Инструкция по установке и удалению антивируса Касперского на серверах Linux (KES for Linux 12)

I

Установка АВЗ от Касперского

Если выполняется первичная установка антивируса на группу хостов (например Oracle), то НЕОБХОДИМО:

1. Сначала выполнить установку на тестовые сервера;

2. Проверить работу хостов с включенным антивирусом;

3. Выяснить какие исключения требуются для корректной работы программного обеспечения и антивируса (эти работы выполняются совместно с группой Инфоком.УППК.АВЗ <cher.it.security@stalcom.com>);

4. После полной проверки выполнять установку на продуктивные сервера;

4.1. После установки агента администрирования, необходим рестарт службы агента администрирования (klnagent);
4.2. После установки программы защиты (KESL) необходимо выполнить рестарт службы программы защиты, а потом агента администрирования;
4.3. Дождаться выполнения задачи "Обновление баз Linux" и выполнить повторный перезапуск служб программы защиты, а потом агента администрирования;

Подготовка к установке приложения

Перед установкой KESL на ОС, проверьте, что:

- Убедиться в том, что на вашем устройстве не установлено стороннее антивирусное программное обеспечение.
- Убедиться в том, что на вашем устройстве не установлено приложение Kaspersky Endpoint Agent для Linux. Если приложение Kaspersky Endpoint Agent для Linux установлено, во время установки отобразится сообщение о необходимости удалить его вручную.
- Убедиться в том, что на вашем устройстве установлен интерпретатор языка Perl версии 5.10 или выше.
- На устройствах с операционными системами, не поддерживающими технологию fanotify, убедиться в том, что установлены:
  - пакеты для компиляции программ и запуска задач (gcc, binutils, glibc, glibc-devel, make);
  - пакет с заголовочными файлами ядра операционной системы для компиляции модулей Kaspersky Endpoint Security.
- В зависимости от операционной системы на вашем устройстве установить один из следующих пакетов:
  - На устройстве с операционной системой SUSE Linux Enterprise Server 15 установить пакет insserv-compat.
  - На устройстве с операционной системой Red Hat Enterprise Linux 8 или РЕД ОС установить пакет perl (sudo apt install perl)
  - На устройстве с операционной системой Red Hat Enterprise Linux 8 или РЕД ОС установить пакет perl-Getopt-Long.
  - На устройстве с операционной системой Red Hat Enterprise Linux или РЕД ОС установить пакет perl-File-Copy. Этот пакет требуется для работы скрипта первоначальной настройки приложения, но по умолчанию может отсутствовать.
- В операционных системах Astra Linux по умолчанию включен запрет трассировки ptrace (Disable ptrace capability), который может влиять на работу приложения Kaspersky Endpoint Security. Для корректной работы Kaspersky Endpoint Security рекомендуется отключить запрет трассировки ptrace при установке Astra Linux. Если Astra Linux уже установлена, инструкцию по включению и выключению этого режима см. насайте Справочного центра Astra Linux(Настройка механизмов защиты и блокировок, разделБлокировка трассировки ptrace).
- Если на вашем устройстве используется ядро Linux ниже 3.16, то нужно убедиться, что служба auditd не запущена или не установлена.
- Требуется установить на вашем устройстве пакет утилит iptables.
- Для запуска приложения требуется убедиться, что учетная запись root является владельцем следующих директорий и только владелец имеет право на запись в них: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.
- Необходима утилита which
- Для ОС РЕД используется библиотека:libxcrypt-compat
- Убедиться в том, что на вашем устройстве установлена библиотека lshw

Дистрибутивы для установки находятся в папке:

(Актуальная) Для версии KESL 12.1\\stal-file-01.severstal.severstalgroup.com\sccmapplication$\Kaspersky\Linux\KES\12.1

Необходимы будут:

klnagent64_15.1.0-20748 (Агент)

kesl 12.1.0.1589 (KESL)

С помощью WinSCP копируем агента и клиента на машину в папку /tmp, где необходима установка АВ3 . Устанавливаем пакеты в соответствии с версией ОС.

