ORBOX

Система контроля качества медиафайлов

Инструкция по установке и настройке

Компания «Теком»
Нижний Новгород
2024 год

СОДЕРЖАНИЕ

1. УСТАНОВКА, НАСТРОЙКА И ЗАПУСК СЕРВЕРА КОНТРОЛЯ НА ОС WINDOWS 10

1.1. Установка сервера контроля

Установка сервера контроля на ОС WIndows 10 производится следующим образом:

1. Извлечь архив в папку, где планируется развернуть сервер.
2. Переместить файл лицензии license.dat в папку с сервером.
3. Установить PostgresSQL версии 15 или выше:
   - скачать установщик по ссылке https://www.enterprisedb.com/downloads/postgres-postgresql-downloads (Рисунок 1, Рисунок 2).

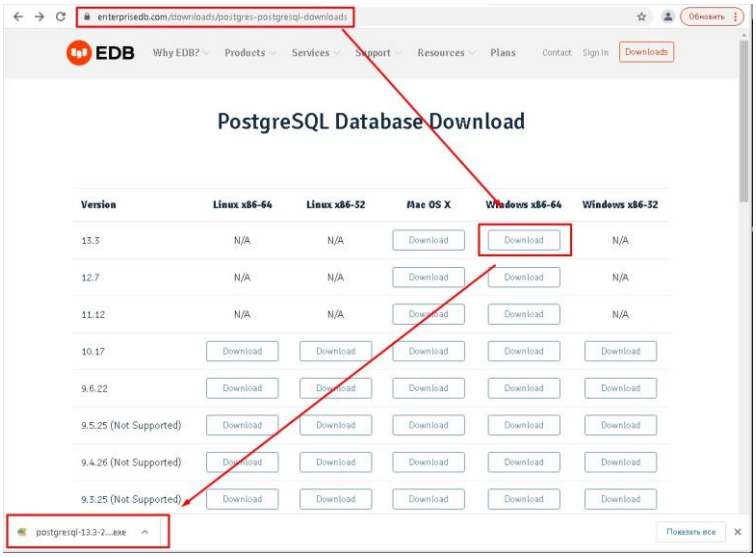

Рисунок 1 – Скачивание установщика PostgresSQL

Рисунок 2 – Запуск установщика PostgresSQL

- указать директорию для установки PostgresSQL (Рисунок 3).

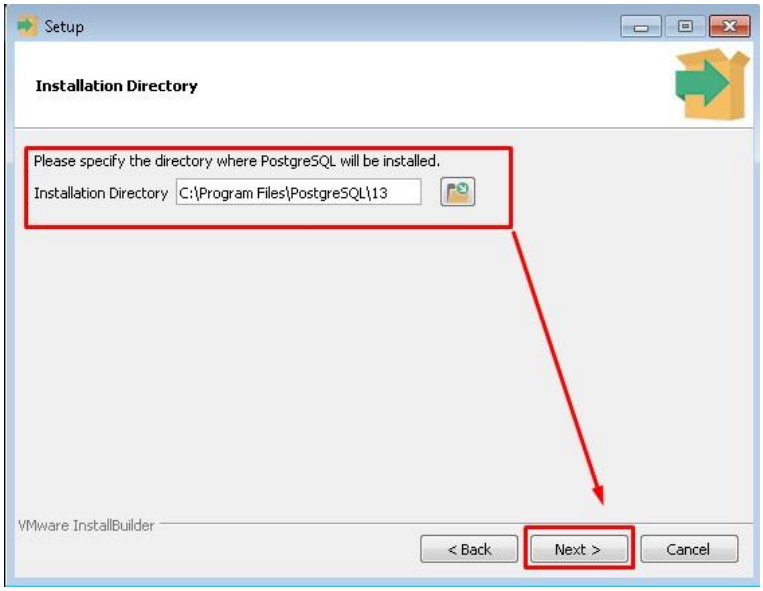

Рисунок 3 – Выбор директории для установки PostgresSQL

- выбрать необходимые компоненты (Рисунок 4).

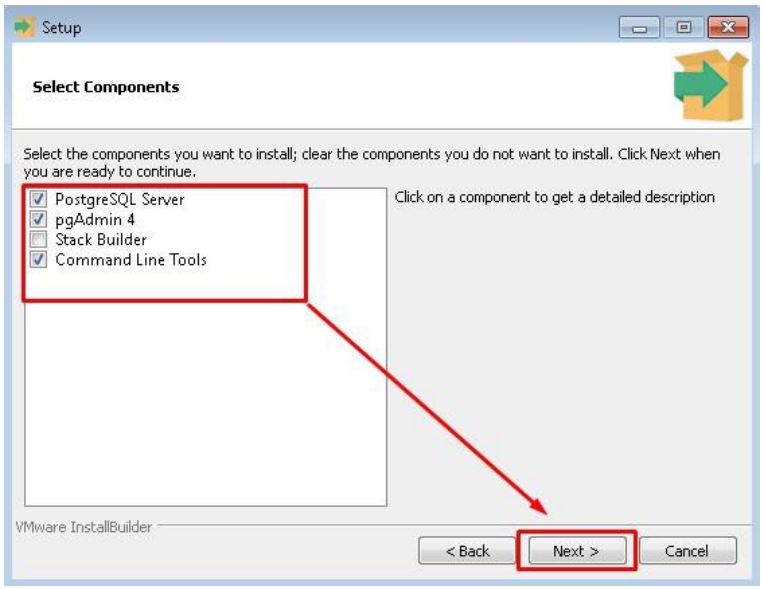

Рисунок 4 – Выбор необходимых для установки компонентов

- выбрать директорию для файлов (Рисунок 5).

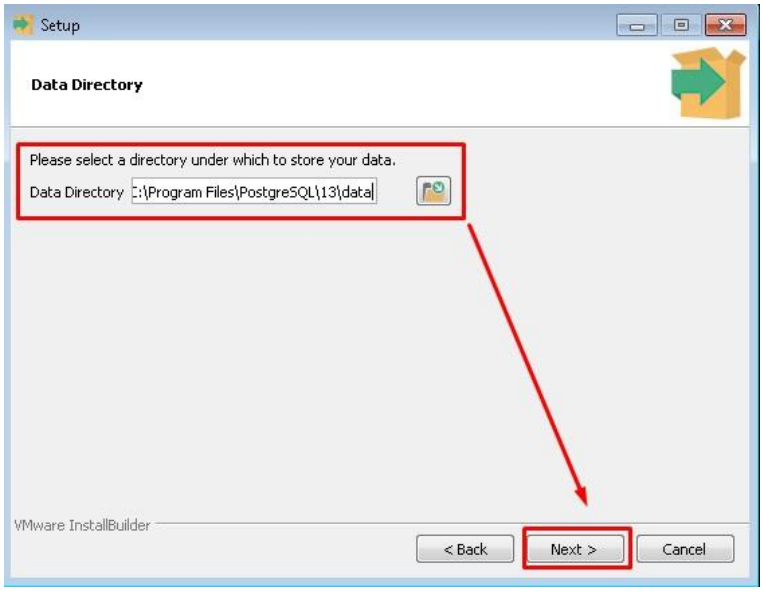

Рисунок 5 – Выбор директории для файлов PostgresSQL

- указать пароль (postgres) (Рисунок 6).

