?????????? ?? ??????????
KATA 7.0.3 - 7.1

??????????????:

1. Проверьте, нет ли ошибок в веб-консоли. Исправьте их, если они есть, или отправьте инцидент в службу поддержки, отметив, что это подготовка к обновлению.
2. Проверьте, что на всех узлах установлено правильное время в BIOS/IPMI или гипервизоре. В противном случае при загрузке с ISO время будет неверным независимо от времени в ОС до обновления. Обновление не удастся, если расхождение во времени будет значительным.
3. Перед обновлением программы с версии 7.0.3 до версии 7.1 рекомендуется предварительно создать резервную копию текущего состояния программы и загрузить ее на жесткий диск вашего компьютера из меню администратора программы или из режима Technical Support Mode. В случае сбоя при обновлении программы или необходимости переустановить Kaspersky Anti Targeted Attack Platform вы сможете воспользоваться сохраненной копией программы. Для выполнения резервной копии вам может потребоваться до 1 Тб места на сетевом хранилище, или подключаемом диске/папке.

   Статья "Резервное копирование Central Node"

   Рекомендуется также ознакомиться с ограничениями для той версии, до которой вы обновляете приложение.
4. Перед обновлением программы с версии 7.0.3 до версии 7.1 на виртуальной среде VMware или любой другой виртуализации. Snapshots не поддерживаются! Однако если вы сделаете снимок в выключенном состоянии VM (выключение только командой меню TUI консоли ssh и только после создания резервной копии!), то это не повредит. Обратите внимание, что восстановление снимка, сделанного более 24 часов назад, скорее всего, не удастся из-за истечения срока действия сертификата Docker. Если вы сделаете выключение и создадите снимок, то после включения снова проверьте пункты 1-2.
5. Задокументируйте где-нибудь сетевую и другую конфигурацию (например, SPAN, ICAP и т. д.) для всех узлов. Эта информация понадобится для узлов, которые будут переустановлены (датчики, sandboxes). Она также может понадобиться в случае, если вам нужно переустановить CN, но восстановление из резервной копии по какой-то причине не удается.
6. Задокументируйте где-нибудь конфигурацию внешних систем (SMTP, POP, ICAP, API, KSMG). Например, коннекторы на серверах Exchange и настройки ICAP на прокси-

серверах.

7. Запланируйте временное отключение блокирующих интеграций во внешних системах (SMTP, POP, ICAP, API, KSMG). Например, коннекторы сервера Exchange, интеграция ICAP на прокси-сервере. Запланируйте их обратное включение (чтобы не забыть об этом). В противном случае внешние системы, интегрированные с KATA, такие как внутренние почтовые серверы, прокси-серверы и т. д., могут получить чрезмерные очереди, получить сбой во время обновления KATA.
8. Если вы используете режим распределенного решения и мультитенантности, вам нужно обновить каждый Central Node в соответствии с описанной ниже процедурой, не отключая при этом SCN от PCN. Отключение SCN от PCN необратимо, повторное подключение SCN к какому-либо серверу PCN не предусмотрено. Обновление должно начинаться с PCN. Не отключайте SCN от PCN. Отключение SCN не допускается, это приведет к технической проблеме, для которой в настоящее время нет WA. Не путайте SCN с сенсорными узлами. Песочницы и сенсорные узлы должны быть отключены, но SCN — нет!.
9. Обновление поставляется в виде пакета обновлений. Пакет входит в комплект поставки приложения.
10. Обновление компонента до версии 7.1 возможно только с версии 7.0.3. Если вы используете более раннюю версию, требуется последовательно обновить версии компонента до версии 7.1.
11. **ВАЖНО:** Перед началом процесса установки необходимо удалить интеграцию компонента Central Node и Sensor, Central Node и Sandbox.
12. Удалите коннекторы и серверы интеграции, если они были добавлены. Агенты EDR/NDR будут выдавать ошибки подключения, поэтому сообщите тому, кто отслеживает события в KSC, о планируемых работах по техническому обслуживанию.
13. **ВАЖНО: Независимо от лицензирования на CN в настройках размера проверьте трафик SPAN: https://support.kaspersky.com/help/KATA/7.0/en-US/247192.htm Если он равен нулю, измените его как минимум на 100 Мбит/с. Выполните следующие команды:**

    ```
    sudo -i

    kata-enable-span
    ```

    Даже если вы не используете обработку зеркалированного трафика со SPAN-портов (в том числе в приложении, работающем с лицензионным ключом KEDR).

14. **Просьба учитывать известные ограничения, связанные с версией 7.1 - https://support.kaspersky.com/help/KATA/7.1/ru-RU/247274.htm**
15. **Важно:** обновление компонентов Sensor и Sandbox не предусмотрено. Для данных компонентов только чистая установка.
16. Дополнительные особенности по обновлению доступны по ссылке: https://support.kaspersky.com/help/KATA/7.1/ru-RU/246850.htm

KATA 7.1 CN ? upgrade files

Дистрибутивы предоставляется сотрудниками Лаборатории Касперского по запросу.

KATA 7.1 CN Astra Edition ? upgrade files

Данная инструкция подходит и для обновления решения Kaspersky Anti Targeted Attack Platform на базе ОС «Астра». Для сборки образа ПО KATA на базе ОС Astra Linux предоставляется необходимый пакет приложений для самостоятельной сборки образа, который необходимо запросить у сотрудника «Лаборатории Касперского» по запросу. При обновлении Central Node на сервере с операционной системой Astra Linux может потребоваться больший объем дискового пространства. Если дискового пространства оказывается недостаточно, процесс обновления прерывается, отображается сообщение о недостаточности дискового пространства.

Чтобы возобновить обновление при нехватке дискового пространства:

1. Создайте резервную копию Central Node и загрузите ее на жесткий диск из меню администратора приложения.
2. Выполните очистку диска с помощью утилиты.