Проверить версию можно командой:

```
cat /etc/os-release
```

```
[kii@spp-kii-test ~]$ cat /etc/os-release
NAME="CentOS Linux"
VERSION="8 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="8"
PLATFORM_ID="platform:el8"
PRETTY_NAME="CentOS Linux 8 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:8"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"

CENTOS_MANTISBT_PROJECT="CentOS-8"
CENTOS_MANTISBT_PROJECT_VERSION="8"
REDHAT_SUPPORT_PRODUCT="centos"
REDHAT_SUPPORT_PRODUCT_VERSION="8"
```

Установка агента администрированияКасперского

Установка Kaspersky Endpoint Security (red-soft.ru)

Подключаемся к машине через putty и вводим команду в зависимости от типа операционной системы

Команда установки для deb-файлов (ОС – Ubuntu, Debian)
sudo apt install /tmp/klnagent64_X_amd64.deb

sudo dnf -y install klnagent64-14.0.0-4646.x86_64.rpm

Команда установки для rpm-файлов (ОС – Centos, RHEL, Fedora)
sudo rpm -i /tmp/klnagent64_X.x86_64.rpm

Дальнейшие действия при установке агента одинаковы для всех типов операционных систем:

Система предлагает запустить пост скрипт для настройки, запускаем

```
sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

```
[Antivir_admin@ksc-test-redos Загрузки]$ sudo rpm -i klnagent64-14.2.0-23324.x86_64.rpm
[sudo] пароль для Antivir_admin:
Installed version is 14.2.0.23324
Kaspersky Network Agent has been installed successfully but
needs to be properly configured before using.
Please run
/opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
script by yourself to configure installed software.
```

a. Предлагается ознакомиться с Лицензионным соглашением нажимаем букву **"Q"** для пролистывания, а затем соглашаемся с ним введя букву **"Y"** и нажимаем **ENTER;**

```
Please enter 'Y' to confirm that you accept the End User License
Agreement. You must accept the terms and conditions of the End
User License Agreement to install the application. Enter 'N'
providing you do not accept the End User License Agreement or
'R' to show it again [N]:
y
```

b. Затем требуется указать DNS-имя Сервера администрирования:
Выбираем свой сервер KSC из таблицы ниже, вводим ip-адрес сервера и нажимаем **ENTER**

