УТВЕРЖДЕН
НПЕШ.60010-03 99-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «KOMRAD ENTERPRISE SIEM»

Руководство администратора

НПЕШ.60010-03 99

Листов 146

2021

Литера «___»

АННОТАЦИЯ

Настоящий документ является собственностью АО "НПО Эшелон" (далее — НПО Эшелон) и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения НПО Эшелон. Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям. НПО Эшелон не аффилировано с такими правообладателями и не производит продукцию, маркированную такими знаками.

В документе содержатся сведения о назначении изделия «Программный комплекс «KOMRAD Enterprise SIEM» НПЕШ.60010-03 (далее — ПК «КОМРАД», изделие, комплекс, система), его архитектуре, условиях применения, последовательности действий администратора, обеспечивающих установку, запуск, конфигурирование, выполнение и завершение программы.

Руководство адресовано специалистам, ответственным за развертывание и системное администрирование средств защиты информации.

Действия по приемке поставленного изделия осуществляются в соответствии с ТУ.

В настоящем руководстве приняты обозначения, указанные в таблице 1.

Таблица 1 – Перечень обозначений принятых в настоящем руководстве

Обозначение	Описание
Совет! Пример: **Совет!** Запустить программу можно командой	Содержит информацию, которая может быть полезна при администрировании ПК «КОМРАД»
Внимание! Пример: **Внимание!** Запустить программу можно командой	Содержит информацию о действиях и событиях, которые необходимо выполнить или могут привести к нежелательным последствиям
Жирный шрифт Пример: Откройте **Панель управления → Службы**	Название элементов интерфейса операционных систем и программ выделено полужирным шрифтом

Обозначение	Описание
Жирный курсив Пример: Откройте файл: ***C:\ProgramFiles\PostgreSQL\12\data\postgresql.conf***	Путь и имя файла выделено жирным курсивом
`Клавиша / сочетание клавиш` Пример: **`Ctrl+Alt+Del`**	Клавиша или сочетание клавиш на клавиатуре

`Листинг сценария или команд`
Пример 1:
`cp pg_dump/*.sql /tmp`
Пример 2:
`CREATE DATABASE “komrad_events”;`
`CREATE DATABASE “komrad-preferences”;`
`CREATE DATABASE “pauth-preferences”;`
`CREATE DATABASE “scanner”;`
	Команды, код и скрипты сценариев, которые необходимо ввести с клавиатуры

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

ПК «КОМРАД» предназначен для сбора, регистрации, анализа событий информационной безопасности, а также выявления признаков инцидентов и реагирования на них.

ПК «КОМРАД» реализует следующие основные функции:

– проводит сбор, регистрацию информации о событиях информационной безопасности;
– позволяет осуществлять мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
– выявляет потенциальные инциденты информационной безопасности в соответствии с заданными критериями фильтрации и корреляции событий;
– оповещает о выявлении потенциальных инцидентов информационной безопасности;
– формирует отчеты об инцидентах информационной безопасности.

Основные характеристики ПК «КОМРАД»:

– поддержка следующих протоколов и механизмов сбора событий syslog, WMI, SQL, SNMP, xFlow, SFTP, локальная машина;
– поддержка формата событий информационной безопасности CEF (Common Event Format).

1.1. Действия по приему поставленного средства

1.1.1. Перечень проверок при приеме

При приеме ПК «КОМРАД» Администратор должен провести следующие проверки:

– проверка комплектности;
– проверка механических требований;
– проверка контрольных суммы информации, записанной на оптическом диске изделия;
– проверка эксплуатационной документации;
– проверка маркировки;
– проверка упаковки.

1.1.2. Проверка комплектности

Проверка комплектности изделия проводится путем сличения состава представленного изделия с комплектностью, указанной в таблицах 3 документов НПЕШ.60010-03ТУ «Технические условия» (ТУ) и НПЕШ.60010-03 ФО «Формуляр» (ФО) на изделие.

Изделие считают выдержавшим проверку, если представленная комплектация соответствует комплектности, указанной в соответствующем разделе ФО и в таблице 3 ТУ на изделие.

1.1.3. Проверка механических требований

Проверка изделия на соответствие требованиям проводится путем внешнего осмотра.

Изделие считается удовлетворяющим требованиям, если при внешнем осмотре не обнаружено деформации и повреждений рабочей поверхности оптического диска.

1.1.4. Проверка контрольных суммы информации, записанной на оптическом диске изделия

Проверку контрольных сумм проводят на аппаратной платформе из состава стенда. Подсчет контрольных сумм производить с использованием утилиты «Инспектор» программного комплекса «Средство анализа защищенности «Сканер-ВС» (Сертификат ФСТЭК № 2204 от 13.11.2010, срок действия до 13.11.2024) по алгоритму «ФИКС (уровень 1)».

Проверка считается успешно выполненной, если полученные контрольные суммы файлов установочного носителя ПК «КОМРАД» соответствуют представленным в п. 1.3.2 и п. 1.3.3 ТУ или разделу 14 ФО.

1.1.5. Проверка эксплуатационной документации

Проверка изделия на соответствие требованиям проводится путем внешнего осмотра.

Внешний осмотр эксплуатационной документации проводится полистно. На графических изображениях и в тексте книг эксплуатационной документации не должно быть темных пятен и не пропечатанных мест, затрудняющих чтение. Линии, цифры, буквы, знаки должны быть четкими, без разрывов и размывов. Книги эксплуатационной документации не должны иметь повреждений.

Изделие считается удовлетворяющим требованиям, если эксплуатационная документация оформлена и изготовлена в соответствии с требованиями ТУ.

1.1.6. Проверка маркировки

Проверку маркировки проводят путем контроля наличия и соответствия маркировки комплекта ПК «КОМРАД», наносимой на нерабочую поверхность установочного носителя с размещенным на нем дистрибутивом изделия, а также наличия и размещения знака соответствия требованиям, указанным в подразделе 1.5 ТУ.

ПК «КОМРАД» считается прошедшим проверку в части маркировки, если маркировка комплекта изделия соответствует требованиям, указанным в подразделе 1.5 ТУ.

1.1.7. Проверка упаковки

Проверку упаковки проводят путем контроля соответствия упаковки установочного носителя, содержащего дистрибутив и документацию на ПК «КОМРАД», а также всего комплекта ПК «КОМРАД» требованиям, указанным в подразделе 1.6 ТУ.

ПК «КОМРАД» считается прошедшим проверку в части упаковки, если упаковка комплекта изделия соответствует требованиям, указанным в подразделе 1.6 ТУ.

1.2. Функции безопасности ПК «КОМРАД»

Перечень функций безопасности:

– ФБ1 «Идентификация и аутентификация пользователей при входе в систему» (ИАФ.1). ПК «КОМРАД» обеспечивает идентификацию и аутентификацию пользователей, являющихся работниками администратора ПК «КОМРАД».

– ФБ2 «Идентификация и аутентификация устройств, с которых было выполнено подключение к системе» (ИАФ.2). В ПК «КОМРАД» до начала функционирования, а также передачи защищаемой информации, осуществляется идентификация и аутентификация устройств и технических средств.

– ФБ3 «Генерация, присвоение, уничтожение идентификаторов для всех объектов системы» (ИАФ.3). В ПК «КОМРАД» установлено и реализовано управление идентификаторами пользователей и устройств. Администратор ПК «КОМРАД» имеет право на создание, присвоение, блокирование и уничтожение идентификаторов пользователей, а ПК «КОМРАД» автоматически создает, присваивает, а авторизованные пользователи уничтожают идентификаторы устройств.

– ФБ4 «Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации» (ИАФ.4). В ПК «КОМРАД» для администратора системы реализованы функции управления средствами аутентификации, в том числе возможность выдачи средств аутентификации пользователям, проверки установленных характеристик пароля, смены пароля пользователям.

– ФБ5 «Защита ввода пароля» (ИАФ.5). В ПК «КОМРАД» реализована защита ввода пароля при аутентификации от визуальной демонстрации пароля, вводимого с клавиатуры (вводимые символы пароля отображаются условными знаками «•»), а также защита от копирования пароля из формы.

– ФБ6 «Идентификация и аутентификация элементов файловой системы» (ИАФ.7). В ПК «КОМРАД» реализована идентификация объектов файловой системы.

– ФБ7 «Ролевая модель доступа к системе» (УПД.2). В ПК «КОМРАД» реализован ролевой метод управления доступом, предусматривающий управление доступом субъектов на основе ролей (пользователи и администраторы), определяемых как набор прав доступа к объектам доступа (прав на выполнение определённого набора действий). Субъекты доступа ПК «КОМРАД»: пользователь, администратор. Объекты доступа ПК «КОМРАД» (вкладки панели главного меню): виджеты, активы, события, инциденты, администрирование.

– ФБ8 «Закрытие сеанса при бездействии» (УПД.10). В ПК «КОМРАД» обеспечено блокирование сеанса доступа пользователя после установленного администратором времени его бездействия (неактивности) или по запросу пользователя.

– ФБ9 «Определение событий безопасности, подлежащих регистрации» (РСБ.1). В ПК «КОМРАД» администратором определены события безопасности, подлежащие регистрации и сроки их хранения. Как минимум подлежат регистрации события о входе, а также попытки доступа входа субъектов доступа в ПК «КОМРАД». События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов обеспечивают возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе;

– ФБ10 «Определение состава и содержания информации о событиях безопасности, подлежащих регистрации» (РСБ.2). В ПК «КОМРАД» есть возможность определения состава и содержания информации о событиях безопасности, раскладывая их на поля событий, как минимум, обеспечивая идентификацию типа события безопасности, даты и времени, идентификации источника, результата события, субъекта доступа, связанного с данным событием безопасности.

– ФБ11 «Сбор, запись и хранение информации о событиях безопасности» (РСБ.3). В ПК «КОМРАД» есть возможность сбора, записи информации о событиях безопасности.

– ФБ12 «Реагирование на сбои при регистрации событий безопасности и программные ошибки, сбои в механизмах сбора информации» (РСБ.4). В ПК «КОМРАД» осуществляется реагирование на сбои при регистрации событий безопасности. Реагирование предусматривает предупреждение (индикация) о сбоях через сигнализатор, цвета которого говорят об определённом состоянии.

– ФБ13 «Мониторинг результатов регистрации событий безопасности и реагирование на них» (РСБ.5). В ПК «КОМРАД» администратору предоставлена возможность осуществлять

мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

– ФБ14 «Защита информации о событиях безопасности» (РСБ.7). В ПК «КОМРАД» обеспечивается защита информации о событиях безопасности с применением мер защиты от неправомерного доступа, уничтожения или модифицирования. Возможность доступа к записям (просмотр и анализ) предоставляется только авторизированным пользователям ПК «КОМРАД».

– ФБ15 «Возможности просмотра информации о действиях отдельных пользователей в информационной системе» (РСБ.8). В ПК «КОМРАД» администраторам предоставляется возможность просмотра и выгрузки отчётов по действиям отдельных пользователей для последующего анализа.

– ФБ16 «Контролирование точности, полноты и корректности данных, вводимых в информационную систему» (ОЦЛ.7). В ПК «КОМРАД» установлены лимиты на вводимые символы, а также проводится проверка на корректность введённых данных, наличие недопустимых символов.

– ФБ17 «Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях» (ОЦЛ.8). В ПК «КОМРАД» осуществляется контроль ошибочных действий по вводу или передаче информации и предупреждение об ошибочных действиях через генерацию сообщений для пользователей.