После очистки диска вы можете возобновить обновление.

?????

Если в процессе обновления возникли ошибки, не пытайтесь повторить установку самостоятельно. Лучше сразу обратиться в техническую поддержку, чтобы специалисты выяснили причину проблемы.

??????????? ?????????? ? ?????? 7.0.3 ?? ?????? 7.1

1. После обновления Kaspersky Anti Targeted Attack Platform до версии 7.1 вам нужно будет заново добавить лицензионные ключи приложения.
2. Допускается кратковременный перерыв в работе приложения, в том числе для отказоустойчивой версии приложения.
3. Если в роли компонента Sensor используется решение Kaspersky Secure Mail Gateway, параметры интеграции с ним сохраняются.
4. Совместимость сервера Central Node 7.1 с компонентами Sensor и Sandbox более ранней версии не поддерживается.
5. Данные компонента Sandbox/Sensor не сохраняются. В приложении не предусмотрена стандартная процедура обновления. Вам требуется установить компонент версии 7.1.

?????????? Central Node ? ?????? 7.0.3 ?? ?????? 7.1

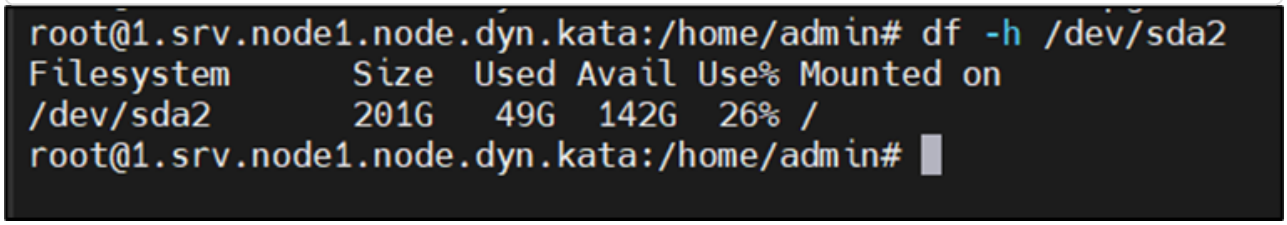
1. Поместите пакет с обновлением приложения на сервер с компонентом Central Node в директорию **/data**.
   - Скаченный архив с помощью WinSCP или другим удобным способом загрузите в домашний каталог пользователя admin **(/home/admin)**.
   - Далее подключитесь по SSH к Central Node, зайдите в **Technical Support Mode** и переключитесь на пользователя **root** командой **sudo su**.
   - Переместите архив в директорию /data командой:

   ```
   mv kata-upgrade-7.1.0.530-x86_64_en-ru-zh.tar.gz /data/
   ```

2. Убедитесь, что размер свободного дискового пространства в файловой системе /dev/sda2 составляет более 100 ГБ.
   Для определения свободного дискового пространства в файловой системе /dev/sda2 воспользуйтесь командой:

   ```
   df -h /dev/sda2
   ```

3. Если вы не используете обработку зеркалированного трафика со SPAN-портов (в том числе в приложении, работающем с лицензионным ключом KEDR).
   Выполните команду:

   ```
   kata-enable-span
   ```

   Если обработка зеркалированного трафика со SPAN-портов выключена, обновление завершается ошибкой.

4. Распакуйте архив с обновлением
   Для распаковки архива воспользуйтесь командой:

   ```
   tar xvf /data/kata-upgrade-7.1.0.530-x86_64_en-ru-zh.tar.gz -C /data/
   ```

```
root@1.srv.node1.node.dyn.kata:/home/admin# tar xvf /data/kata-upgrade-7.1.0.530-x86_64_en-ru-zh.tar.gz -C /data/
upgrade/
upgrade/astra_image_versions.json
upgrade/images_astra.tar.gz
upgrade/images_common.tar.gz
upgrade/images_ubuntu.tar.gz
upgrade/run_kata_upgrade.py
upgrade/tools_pgcopydb
upgrade/ubuntu_image_versions.json
upgrade/whl/
upgrade/whl/kata_antiaptdb_cleaner/
upgrade/whl/kata_antiaptdb_cleaner/Flask-2.0.1-py3-none-any.whl
upgrade/whl/kata_antiaptdb_cleaner/MarkupSafe-3.0.2-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl
upgrade/whl/kata_antiaptdb_cleaner/SQLAlchemy-1.4.31.tar.gz
upgrade/whl/kata_antiaptdb_cleaner/Werkzeug-2.0.2-py3-none-any.whl
upgrade/whl/kata_antiaptdb_cleaner/attrs-25.1.0-py3-none-any.whl
upgrade/whl/kata_antiaptdb_cleaner/boto3-1.17.43-py2.py3-none-any.whl
```

5. Выполните последовательность команд:

```
mkdir -p /data/install_data


cp /etc/kaspersky/swarm/*_image_versions.json /data/install_data
```

```
root@1.srv.node1.node.dyn.kata:/home/admin# mkdir -p /data/install_data
root@1.srv.node1.node.dyn.kata:/home/admin# cp /etc/kaspersky/swarm/*_image_versions.json /data/install_data
root@1.srv.node1.node.dyn.kata:/home/admin#
```

6. Установите пакет с обновлением
   - Перейдите в каталог выполнив команду:

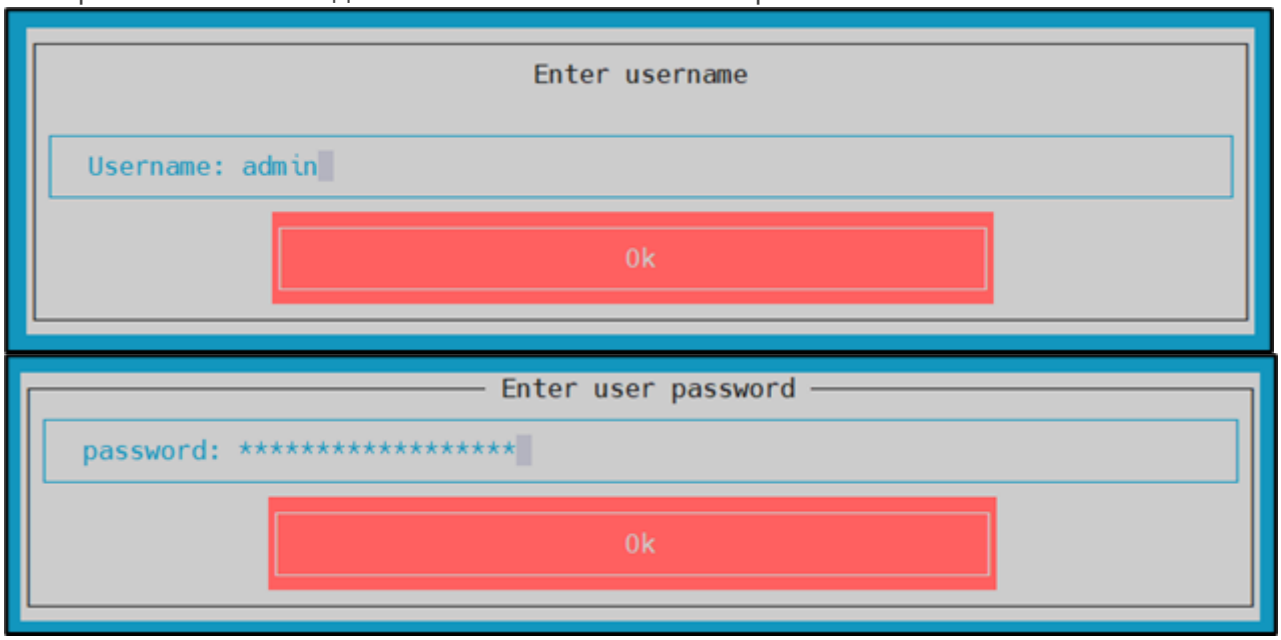
     ```
     cd /data/upgrade
     ```

   - Запустите скрипт командой:

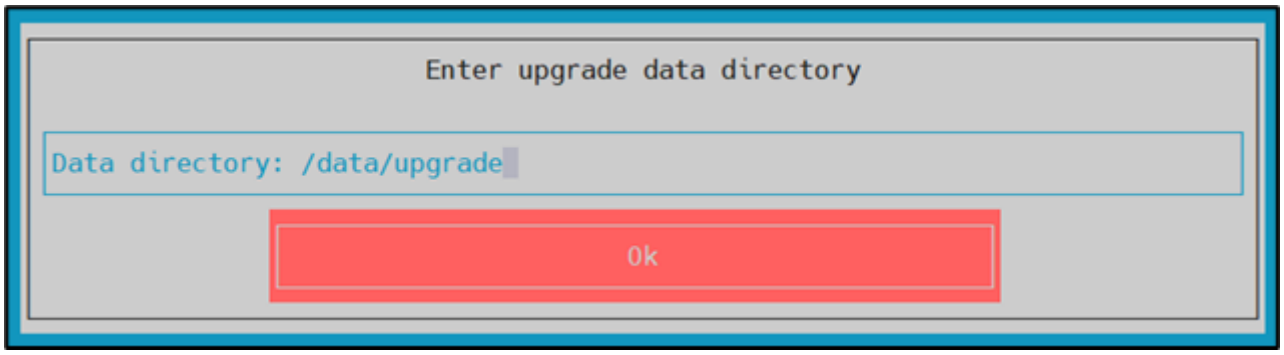
     ```
     ./run_kata_upgrade.py --clear-venv
     ```

```
root@1.srv.node1.node.dyn.kata:/home/admin# cd /data/upgrade/
root@1.srv.node1.node.dyn.kata:/data/upgrade# ./run_kata_upgrade.py --clear-venv
```

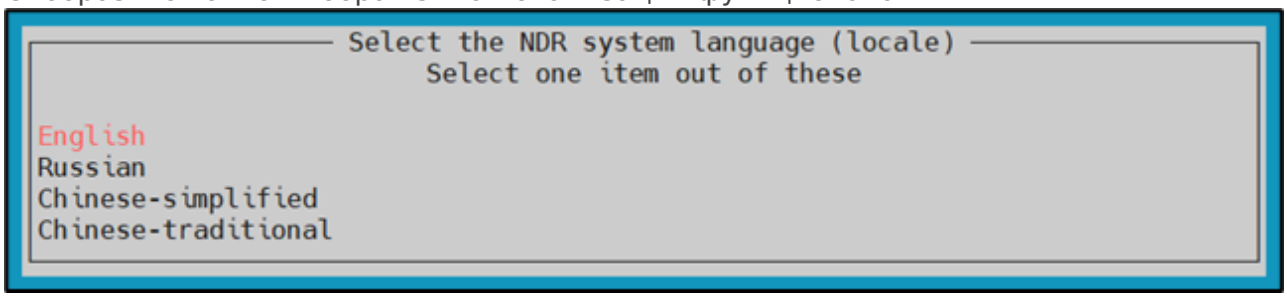
7. Отобразится окно ввода имени пользователя и пароля.



8. Отобразится окно ввода пути к архиву с обновлением. Значение по умолчанию: /data/upgrade. Выберите кнопку OK и нажмите на клавишу Enter.

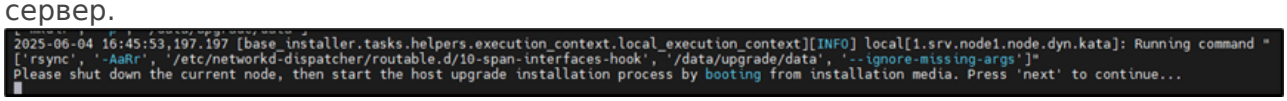


9. Отобразится окно выбора языка локализации функционала NDR.