```
Please enter Administration Server DNS-name or static IP-address
stal-ksc.severstal.severstalgroup.com
```

КСПД сервер KSC:

Имя KSC	**IP KSC**
stal-ksc	10.120.0.81

АСУТП сервера KSC:

KSC - сервера управления антивирусом - Severstal Knowledge Base - Severstal Knowledge Base

Имя сервера KSC	**IP сервера KSC**	**IP зоны ДМЗ**	**Производство/Цех**
asutp-ksc	10.120.2.21	10.99.0.0/16 10.99.10.0/24 10.99.250.0/24	Общие сервисы АСУ ТП Вторчермет Тестовая сеть для Байнина Д.
blg-ksc	10.57.134.5	10.57.	Яковлевский ГОК
chr-infr-ksc	10.99.120.81	10.99.120. 10.99.128.	Инфраструктура единого технологического домена
cpm2-uol-ksc	10.99.11.118	10.99.11.0/24 10.96.45.192/28 10.96.47.128/26	УОЛ Севергал, ЦПМ2
cpm2-uppm-ksc	10.96.102.77	10.99.12	УППМ, ЦПМ2
espc-ksc	10.99.7.118	10.99.7	ЭСПЦ
itz-ksc	10.9.20.118	10.9.20.	Ижорский трубный завод, Колпино
kadp-ksc	10.99.6.118	10.99.5 10.99.6	АГП и ДП
karo-asutp-ksc	10.32.140.10	10.32.	Карельский окатыш

khp-ksc	10.99.2.118	10.99.2	КХП (коксохимпроизводство)
kp-ksc	10.99.13.118	10.99.13	КП (конвертерное производство)
lpc1-ksc	10.99.14.118	10.96.231 10.99.14	ЛПЦ-1 (листопрокатный цех 1)
lpc2-ksc	10.99.40.118	10.99.40 10.96.188.96	ЛПЦ-2 (листопрокатный цех 2)
lpc3-ksc	10.8.20.118	10.8.20.0/24	ЛПЦ-3 (листопрокатный цех 3), Колпино
metiz-ksc	10.100.184.12	10.100.0.0/16	Северсталь-метиз
oln-asutp-ksc1	10.28.37.1	10.28.	Олкон
phl-ksc	10.99.16.44	10.99.16. 10.99.116. 10.96.152.64 10.96.143.0/24	Производство холодного проката
spp-ksc	10.99.17.118	10.99.17. 10.99.15. 10.96.225.	Сортопрокатное производство ЦГП (цех гнутых профилей) Старая ДМЗ СПП
stal-ksc	10.120.0.81	только КСПД 10.99.251. 10.99.173	КСПД всех площадок + сервера Череповца Резервное коп. 3D-склад
tpz-ksc	10.117.35.49	10.117.35.	Трубопрокатное производство, Шексна
uge-ksc	10.99.1.118	10.99.1. 10.96.2.	Управление главного энергетика
vlg-ksc	10.56.252.1	10.56.	Северсталь-метиз Волгоград

c. Затем требуется указать номер порта Сервера администрирования (по умолчанию 14000), ***пропускаем шаг клавишей ENTER;***
d. Затем требуетсяуказать номер SSL-порта Сервера администрирования (по умолчанию 13000), ***пропускаем шаг клавишей ENTER;***
e. Затем требуетсядать согласие на использование SSL-шифрования (по умолчанию "ДА"),***пропускаем шаг клавишей ENTER;***

```
Please enter Administration Server port number [14000]:

Please enter Administration Server ssl port number [13000]:

Please enter 'Y' to confirm that you want to use SSL encryption
or enter 'N' to use non-encrypted communication [Y]:
```

f. Затем требуетсянастроить шлюз соединения (по умолчанию "Do not configure connection gateway"), ***пропускаем шаг клавишей ENTER;***

```
The Network Agent being installed can be used as connection
gateway. It will allow you to connect to Administration Server
using the specified connection gateway.

1) Do not configure connection gateway
2) Do not use connection gateway
3) Connect to server using connection gateway
4) Use as connection gateway
Please choose connection gateway mode: [1]:
```

g. Для проверки подключения к серверу KSC необходимо выполнить команду:

Проверка работы агента администрирования

```
/opt/kaspersky/klnagent64/bin/klnagchk
```

В выводе должно быть сообщено об успешной работе агента и подключении к серверу. Если имеются ошибки транспортного уровня, то необходимо проверить соединение до сервера и если открыть необходимые порты на сети, согласно ACL.

```
[Antivir_admin@ksc-test-redos ~]$ /opt/kaspersky/klnagent64/bin/klnagchk
Starting klnagchk utility
Checking command-line arguments...OK
Initializing basic libraries...OK
Current host is 'ksc-test-redos.severstal.severstalgroup.com'
Network agent version is '14.2.0.23324'


Reading settings...OK
Checking settings...OK
Administration Agent settings:
  Server address: 'stal-ksc.severstal.severstalgroup.com'
  Use SSL: 1
  Compress traffic: 1
  Server SSL ports: '13000'
  Server ports: '14000'
  Use proxy: 0
  Certificate: present
  Open UDP port: 1
  UDP ports: '15000'

  Ping period, minutes: 30
  Conn timeout, s: 30
  RW timeout, s: 180
  HostId: 845bf3a8-d09f-4dc6-bc39-2c7d096210b8