– ФБ18 «Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей, в том числе внешних пользователей» (УПД.1). В ПК «КОМРАД» реализована возможность администратору ПК «КОМРАД» заводить, активировать, блокировать и уничтожать учётные записи пользователей, а также корректировать, при необходимости.

1.3. Требования к среде функционирования

Изделие должно эксплуатироваться на технических средствах под управлением следующих ОС:

– Astra Linux Special Edition, версия не ниже 1.6 update 6;

– Debian, версия не ниже 7;

– Ubuntu, версия не ниже 20;

– ОСОН «ОСнова», версия 2.

Для обеспечения безопасности среды функционирования необходимо использовать либо ОСОН «ОСнова», либо ОС Astra Linux Special Edition, входящие в Государственный реестр сертифицированных средств защиты информации ФСТЭК России. ОС Debian и ОС Ubuntu не являются сертифицированными, и требуют, в общем случае, установки сертифицированных средств защиты информации от несанкционированного доступа.

Для обеспечения выполнения требований для реализации функций безопасности среды функционирования ПК «КОМРАД», необходимо:

– осуществление ввода в эксплуатацию и эксплуатации ПК «КОМРАД» в соответствии с требованиями эксплуатационной документации;

– хранение компакт-дисков с размещенной на них ПК «КОМРАД» в периоды времени, предшествующие и последующие непосредственной эксплуатации ПК «КОМРАД» только в упаковке;

– наличие администратора безопасности (администратора ПК «КОМРАД»), отвечающего за правильную настройку и эксплуатацию ПК «КОМРАД»;

– предотвращение несанкционированного доступа к идентификаторам и паролям администратора ПК «КОМРАД» и пользователей ПК «КОМРАД»;

– применение сертифицированного в системе сертификации ФСТЭК России средства контроля целостности для периодического контроля целостности файлов ПК «КОМРАД»;

– регулярная проверка ПК «КОМРАД» и среды его функционирования на наличие вредоносных компьютерных программ с использованием сертифицированных в системе сертификации ФСТЭК России средств антивирусной защиты;

– отключение служб автоматического обновления, аутентификации, основанной на сервисах глобальной идентификации и аутентификации, а также всех неиспользуемых сетевых сервисов;

– физическая защита элементов информационной системы, на которых установлено ПК «КОМРАД»;

– использование сертифицированных в системе сертификации ФСТЭК России систем обнаружения вторжений и средств межсетевого экранирования при подключении автоматизированных рабочих мест и серверов с установленным ПК «КОМРАД» к внешним информационным системам;

– запрет использование ПК «КОМРАД» для обработки информации, содержащей сведения, составляющие государственную тайну;

– прекращение работы в случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения. По данному факту должно быть проведено служебное расследование комиссией и организованы работы по анализу и ликвидации негативных последствий данного нарушения;

– применение ПК «КОМРАД» совместно с сертифицированными в системе сертификации ФСТЭК России средствами доверенной загрузки соответствующих классов, при использовании в информационных системах, требующих доверенной загрузки;

– использование средств маскирования информации при первоначальном назначении или при перераспределении внешней памяти (НЖМД) для предотвращения доступа субъекта к остаточной информации;

– контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости администраторами безопасности;

– нахождение сервера с установленным ПК «КОМРАД», источниками событий ИБ, а также АРМ администраторов ПК «КОМРАД» и пользователей ПК «КОМРАД» в контролируемой зоне. При подключении к ПК «КОМРАД» должны применяться средства криптографической защиты информации, имеющие действующий сертификат ФСБ России. Подключение к ПК «КОМРАД» из незащищенных сетей, недоверенных или неконтролируемых зон не допускается;

– запрет внесения изменений в настройки/файлы ПК «КОМРАД» после первичной настройки и установки в соответствии с эксплуатационной документацией;

– установка ПК «КОМРАД» на оборудование, соответствующее требованиям, определенным в Формуляре (НПЕШ.60010-03 30);

– обеспечение физической сохранности ЭВМ с установленным ПК «КОМРАД» и исключение возможности доступа к ней/ним посторонних лиц;

– своевременная установка в среде функционирования изделия актуальных обновлений и патчей программного обеспечения, выпущенных разработчиками данного программного обеспечения;

– проведение периодической проверки на наличие актуальных уязвимостей в ПК «КОМРАД» и среде его функционирования с использованием средств анализа защищенности;

– каналы управления ПК «КОМРАД», расположенные в пределах контролируемой зоны, должны быть защищены организационно-техническими мерами. Для защиты каналов

управления ПК «КОМРАД», выходящих за пределы контролируемой зоны, должны применяться методы и средства криптографической защиты, сертифицированные ФСБ России в установленном порядке или должен быть запрещен удаленный доступ для администрирования ПК «КОМРАД» по незащищённым каналам связи.

2. АРХИТЕКТУРА И СТРУКТУРА СЛУЖБ

ПК «КОМРАД» включает в себя подсистемы, которые разворачиваются на серверной части продукта, баз данных и служб сбора событий, устанавливаемых на некоторых типах источников событий информационной безопасности (узлы под управлением ОС Windows). Функционал ПК «КОМРАД» реализуется набором служб, разворачиваемых на серверной части.

В зависимости от типа лицензии, компоненты могут размещаться как на одном сервере, так и на нескольких, что позволяет внедрять ПК «КОМРАД» в территориально-распределенных подразделениях с возможностью, как централизованного управления, так и автономной работы подразделений при работе с инцидентами.

Общая схема размещения ПК «КОМРАД» представлена на рис.1.

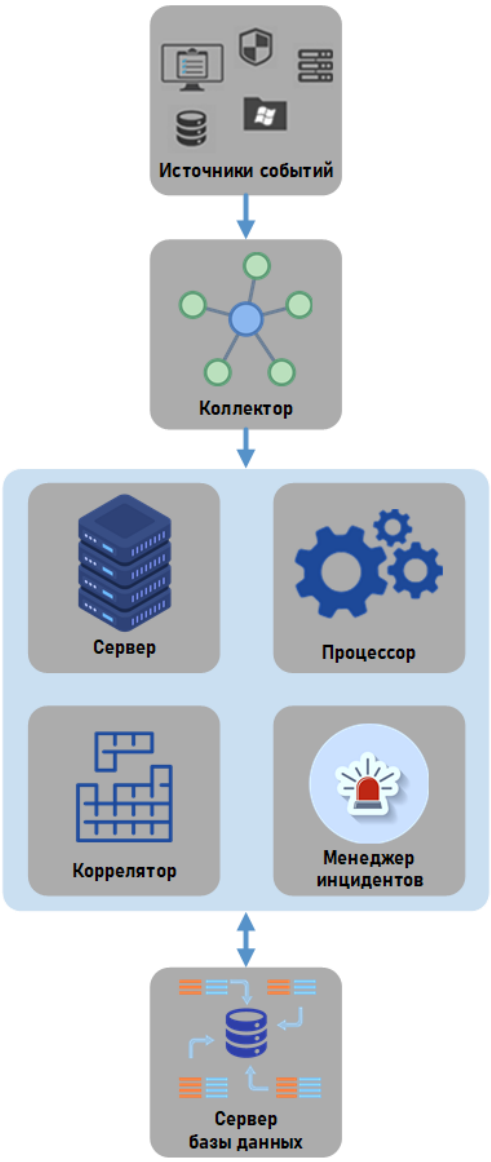

Рисунок 1 – Общая схема размещения ПК «КОМРАД»

В состав ПК «КОМРАД» входят следующие подсистемы:

1) Служба SIEM ПК «КОМРАД» Сервер;

2) Служба SIEM ПК «КОМРАД» Процессор;

3) Службы SIEM ПК «КОМРАД» Коллекторы (файловый, WMI, Syslog, SQL, SNMP, xFlow);

4) Служба SIEM ПК «КОМРАД» Менеджер инцидентов;

5) Служба SIEM ПК «КОМРАД» Диспетчер корреляции;

6) Служба SIEM ПК «КОМРАД» Коррелятор;

7) Служба SIEM ПК «КОМРАД» Реактор;

8) Служба SIEM ПК «КОМРАД» Сканер;

9) Служба SIEM ПК «КОМРАД» Подсистема авторизации;

10) Служба SIEM ПК «КОМРАД» Интеграционная шина Комрад;

11) Служба SIEM ПК «КОМРАД» Резервное копирование и восстановление;

12) Пользовательский интерфейс.

В состав среды функционирования для ПК «КОМРАД» входят:

1) СУБД PostgreSQL (версии 9.6 из состава репозитория Astra Special Edition, 11 из состава репозитория ОСОН «ОСнова», сертифицированная версия из государственного реестра сертифицированных средств защиты информации ФСТЭК);

2) СУБД ClickHouse версии 21.11.1 из состава дистрибутива ПК «КОМРАД»;

3) Nmap версии 7.91 из состава дистрибутива «ПК КОМРАД»;

4) Операционные системы, указанные в п. 1.3.

2.1. Служба SIEM ПК «КОМРАД» Сервер

Подсистема предназначена для агрегирования действий других подсистем и маршрутизации уведомлений и включает в себя следующие модули:

– диспетчер коллекторов;

– плагины;

– главный узел;

– менеджер push-уведомлений;

– менеджер рассылок;

– менеджер отчётов;

– диспетчер виджетов.

2.2. Служба SIEM ПК «КОМРАД» Процессор

Подсистема предназначена для обогащения, фильтрации и индексации событий безопасности и включает в себя следующие модули:

– индексация;

– обработка событий;

– управление фильтрацией;

– статистика событий.

2.3. Службы SIEM ПК «КОМРАД» Коллекторы (файловый, Syslog, SQL, SNMP, xFlow, WMI)

Подсистема предназначена для сбора событий по различным протоколам и стандартам.

Полученные события обрабатываются в соответствии с правилами нормализации.

Подсистема включает в себя следующие модули:

– блок управления коллектором;

– извлечение структуры;

– буфер событий.

Перечень и описание коллекторов ПК «КОМРАД» представлены в таблице 2.

Таблица 2 – Коллекторы ПК «КОМРАД»

Имя службы	Описание
Komrad File Collector *(komrad-file-collector)*	Получение данных с локальных и удаленных файлов
Komrad SNMP Collector *(komrad-snmp-collector)*	Контролирует параметры устройства и сети по SNMP-протоколу
Komrad SQL Collector *(komrad-sql-collector)*	Отслеживает событий баз данных SQL, содержащие события из различных источников
Komrad Syslog Collector *(komrad-syslog-collector)*	Собирает события системного журнала, перенаправленные другими системами
Komrad xFlow Collector *(komrad-xflow-collector)*	Собирает и анализирует трафик sFlow и NetFlow и обнаруживает в нем аномалии
Komrad WMI-agent *(komrad-wmi-agent)*	Управляет средствами сбора событий с ОС Windows

2.4. Служба SIEM ПК «КОМРАД» Менеджер инцидентов

Подсистема предназначена для управления инцидентами и включает в себя следующие модули:

– управление инцидентами;

– наблюдение за инцидентами;

– регистратор;

– статистика.

2.5. Служба SIEM ПК «КОМРАД» Диспетчер корреляции

Подсистема предназначена для управления корреляторами и включает в себя следующие модули:

– управление корреляторами;

– управление директивами.

2.6. Служба SIEM ПК «КОМРАД» Коррелятор

Подсистема предназначена для обнаружения, идентификации и регистрации инцидентов согласно директивам корреляции. Подсистема состоит из потокового коррелятора.

