы и ее производительностью. Например, по мнению вирусных экспертов «Лаборатории Касперского» можно без опасения добавлять в исключения файлы данных и индексные файлы баз данных. Считается, что опасность проникновения вирусов через такие файлы отсутствует.

О настройке исключений для снижения влияния на производительность целевого устройства см. также в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/206054.htm.

Рекомендации для типовых серверных ролей

Сервер БД Postgresql

Для БД Postgresql критически важно, чтобы не было даже малейших задержек в файловых операциях с файлами данных и Write Ahead Log файлами (WAL). Также рекомендуется исключить из проверки файловые операции процессов Postgresql.

Для типовой установки Postgresql эти файлы (в том числе исполняемые файлы Postgresql) распложены по путям:

- /var/lib/postgresql/13/main – директория с данными;
- /var/lib/postgresql/13/main/pg_wal – файлы WAL;
- /usr/lib/postgresql/13/bin/ – исполняемые файлы.

Уточните у администраторов БД, как это настроено на вашем устройстве.

Первые два пути мы рекомендуем добавить в глобальные исключения из проверки (см. в справке: https://support.kaspersky.com/KES4Linux/12.0.0/ru-RU/248490.htm).

Если пути к директории с данными и к файлам WAL не являются отдельными точками монтирования в системе (список точек монтирования можно посмотреть в выводе команды mount), нужно сделать из них точки монтирования. Например, чтобы создать точку монтирования из директории с данными для типовой установки Postgresql /var/lib/postgresql/13/main, надо выполнить следующую команду:

```
mount --bind /var/lib/postgresql/13/main/ /var/lib/postgresql/13/main
```

Добавлять отдельную точку монтирования для директории с файлами WAL в данном случае не понадобится, так как она уже будет принадлежать точке монтирования /var/lib/postgresql/13/main.

Далее надо добавить глобальное исключение:

```
# kesl-control --set-app-settings
ExcludedMountPoint.item_0000=/var/lib/postgresql/13/main
```

Чтобы созданная с помощью mount --bind точка монтирования осталась в системе после перезагрузки, добавьте в файл /etc/fstab следующую строку:

```
/var/lib/postgresql/13/main /var/lib/postgresql/13/main none defaults,bind 0 0
```

Для применения указанных выше глобальных исключений надо перезапустить приложение:

```
# systemctl restart kesl.service
```

Веб-сервер

При типовом использовании веб-сервера в случае большой пользовательской нагрузки на сервер и работе по протоколу HTTPS серьезное влияние на потребление системных ресурсов оказывают задачи Защита от веб-угроз и Защита от сетевых угроз из-за расходов на расшифровку HTTPS-трафика. В этом случае рекомендуется выключить задачи Защита от веб-угроз и Защита от сетевых угроз.

Proxy-сервер

В случае с proxy-сервером или load balancer, установленным на целевом устройстве, рекомендуется выключить задачи Защита от веб-угроз и Защита от сетевых угроз.