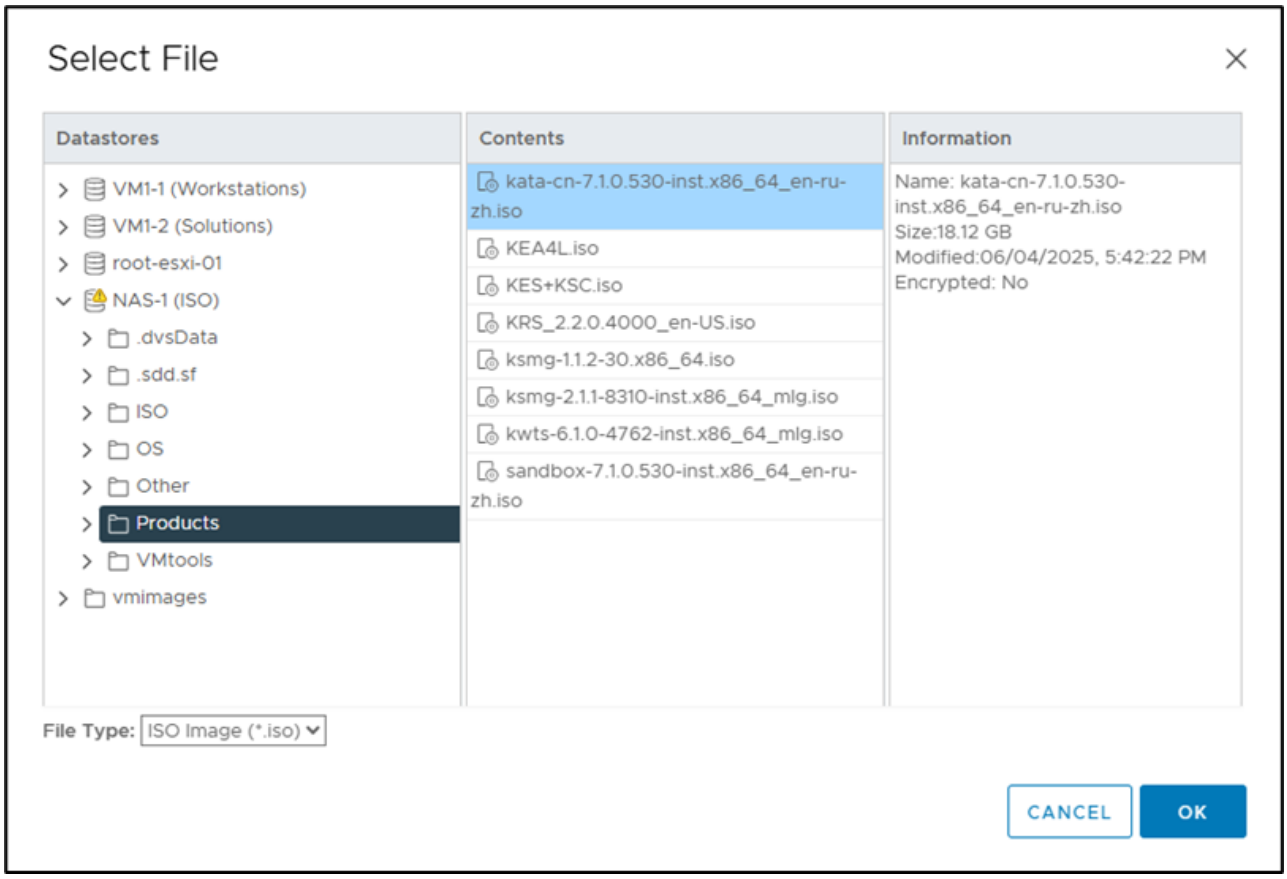


10. Через некоторое время в консоли отобразится сообщение о необходимости выключения сервера.

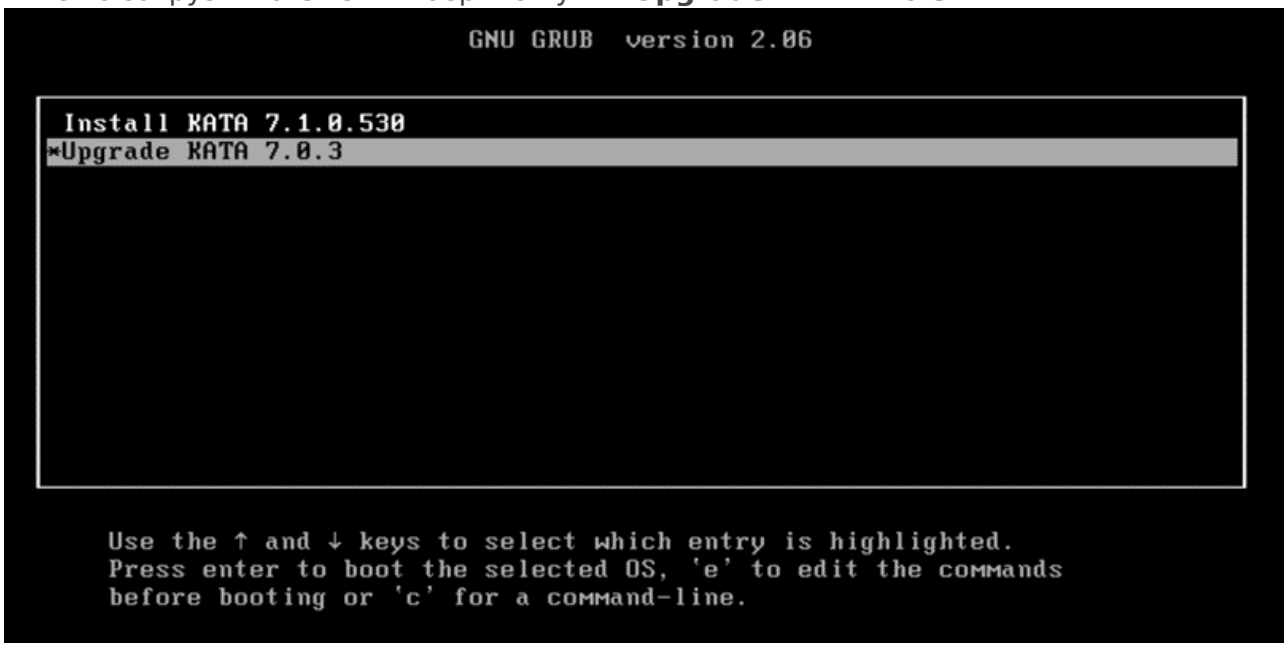
    После отображения сообщения о необходимости выключения сервера выключите сервер.