2.7. Служба SIEM ПК «КОМРАД» Реактор

Подсистема предназначена для запуска скриптов реагирования на инцидент и включает в себя модуль реакции на инциденты.

2.8. Служба SIEM ПК «КОМРАД» Сканер

Подсистема предназначена для управления активами и включает в себя следующие модули:

– диспетчер активов;

– сканирование.

2.9. Служба SIEM ПК «КОМРАД» Подсистема авторизации

Подсистема предназначена для управления доступом к функционалу программного комплекса и включает в себя следующие модули:

– авторизация;

– аутентификация;

– администрирование.

2.10. Служба SIEM ПК «КОМРАД» Интеграционная шина Комрад

Подсистема предназначена для передачи событий и прочей информации между подсистемами ПК «КОМРАД».

2.11. Служба SIEM ПК «КОМРАД» Резервное копирование и восстановление

Подсистема предназначена для резервного копирования и восстановления событий, инцидентов, правил корреляции и фильтров и включает в себя модули:

– резервное копирование;

– локальное облачное хранилища «Komrad-S3»;

– мониторинг.

2.12. Пользовательский интерфейс

Подсистема предназначена для отображения данных для пользователя.

2.13. СУБД ClickHouse

Не является подсистемой ПК «КОМРАД», но обеспечивает выполнение функций по хранению данных ПК «КОМРАД».

При установке ПК «КОМАРД» создается и используется база данных, представленная в таблице 3.

Таблица 3 – База данных в ClickHouse

№	Название	Описание
1	БД «komrad_events»	База данных предназначена для хранения индексов событий, нормализованных и исходных событий

2.14. СУБД PostgreSQL

Не является подсистемой ПК «КОМРАД», но обеспечивает выполнение функций по хранению данных ПК «КОМРАД».

При установке ПК «КОМРАД» создаются и используются базы данных, представленные в таблице 4.

Таблица 4 – Базы данных в PostgreSQL

№	Название	Описание
1	БД «komrad-preferences»	База данных предназначена для хранения обнаруженных, идентифицированных и зарегистрированных инцидентов и директив (правил) корреляции, а также для хранения настроек конфигурации коллекторов, плагинов, рассылок, конфигурации виджетов, ГосСОПКА, push-уведомлений, правил фильтров
2	БД «pauth-preferences»	База данных предназначена для хранения данных системы авторизации
3	БД «scanner»	База данных предназначена для хранения данных об активах

2.15. Nmap

Не является подсистемой ПК «КОМРАД», но обеспечивает выполнение функций по разнообразному настраиваемому сканированию IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб).

Является свободной утилитой.

2.16. Структура директорий

Файлы необходимые для работы ПК «КОМРАД» находятся в директориях, указанных в таблице 5.

Таблица 5 – Структура директорий

ОС	Директории
Linux	1) Исполняемые файлы находятся в папке: ***/etc/echelon/komrad/*** 2) Папка для размещения лицензии: ***/etc/echelon/komrad/license*** 3) Конфигурационные файлы: – Сервер: ***/etc/echelon/komrad/komrad-server*** – Процессор: ***/etc/echelon/komrad/komrad-processor*** – Интеграционная шина: ***/etc/echelon/komrad/komrad-bus*** – Менеджер инцидентов: ***/etc/echelon/komrad/incident-manager*** – Диспетчер корреляции: ***/etc/echelon/komrad/correlation-dispatcher*** – Реактор: ***/etc/echelon/komrad/komrad-reactor*** – Сканер: ***/etc/echelon/komrad/komrad-scanner*** – Подсистема авторизации: ***/etc/echelon/komrad/pauth-server*** – Хранилище: ***/etc/postgresql***

ОС	Директории
	– Файловый коллектор: ***/etc/echelon/komrad/ file-collector*** – SNMP коллектор: ***/etc/echelon/komrad/snmp-collector*** – SQL коллектор: ***/etc/echelon/komrad/sql-collector*** – Syslog коллектор: ***/etc/echelon/komrad/syslog-collector*** – XFLOW коллектор: ***/etc/echelon/xflow-collector*** 4) Папки для сертификатов – корневого сертификата: ***/var/lib/echelon/komrad/certs/ca.pem***, ***/var/lib/echelon/komrad/certs/CAs/ca.pem*** и ***/var/lib/echelon/komrad/certs/ca-key.pem*** – серверный сертификат: ***/var/lib/echelon/komrad/certs/server.pem*** и ***/var/lib/echelon/komrad/certs/server-key.pem*** – клиентский сертификат: ***/var/lib/echelon/komrad/certs/client.pem*** и ***/var/lib/echelon/komrad/certs/client-key.pem***

2.17. Используемые порты

В ПК «КОМРАД» для работы служб используются порты, указанные в таблице 6.

Таблица 6 – Используемые порты для работы служб

Сервис	Порт	Примечание
Доступ к панели управления	<IP сервера KOMRAD >:443	Панель управления ПК «КОМРАД»
KOMRAD-S3	<IP сервера KOMRAD>:9050	Панель управления объектовым хранилищем
СУБД PostgreSQL	5432	
СУБД ClickHouse	9000	
SMTP	25 или 443	
WMI-агент	3490	Порт коллектора в ПК «КОМРАД»
Syslog	49000 (TCP), 49050 (UDP)	Порт коллектора в ПК «КОМРАД»
sFlow	2055 (TCP, UDP)	Порт коллектора в ПК «КОМРАД»
IPFIX	4741 (TCP, UDP)	Порт коллектора в ПК «КОМРАД»
NetFlow v5	49300 (TCP, UDP)	Порт коллектора в ПК «КОМРАД»
NetFlow v9	49400 (TCP, UDP)	Порт коллектора в ПК «КОМРАД»

3. УСТАНОВКА И ЗАГРУЗКА

3.1. Выбор архитектуры инсталляции

3.1.1. Один узел, все службы на одном узле (лицензия BASE, All-in-One, Enterprise)

Общая схема размещения ПК «КОМРАД» при данном подходе к выбору архитектуры представлена на рис. 2.

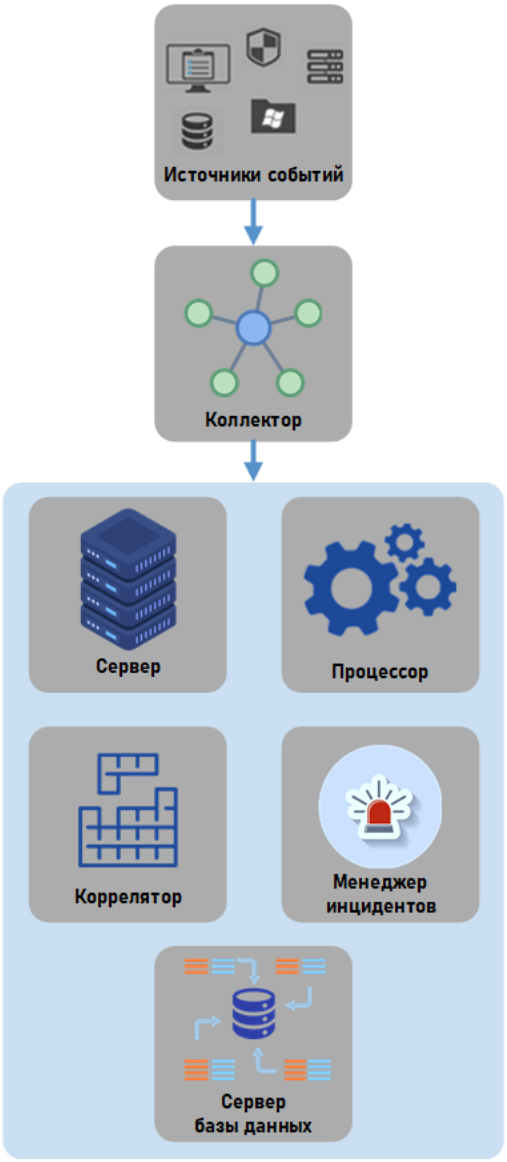

Рисунок 2 – Общая схема размещения ПК «КОМРАД»

Описание:

– все компоненты ПК «КОМРАД» устанавливаются на один сервер;

– рекомендации:

1) постоянный мониторинг свободного места в файловой системе из-за постоянной записи событий в базы данных;

2) количество EPS зависит от мощности сервера, а также от загруженности центрального процессора. Чем больше центральный процессор загружен другими процессами, тем меньшее количество событий от источников он будет нормализовать в коррелляторе;

3) при достижении 70% загруженности процессора и подсистемы жестких дисков рекомендуем перенести СУБД на отдельный сервер. Так снизится нагрузка на процессор и файловую подсистему;

4) резервные копии баз данных храните в другом дисковом массиве, желательно в системе хранения данных (СХД).

3.1.2. Один узел, база данных на другом узле (лицензия BASE, AIO, Enterprise)

Общая схема размещения ПК «КОМРАД» при данном подходе к выбору архитектуры представлена на рис. 3.

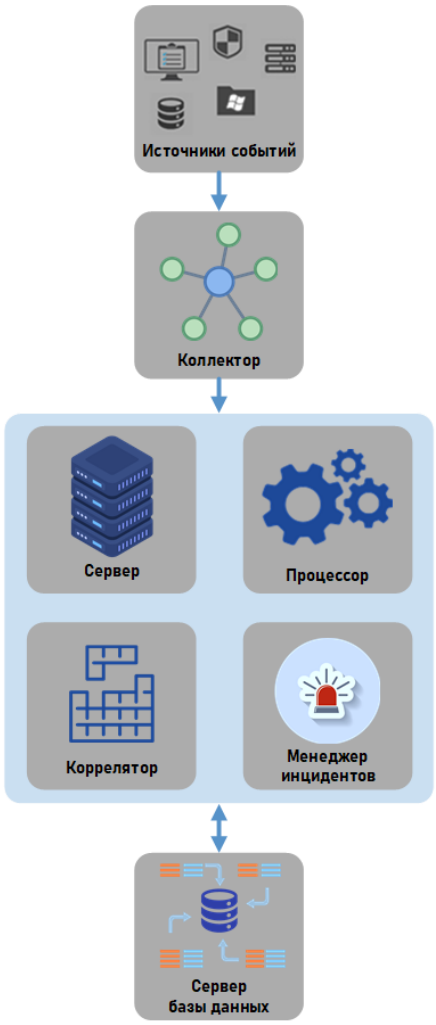

Рисунок 3 – Общая схема размещения ПК «КОМРАД»

Описание:

– все компоненты ПК «КОМРАД» устанавливаются на один сервер;

– сервер СУБД разворачивается на отдельном узле.

3.1.3. Один узел, коллекторы на разных узлах (лицензия Enterprise)

Общая схема размещения ПК «КОМРАД» при данном подходе к выбору архитектуры представлена на рис. 4.