Update agents location(s):
    cher-na-02.severstal.severstalgroup.com:13000 (SSL)
    cher-na-02.severstal.severstalgroup.com:14000
    cher-na-01.severstal.severstalgroup.com:13000 (SSL)
    cher-na-01.severstal.severstalgroup.com:14000


Connecting to server...OK

Connecting to the Administration Agent...OK
Administration Agent is running
Acquire Administration Agent statistics...OK
  Administration Agent statistics:
  Ping count: 182
  Succ. pings: 182
  Sync count: 29
  Succ. syncs: 29
  Last ping: 02.09.2024 07:04:41 GMT (02.09.2024 10:04:41)


Deinitializing basic libraries...OK
```

h. Дополнительно возможно уточнить подключение хоста уИнфоком.УППК.АВЗ <cher.it.security@stalcom.com>

Установка клиента Касперского (KESL)

Вводим команду в зависимости от типа операционной системы:

Команда установки для deb-файлов (ОС – Ubuntu, Debian)
sudo apt install /tmp/kesl_X_amd64.deb

Команда установки для rpm-файлов (ОС – Centos, RHEL, Fedora)
sudo rpm -i /tmp/kesl-X.x86_64.rpm

Дальнейшие действия при установке клиента одинаковы для всех типов операционных систем:

Система предлагает запустить пост скрипт для настройки, запускаем:

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

```
[Antivir_admin@ksc-test-redos /]$ sudo /opt/kaspersky/kesl/bin/kesl-setup.pl

Kaspersky Endpoint Security 12.0 for Linux version 12.0.0.6672
```

1. При установке версии KESL 12.+ будет выбор варианта использования - Standalone или Light Agent. ***Отклоняем условия вводом буквы "N"и нажимаем ENTER;***

```
Specifying the application usage mode

You can use Kaspersky Endpoint Security for Linux in standalone mode to
protect devices running Linux operating systems or in Light Agent mode to
protect virtual machines running Linux guest operating systems. Do you want
to use the application in Light Agent mode? [n]: n
```

2. Предлагается выбор языка, (по умолчанию en_EN),***пропускаем шаг клавишей ENTER;***

```
Setting up the Anti-Malware Service default locale

The specified locale will be used to show user agreements in this script
and send events to Kaspersky Security Center.
List of available locales:
- ru_RU.UTF-8
- de_DE.UTF-8
- en_US.UTF-8
- fr_FR.UTF-8
- ja_JP.UTF-8
- zh_CN.UTF-8
[ru_RU.UTF-8]:

Anti-Malware Service default locale is changed to 'ru_RU.UTF-8'.
Service will be restarted if it is already running.
```

3. Затем появляется Лицензионное соглашение и Политика Конфиденциальности. ***Пролистываем его вводом буквы "Q";***
4. Затем требуется принять Лицензионное соглашение.***Принимаем его вводом буквы "Y"и нажимаем ENTER;***

```
Accepting the End User License Agreement (EULA) and Privacy Policy

Please confirm that you have fully read, understand, and accept the End
User License Agreement (EULA) and Privacy Policy to continue.

NOTE: To quit the EULA and Privacy Policy viewer, press the Q key.

Press ENTER to display the EULA and Privacy Policy:


Read EULA and Privacy Policy from file "/opt/kaspersky/kesl/doc/license.ru"
(utf-8) if it cannot be read here.

I confirm that I have fully read, understand, and accept the terms and
conditions of this End User License Agreement [y/n]:
```

5. Затем требуется принятьПолитику Конфиденциальности***. Принимаем ее вводом буквы"Y"и нажимаем ENTER;***

```
I am aware and agree that my data will be handled and transmitted
(including to third countries) as described in the Privacy Policy. I
confirm that I have fully read and understand the Privacy Policy [y/n]:
```

6. Затем требуется принять или отклонить условия Положения о Kaspersky Security Network (KSN). ***Отклоняем условия вводом буквы "N"и нажимаем ENTER;***

```
Configuring KSN

I confirm that I have fully read, understand, and accept the terms and
conditions of the Kaspersky Security Network Statement (KSN Statement is
available here: '/opt/kaspersky/kesl/doc/ksn_license.ru') [y/n]: n
```

7. Затем требуется указать пользователя, которому нужно предоставить права администратора,***пропускаем шаг клавишей ENTER;***

```
Granting the Administrator role

Only users with the Administrator role have full access to the program
management by command line and GUI.