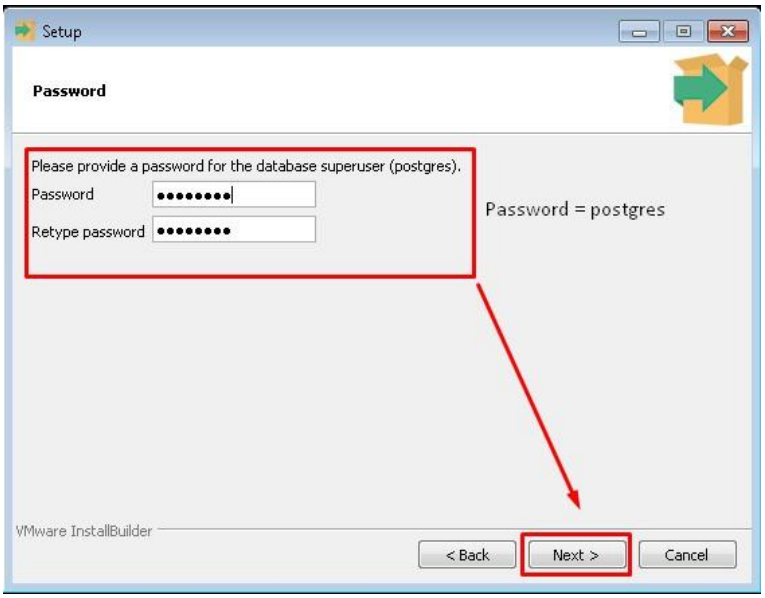

Рисунок 6 – Ввод пароля PostgresSQL

- указать порт (Рисунок 7).

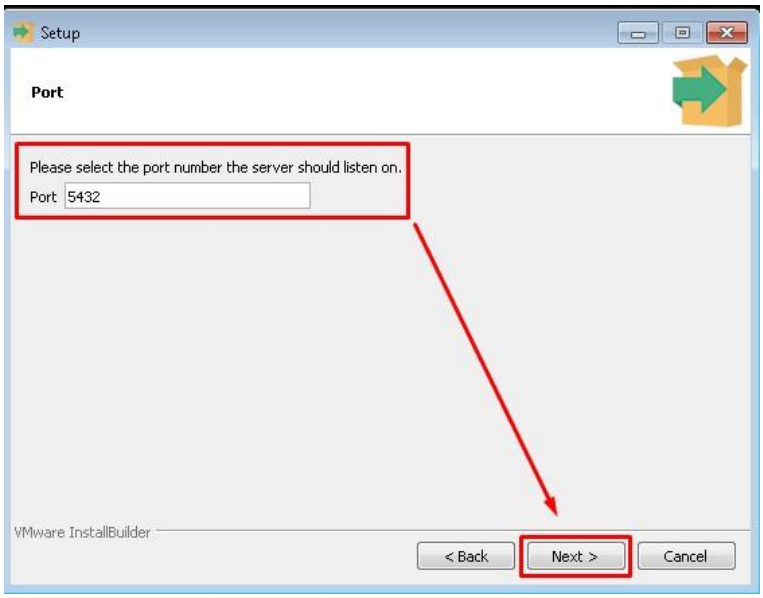

Рисунок 7 – Ввод порта PostgresSQL

- выбрать дополнительные опции (Рисунок 8).

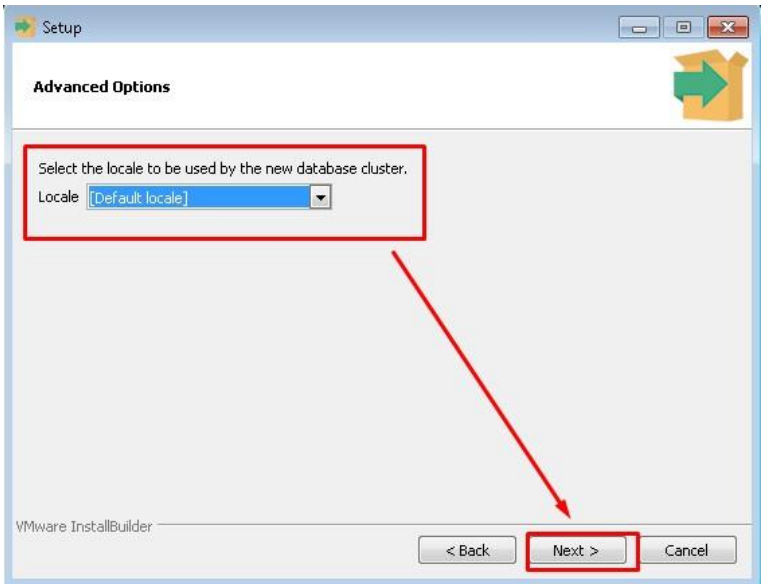

Рисунок 8 – Выбор дополнительных опций установки

- закончить установку с выбранными параметрами (Рисунок 9, Рисунок 10).