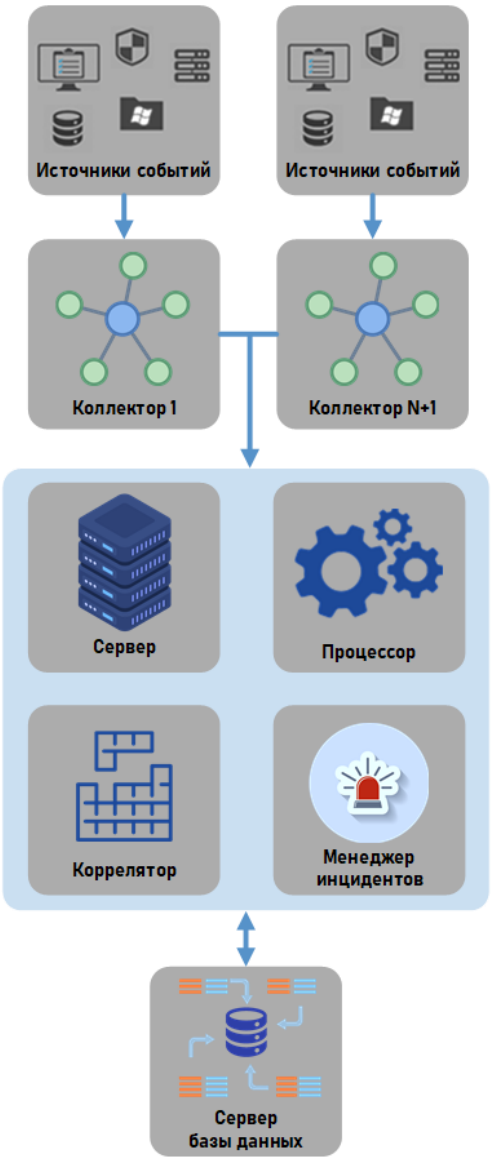

Рисунок 4 – Общая схема размещения ПК «КОМРАД»

Описание:

– все компоненты ПК «КОМРАД» устанавливаются на один сервер;

– сервер СУБД разворачивается на отдельном узле;

– коллекторы устанавливаются на разных узлах.

Данная схема позволит собирать события с территориально-распределенных объектов. На территориально-распределенных объектах достаточно установить интеграционную шину и необходимые коллекторы для сбора событий с источников.

В случае обрыва связи с территориально-распределенными объектами, коллекторы на узлах продолжат работать и при восстановлении связи передадут все события в центральный узел.

3.1.4. Один центральный узел с сервером, службы процессора, коррелятора, менеджера инцидентов, коллекторы на разных узлах (лицензия Enterprise)

Общая схема размещения ПК «КОМРАД» при данном подходе к выбору архитектуры представлена на рис. 5.

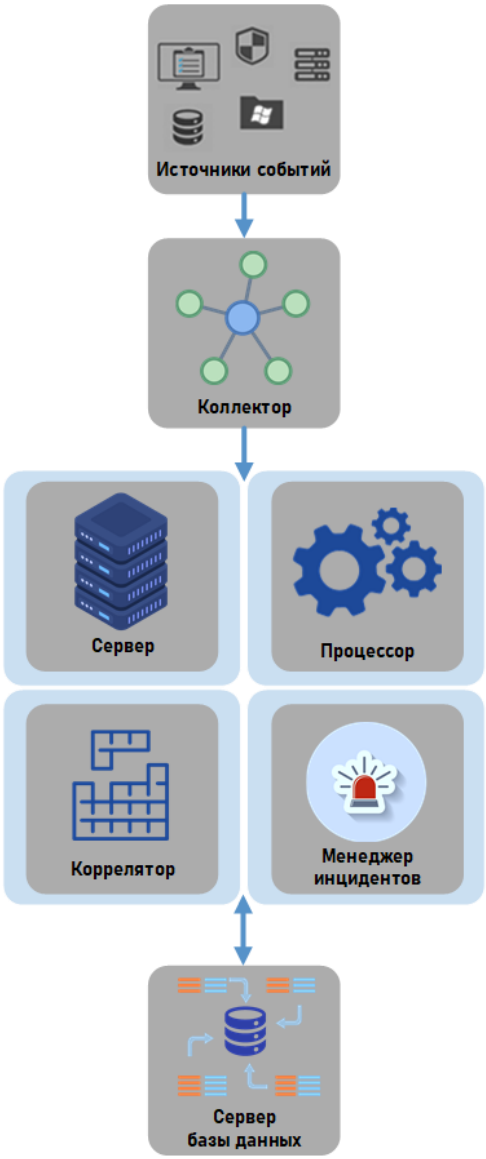

Рисунок 5 – Общая схема размещения ПК «КОМРАД»

Описание:

– все компоненты ПК «КОМРАД» устанавливаются на разных узлах.

Данная схема позволит разнести компоненты ПК «КОМРАД» по разным узлам с целью увеличения производительности, а также в случаях, когда текущие аппаратные мощности сервера не справляются с нагрузкой.

3.2. Установка на Astra Linux Special Edition

В ПК «КОМРАД» в зависимости от типа лицензии возможны следующие варианты установок:

– все компоненты на одном узел;

– компоненты ПК «КОМРАД» на одном узле, СУБД PostgreSQL и ClickHouse на отдельном узле;

– территориально-распределенная установка (при выборе этого вида установки обратитесь в тех. поддержку).

3.2.1. Поставляемые компоненты

Дистрибутив ПК «КОМРАД» представлен в таблице 7.

Таблица 7 – Дистрибутив ПК «КОМРАД»

Название компонента	Папка	Описание
clickhouse-client_21.11.1_all_signed.deb clickhouse-client_21.11.1_all_signed.deb.asc clickhouse-common-static_21.11.1_amd64_signed.deb clickhouse-common-static_21.11.1_amd64_signed.deb.asc clickhouse-server_21.11.1_all_signed.deb clickhouse-server_21.11.1_all_signed.deb.asc	/astra/db/clickhouse	СУБД Clickhouse
correlation-dispatcher_v4.1.33_amd64.deb correlation-dispatcher_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для управления корреляторами
echelontls_v4.1.33_amd64.deb echelontls_v4.1.33_amd64.deb.asc	/astra/deb	Утилита генерации сертификатов
file-collector_v4.1.33_amd64.deb file-collector_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для сбора событий из файлов
incident-manager_v4.1.33_amd64.deb incident-manager_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для управления инцидентами
komrad-backup_v4.1.33_amd64.deb	/astra/deb	Модуль предназначен

Название компонента	Папка	Описание
komrad-backup_v4.1.33_amd64.deb.asc		для управления резервным копированием и восстановлением
komrad-bus_v4.1.33_amd64.deb komrad-bus_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для передачи событий и прочей информации между подсистемами ПК «КОМРАД»
komrad-cli_v4.1.33_amd64.deb komrad-cli_v4.1.33_amd64.deb.asc	/astra/deb	Консольный интерфейс
komrad-correlator_v4.1.33_amd64.deb komrad-correlator_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для управления корреляторами
komrad-processor_v4.1.33_amd64.deb komrad-processor_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для обогащения, фильтрации и индексации событий безопасности
komrad-reactor-cef_v4.1.33_amd64.deb komrad-reactor-cef_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для запуска скриптов реагирования на инцидент в формате CEF
komrad-reactor_v4.1.33_amd64.deb komrad-reactor_v4.1.33_amd64.deb	/astra/deb	Модуль предназначен для запуска скриптов реагирования на инцидент
komrad-s3_v4.1.34_amd64.deb komrad-s3_v4.1.34_amd64.deb.asc	/astra/deb	Модуль предназначен для создания

Название компонента	Папка	Описание
		объектового хранилища системы резервного копирования и восстановления
komrad-scanner_v4.1.33_amd64.deb komrad-scanner_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для управления активами
komrad-server_v4.1.33_amd64.deb komrad-server_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для агрегирования действий других подсистем и маршрутизации уведомлений
komrad-vault_v4.1.33_amd64.deb komrad-vault_v4.1.33_amd64.deb.asc	/astra/deb	Подсистема предназначена для управления выпущенными сертификатами
pauth-server_v4.1.33_amd64.deb pauth-server_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для управления доступом к функционалу программного комплекса
pauthctl_v4.1.33_amd64.deb pauthctl_v4.1.33_amd64.deb.asc	/astra/deb	Утилита для работы с пользователями в командной строке
snmp-collector_v4.1.34_amd64.deb snmp-collector_v4.1.34_amd64.deb.asc	/astra/deb	Модуль предназначен для сбора событий по SNMP
sql-collector_v4.1.33_amd64.deb	/astra/deb	Модуль предназначен

Название компонента	Папка	Описание
sql-collector_v4.1.33_amd64.deb.asc		для сбора событий из СУБД
sqlx-collector_v4.1.33_amd64.deb sqlx-collector_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для сбора событий из СУБД
syslog-collector_v4.1.33_amd64.deb syslog-collector_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для сбора событий по Syslog
xflow-collector_v4.1.33_amd64.deb xflow-collector_v4.1.33_amd64.deb.asc	/astra/deb	Модуль предназначен для сбора событий sFlow и NetFlow
astra_echelon_pub_key.gpg	/astra/keys	Открытый ключ для проверки подлинности
syslog_collector_root.sh	/astra/scripts	Скрипт для syslog-collector
nmap-7.91-komrad_signed.deb nmap-7.91-komrad_signed.deb.asc	/astra/tools	Сканер сети
komrad-cli.exe komrad-cli.exe.asc	/astra/windows/cli	Консольный интерфейс
sql-collector.exe sql-collector.exe.asc sql-collector.yaml sql-collector.yaml.asc	/astra/windows/sql-collector	Модуль предназначен для сбора событий из СУБД из Windows
wmi-agent.exe wmi-agent.exe.asc wmi-agent.yaml wmi-agent.yaml.asc	/astra/windows/wmi-agent	Модуль предназначен для сбора событий по WMI

3.2.2. Аппаратные требования

В таблице 8 приведены ориентировочные значения технических данных аппаратной платформы.

Таблица 8 – Требования к аппаратной платформе

Тип лицензии	CPU	RAM	SSD\HDD
Base	Минимум – 2 ядра Рекомендовано – от 2-х ядер	Минимум – 2 Гб Рекомендовано – 4 Гб	От 100 Гб
All-in-One	Минимум – 2 ядра Рекомендовано – 4 ядра	Минимум – 8 Гб Рекомендовано – 16 Гб	От 1 Тб
Enterprise	Минимум – 4 ядра Рекомендовано – 8 ядра	Минимум – 32 Гб Рекомендовано – 128 Гб	От 10 Тб

При выборе аппаратной части необходимо провести консультацию с техническим специалистом для предварительной оценки и рекомендаций при выборе аппаратной части.

Увеличение количества источников и\или увеличение количества событий от существующих источников повлечёт за собой увеличение ресурсов.

Внимание! Для установки ПК «КОМРАД» на Astra Linux Special Edition необходимы наличие:

– установочного диска, диска с обновлением или развёрнутого сетевого репозитория;

– установка ПК «КОМРАД» должна производиться без включённой (выключенной) функцией создания замкнутой программной среды (ЗПС);

– на ОС Astra Linux Special Edition версия не ниже 1.6 должно быть установлено последнее обновление системы безопасности;

– необходимо наличие идентификационной информации для запуска из-под суперпользователя;

– для установки недостающих пакетов можно использовать терминал или воспользоваться графическим менеджером пакетов, например Synaptic.

3.2.3. Установка всех компонентов на один узел

Поддерживаемые лицензии: Base, All-in-One, Enterprise.