Specify user to grant the 'admin' role to (leave empty to skip):
```

8. Включение автоматической настройки SELinux (Этот шаг отображается, только если в вашей операционной системе установлена система SELinux). SELinux - система принудительного контроля доступа, которая использует политику привилегий для сервисов и пользователей. Политика SELinux по умолчанию ограничивает нетривиальные механизмы работы KESL, что приводит к различным проблемам в работе продукта. При наличии данной системы***Принимаем ее вводом буквы"Y"и нажимаем ENTER;***

После этого установка клиента KES for Linux завершена. Проверяем в консоли Касперского, иногда может потребоваться перезагрузка системы.

Для того, чтобы запустить принудительное обновление баз KESL, необходимо:

1. Синхронизироваться с серверов администрирования /opt/kaspersky/klnagent64/bin/klnagchk

2. Найти через команду kesl-control --get-task-list, в списке задачу "Name: SC:Обновление KESL 12"

3. Запустить задачу командой kesl-control --start-task <ID задачи обновления> -W

```
Name: SC:Обновление KESL 12
    ID      : 100
    Type    : Update
    State   : Stopped
root@stal-kse:/home/oper# kesl-control --start-task 100 -W
```

4. Запустить задачу командой kesl-control - -app-info для проверки работы АВ3, получения обновлений и ключа лицензий

Удаление антивируса Касперского

1. **Удаление Клиента Администрирования (KESL).**
   a. Чтобы удалить Kaspersky Endpoint Security, установленный из пакета формата RPM, выполните следующую команду:

Удаление клиента
`# rpm -e kesl`

   b. Чтобы удалить Kaspersky Endpoint Security, установленный из пакета формата DEB, выполните следующую команду:

Удаление клиента
`# apt-get remove kesl`

   c. Чтобы удалить Kaspersky Endpoint Agent, установленный из пакета формата DEB, выполните следующую команду:

Удаление клиента

```
# apt-get remove epagent
```

2. **Удаление агента.**
   a. Чтобы удалить Агент администрирования, установленный из пакета формата RPM, выполните следующую команду:

Удаление агента

```
# rpm -e klnagent
```

   b. Чтобы удалить Агент администрирования, установленный из пакета формата DEB, выполните следующую команду:

Удаление агента

```
# apt-get remove klnagent
```

Программа автоматически выполняет процедуру удаления. По завершении программа выводит сообщение о результатах удаления.

Полезные команды

Вызов набора команд управления KESL

```
kesl-control --help
```

Вывод информации о KES

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

Вывод информации о задачах

```
kesl-control --get-task-list
```

Смена сервера администрирования

```
/opt/kaspersky/klnagent64/bin/klmover -address *  *
```

Проверка работы агента администрирования

```
/opt/kaspersky/klnagent64/bin/klnagchk
```

Исключения точек монтирования

```
kesl-control -T --get-app-settings
```

Исключения из проверки файлов и процессов

```
sudo kesl-control -T --get-settings 1
```

Исключения задачи Анализ поведения