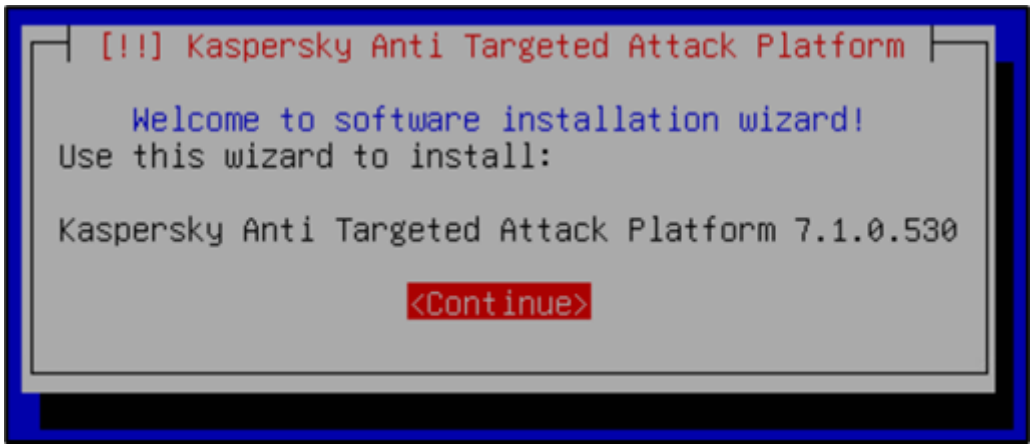
11. Смонтируйте iso-образ с Kaspersky Anti Targeted Attack Platform версии 7.1 и перезагрузите сервер.
    В параметрах BIOS включите загрузку с CD/DVD-ROM. Если вы производите обновление на платформе VMware, то в процессе загрузки ОС нажмите **ESC** для выбора источника загрузки, в нашем случае CD/DVD-ROM.



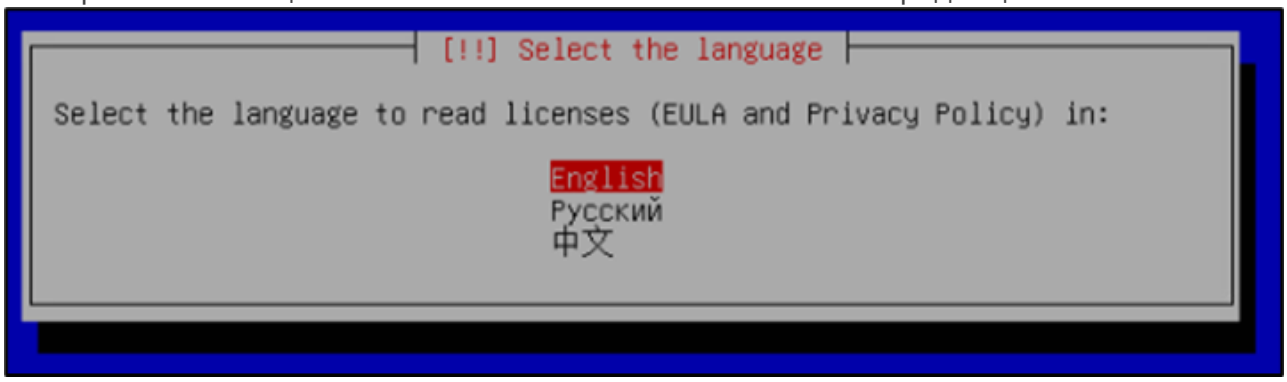
12. В меню загрузчика GRUB выберите пункт **Upgrade KATA 7.0.3**



13. В консоли отобразится загрузка ОС. Нажмите **“Continue”**.