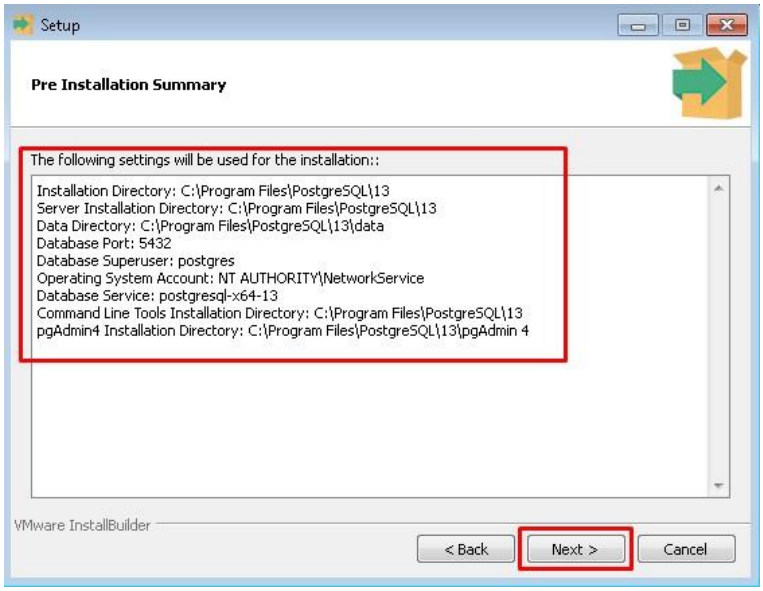

Рисунок 9 – Просмотр выбранных параметров установки

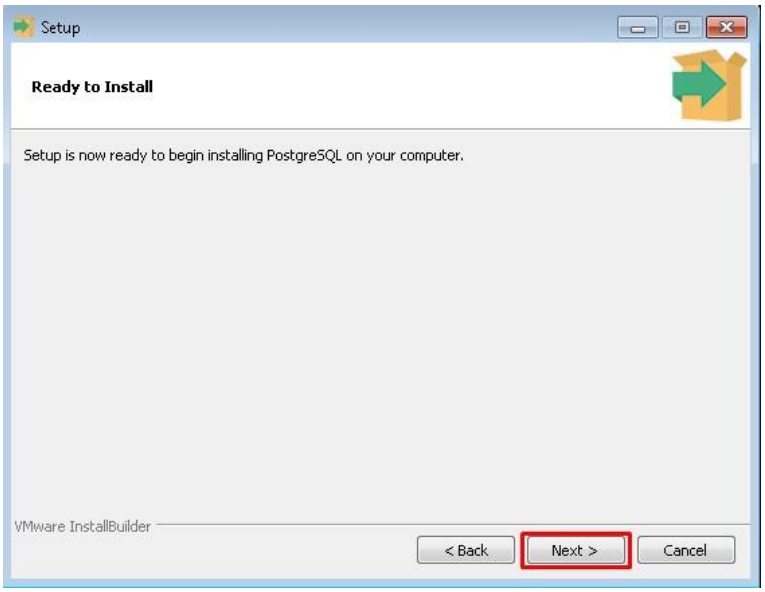

Рисунок 10 – Окончание установки PostgresSQL

1.2. Настройка сервера контроля

Настройки сервера контроля выполняется с помощью файла appsettings.json, который находится в папке с сервером.

Описание настроек сервера:

- HttpPort – Порт веб-сервера при использовании HTTP;
- Https - порт веб-сервера при использовании HTTPs;
- UseSSL – Использовать защищенное соединение (https);
- CertificatePath – Путь к .pfx сертификату;
- CertificatePassword – Пароль к файлу сертификата;
- DatabaseConnectionString – имя строки подключения. SQLite или Postgres. Резервирование работает только с Postgres;
- NormalizationOutputFolder – Имя подпапки для нормализованных файлов;
- Language – язык интерфейса;
- DarkMode – Тёмный режим;
- DateFormat – отображаемый формат даты;
- LDAPAuthEnabled – Разрешить аутентификацию LDAP;
- LDAPServer – Сервер для подключения к Active Directory. Используется для валидации доменных параметров доступа и для поиска пользователей при включенной LDAP аутентификации;

- LDAPDomain – Домен для подключения к Active Directory. Используется для поиска пользователей при включенной LDAP аутентификации;
- LDAPUserName – имя доменного пользователя для подключения к Active Directory ;
- LDAPUserPassword – пароль доменного пользователя для подключения к Active Directory;
- FileWatcher – Вотчер для файловой системы, который будет использован;
- LastWriteTimeWaitSeconds – минимальное время, которое должно пройти после записи файла до момента, когда он станет доступным для анализа;
- MaxAgeOfFilesWhenSourceRestart – файлы старше, чем указанное значение (в днях), не будут добавлены в очередь при перезагрузке источника или старте сервера контроля;
- NotProcessAlreadyProcessedFiles – не обрабатывать уже обработанные файлы повторно;
- MxfAtomWaitingByTimer – Выполнять сбор файлов MXF OP-Atom бандла по таймеру;
- MxfAtomProcessMissingMaterialStructure – Продолжить анализ MXF OP-Atom файлов с отсутствующей структурой материала;
- TimeoutDeclinedTask – Время (в миллисекундах), которое задача со статусом Declined будет висеть в списке необработанных файлов, до следующей отправки серверу анализа;
- RetryErrorJobsErrorCodes – Список кодов ошибок, при которых требуется отправка задачи на повторный анализ;
- MaxResultsInReport – Максимальное число результатов в сводном отчёте
- VideoDefinitions – список предустановленных разрешений видео;
- Containers – список поддерживаемых видеоконтейнеров;
- VideoCodecs – список поддерживаемых семейств видеокодеков, используется для выбора шаблона анализа файлов;
- VideoCodecsCommertialNames – список специфических версий видеокодеков, поддерживаемых для выбора шаблона анализа файлов;
- AudioCodecs – список поддерживаемых аудиокодеков, через пробел;
- Tests – тесты по категориям;
- UseSmpteDuration – использовать формат SMPTE Timecode при отображении длительности видео;
- Replication – настройки резервирования;
- ServerReplicationEnabled – Резервирование Сервера Контроля включено (true) или отключено (false);

- Port – Порт для синхронизации резервирования (для текущего узла);
- ServerNodes – Узлы резервирования Сервера Контроля в формате АДРЕС:ПОРТ, включая текущий узел. Порядок указания узлов соответствует приоритету при выборе основного узла (первый имеет высший приоритет);
- DatabaseReplicationEnabled – Резервирование БД включено (true) или отключено (false);
- DatabaseNodes – Узлы резервирования БД CocroachDB в формате ХОСТ:ПОРТ

1.3. Запуск сервера контроля в режиме консольного приложения

Запуск сервера контроля в режиме консольного приложения производится следующим образом:

1. Открыть консоль или PowerShell в режиме администратора.
2. Перейти в папку с сервером контроля.
3. Запустить сервер контроля командой “Orbox.exe”.

1.4. Запуск сервера контроля в режиме Windows Service

Запуск сервера контроля в режиме Windows Service производится следующим образом:

1. Открыть консоль или PowerShell в режиме администратора.
2. Перейти в папку с сервером контроля.
3. Запустить сервер контроля в режиме консольного приложения командой “Orbox.exe”, дождаться успешной миграции базы данных, после чего остановить сервер контроля (пункт обязателен для успешной миграции базы данных).
4. Установить сервис командой “Orbox.exe –i”.
5. Открыть список служб с помощью команды services.msc.
6. Запустить службу "ORBOX".

1.5. Обновление сервера контроля

Процедура обновления сервера контроля выполняется следующим образом:

1. Остановить сервер контроля:
   a. Если сервер запущен как консольное приложение, то необходимо нажать CTRL+C;

   b. Если сервер запущен как служба, то необходимо остановить службу "ORBOX".
2. Сделать резервную копию файлов из папки: C:\ProgramData\Orbox\.
3. Извлечь архив с новой версией сервера контроля.
4. Запустить сервер контроля:
   a. Если сервер был запущен как сервис, то перед запуском необходимо переустановить службу. Для этого нужно сначала удалить службу, запустив команду “Orbox.exe –u” с помощью PowerShell (из папки с сервером контроля), а затем установить службу, запустив команду “Orbox.exe –i” с помощью PowerShell (из папки с новым сервером контроля);
   b. Если требуется обновить базу данных, это нужно сделать до запуска сервера контроля.