```
kesl-control --get-settings 20
```

Аппаратные и программные требования

Минимальные аппаратные требования:

- процессор Core™ 2 Duo 1.86 ГГц или выше;
- раздел подкачки не менее 1ГБ;
- 1 ГБ оперативной памяти для 32-битных операционных систем, 2 ГБ оперативной памяти для 64-битных операционных систем;
- 4 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов;

Минимальные аппаратные требования для архитектуры Arm:

- процессор Armv8.2-A Kunpeng 920 или Armv8-A Baikal-M (BE-M1000) или платформа m-TrusT Терминал;
- раздел подкачки не менее 1ГБ;
- 2 ГБ оперативной памяти;
- 3 ГБ свободного места на жестком диске для установки приложения и хранения временных файлов и файлов журналов;

Для установки Kaspersky Endpoint Security на устройстве должна быть установлена одна из следующих операционных систем:

- 32-битные операционные системы:
  - CentOS 6.7 и выше.
  - Debian GNU/Linux 11.0 и выше.
  - Debian GNU/Linux 12.0 и выше.
  - Mageia™ 4.
  - Red Hat® Enterprise Linux® 6.7 и выше.
  - Альт 8 СП Рабочая Станция.
  - Альт 8 СП Сервер.
  - Альт Рабочая Станция 10.
  - Альт СП Рабочая Станция релиз 10.
- 64-битные операционные системы:
  - AlmaLinux OS 8 и выше.
  - AlmaLinux OS 9 и выше.
  - AlterOS® 7.5 и выше.
  - Amazon™ Linux 2.
  - Astra Linux Common Edition 2.12.
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
  - Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
  - Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
  - CentOS 6.7 и выше.
  - CentOS 7.2 и выше.
  - CentOS Stream 8.
  - CentOS Stream 9.
  - Debian GNU/Linux 11.0 и выше.
  - Debian GNU/Linux 12.0 и выше.
  - EMIAS 1.0 и выше.
  - EulerOS 2.0 SP5.
  - Kylin 10.
  - Linux Mint 20.3 и выше.
  - Linux Mint 21.1 и выше.
  - openSUSE Leap 15.0 и выше.
  - Oracle Linux 7.3 и выше.
  - Oracle Linux 8.0 и выше.
  - Oracle Linux 9.0 и выше.
  - Red Hat Enterprise Linux 6.7 и выше.
  - Red Hat Enterprise Linux 7.2 и выше.
  - Red Hat Enterprise Linux 8.0 и выше.
  - Red Hat Enterprise Linux 9.0 и выше.
  - Rocky Linux 8.5 и выше.
  - Rocky Linux 9.1.
  - SberLinux 8.8 (Dykhtau).
  - SUSE Linux Enterprise Server 12.5 и выше.
  - SUSE Linux Enterprise Server 15 и выше.
  - Ubuntu® 20.04 LTS.

    - Ubuntu 22.04 LTS.
    - Альт 8 СП Рабочая станция.
    - Альт 8 СП Сервер.
    - Альт Рабочая Станция 10.
    - Альт Сервер 10.
    - Альт СП Рабочая Станция релиз 10.
    - Альт СП Сервер релиз 10.
    - Атлант, сборка Alcyone, версия 2022.02.
    - Гослинукс 7.17.
    - Гослинукс 7.2.
    - МСВСФЕРА 9.2 СЕРВЕР.
    - МСВСФЕРА 9.2 АРМ.
    - РЕД ОС® 7.3.
    - РЕД ОС 8.0.
    - РОСА "Кобальт" 7.9.
    - РОСА "Хром" 12.
    - СинтезМ-Клиент 8.6.
    - СинтезМ-Сервер 8.6.
- 64-битные операционные системы для архитектуры Arm:
    - Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
    - CentOS Stream 9.
    - EulerOS 2.0 SP8.
    - SUSE Linux Enterprise Server 15.
    - Ubuntu 22.04 LTS.
    - Альт Рабочая Станция 10.
    - Альт Сервер 10.
    - Альт СП Рабочая Станция релиз 10.
    - Альт СП Сервер релиз 10.
    - РЕД ОС 7.3.

Из-за ограничений технологии fanotify приложение не поддерживает работу со следующими файловыми системами: autofs, binfmt_misc, cgroup, configfs, debugfs, devpts, devtmpfs, fuse, fuse.gvfsd-fuse, gfs2, gvfs, hugetlbfs, mqueue, nfsd, proc, parsecfs, pipefs, pstore, usbfs, rpc_pipefs, securityfs, selinuxfs, sysfs, tracefs.