Для работы ПК «КОМРАД» на ОС Astra Linux Special Edition в режиме замкнутой программной среды (ЗПС) после установки по основной инструкции нужно:

1) скопировать файл открытого ключа:

```
sudo cp astra/keys/astra_echelon_pub_key.gpg /etc/digsig/keys/
```

2) открыть файл конфигурации:

```
sudo nano /etc/digsig/digsig_initramfs.conf
```

3) включить политику ЗПС:

```
DIGSIG_ELF_MODE=1
```

4) выполнить:

```
sudo update-initramfs -u -k all
```

5) перезагрузить систему (после перезагрузки система загрузится уже в режиме ЗПС), выполнив:

```
sudo reboot
```

3.2.3.1. Шаг 1. Установка и настройка PostgreSQL 9.6 и ClickHouse

1) Установите и настройте PostgreSQL 9.6, выполнив команду в терминале:

```
sudo apt install postgresql ca-certificates -y
```

2) Перейдите в папку с дистрибутивом ***/astra/db/clickhouse/*** и в терминале введите:

```
sudo dpkg -i ./*.deb
```

Укажите пароль для пользователя «default».

3) Запустите ClickHouse командой в терминале:

```
sudo service clickhouse-server start
```

4) Создайте пароль для ClickHouse командой в терминале, указав вместо `pass` ваш пароль:

Внимание! Команда пишется в одну строчку:

```
echo "pass"; echo -n "pass" | sha256sum | tr -d '-'
```

В первой строке результата – пароль (`pass`). Вторая строка – соответствующий ему хэш SHA256 (`pass_SHA256`).

5) Создайте и откройте на редактирование файл:

```
sudo nano /etc/clickhouse-server/users.d/komrad.xml
```

Заполните содержимое файла следующим фрагментом:

```
<yandex>
    <users>
        <komrad>
            <password remove='1' />
            <password_sha256_hex>pass_SHA256</password_sha256_hex>
        </komrad>
```

```
    </users>
</yandex>
```

Где вместо pass_SHA256 вставьте сгенерированный хэш, соответствующий вашему паролю.

6) Откройте файл, выполнив:

```
sudo nano /etc/clickhouse-server/users.xml
```

Добавьте пользователя komrad в группу пользователей, для чего приведите фрагмент файла к виду:

```
    <!-- Users and ACL. -->
    <users>
        <komrad>
                <access_management>1</access_management>
                <password></password>
        </komrad>
        <!-- If user name was not specified, 'default' user is used. -->
        <default>
```

7) Перезапустите сервер ClickHouse, выполнив:

```
sudo systemctl restart clickhouse-server.service
```

3.2.3.2. Шаг 2. Задание прав пользователя на создание баз данных и создание базы данных

1) Чтобы создать нового пользователя, откройте аккаунт стандартного пользователя:

```
sudo su - postgres
```

2) Наделите пользователя правами на создание новых баз данных, где вместо pass – установите пароль для пользователя postgres:

```
psql -c "ALTER USER postgres WITH CREATEDB LOGIN PASSWORD 'pass';"
```

3) Установите расширение, выполнив:

```
psql -c "CREATE EXTENSION pg_trgm;"
```

4) Создайте базы данных, выполнив:

```
createdb -O postgres komrad-preferences
createdb -O postgres pauth-preferences
```

```
createdb -O postgres scanner
exit
```

5) Запустите клиент ClickHouse, используя данные пользователя komrad, где вместо pass – укажите пароль, заданный в шаге 1 при установке ClickHouse:

```
clickhouse-client --user=komrad --password=pass
```

6) Создайте базу данных, выполнив:

```
CREATE DATABASE komrad_events
exit
```

3.2.3.3. Шаг 3. Установка модуль сканирования сети Nmap

Перейдите в папку с утилитами ***/astra/tools*** и через терминал выполните команду:

```
sudo dpkg -i ./*.deb
```

3.2.3.4. Шаг 4. Установка ПК «КОМРАД»

Перейдите в папку с дистрибутивом ***/astra/deb*** и через терминал выполните команду:

```
sudo dpkg -i ./*.deb
```

3.2.3.5. Шаг 5. Редактирование yaml-файлов

1) Откройте файл ***komrad-processor.yaml***, выполнив через команду в терминале:

```
sudo nano /etc/echelon/komrad/komrad-processor/komrad-processor.yaml
```

Приведите фрагмент файла к данному виду:

```
# Настройки подключения к бд хранящей конфигурацию виджетов
widgetsdb:
  TLSCertPath: /var/lib/echelon/komrad/certs/client.pem
  TLSKeyPath: /var/lib/echelon/komrad/certs/client-key.pem
  TLSRootCAPath: /var/lib/echelon/komrad/certs/ca.pem
  db: komrad-preferences
  host: localhost
  password: pass # укажите пароль для пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres
```

```
# Настройки хранилища событий информационной безопасности
storage:
  # Тип хранилища, в данной версии поддерживается только:
  # - timescale - PostgreSQL 12+ с плагином TimescaleDB 2.2.1+
  # - clickhouse - ClickHouse v21.7.8.58-stable
  # Для ОС "Основа" поддерживается PostgreSQL 11 с TimescaleDB 2.2.1
  kind: clickhouse
  clickhouse:
    # Название БД
    name: komrad_events
    user: komrad
    password: pass # укажите пароль для пользователя komrad (ClickHouse)
    # Адрес хоста с ClickHouse-server
    host: localhost
    # Порт ClickHouse-server
    port: 9000
    # Режим работы - с TLS или без
    sslmode: disable
```

2) Откройте файл ***komrad-server.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-server/komrad-server.yaml
```

Отредактируйте:

```
database:
pg:
  db: komrad-preferences
  host: localhost
  password: pass # укажите пароль для пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres
```

3) Откройте файл ***correlation-dispatcher.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/correlation-dispatcher/correlation-dispatcher.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@localhost:5432/komrad-preferences?sslmode...
```

```
CorrelatorController:
  # Настройка подключения к БД PostgreSQL в формате URL для корреляторов.
  CorrelatorDB:postgres://postgres:pass@localhost:5432/komrad-preferences?sslmode...
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

4) Откройте файл ***incident-manager.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/incident-manager/incident-manager.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@localhost:5432/komrad-preferences?sslmode...
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

5) Откройте файл ***pauth-server.yaml*** выполнив:

```
sudo nano /etc/echelon/komrad/pauth-server/pauth-server.yaml
```

Отредактируйте:

```
database: postgres://postgres:pass@localhost:5432/pauth-preferences?sslmode...
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

6) Откройте ***komrad-scanner-config.json***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-scanner/komrad-scanner-config.json
```

Отредактируйте:

```
"Main": {
      "Driver": "postgres",
      "Host": "localhost",
      "Port": 5432,
      "DBName": "scanner",
      "User": "postgres",
      "Password": "pass",
      "SSLMode": "disable"
            }
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

7) Откройте ***postgresql.conf***, выполнив:

```
sudo nano /etc/postgresql/9.6/main/postgresql.conf
```

Раскомментируйте и добавьте пути до сертификатов:

```
ssl = on
ssl_ca_file = '/var/lib/echelon/komrad/certs/ca.pem'
ssl_key_file = '/var/lib/echelon/komrad/certs/server-key.pem'
ssl_cert_file = '/var/lib/echelon/komrad/certs/server.pem'
```

8) Перезагрузите сервисы, выполнив команду в одну строчку:

```
sudo systemctl restart postgresql komrad-server komrad-processor komrad-scanner pauth-server correlation-dispatcher incident-manager
```

3.2.3.6. Шаг 6. Создание ролей администратора и пользователя с правами администратора

Создайте роль администратора и пользователя с правами администратора через команды в терминале.

Внимание! Каждая отдельная команда пишется одну строчку:

```
sudo pauthctl role add admin --migrate --conn "postgresql://postgres:pass@localhost:5432/pauth-preferences"
```

О успешном добавлении роли `admin` в строке сервиса будет строка:

INFO roles added {"role_names": ["admin"], "status": "success"}

```
sudo pauthctl role add user --conn "postgresql://postgres:pass@localhost:5432/pauth-preferences"
```

О успешном добавлении роли `user` в строке сервиса будет строка:

INFO roles added {"role_names": ["user"], "status": "success"}

```
sudo pauthctl user add --email name@domain.com --login admin --roles admin --password admin --conn "postgresql://postgres:pass@localhost:5432/pauth-preferences"
```

Где:

1) `pass` – укажите пароль пользователя postgres (PostgreSQL);

2) `--e-mail name@domain.com` – укажите свой e-mail адрес администратора;

3) `--login admin` – укажите свой логин администратора;

4) `--password admin` – укажите свой пароль администратора.

3.2.3.7. Шаг 7. Перенос лицензии

1) Удалите демо-лицензию из папки ***/etc/echelon/komrad/license*** командой в терминале:

```
sudo rm /etc/echelon/komrad/license/license.lic
```

2) Скопируйте в папку ***/etc/echelon/komrad/license*** файл лицензии с расширением (***.lic***).

3) Перезапустите сервисы komrad-server, komrad-processor, pauth-server командой в терминале:

```
sudo systemctl restart komrad-server komrad-processor pauth-server
```

3.2.3.8. Шаг 8. Создание сертификатов

Внимание! Дальнейшие действия желательно выполнять на отдельной ЭВМ, где в дальнейшем будут храниться корневые сертификаты, необходимые для корректной работы компонентов ПК «КОМРАД».

Создание сертификатов:

1) создайте на жестком диске папку ***/tls***;

Совет! Команда для создания папки:

```
mkdir tls
```

2) перейдите в папку ***/tls*** и выполните команду в терминале для создания корневого сертификата:

```
cd tls
echelontls ca --organization “Echelon”
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***ca.pem*** и ***ca-key.pem.***

3) создайте серверный сертификат командой в терминале:

```
echelontls cert --organization “Echelon” localhost 127.0.0.1 $(hostname -I) $(hostname)
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***server.pem*** и ***server-key.pem***

4) создайте клиентский сертификат командой в терминале:

```
echelontls cert --client
```

В папке ***/tls*** сгенерируются два файла ***client.pem*** и ***client-key.pem***

5) создайте сертификат для браузера командой в терминале:

```
echelontls browser
```

Внимание! При генерации сертификата для браузера, утилита komradtls попросит задать пароль. Этот пароль потребуется при добавлении сертификата в браузер, поэтому запомните этот пароль.

В папке ***/tls*** сгенерируется файл ***client-browser.p12***.

3.2.3.9. Шаг 9. Удаление сертификатов по умолчанию

Удалите все сертификаты из папки с сертификатами по умолчанию командой в терминале:

```
sudo rm /var/lib/echelon/komrad/certs/CAs/*
sudo rm /var/lib/echelon/komrad/certs/*
```

3.2.3.10. Шаг 10. Копирование сертификатов

Скопируйте сертификаты в следующие папки:

1) файлы ***ca.pem***, ***server.pem***, ***server-key.pem,*** ***client.pem,*** ***client-key.pem*** в ***/var/lib/echelon/komrad/komrad-server/certs/*** командой терминале:

```
sudo cp ca.pem server.pem server-key.pem client.pem client-key.pem
/var/lib/echelon/komrad/certs/
```

Внимание! Команда выполняется в одну строчку.

2) файл ***ca.pem*** в ***/var/lib/echelon/komrad/certs/CAs/*** командой:

```
sudo cp ca.pem /var/lib/echelon/komrad/certs/CAs/
```

3.2.3.11. Шаг 11. Изменение владельца файлов на komrad:komrad и предоставление прав сертификатам

Введите команды в терминале:

```
sudo chown komrad:komrad  /etc/echelon/komrad/license/имя_лицензии.lic
sudo chown -R komrad:komrad  /var/lib/echelon/komrad/certs
sudo chmod -R 755 /var/lib/echelon/komrad/certs
sudo chmod 0640 /var/lib/echelon/komrad/certs/server-key.pem
sudo chown root:komrad /var/lib/echelon/komrad/certs/server-key.pem
sudo usermod -a -G komrad postgres
sudo chmod 755 client-browser.p12
```

Где в имя_лицензии – укажите наименование файла лицензии.