1.6. Обновление базы данных

Обновление базы данных выполняется следующим образом:

1. Остановить сервер контроля:
   a. Если сервер запущён как консольное приложение, необходимо нажать CTRL+C и подтвердить остановку;
   b. Если сервер запущен как служба, необходимо остановить службу "ORBOX".
2. Установить новую версию сервера контроля.
3. Открыть консоль или PowerShell в режиме администратора.
4. Перейти в папку с сервером контроля.
5. Запустить сервер контроля с ключом –m или –migrate и номером версии базы данных, которая была установлена ранее:
   a. Номер версии базы данных совпадает с третьей цифрой в версии приложения. Например, если предыдущая установленная версия – 4.204.67.10, номер версии базы будет 67;
   b. Полностью команда запуска будет выглядеть так: Orbox.exe -migrate X или Orbox.exe -m X, где X – номер версии базы.
6. Произойдёт миграция базы до новой версии. По окончании появится сообщение об успешной миграции.
7. Далее сервер контроля может быть запущен в рабочем режиме (как консоль или служба).

1.7. Дополнительная информация

Логи сервера контроля (log.txt) находятся в папке: C:\ProgramData\Orbox\log\.

2. УСТАНОВКА, НАСТРОЙКА И ЗАПУСК СЕРВЕРА КОНТРОЛЯ НА ОС DEBIAN 11

2.1. Автоматическая установка и удаление сервера контроля

Установка сервера контроля производится следующим образом:

Примечание: Все команды, описанные ниже, должны выполняться из-под root пользователя или из-под пользователя с root привилегиями:

1. Установить PostgreSQL версии 15 или выше:

   Установить postgresql:

```
sudo apt update && sudo apt upgrade
sudo apt install postgresql-15
```

   Установить пароль для пользователя postgres:

```
sudo passwd postgres
```

   Перейти в консоль postgresql:

```
su - postgres
psql
```

   Создать параметры доступа для базы данных (они так же будут указаны в файле конфигурации appsettings.json):

```
ALTER USER user_name PASSWORD 'new_password';
exit
```

   Например, чтобы создать параметры, которые указаны в файле конфигурации сервера контроля по умолчанию:

```
ALTER USER postgres PASSWORD 'postgres';
exit
```

2. Скопировать на машину, где планируется установить сервер контроля, 2 файла orboxserver-x.xxx.xxx.xx-lic-deb11-amd64.deb и wkhtmltox_x.x.x.x-x.bullseye_amd64.deb
3. Из папки, где находится файлы, выполнить команды:

```
sudo apt install ./wkhtmltox_x.x.x.x-x.bullseye_amd64.deb
sudo apt install ./orboxserver-x.xxx.xxx.xx-lic-deb11-amd64.deb
```

4. Поместить файл лицензии license.dat в папку с сервером контроля: /opt/tecom/orbox-server.

5. Для удаления сервера контроля выполнить команду:

```
sudo apt purge orbox-server
```

2.2. Настройка сервера контроля

Перед первоначальной настройкой сервера контроля необходимо настроить работу с портами, т.к. по умолчанию в Linux-системах порты ниже 1024 требуют root привилегий. Есть три варианта настройки:

1. Работа с портами по умолчанию. Данный вариант никаких дополнительных пред-настроек не требует, сервер контроля будет работать на том порту, который был указан в файле конфигурации. Но в таком случае, для доступа к UI сервера контроля, необходимо дополнительно указывать порт в строке браузера (например, в случае работы на порту 8081, для доступа к UI необходимо будет использовать полную ссылку: https://111.111.111.111:8081).
2. Перенаправление портов с использованием nftables. В данном варианте используется пакет nftables для перенаправления портов. Сервер контроля будет работать на портах по умолчанию (8080 для http и 8081 для https), но в браузере UI сервера контроля будет доступен без дополнительного указания порта (Пример: https://111.111.111.111). Настройка производится следующим образом:
    - Проверить, был ли ранее на машину установлен пакет nftables. Если он в системе отсутствует, то необходимо установить его командой:

```
sudo apt-get –y install nftables
```

    - Перейти в папку с установленным сервером контроля. Скрипту setup-firewall.sh необходимо дать права на выполнение:

```
sudo chmod +x ./setup-firewall.sh
```

      После запустить его командой:

```
sudo ./setup-firewall.sh
```

      Выбрать 3 вариант для предварительной очистки настроек портов.
    - Повторно запустить скрипт setup-firewall.sh , ввести цифру 1 и нажать Enter. После можно производить дальнейшую настройку сервера контроля (порты необходимо оставить по умолчанию: 8080 и 8081 для http и https соответственно).

3. Отмена требования root привилегий для портов 80 и выше. В данном варианте будут ограничены порты ниже 80. Сервер контроля будет работать на портах 80 и 443 для http и https соответственно, в браузере UI сервера контроля будет также доступен без дополнительного указания порта (https://111.111.111.111). Настройка производится следующим образом:
    - Перейти в папку с установленным сервером контроля. Скрипту setup-firewall.sh необходимо дать права на выполнение:

```
sudo chmod +x ./setup-firewall.sh
```

После запустить его командой:

```
sudo ./setup-firewall.sh
```

Выбрать 3 вариант для предварительной очистки настроек портов.

- Проверить, был ли ранее на машину установлен пакет nftables. Если он присутствует в системе, то необходимо его вначале остановить:

```
sudo systemctl stop nftables
```

Затем удалить командой:

```
sudo apt-get --purge remove nftables
```

- Повторно запустить скрипт setup-firewall.sh , ввести цифру 2 и нажать Enter. После этого можно производить дальнейшую настройку сервера контроля. Порты по умолчанию будут заменены скриптом на 80 и 443 для http и https соответственно.

Примечание: в случае переключения между вариантами настроек портов, необходимо до переключения запускать скрипт setup-firewall.sh и выбрать 3 вариант для очистки предыдущих настроек. В случае если скрипт не удаляет настройки до конца (например, останавливается после строчки, сообщающей о том, что конфигурационный файл nftables не был найден), необходимо открыть на редактирование скрипт setup-firewall.sh :

```
sudo nano setup-firewall.sh
```

и закомментировать (#) строчку “set –e” в начале скрипта, после чего повторить процедуру очистки настроек.

Дальнейшая настройка сервера контроля производится следующим образом:

Конфигурационный файл с настройками сервера контроля находится в директории: /opt/tecom/orbox-server/appsettings.json.

Настройки сервера контроля в файле appsettings.json при установке на ОС Debian 11 идентичны настройкам при установке на ОС Windows 10.

Сервер контроля может быть запущен как консольное приложение и как сервис.

Для того чтобы открыть UI СК в браузере, используя порт по умолчанию (80 для http или 443 для https), достаточно ввести IP адрес без указания порта. В случае если используется порт, отличный от порта по умолчанию, необходимо ввести IP адрес СК в следующем формате: xxx.xxx.xxx.xxx:pppp (где pppp это номер порта).