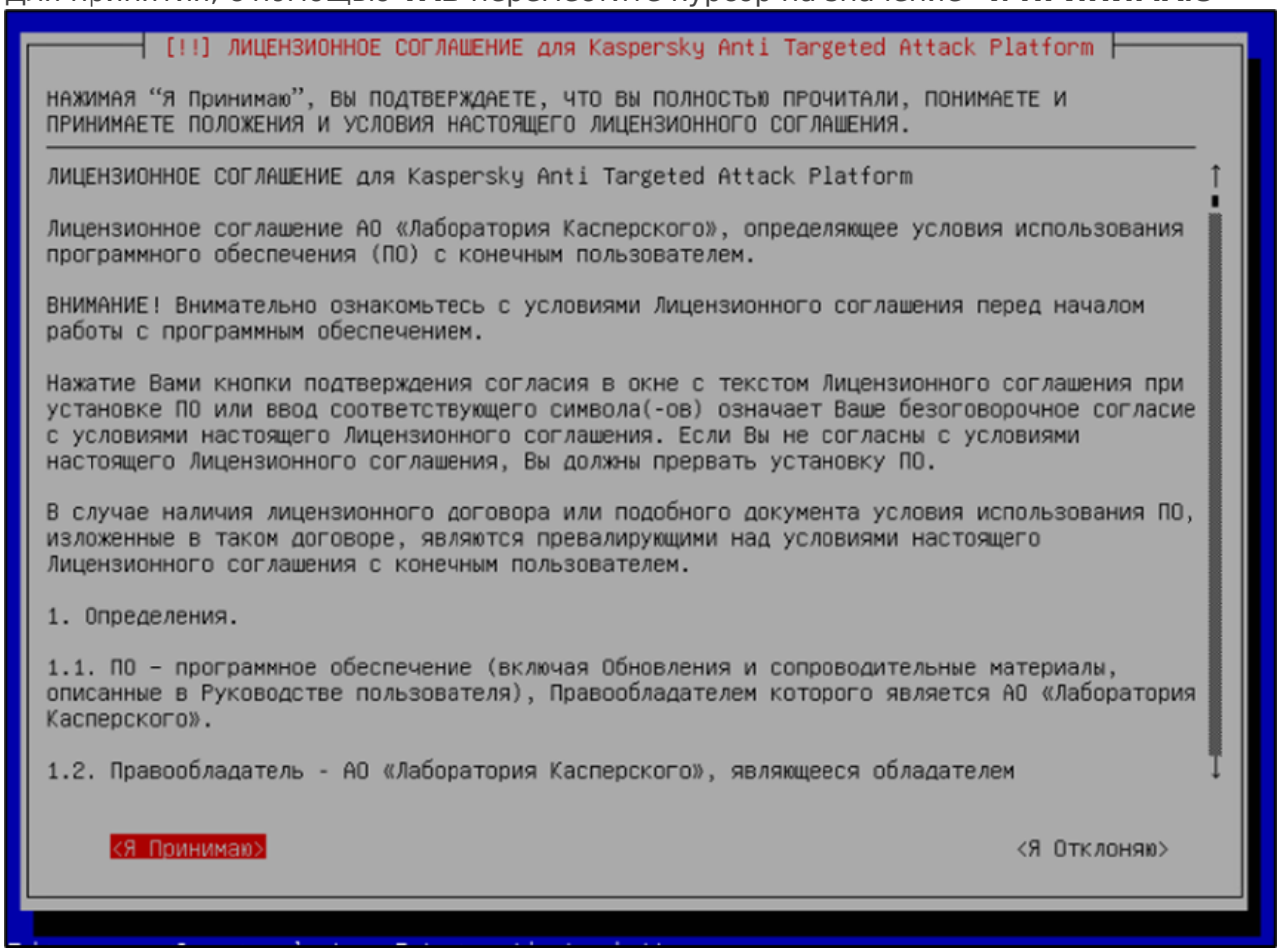


14. Выберите язык лицензионного соглашения и политики конфиденциальности.



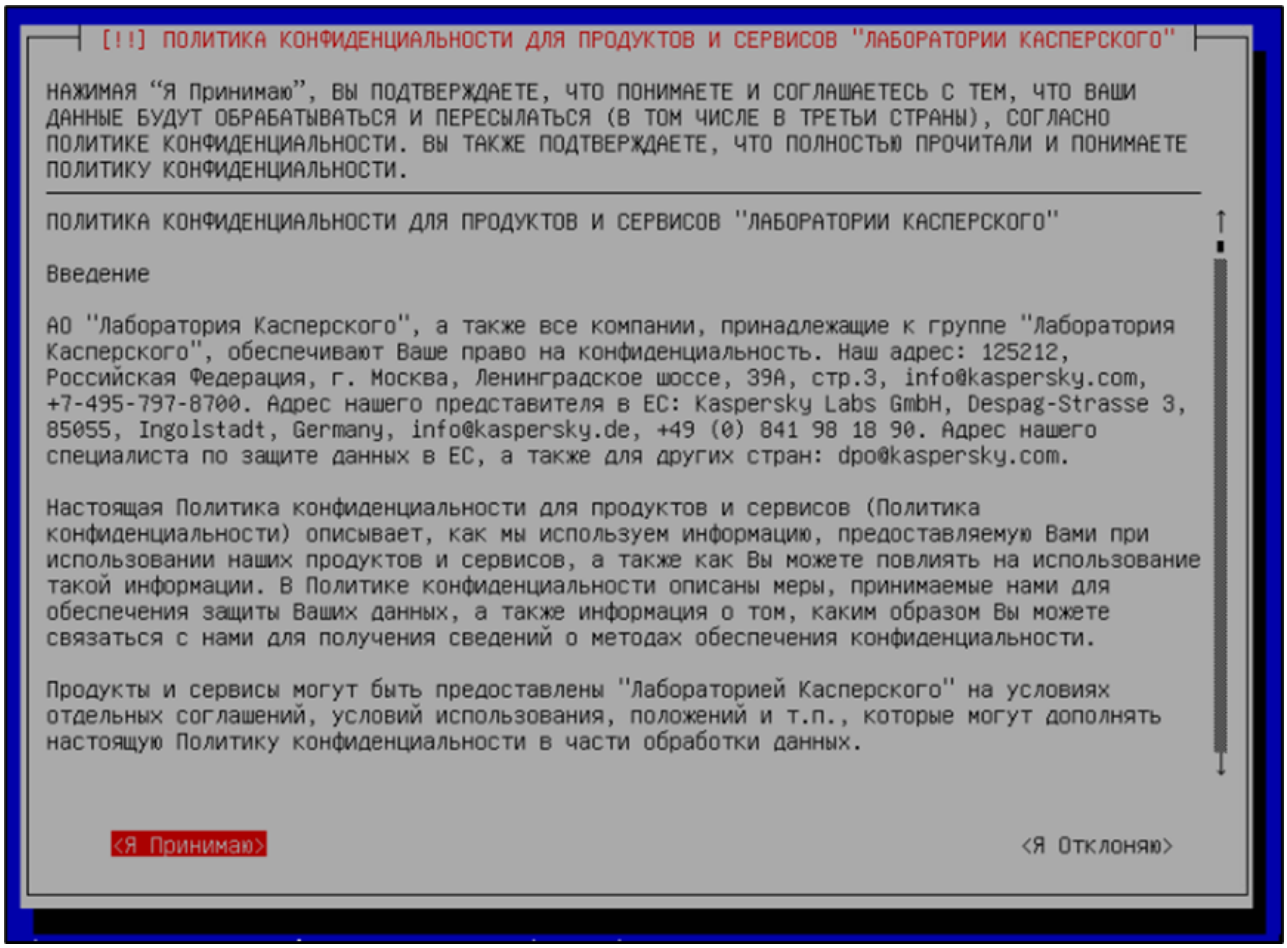
15. Ознакомьтесь с лицензионным соглашением.