3.2.3.12. Шаг 12. Перезапуск сервисов

Перезагрузите систему.

3.2.3.13. Шаг 13. Установка корневого и браузерного сертификатов в браузере

Выполните следующие действия:

1) откройте **Firefox → Настройки → Приватность и защита → Сертификаты → Просмотр сертификатов**;

2) перейдите во вкладку **Ваши сертификаты** меню **Управления сертификатами;**

3) импортируйте сертификаты ***ca.pem*** в «Доверенные корневые центры сертификации» и ***client-browser.p12*** в «Личные», при этом потребуется указать пароль установленный, при генерации браузерного сертификата в Шаге 8;

4) перезагрузите браузер.

3.2.3.14. Шаг 14. Конец

ПК «КОМРАД» установлен и доступен по адресу https://localhost.

3.2.4. Установка компонентов ПК «КОМРАД» на одном узле, СУБД PostgreSQL и ClickHouse на другом

Поддерживаемые лицензии: Base, All-in-One, Enterprise.

Установка ПК «КОМРАД» должна производиться без включённой (выключенной) функции создания ЗПС.

Для работы ПК «КОМРАД» на ОС Astra Linux Special Edition в режиме замкнутой программной среды (ЗПС) после установки по основной инструкции нужно:

1) скопировать файл открытого ключа:

```
sudo cp astra/keys/astra_echelon_pub_key.gpg /etc/digsig/keys/
```

2) открыть файл конфигурации:

```
sudo nano /etc/digsig/digsig_initramfs.conf
```

3) включить политику ЗПС:

```
DIGSIG_ELF_MODE=1
```

4) выполнить:

```
sudo update-initramfs -u -k all
```

5) перезагрузить систему (после перезагрузки система загрузится уже в режиме ЗПС), выполнив:

```
sudo reboot
```

Установка ПК «КОМРАД» будет состоять из двух этапов:

– на первом этапе установка и настройка PostgreSQL 9.6 и ClickHouse;

– на втором этапе установка и настройка ПК «КОМРАД».

Внимание! Для установки ПК «КОМРАД» на Astra Linux Special Edition необходимы наличие:

– установочного диска, диска с обновлением или развёрнутого сетевого репозитория;

– на ОС Astra Linux Special Edition должно быть установлено последнее обновление системы безопасности;

– необходимо наличие идентификационной информации для запуска из-под суперпользователя;

– для установки недостающих пакетов можно использовать как терминал (**`Ctrl + T`**) или воспользоваться графическим менеджером пакетов, например Synaptic.

3.2.4.1. Этап 1. Шаг 1. Установка и настройка PostgreSQL 9.6 и Clickhouse

1) Установите и настройте PostgreSQL 9.6, выполнив команду в терминале:

```
sudo apt install postgresql ca-certificates -y
```

2) Перейдите в папку с дистрибутивом ***/astra/db/clickhouse/*** и в терминале введите:

```
sudo dpkg -i ./*.deb
```

Укажите пароль для пользователя «default».

3) Запустите ClickHouse командой в терминале:

```
sudo service clickhouse-server start
```

4) Создайте пароль для ClickHouse командой в терминале, указав вместо `pass` ваш пароль:

Внимание! Команда пишется в одну строчку:

```
echo "pass"; echo -n "pass" | sha256sum | tr -d '-'
```

В первой строке результата – пароль (`pass`). Вторая строка – соответствующий ему хэш SHA256 (`pass_SHA256`).

5) Создайте и откройте на редактирование файл:

```
sudo nano /etc/clickhouse-server/users.d/komrad.xml
```

Заполните содержимое файла следующим фрагментом:

```
<yandex>
    <users>
        <komrad>
            <password remove='1' />
            <password_sha256_hex>pass_SHA256</password_sha256_hex>
        </komrad>
    </users>
</yandex>
```

Где вместо `pass_SHA256` вставьте сгенерированный хэш, соответствующий вашему паролю.

6) Откройте файл, выполнив:

```
sudo nano /etc/clickhouse-server/users.xml
```

Добавьте пользователя komrad в группу пользователей, для чего приведите фрагмент файла к виду:

```
    <!-- Users and ACL. -->
```

```
    <users>
        <komrad>
                <access_management>1</access_management>
                <password></password>
        </komrad>
        <!-- If user name was not specified, 'default' user is used. -->
        <default>
```

7) Перезапустите сервер ClickHouse, выполнив:

```
sudo systemctl restart clickhouse-server.service
```

3.2.4.2. Этап 2. Шаг 2. Задание прав пользователя на создание баз данных и создание базы данных

1) Чтобы создать нового пользователя, откройте аккаунт стандартного пользователя:

```
sudo su - postgres
```

2) Наделите пользователя правами на создание новых баз данных, где вместо `pass` – установите пароль для пользователя postgres:

```
psql -c "ALTER USER postgres WITH CREATEDB LOGIN PASSWORD 'pass';"
```

3) Установите расширение, выполнив:

```
psql -c "CREATE EXTENSION pg_trgm;"
```

4) Создайте базы данных, выполнив:

```
createdb -O postgres komrad-preferences
createdb -O postgres pauth-preferences
createdb -O postgres scanner
exit
```

5) Запустите клиент ClickHouse, используя данные пользователя komrad, где вместо `pass` – укажите пароль, заданный в шаге 1 при установке ClickHouse:

```
clickhouse-client --user=komrad --password=pass
```

6) Создайте базу данных, выполнив:

```
CREATE DATABASE komrad_events
exit
```

3.2.4.3. Этап 1. Шаг 3. Настройка подключения к базам данных с удаленных узлов

По умолчанию, серверы баз данных разрешают подключение только с локального компьютера. Для подключения с удаленных систем необходимо отредактировать три файла ***postgresql.conf***, ***pg_hba.conf*** и ***config.xml***.

1) Откройте для редактирования файл ***postgresql.conf***, выполнив:

```
sudo nano /etc/postgresql/9.6/main/postgresql.conf
```

Затем раскомментируйте строку, содержащую `# listen_addresses = `localhost``, убрав # перед строкой, и отредактируйте, чтобы получилось, как в следующем файле:

```
#------------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------------------

# - Connection Settings -

listen_addresses = '*'                  # what IP address(es) to listen on;
                                        # comma-separated list of addresses;
                                        # defaults to 'localhost'; use '*' for all
                                        # (change requires restart)
```

Совет! В данном примере мы разрешили прослушивание запросов на всех IP-адресах (*), но, если требуется более безопасная настройка, можно перечислить последние через пробел.

Например: `listen_addresses = ` 192.168.0.15 10.10.0.16 `.`

Сохраните файл и закройте его.

2) Откройте для редактирования файл ***pg_hba.conf***, выполнив:

```
sudo nano /etc/postgresql/9.6/main/pg_hba.conf
```

После последней строки файла с новой строки добавить:

```
host    all     postgres    IP-адрес_ПК_КОМРАД/32    md5
```

Где IP-адрес_ПК_КОМРАД – IP-адрес хоста, с которого будет подключение.

Сохраните файл и закройте его, после чего перезапустите службу, выполнив:

```
sudo systemctl restart postgresql
```

3) Откройте для редактирования файл ***config.xml***, выполнив:

```
sudo nano /etc/clickhouse-server/config.xml
```

Затем раскомментируйте строку, содержащую <!-- <listen_host>0.0.0.0</listen_host> -->, как в следующем файле:

```
...
 <interserver_http_host>example.yandex.ru</interserver_http_host>
    -->

    <!-- Listen specified host. use :: (wildcard IPv6 address), if you want to
accept connections both with IPv4 and IPv6 from everywhere. -->
    <!-- <listen_host>::</listen_host> -->
    <!-- Same for hosts with disabled ipv6: -->
    <listen_host>0.0.0.0</listen_host>

    <!-- Default values - try listen localhost on ipv4 and ipv6: -->
    <!--
    <listen_host>::1</listen_host>
    <listen_host>127.0.0.1</listen_host>
    -->
...
```

Сохраните файл и закройте его. Для применения новой конфигурации перезапустите службу, выполнив:

```
sudo service clickhouse-server restart
```

Вы не увидите вывод этой команды. Сервер ClickHouse прослушивает порт 8123 для HTTP-соединений и порт 9000 для соединений из clickhouse-client. Разрешите доступ к обоим портам для IP-адреса вашего сервера, где будет установлен ПК «КОМРАД» с помощью следующих команд:

```
sudo ufw allow from IP_адрес_ПК_КОМРАД/32 to any port 8123
sudo ufw allow from IP_адрес_ПК_КОМРАД/32 to any port 9000
```

Вы увидите вывод о добавлении роли для обеих команд, который показывает, что вы включили доступ к обоим портам.

3.2.4.4. Этап 2. Шаг 1. Начало

Скопируйте папку ***/komrad/astra*** с установочного носителя на узел, где будет работать ПК «КОМРАД».

3.2.4.5. Этап 2. Шаг 2. Установка Nmap

Перейдите в папку ***/tools*** и выполните команду**:**

```
sudo dpkg -i ./*.deb
```

3.2.4.6. Этап 2. Шаг 3. Установка ПК «КОМРАД»

Перейдите в папку с дистрибутивом ***/astra/deb*** и через терминал выполните команду:

```
sudo dpkg -i ./*.deb
```

3.2.4.7. Этап 2. Шаг 4. Редактирование yaml-файлов

Для работы с удаленной базой данных, необходимо в yaml файлах указать информацию по подключению к ней:

1) Откройте файл ***komrad-server.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-server/komrad-server.yaml
```

Отредактируйте:

```
cors:
  enabled: true #– параметр true разрешает доступ только для устройств, внесённых в список allowedorigins, в случае, если ваше устройство не находится в списке allowedorigins, то можете внести его в этот список самостоятельно. Параметр false разрешает доступ для всех устройств, список allowedorigins при этом не создает ограничений.
    # При возникновении ошибок с CORS возможный выход - небезопасная настройка `allowedorigins: ["*"]`
    # allowedorigins: ["*"]
    allowedorigins:
      - https://IP-адрес_БД #– укажите IP-адрес сервера БД
      - https://localhost:443
      - https://localhost:3400
      - http://localhost:8080
      - https://localhost
      - https://localhost:3400
      # Сервис komrad-s3 раздаёт отчёты, изображения и должен быть упомянут в разрешённых источниках CORS
      - https://localhost:9050
      # - https://komrad-s3.enterprise.lan:9000
      # - https://komrad.enterprise.lan:443
secure:
    # Список FQDN от которых разрешены запросы, если список пустой - запросы со всех
    # хостов будут приниматься.
    AllowedHosts:
```

```
      - IP-адрес_БД #– укажите IP-адрес сервера БД
      - localhost
      - localhost:3400
      - localhost:443
      - localhost:8080
      - localhost
      - localhost:443
      - komrad.enterprise.lan
database:
pg:
  db: komrad-preferences
  host: IP-адрес_БД #– укажите IP-адрес сервера БД
  password: pass #– укажите пароль пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres
monitoring:
  http:
    dbpreferences:
      url: IP-адрес_БД:5432 #– укажите IP-адрес сервера БД
      interval: 10s
    dbevents:
      url: IP-адрес_БД:9000 #– укажите IP-адрес сервера БД
      interval: 10s
```

2) Откройте файл ***correlation-dispatcher.yaml***, выполнив***:***