2.3. Запуск сервера контроля в режиме консольного приложения

Запуск сервера контроля в режиме консольного приложения производится следующим образом:

1. Перейти в директорию, где находится исполняемый файл:

```
cd /opt/tecom/orbox-server
```

2. Запустить сервер контроля с помощью команды:

```
./run.sh
```

2.4. Запуск сервера контроля в режиме сервиса

1. Выполнить команду:

```
sudo systemctl daemon-reload
```

2. Добавить сервис сервера контроля в автозапуск:

```
sudo systemctl enable orbox-server.service
```

3. Запустить сервис сервера контроля с помощью команды:

```
sudo systemctl start orbox-server.service
```

2.5. Обновление сервера контроля

Обновление сервера контроля производится следующим образом:

1. Остановить сервер контроля:
   a. Если сервер запущен как консольное приложение, то необходимо нажать CTRL+C;

b. Если сервер запущен как сервис, то необходимо выполнить команду:

```
sudo systemctl stop orbox-server.service
```

2. Скопировать на машину файл:

   orboxserver-x.xxx.xxx.xx-lic-deb11-amd64.deb

3. Для обновления сервера контроля запустить команду:

```
sudo apt install ./orboxserver-x.xxx.xxx.xx-lic-deb11-amd64.deb
```

4. Выполнить команду:

```
sudo systemctl daemon-reload
```

5. Выполнить повторную настройку сервера контроля в файле:
   /opt/tecom/orbox-server/appsettings.json

6. Запустить сервер контроля в штатном режиме.

2.6. Дополнительная информация

Логи сервера контроля (log.txt) находятся в папке: /home/*user*/.config/orbox-server/log/ где *user* это имя пользователя, из-под которого запускался сервер контроля (по умолчанию при запуске сервера контроля в режиме сервиса это orboxserver).

3. УСТАНОВКА, НАСТРОЙКА И ЗАПУСК СЕРВЕРА АНАЛИЗА НА ОС DEBIAN 11

3.1. Автоматическая установка и удаление сервера анализа

Установка сервера анализа производится следующим образом:

Примечание: Все команды, описанные ниже, должны выполняться из-под root пользователя или из-под пользователя с root привилегиями:

1. Скопировать на машину, где планируется установить сервер анализа 2 файла:

   orbox-analyzer-x.xx.xxx.deb

   install-orbox-analyzer-debian.sh

2. Установить для скрипта install-orbox-analyzer-debian.sh права на выполнение:

```
sudo chmod +x ./install-orbox-analyzer-debian.sh
```

3. Для установки анализатора выполнить команду:

```
sudo ./install-orbox-analyzer-debian.sh
```

Для удаления анализатора выполнить команду:

```
sudo apt purge orbox-analyzer
```

3.2. Настройка сервера анализа

Конфиг-файл сервера анализа находятся в директории: /home/orbox/.config/orbox/conf . Скрипт, с помощью которого рекомендуется редактировать конфиг-файл находится в директории: /opt/tecom/orbox-analyzer/bin/ .

Сервер анализа может быть запущен как консольное приложение или как сервис.

Если сервер анализа необходимо запустить как консольное приложение, настройки нужно править для того пользователя, из-под которого планируется запускать приложение. Сервер анализа рекомендуется запускать только из-под пользователя orbox.

При запуске сервера анализа в режиме сервиса будут использованы настройки пользователя orbox, поэтому нужно править настройки от имени этого пользователя.

Настройка сервера анализа от имени пользователя orbox может быть осуществлена с помощью команды:

```
sudo su –l orbox
cd /opt/tecom/orbox-analyzer/bin
./run-analyzer.sh --config-analyzer
```

Настройка журналирования для пользователя orbox выполняется с помощью команды:

```
sudo su –l orbox
cd /opt/tecom/orbox-analyzer/bin
./run-analyzer.sh --config-log
```

Обновление конфигов, ресурсов и редактирование настроек для текущего пользователя выполняется с помощью команд:

Обновление конфигов:

```
cd /opt/tecom/orbox-analyzer/bin
./run-analyzer.sh --config-update
```

Обновление ресурсов:

```
cd /opt/tecom/orbox-analyzer/bin
./run-analyzer.sh --resource-update
```

Редактирование настроек:

```
cd /opt/tecom/orbox-analyzer/bin
./run-analyzer.sh --config-analyzer
```

Настройка журналирования выполняется с помощью команды:

```
cd /opt/tecom/orbox-analyzer/bin
./run-analyzer.sh --config-log
```

Описание настроек сервера анализа:

- ControlServerAddress1 – IP адрес основного сервера контроля;
- ControlServerPort1 – порт для коммуникации с основным сервером контроля;
- ControlServerCertificatePath1 – путь до SSL сертификата основного сервера контроля;
- ControlServerCertificateEcdh1 – опциональный параметр, определяющий тип эллиптической кривой в случае использования соответствующего SSL сертификата для основного сервера контроля;
- ControlServerAddress2 – IP адрес резервного сервера контроля. Если использование резервного сервера контроля не планируется, то эту настройку необходимо удалить или указать в ней IP адрес основного сервера контроля;
- ControlServerPort2 – порт для коммуникации с резервным сервером контроля. Если использование резервного сервера контроля не планируется, то эту настройку необходимо удалить или указать в ней порт основного сервера контроля;
- ControlServerCertificateEcdh2 – опциональный параметр, определяющий тип эллиптической кривой в случае использования соответствующего SSL сертификата для резервного сервера контроля;
- ControlServerCertificatePath2 – путь до SSL сертификата резервного сервера контроля;
- UseHTTPS – использовать (true) или нет (false) HTTPs для взаимодействия СА и СК;
- AnalyzerServerInterface – сетевой интерфейс для коммуникации с сервером контроля;
- CountEmptyResponceToFlush - количество пустых ответов от СК для очистки внутренних буферов;
- ThreadsCount – размер пулла потоков создаваемых модулей;
- NormalizationNumThreads – кол-во потоков, которое будет использовать для нормализации аудио;
- ColorComponentsLevelTesNumThreads – кол-во потоков, которое будет использоваться в тесте «Уровень цветовых компонент»;
- VectorscopeTestNumThreads – кол-во потоков, которое будет использоваться в тесте «Уровень насыщенности»;
- BlackWhiteLevelAssesstmentTestNumThreads – кол-во потоков, которое будет использоваться в тесте «Уровень черного и белого»;

- InterlacementDetectionTestNumThreads – кол-во потоков, которое будет использоваться в тестах «Гребёнка» и «Тип развёртки»;
- VideoDecThreadCount – кол-во потоков, которое будет использоваться в процессе декодирования кадров;
- VideoDecThreadTypeMap – метод декодирования, который будет использоваться (slice или frame). Можно задать индивидуально для каждого кодека;
- FrameBufferMaxSize – максимальное кол-во кадров в очереди;
- ParseSpeed – параметр, регулирующий скорость чтения метаданных и их детализацию (чем меньше, тем быстрее считываются метаданные, но с меньшей детализацией);
- CompressionTestNumThreads – кол-во потоков, которое будет использоваться в тесте «Артефакты сжатия»;
- CompressionBlockingTest_BatchSize – кол-во кадров, которые будут обрабатываться параллельно в тесте «Артефакты сжатия»;
- ArtifactsTestUseYUVcomponentCheck – включение/выключение проверки YUV компоненты в тесте на артефакты потери данных;
- DataLossArtifactsTest_BatchSize – кол-во кадров, которые будут обрабатываться параллельно в тесте «Артефакты потери данных»;
- DataLossMacroblockTestNumThread – количество потоков, которые будут использоваться в тесте «Артефакты потери данных в макроблоках»;
- DataLossMacroblockTest_BatchSize – кол-во кадров, которые будут обрабатываться параллельно в тесте «Артефакты потери данных в макроблоках»;