    Для принятия, с помощью **TAB** переместите курсор на значение **«Я ПРИНИМАЮ»**



16. Ознакомьтесь с политикой конфиденциальности.

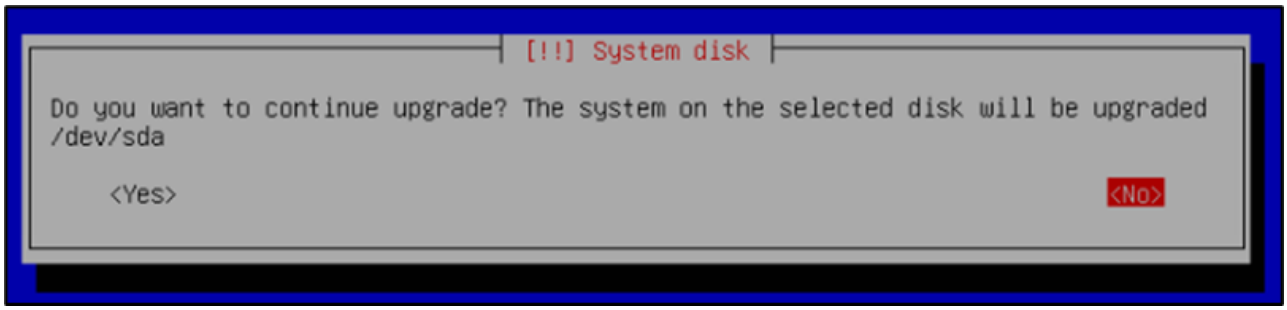
    Для принятия, с помощью **TAB** переместите курсор на значение **«Я ПРИНИМАЮ»**



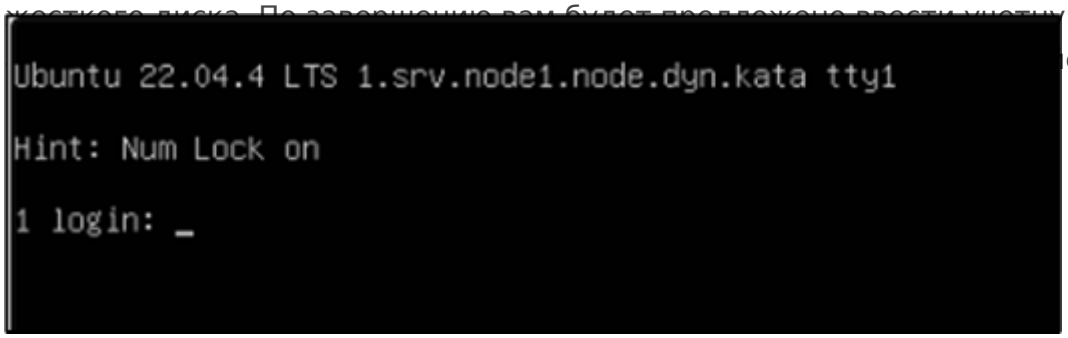
17. Выберите диск для установки компонента (**обязательно sda**).



18. Согласитесь с продолжением обновления системы.



19. Дождитесь окончания процесса обновления.
    В процессе обновления система может перезагрузиться и продолжить процесс с жесткого диска. По завершению вам будет предложено ввести учетную запись



    ком.

    Перед первым использованием убедитесь, что контейнеры не находятся в состоянии Starting, для этого воспользуйтесь командой:

```
docker ps | grep start
```

    Если вывод оказался не пустым, то подождите 10-15 минут и повторно проверьте. Когда вывод будет пустым, то можете продолжить знакомиться с новыми функциями системы.
    Не забудьте повторно добавить лицензии и произвести интеграцию с новыми версиями Sandbox и Sensor.

    На этом процесс обновления Central Node завершен.



20. По факту завершения обновления рекомендуем удалить загруженный архив с обновлением для высвобождения пространства, выполнив следующую команду.

```
rm -rf /data/kata-upgrade-7.1.0.530-x86_64_en-ru-zh.tar.gz
```

```
root@1.srv.node1.node.dyn.kata:/home/admin# cd /data/
root@1.srv.node1.node.dyn.kata:/data# ls -l
total 15831792
-rw-r--r--  1 root  root          305 Mar 28 17:28 debconf_menu_answers.ini
drwxr-xr-x  9 root  root         4096 Mar 28 17:47 install_data
-rw-rw-r--  1 admin admin 16211712000 Mar 28 16:15 kata-upgrade-7.0.3.520-x86_64
_en-ru.tar.gz
drwxr-xr-x  2 root  root         4096 Mar 28 14:26 local_persist
drwx------  2 root  root        16384 Mar 28 12:50 lost+found
drwxr-xr-x  4 root  root         4096 Mar 28 14:26 storage
drwxr-xr-x 11 root  root         4096 Mar 28 17:21 volumes
root@1.srv.node1.node.dyn.kata:/data# rm -f kata-upgrade-7.0.3.520-x86_64_en-ru.tar.gz
```

??????????????:

После обновления компонента Central Node, который использовался в **режиме распределенного решения или мультитенантности, до версии 7.1** может отсутствовать встроенный Sensor (Embedded Sensor). Чтобы устранить данную проблему выполните следующие действия:

1. Войдите в консоль управления того сервера Central Node, на котором требуется восстановить встроенный Sensor, по протоколу SSH или через терминал.