Параметры теста «Калибровочные таблицы»:

- TestCardTestNumTreads – количество потоков, которые будут использоваться в тесте «Калибровочные таблицы»;
- TestCardResizeImageWidth – ширина, до которой будет сжат кадр перед обработкой;
- TestCardResizeImageHeight – высота, до которой будет сжат кадр перед обработкой;
- TestCardImageSimilarityPercent – минимальный процент «схожести» между анализируемым кадром и шаблоном таблицы, для того чтобы принять решение о том, что задетектирована калибровочная таблица;
- TestCardImageDilatingSize – специфический параметр, используемый в алгоритме;

- UseTestCardFastMode - включение/выключение быстрого режима в тесте «Калибровочные таблицы»;
- TestCardTest_BatchSize – кол-во кадров, которые будут обрабатываться параллельно в тесте «Калибровочные таблицы»;

Параметры теста «Микропланы»:

- ShotTransitionHistogrammDiffThreshold – параметр, устанавливающий допустимую разницу гистограммы между кадрами в тесте «Микропланы»;
- ShotTransitionMinimalSequenceLength – минимальная длина последовательности кадров, которая признана содержащей некорректные результаты. В дальнейшем эти результаты будут удалены из итоговой последовательности;
- ShotTransitionSobelMetricThreshold – специфический параметр, используемый в алгоритме, чем выше значение, тем больше допускается разность кадров;
- ShotTransitionMssimDiffThresholdValue – специфический параметр, используемый в алгоритме, чем выше значение, тем больше допускается разность кадров;

Параметры теста «Цветные кадры»:

- ColorFramesResizeImageWidth – ширина, до которой будет сжат кадр перед обработкой;
- ColorFramesResizeImageHeight – высота, до которой будет сжат кадр перед обработкой;
- ColorFramesPossiblePixelsInaccuracy – допустимая неточность при сравнении пикселей. То есть, если значения соответствующих компонент двух пикселей отличаются на значение, меньшее данного параметра, то пиксели считаются одинаковыми;
- PossibleDifferentColorsInFrame – допустимое количество различных цветов в кадре;
- PercentOfDominantColor – процент доминирующего цветка в кадре;
- ColorFramesTestNumThreads – количество потоков, которое будет использоваться в тесте «Цветные кадры»;

Параметры теста «Тестовый сигнал»:

- AudioTestSignalTestCalcWindowShift – сдвиг окна, в процентах;
- AudioTestSignalTestPercentOfMagnitude – процент мощности сигнала 1000 Гц, для того чтобы считать звук в анализируемом окне тестовым сигналом.

Параметры теста «Gamut-ошибки»:

- GamutErrorsTest_NumThreads – кол-во потоков;
- GamutErrorsTest_Batchsize – кол-во кадров, которые будут обрабатываться параллельно;
- GamutErrorsTest_8bit_PrefferredMin – предпочитаемое минимальное значение для 8-битного файла (в соответствии с EBU R 103 v3);
- GamutErrorsTest_8bit_PrefferredMax - предпочитаемое максимальное значение для 8-битного файла (в соответствии с EBU R 103 v3);
- GamutErrorsTest_10bit_PrefferredMin - предпочитаемое минимальное значение для 10-битного файла (в соответствии с EBU R 103 v3);
- GamutErrorsTest_10bit_PrefferredMax - предпочитаемое максимальное значение для 10-битного файла (в соответствии с EBU R 103 v3);
- GamutErrorsTest_12bit_PrefferredMin - предпочитаемое минимальное значение для 12-битного файла (в соответствии с EBU R 103 v3);
- GamutErrorsTest_12bit_PrefferredMax - предпочитаемое максимальное значение для 12-битного файла (в соответствии с EBU R 103 v3);
- GamutErrorsTest_16bit_PrefferredMin - предпочитаемое минимальное значение для 16-битного файла (в соответствии с EBU R 103 v3);
- GamutErrorsTest_16bit_PrefferredMax - предпочитаемое максимальное значение для 16-битного файла (в соответствии с EBU R 103 v3);
- GamutErrorsTest_Dev_Mode_enabled – Режим разработчика. Вы можете включить этот флаг для рендеринга неудачных кадров в отдельные изображения. Также для каждого кадра файла будет напечатана информация о количестве битых пикселей;
- GamutErrorsTest_Temp_folder – Папка, куда будут сохранены изображения;

Параметры теста «Детектирование шума»:

- NoiseDetectionTest_NumThreads – кол-во потоков;
- NoiseDetectionTest_BatchSize – кол-во кадров, которые будут обрабатываться параллельно;
- NoiseDetectionTest_BlockSize – размер блока;
- NoiseDetectionTest_NoiseThreshold – пороговое значение шума;

Очередь сегментов Hls:

- HlsSegmentsQueue_MaxBufferSizeMb – размер буфера очереди Hls сегментов;
- HlsSegmentsQueue_MaxOutBlockSizeKb – максимальный размер блока на выходе;

Ограничения памяти:

- MemLimitAlarmLevelPercent – порог использования памяти для отключения параллелизма, где 0 – никогда не отключать;
- MemLimitCriticalLevelPercent – порог использования памяти до аварийного завершения анализа, где 0 – никогда не завершать аварийно;

- AllowQsvDecoding – использовать QSV декодер если есть такая возможность. Всегда отключено для HDR файлов;

Параметры теста «Интегральная метрика качества»:

- PictureQualityScore_DevModeEnabled – включения режима разработчика;
- PictureQualityScore_TestsWeights – веса зависимых тестов для расчета качества;

Параметры теста «Корректность заголовка»:

- TitleCorrectnessTest_Regex - регулярное выражение для проверки заголовка в тесте «Корректность заголовка»;

Параметры теста «Несоответствие стерео/моно сигнала»:

- MonoStereoTest_WindowSizeMsec – размер окна для поиска дефектов;
- MonoStereoTest_WindowShiftPercent – значение сдвига для перемещения по окну;
- MonoStereoTest_PercentMonoSamplesInWindow - если процент моно-сэмплов в окне равен или больше этого значения, окно является моно;

- ProcMountsPath – путь к /proc/mounts;

Описание настроек журналирования:

- logging.loggers.root.channel – название класса для журналирования;

- logging.loggers.root.level – уровень журналирования (trace, debug, notice, information, warning, error, critical, fatal);
- logging.formatters.f1.class – класс для форматирования;
- logging.formatters.f1.pattern – шаблон вывода сообщений в логах;
- logging.formatters.f1.times – время, которое будет использоваться в логах;
- logging.channels.c1.class – класс для вывода в консоль;
- logging.channels.c1.formatter – указывает на использование класса f1 для форматирования;
- logging.channels.c2.class – класс для вывода в файл;
- logging.channels.c2.path – путь к файлу логов;
- logging.channels.c2.formatter – указывает на использование класса f1 для форматирования;
- logging.channels.c2.rotation – максимальный размер файла;
- logging.channels.c2.archive – имя архива;
- logging.channels.c2.compress – использовать сжатие;
- logging.channels.c2.purgeCount – максимальное число заархивированных файлов;
- logging.channels.splitter.class – класс для режима вывода;
- logging.channels.splitter.channels – режим вывода логов (c1 – вывод в консоль, c2 – вывод в файл).

3.3. Запуск сервера анализа в режиме консольного приложения

Запуск сервера анализа в режиме консольного приложения производится следующим образом:

1. Перейти в директорию, где находится исполняемый файл:

```
cd /opt/tecom/orbox-analyzer/bin
```

2. Запустить сервер анализа с помощью команды:

```
sudo ./run-analyzer.sh --run
```

3.4. Запуск сервера анализа в режиме сервиса

При запуске сервера анализа в режиме сервиса используются настройки сервера анализа, которые были сделаны из-под пользователя orbox. Необходимо убедиться, что настройки сделаны именно из-под этого пользователя.

1. Выполнить команду:

```
sudo systemctl daemon-reload
```

2. Добавить сервис сервера анализа в автозапуск:

```
sudo systemctl enable orbox-analyzer.service
```

3. Запустить сервис сервера анализа с помощью команды:

```
sudo systemctl start orbox-analyzer.service
```

3.5. Обновление сервера анализа

Обновление сервера анализа производится следующим образом:

1. Остановить сервер анализа:
   a. Если сервер запущен как консольное приложение, то необходимо нажать CTRL+C;
   b. Если сервер запущен как сервис, то необходимо выполнить команду:

```
sudo systemctl stop orbox-analyzer.service
```

2. Скопировать на машину 2 файла:
   orbox-analyzer-x.xx.xxx.deb
   install-orbox-analyzer-debian.sh
3. Установить для скрипта права на выполнение install-orbox-analyzer-debian.sh

```
sudo chmod +x ./install-orbox-analyzer-debian.sh
```

4. Для обновления анализатора запустить скрипт установки:

```
sudo ./install-orbox-analyzer-debian.sh
```

5. Выполнить команду:

```
sudo systemctl daemon-reload
```

6. Выполнить обновление конфигов, ресурсов и повторную настройку для текущего пользователя, выполнив команды:
   Обновление конфигов:

```
cd /opt/tecom/orbox-analyzer/bin
```

```
./run-analyzer.sh --config-update
```

Обновление ресурсов:

```
cd /opt/tecom/orbox-analyzer/bin
./run-analyzer.sh --resource-update
```

Редактирование настроек:

```
cd /opt/tecom/orbox-analyzer/bin
./run-analyzer.sh --config-analyzer
```

Выполнить настройку для пользователя orbox, выполнив команду:

```
./run-analyzer.sh --user orbox --config-analyzer
```

7. Запустить сервер анализа в штатном режиме.

3.6. Настройка локализации

Важно: Изменение локали действует до выхода пользователя из сеанса.

3.6.1. Проверка текущей локализации

Для того чтобы проверить текущую локализацию нужно выполнить команду **locale**.

```
LANG=ru_RU.UTF-8
LANGUAGE=
LC_CTYPE="ru_RU.UTF-8"
LC_NUMERIC="ru_RU.UTF-8"
LC_TIME="ru_RU.UTF-8"
LC_COLLATE="ru_RU.UTF-8"
LC_MONETARY="ru_RU.UTF-8"
LC_MESSAGES="ru_RU.UTF-8"
LC_PAPER="ru_RU.UTF-8"
LC_NAME="ru_RU.UTF-8"
LC_ADDRESS="ru_RU.UTF-8"
LC_TELEPHONE="ru_RU.UTF-8"
LC_MEASUREMENT="ru_RU.UTF-8"
LC_IDENTIFICATION="ru_RU.UTF-8"
LC_ALL=
```

В данном случае видно, что установлена русская локаль (значение переменной LANG установлено в ru_RU.UTF-8). В случае английской локали должно быть установлено значение en_US.utf8.

3.6.2. Установленные в системе локали (доступные для выбора)

Посмотреть установленные в системе локали можно с помощью команды **locale –a:**

```
C
C.UTF-8
en_US.utf8
POSIX
ru_RU.utf8
```

Данный вывод означает, что в системе доступны и русская и английская локали. Если необходимая локаль отсутствует в списке, ее нужно установить согласно разделу "Установка новой локали в систему".

3.6.3. Установка новой локали в систему

Если в результате выполнения команды locale -a, нужная локаль отсутствует в списке, ее нужно установить:

1. Открыть файл /etc/locale.gen с правами root:

```
sudo nano /etc/locale.gen
```

В файле можно увидеть список доступных для установки локалей:

```
# This file lists locales that you wish to have built. You can find
a list
# of valid supported locales at /usr/share/i18n/SUPPORTED, and you
can add
# user defined locales to /usr/local/share/i18n/SUPPORTED. If you
change
# this file, you need to rerun locale-gen.

# aa_DJ ISO-8859-1
# aa_DJ.UTF-8 UTF-8
```

```
# aa_ER UTF-8
# aa_ER@saaho UTF-8
# aa_ET UTF-8
# af_ZA ISO-8859-1
# af_ZA.UTF-8 UTF-8
# ak_GH UTF-8
# am_ET UTF-8
# an_ES ISO-8859-15
# an_ES.UTF-8 UTF-8
# anp_IN UTF-8
...
```

2. Раскомментировать нужную локаль, убрав # в начале строки.
3. Выполнить команду:

```
sudo locale-gen
```

4. Выполнить команду:

```
sudo update-locale
```

После выполнения данных шагов должна стать доступной новая локаль. Проверка доступности производится выполнением команды:

```
locale -a)
```

3.6.4. Выбор локали из списка установленных в системе

Для того чтобы применить одну из установленных в системе локалей нужно выполнить следующую команду:

```
export LANG="ru_RU.utf8"
```

В данном случае выбирается русская локаль. Для выбора английской локали переменной "LANG" нужно присвоить значение "en_US.utf8".

Если язык не установился, необходимо установить приоритет локали согласно разделу "Установка приоритета локали".

3.6.5. Установка приоритета локали

Проверить приоритет локали можно через переменную "LANGUAGE".