   ```
   Ubuntu 22.04.4 LTS 1.srv.node1.node.dyn.kata tty1

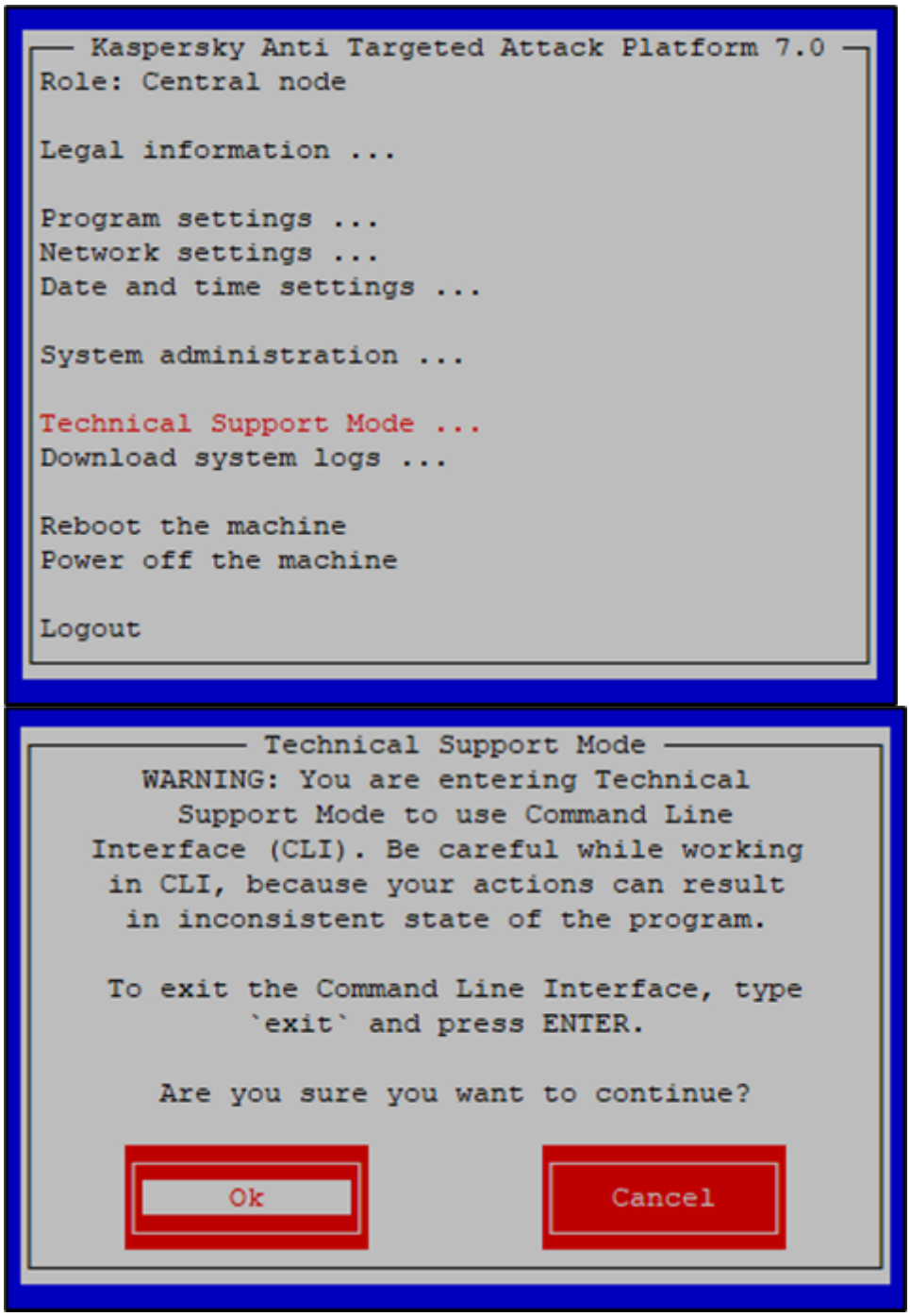
   Hint: Num Lock on

   1 login: _
   ```

2. В меню администратора приложения выберите режим **Technical Support Mode**.

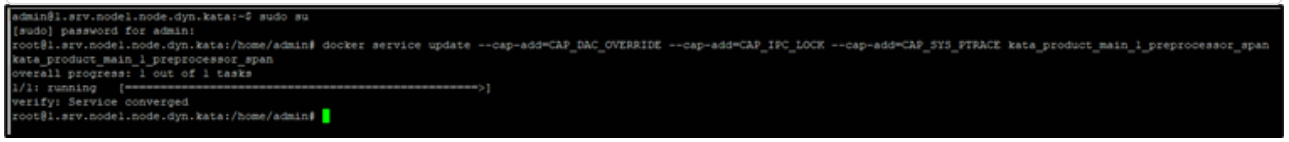
   Нажмите на клавишу **ENTER**.
   Отобразится окно подтверждения входа в режим **Technical Support Mode**.

   Подтвердите, что хотите выполнять действия с приложением в режиме **Technical Support Mode**. Для этого выберите **Yes** и нажмите на клавишу **ENTER**.



3. Перейдите в режим root и выполните следующую команду:

```
docker service update --cap-add=CAP_DAC_OVERRIDE --cap-add=CAP_IPC_LOCK --cap-add=CAP_SYS_PTRACE kata_product_main_1_preprocessor_span
```



?????????? Sensor ????? ???????????.

Revision #23
Created 24 July 2025 14:04:21 by Александр
Updated 6 February 2026 10:55:04 by Кирилл