Пример: если необходимо чтобы русская локаль была в приоритете, установить значение переменной в "ru_RU:en_US:en".

```
export LANGUAGE="ru_RU:en_US:en"
```

4. УСТАНОВКА И НАСТРОЙКА СЕРВЕРА АНАЛИЗА ИЗ FLATPACK ПАКЕТА

Важно:

- В настоящий момент поддерживается установка flatpack пакета на операционные системы Debian 11, Ubuntu 20.04, CentOS7 и AltLinux.
- Все команды, описанные ниже, должны выполняться из-под root пользователя или из-под пользователя с root привилегиями.
- Перед установкой сервера анализа из flatpack пакета требуется проверить директории с файлами конфигурации (/home/orbox/.config/orbox/conf) и, если они есть, то их нужно удалить, в противном случае файлы конфигурации не будут созданы.

Процесс установки и настройки выглядит следующим образом:

1. Скопируйте на машину, где планируется установить сервер анализа 3 файла:

   install-orbox-flatpak.sh

   org.tecom.orbox.flatpak

   flatpakLibs.tar.gz

2. Установите для скрипта права на выполнение install-orbox-flatpak.sh.:

```
sudo chmod +x ./ install-orbox-flatpak.sh
```

3. Для установки анализатора выполните команду:

```
sudo ./install-orbox-flatpak.sh
```

4. После установки скрипт выведет следующую подсказку о дальнейших действиях для настройки сервера анализа:

```
sudo su -l orbox
flatpak run org.tecom.Orbox --tui-configurator
sudo su -l user
Then enable autostart:
sudo systemctl enable orbox-analyzer-flatpak.service
Then start service:
```

```
sudo systemctl start orbox-analyzer-flatpak.service
```

Необходимо выполнить эти действия последовательно. Ниже представлено более подробное описание выполняемых действий.

- Открытие сессии пользователя orbox:

```
sudo su -l orbox
```

- Запуск графического конфигуратора сервера анализа. Открыв графический конфигуратор, необходимо выполнить настройки подключения к серверу контроля:

```
flatpak run org.tecom.Orbox --tui-configurator
```

Запуск конфигуратора можно заменить командами, которые откроют текстовый файл для редактирования:

```
flatpak run org.tecom.Orbox --config-analyzer
flatpak run org.tecom.Orbox --config-log
```

Подробная информация о настройке сервера анализа представлена в разделе "Настройка сервера анализа".

- Открытие сессии пользователя user:

```
sudo su –l user
```

- Включение автозапуска сервиса сервера анализа:

```
sudo systemctl enable orbox-analyzer-flatpak.service
```

- Запуск сервера анализа:

```
sudo systemctl start orbox-analyzer-flatpak.service
```

5. НАСТРОЙКА СЕРВЕРА АНАЛИЗА И СЕРВЕРА КОНТРОЛЯ ДЛЯ РАБОТЫ НА ОДНОЙ МАШИНЕ

В случае установки системы сервера анализа и сервера контроля на одной и той же машине, шаги по установке не будут отличаться от приведенных выше, актуальных для установки на двух

разных debian машинах. Необходимо дополнительно выполнить следующие шаги после основной установки:

1. Открыть на редактирование файлы любым редактором /etc/systemd/system/orbox-server.service и /etc/systemd/system/orbox-analyzer.service и раскомментировать строку "Slice=" убрав “#” перед строкой:

```
sudo nano /etc/systemd/system/orbox-server.service
sudo nano /etc/systemd/system/orbox-analyzer.service
```

2. В конфиг-файле сервера анализа изменить значение параметра MemLimitInMB с 1024 на 6144:

```
sudo su –l orbox
cd /opt/tecom/orbox-analyzer/bin
./run-analyzer.sh –config-analyzer
```

3. Выполнить команды:

```
systemctl daemon-reload
systemctl restart orbox-server.service
systemctl restart orbox-analyzer.service
```

6. ВОЗМОЖНЫЕ ПРОБЛЕМЫ

1. *После установки системы Анализатор и СК не видят друг друга.*

   Если в логах анализатора мы видим проблему про SSL сертификат, то не факт, что проблема именно в нем:

   ```
   CommunicationModule[#3]          2018-07-05          13:54:32.816
   CommunicationModule: [Error] HTTP Timeout connection error
   CommunicationModule[#3]          2018-07-05          13:54:32.816
   CommunicationModule: [Error] SSL exception. Error msg: No
   certificate available
   CommunicationModule[#3]          2018-07-05          13:54:32.816
   CommunicationModule: [Error] Unable to establish connection with
   control server
   ```

   Необходимо проверить настройки Firewall. Если он включен, то это может являться проблемой. Если целиком его отключить нельзя, то необходимо добавить исключающие правила для портов 3110 и 8715.

Также может помочь перезагрузка сервера контроля.

В случае если в интерфейсе СК появляется подключенные СА, но не обновляет свой “heartbeat”, при этом постоянно меняя статус с «Подключен» на «Потерян» и обратно, значит проблема, вероятно, в SSL сертификате. Необходимо проверить что до него правильно указан путь в конфиге СА, а так же что у пользователя, из-под которого запущен СА, есть права на доступ к этой папке, в которой лежит сертификат.

2. *Проблема с падением анализатора при первом подключении источника.*

   Необходимо проверить файл /etc/hosts. Он должен иметь следующий вид:

```
127.0.0.1       localhost
127.0.1.1       orbox-analyzer
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

   где вместо orbox-analyzer должно быть написано имя вашего хоста. Имя хоста можно узнать, выполнив команду uname -n или hostname.

3. *Невозможно подключиться к расшареной папке на Linux из-под Windows 10.*

   В редакторе реестра необходимо изменить значение: HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters\AllowInsecureGuestAuth (DWORD) с 0 на 1 и перезагрузить машину.

4. *Сервер контроля не подключает сетевую папку, хотя она подключена в проводнике.*

   Такое часто происходит, если через проводник сетевая папка была подключена с другими данными аутентификации; для исправления можно попробовать выполнить команду:

```
net use \\192.168.12.12\IPC$ /delete
```

   где 192.168.12.12 – IP адрес вашей сетевой папки. Так же можно попробовать удалить данные аутентификации через windows vault.

5. *Ошибка монтирования при анализе файла.*

   Если анализ файла завершился с ошибкой вида:

   "Mount error message: Failed to mount Windows share: Invalid argument" или иной ошибкой монтирования, необходимо сделать следующее:

   - Перезапустить службу «Сервер»;

- Перезапустить сервер контроля;
- Перезапустить сервер анализа.

6. *Ошибка при запуске Сервера Контроля, при выборе Postgres базы данных.*

Если в результате запуска вы видите ошибку типа:

"no pg_hba.conf entry for host", необходимо сделать следующее:

- Открыть папку, куда был установлен Postgres (C:\Program Files\PostgreSQL\12(\);
- Найти файл pg_hba.conf и отредактировать его;
- Добавить в него строку:

host all postgres 192.168.13.218/32 md5

где:

– postgres – DB name

– 192.168.13.218/32 – IP машины, на которой установлен Postgres.