```
sudo nano /etc/echelon/komrad/correlation-dispatcher/correlation-dispatcher.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@IP-адрес_БД:5432/komrad-preferences?sslmode...
CorrelatorController:
  # Настройка подключения к БД PostgreSQL в формате URL для корреляторов.
  CorrelatorDB:postgres://postgres:pass@IP-адрес_БД:5432/komrad-preferences?sslmode...
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

3) Откройте файл ***incident-manager.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/incident-manager/incident-manager.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@IP-адрес_БД:5432/komrad-preferences?sslmode...
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

4) Откройте файл ***komrad-processor.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-processor/komrad-processor.yaml
```

Отредактируйте:

```
# Настройки подключения к бд хранящей конфигурацию виджетов
widgetsdb:
  TLSCertPath: /var/lib/echelon/komrad/certs/client.pem
  TLSKeyPath: /var/lib/echelon/komrad/certs/client-key.pem
  TLSRootCAPath: /var/lib/echelon/komrad/certs/ca.pem
  db: komrad-preferences
  host: IP-адрес_БД
  password: pass # укажите пароль пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres
# Настройки хранилища событий информационной безопасности
storage:
  # Тип хранилища, в данной версии поддерживается только:
  # - timescale - PostgreSQL 12+ с плагином TimescaleDB 2.2.1+
  # - clickhouse - ClickHouse v21.7.8.58-stable
  # Для ОС "Основа" поддерживается PostgreSQL 11 с TimescaleDB 2.2.1
  kind: clickhouse
  clickhouse:
    # Название БД
```

```
    name: komrad_events
    user: komrad
    password: pass # укажите пароль пользователя komrad (ClickHouse)
    # Адрес хоста с ClickHouse-server
    host: IP-адрес_БД
    # Порт ClickHouse-server
    port: 9000
    # Режим работы - с TLS или без
    sslmode: disable
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароли.

5) Откройте файл ***pauth-server.yaml*** выполнив:

```
sudo nano /etc/echelon/komrad/pauth-server/pauth-server.yaml
```

Отредактируйте:

```
database: postgres://postgres:pass@IP-адрес_БД:5432/pauth-preferences?sslmode...
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

6) Откройте ***komrad-scanner-config.json***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-scanner/komrad-scanner-config.json
```

Отредактируйте:

```
"Main": {
      "Driver": "postgres",
      "Host": "IP-адрес_БД ",
      "Port": 5432,
      "DBName": "scanner",
      "User": "postgres",
      "Password": "pass",
      "SSLMode": "disable"
            }
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

3.2.4.8. Этап 2. Шаг 5. Перезапуск служб

Перезагрузите службы, выполнив:

```
sudo systemctl restart komrad-server komrad-processor komrad-scanner pauth-server correlation-dispatcher incident-manager
```

3.2.4.9. Этап 2. Шаг 6. Создание ролей администратора и пользователя с правами администратора

Создайте роль администратора и пользователя с правами администратора.

Внимание! Все команды пишутся в одну строчку.

```
sudo pauthctl role add admin --conn postgresql://postgres:pass@IP-адрес_БД:5432/pauth-preferences
```

О успешном добавлении роли admin в строке сервиса будет строка:

INFO roles added {"role_names": ["admin"], "status": "success"}

```
sudo pauthctl role add user --conn postgresql://postgres:pass@IP-адрес_БД:5432/pauth-preferences
```

О успешном добавлении роли user в строке сервиса будет строка:

INFO roles added {"role_names": ["user"], "status": "success"}

```
sudo pauthctl user add --email name@domain.com --login admin --roles admin --password admin --conn postgresql://postgres:pass@IP-адрес_БД:5432/pauth-preferences
```

Где:

1) IP-адрес_БД – IP-адрес БД;

2) pass – укажите пароль пользователя postgres (PostgreSQL);

3) --e-mail name@domain.com – укажите свой e-mail адрес администратора;

4) --login admin – укажите свой логин администратора;

5) --password admin – укажите свой пароль администратора.

3.2.4.10. Этап 2. Шаг 7. Перенос лицензии

1) Удалите установочную demo-лицензию из папки ***/etc/echelon/komrad/license:***

```
sudo rm /etc/echelon/komrad/license/license.lic
```

2) Скопируйте в папку ***/etc/echelon/komrad/license*** файл лицензии с расширением (***.lic***).

3) Перезапустите сервисы komrad-server, komrad-processor, pauth-server:

```
sudo systemctl restart komrad-server komrad-processor pauth-server
```

3.2.4.11. Этап 2. Шаг 8. Создание сертификатов

Внимание! Дальнейшие действия желательно выполнять на отдельной ЭВМ, где в дальнейшем будут храниться корневые сертификаты, необходимые для корректной работы компонентов ПК «КОМРАД».

Создание сертификатов:

1) создайте на жестком диске папку ***tls***, выполнив:

```
mkdir tls
```

2) перейдите в папку ***/tls***:

```
cd tls
```

3) выполните команду для создания корневого сертификата:

```
echelontls ca --organization “Echelon”
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***ca.pem*** и ***ca-key.pem.***

4) создайте серверный сертификат, выполнив:

```
echelontls cert --organization “Echelon” localhost 127.0.0.1 $(hostname -I) $(hostname)
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***server.pem*** и ***server-key.pem***

5) создайте клиентский сертификат, выполнив:

```
echelontls cert --client
```

В папке ***/tls*** сгенерируются два файла ***client.pem*** и ***client-key.pem***

6) создайте сертификат для браузера, выполнив:

```
echelontls browser
```

В папке ***/tls*** сгенерируется файл ***client-browser.p12***.

Внимание! При генерации сертификата для браузера, утилита komradtls попросит задать пароль. Этот пароль потребуется при добавлении сертификата в браузер. Запомните этот пароль.

3.2.4.12. Этап 2. Шаг 9. Удаление сертификатов по умолчанию

Удалите все сертификаты из папки с сертификатами по умолчанию:

```
sudo rm /var/lib/echelon/komrad/certs/CAs/*
```

```
sudo rm /var/lib/echelon/komrad/certs/*
```

3.2.4.13. Этап 2. Шаг 10. Копирование сертификатов

Скопируйте сертификаты в следующие папки:

1) файлы ***ca.pem, server.pem, server-key.pem, client.pem, client-key.pem*** в ***/var/lib/echelon/komrad/certs/*** командой:

```
sudo cp ca.pem server.pem server-key.pem client.pem client-key.pem /var/lib/echelon/komrad/certs/
```

Внимание! Команда выполняется в одну строчку.

2) файл ***ca.pem*** в ***/var/lib/echelon/komrad/certs/CAs*** командой:

```
sudo cp ca.pem /var/lib/echelon/komrad/certs/CAs
```

3.2.4.14. Этап 2. Шаг 11. Изменение владельца файлов на komrad:komrad и предоставление прав сертификатам

На машине с ПК «КОМРАД» введите в терминале:

```
sudo chown komrad:komrad  /etc/echelon/komrad/license/имя_лицензии.lic
sudo chown -R komrad:komrad  /var/lib/echelon/komrad/certs
sudo chmod -R 755 /var/lib/echelon/komrad/certs
sudo chmod 0640 /var/lib/echelon/komrad/certs/server-key.pem
sudo chown root:komrad /var/lib/echelon/komrad/certs/server-key.pem
sudo usermod -a -G komrad postgres
sudo chmod 755 client-browser.p12
```

Где в имя_лицензии – укажите наименование файла лицензии.

3.2.4.15. Этап 2. Шаг 12. Изменение владельца файлов на postgres:postgres

На машине с БД создайте папку:

```
sudo mkdir -p /var/lib/echelon/komrad/certs
```

Далее перенесите сгенерированные сертификаты ***ca.pem***, ***server-key.pem***, ***server.pem*** в папку ***/var/lib/echelon/komrad/certs***.

На машине с БД введите в терминале:

```
sudo chown -R postgres:postgres /var/lib/echelon/komrad/certs
sudo chmod -R 755 /var/lib/echelon/komrad/certs
sudo chmod 0640 /var/lib/echelon/komrad/certs/server-key.pem
sudo chown root:postgres /var/lib/echelon/komrad/certs/server-key.pem
sudo usermod -a -G postgres postgres
```

```
sudo chmod 755 client-browser.p12
```

Проверьте наличие указанных путей до сертификатов в файле ***postgresql.conf***.

Для открытия файла введите:

```
sudo nano /etc/postgresql/9.6/main/postgresql.conf
```

Раскомментируйте и добавьте пути до сертификатов:

```
ssl = on
ssl_ca_file = '/var/lib/echelon/komrad/certs/ca.pem'
ssl_key_file = '/var/lib/echelon/komrad/certs/server-key.pem'
ssl_cert_file = '/var/lib/echelon/komrad/certs/server.pem'
```

3.2.4.16. Этап 2. Шаг 13. Перезапуск сервисов

Перезагрузите системы.

3.2.4.17. Этап 2. Шаг 14. Установка корневых сертификатов в браузере

Выполните следующие действия:

1) откройте **Firefox → Настройки → Приватность и защита → Сертификаты → Просмотр сертификатов**;

2) перейдите во вкладку **Ваши сертификаты** меню **Управления сертификатами;**

3) импортируйте сертификаты ***ca.pem*** в «Доверенные корневые центры сертификации» и ***client-browser.p12*** в «Личные», при этом потребуется указать пароль установленный, при генерации браузерного сертификата в Шаге 8, этапа 2;

4) перезагрузите браузер.

3.2.4.18. Этап 2. Шаг 15. Конец

ПК «КОМРАД» установлен и доступен по адресу https://localhost.

Для работы ПК «КОМРАД» на ОС Astra Linux Special Edition в режиме замкнутой программной среды (ЗПС) после установки по основной инструкции нужно:

1) скопировать файл открытого ключа:

```
sudo cp astra_echelon_pub_key.gpg /etc/digsig/keys/
```

2) открыть файл конфигурации:

```
sudo nano /etc/digsig/digsig_initramfs.conf
```

3) включить политику ЗПС:

```
DIGSIG_ELF_MODE=1
```

4) выполнить:

```
sudo update-initramfs -u -k all
```

5) перезагрузить систему (после перезагрузки система загрузится уже в режиме ЗПС).

3.3. Установка на ОСОН «ОСнова», версия 2

В ПК «КОМРАД» в зависимости от типа лицензии возможны следующие варианты установок:

– все компоненты на одном узел;

– компоненты ПК «КОМРАД» на одном узле, СУБД PostgreSQL и ClickHouse на отдельном узле;

– территориально-распределенная установка (при выборе этого вида установки обратитесь в тех. поддержку).

3.3.1. Поставляемые компоненты

Дистрибутив ПК «КОМРАД» представлен в таблице 9.

Таблица 9 – Дистрибутив ПК «КОМРАД»

Название компонента	Папка	Описание
clickhouse-client_21.11.1_all_signed.deb clickhouse-client_21.11.1_all_signed.deb.asc clickhouse-common-static_21.11.1_amd64_signed.deb clickhouse-common-static_21.11.1_amd64_signed.deb.asc clickhouse-server_21.11.1_all_signed.deb clickhouse-server_21.11.1_all_signed.deb.asc	/osnova/db/clickhouse	СУБД Clickhouse
correlation-dispatcher_v4.1.33_amd64.deb correlation-dispatcher_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для управления коррелляторами
echelontls_v4.1.33_amd64.deb echelontls_v4.1.33_amd64.deb.asc	/osnova/deb	Утилита генерации сертификатов
file-collector_v4.1.33_amd64.deb file-collector_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для сбора событий из файлов
incident-manager_v4.1.33_amd64.deb incident-manager_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для управления инцидентами
komrad-backup_v4.1.33_amd64.deb	/osnova/deb	Модуль предназначен

Название компонента	Папка	Описание
komrad-backup_v4.1.33_amd64.deb.asc		для управления резервным копированием и восстановлением
komrad-bus_v4.1.33_amd64.deb komrad-bus_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для передачи событий и прочей информации между подсистемами ПК «КОМРАД»
komrad-cli_v4.1.33_amd64.deb komrad-cli_v4.1.33_amd64.deb.asc	/osnova/deb	Консольный интерфейс
komrad-correlator_v4.1.33_amd64.deb komrad-correlator_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для управления коррелляторами
komrad-processor_v4.1.33_amd64.deb komrad-processor_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для обогащения, фильтрации и индексации событий безопасности
komrad-reactor-cef_v4.1.33_amd64.deb komrad-reactor-cef_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для запуска скриптов реагирования на инцидент в формате CEF
komrad-reactor_v4.1.33_amd64.deb komrad-reactor_v4.1.33_amd64.deb	/osnova/deb	Модуль предназначен для запуска скриптов реагирования на инцидент
komrad-s3_v4.1.34_amd64.deb komrad-s3_v4.1.34_amd64.deb.asc	/osnova/deb	Модуль предназначен для создания объектового хранилища системы

Название компонента	Папка	Описание
		резервного копирования и восстановления
komrad-scanner_v4.1.33_amd64.deb komrad-scanner_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для управления активами
komrad-server_v4.1.33_amd64.deb komrad-server_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для агрегирования действий других подсистем и маршрутизации уведомлений
komrad-vault_v4.1.33_amd64.deb komrad-vault_v4.1.33_amd64.deb.asc	/osnova/deb	Подсистема предназначена для управления выпущенными сертификатами
pauth-server_v4.1.33_amd64.deb pauth-server_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для управления доступом к функционалу программного комплекса
pauthctl_v4.1.33_amd64.deb pauthctl_v4.1.33_amd64.deb.asc	/osnova/deb	Утилита для работы с пользователями в командной строке
snmp-collector_v4.1.34_amd64.deb snmp-collector_v4.1.34_amd64.deb.asc	/osnova/deb	Модуль предназначен для сбора событий по SNMP
sql-collector_v4.1.33_amd64.deb sql-collector_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для сбора событий из СУБД
sqlx-collector_v4.1.33_amd64.deb sqlx-collector_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для сбора событий из

Название компонента	Папка	Описание
		СУБД
syslog-collector_v4.1.33_amd64.deb syslog-collector_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для сбора событий по Syslog
xflow-collector_v4.1.33_amd64.deb xflow-collector_v4.1.33_amd64.deb.asc	/osnova/deb	Модуль предназначен для сбора событий sFlow и NetFlow
echelon.der	/osnova/keys	Открытый ключ для проверки подлинности
syslog_collector_root.sh	/osnova/scripts	Скрипт для syslog-collector
nmap.deb nmap.deb.asc	/osnova/tools	Сканер сети
komrad-cli.exe komrad-cli.exe.asc	/osnova/windows/gossopka	Консольный интерфейс
sql-collector.exe sql-collector.exe.asc sql-collector.yaml sql-collector.yaml.asc	/osnova/windows/sql-collector	Модуль предназначен для сбора событий из СУБД из Windows
wmi-agent.exe wmi-agent.exe.asc wmi-agent.yaml wmi-agent.yaml.asc	/osnova/windows/wmi-agent	Модуль предназначен для сбора событий по WMI

3.3.2. Аппаратные требования

В таблице 10 приведены ориентировочные значения технических данных аппаратной платформы.

Таблица 10 – Требования к аппаратной платформе

Тип лицензии	CPU	RAM	SSD\HDD
Base	Минимум – 2 ядра Рекомендовано – от 2-х ядер	Минимум – 2 Гб Рекомендовано – 4 Гб	От 100 Гб

Тип лицензии	CPU	RAM	SSD\HDD
All-in-One	Минимум – 2 ядра Рекомендовано – 4 ядра	Минимум – 8 Гб Рекомендовано – 16 Гб	От 1 Тб
Enterprise	Минимум – 4 ядра Рекомендовано – 8 ядра	Минимум – 32 Гб Рекомендовано – 128 Гб	От 10 Тб

При выборе аппаратной части необходимо провести консультацию с техническим специалистом для предварительной оценки и рекомендаций при выборе аппаратной части.

Увеличение количества источников и\или увеличение количества событий от существующих источников повлечёт за собой увеличение ресурсов.

3.3.3. Установка всех компонентов на один узел

Поддерживаемые лицензии: Base, All-in-One, Enterprise.

Установка ПК «КОМРАД» должна производиться без включённой (выключенной) функцией создания ЗПС.

Внимание! Для установки ПК «КОМРАД» на ОСОН «ОСнова» необходимы наличие:

– доступ к репозиторию;

– ОСОН «ОСнова», версия 2;

Для работы ПК «КОМРАД» на ОСОН «ОСнова» в режиме замкнутой программной среды (ЗПС) после установки по основной инструкции нужно:

1) скопировать файл открытого ключа:

```
sudo cp echelon.der /etc/ima/certs/
```

2) включить политику ЗПС:

```
sudo rm /etc/ima/policy
sudo ln -s /etc/ima/policy.d/appraise /etc/ima/policy
sudo update-initramfs -u -k all
```

3) перезагрузить систему (после перезагрузки система загрузится уже в режиме ЗПС):

```
sudo reboot
```

Совет! Для выхода из режима ЗПС выполните команды:

```
sudo rm /etc/ima/policy
sudo ln -s /etc/ima/policy.d/empty /etc/ima/policy
sudo update-initramfs -u -k all
sudo reboot
```

3.3.3.1. Шаг 1. Установка и настройка PostgreSQL 11 и Clickhouse

1) Установите и настройте PostgreSQL 11, выполнив команду в терминале:

```
sudo apt install postgresql -y
```

2) Перейдите в папку с дистрибутивом ***/osnova/db/clickhouse/*** и в терминале введите:

```
sudo dpkg -i ./*.deb
```

Укажите пароль для пользователя «default».

3) Запустите ClickHouse командой в терминале:

```
sudo service clickhouse-server start
```

4) Создайте пароль для ClickHouse командой в терминале, указав вместо `pass` ваш пароль:

Внимание! Команда пишется в одну строчку:

```
echo "pass"; echo -n "pass" | sha256sum | tr -d '-'
```

В первой строке результата – пароль (`pass`). Вторая строка – соответствующий ему хэш SHA256 (`pass_SHA256`).

5) Создайте и откройте на редактирование файл:

```
sudo nano /etc/clickhouse-server/users.d/komrad.xml
```

Заполните содержимое файла следующим фрагментом:

```
<yandex>
    <users>
        <komrad>
            <password remove='1' />
            <password_sha256_hex>pass_SHA256</password_sha256_hex>
        </komrad>
    </users>
</yandex>
```

Где вместо `pass_SHA256` вставьте сгенерированный хэш, соответствующий вашему паролю.

6) Откройте файл, выполнив:

```
sudo nano /etc/clickhouse-server/users.xml
```

Добавьте пользователя komrad в группу пользователей, для чего приведите фрагмент файла к виду:

```
<!-- Users and ACL. -->
<users>
    <komrad>
            <access_management>1</access_management>
            <password></password>
    </komrad>
    <!-- If user name was not specified, 'default' user is used. -->
    <default>
```

7) Перезапустите сервер ClickHouse, выполнив:

```
sudo systemctl restart clickhouse-server.service
```

3.3.3.2. Шаг 2. Задание прав пользователя на создание баз данных и создание базы данных

1) Чтобы создать нового пользователя, откройте аккаунт стандартного пользователя:

```
sudo su - postgres
```

2) Наделите пользователя правами на создание новых баз данных, где вместо `pass` – установите пароль для пользователя postgres:

```
psql -c "ALTER USER postgres WITH CREATEDB LOGIN PASSWORD 'pass';"
```

3) Установите расширение, выполнив:

```
psql -c "CREATE EXTENSION pg_trgm;"
```

4) Создайте базы данных, выполнив:

```
createdb -O postgres komrad-preferences
createdb -O postgres pauth-preferences
createdb -O postgres scanner
exit
```

5) Запустите клиент ClickHouse, используя данные пользователя komrad, где вместо `pass` – укажите пароль, заданный в шаге 1 при установке ClickHouse:

```
clickhouse-client --user=komrad --password=pass
```

6) Создайте базу данных, выполнив:

```
CREATE DATABASE komrad_events
```

```
exit
```

3.3.3.3. Шаг 3. Установка модуль сканирования сети Nmap

Перейдите в папку с утилитами ***/osnova/tools*** и через терминал выполните команду:

```
sudo dpkg -i ./*.deb
```

3.3.3.4. Шаг 4. Установка ПК «КОМРАД»

Перейдите в папку с дистрибутивом ***/osnova/deb*** и через терминал выполните команду:

```
sudo dpkg -i ./*.deb
```

3.3.3.5. Шаг 5. Редактирование yaml-файлов

1) Откройте файл ***komrad-processor.yaml***, выполнив через команду в терминале:

```
sudo nano /etc/echelon/komrad/komrad-processor/komrad-processor.yaml
```

Приведите фрагмент файла к данному виду:

```
# Настройки подключения к бд хранящей конфигурацию виджетов
widgetsdb:
  TLSCertPath: /var/lib/echelon/komrad/certs/client.pem
  TLSKeyPath: /var/lib/echelon/komrad/certs/client-key.pem
  TLSRootCAPath: /var/lib/echelon/komrad/certs/ca.pem
  db: komrad-preferences
  host: localhost
  password: pass # укажите пароль для пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres

# Настройки хранилища событий информационной безопасности
storage:
  # Тип хранилища, в данной версии поддерживается только:
  # - timescale - PostgreSQL 12+ с плагином TimescaleDB 2.2.1+
  # - clickhouse - ClickHouse v21.7.8.58-stable
  # Для ОС "Основа" поддерживается PostgreSQL 11 с TimescaleDB 2.2.1
  kind: clickhouse
  clickhouse:
```

```
    # Название БД
    name: komrad_events
    user: komrad
    password: pass # укажите пароль для пользователя komrad (ClickHouse)
    # Адрес хоста с ClickHouse-server
    host: localhost
    # Порт ClickHouse-server
    port: 9000
    # Режим работы - с TLS или без
    sslmode: disable
```

2) Откройте файл ***komrad-server.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-server/komrad-server.yaml
```

Отредактируйте:

```
database:
pg:
  db: komrad-preferences
  host: localhost
  password: pass # укажите пароль для пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres
```

3) Откройте файл ***correlation-dispatcher.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/correlation-dispatcher/correlation-dispatcher.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@localhost:5432/komrad-preferences?sslmode...
CorrelatorController:
  # Настройка подключения к БД PostgreSQL в формате URL для коррелляторов.
  CorrelatorDB:postgres://postgres:pass@localhost:5432/komrad-preferences?sslmode...
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

4) Откройте файл ***incident-manager.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/incident-manager/incident-manager.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@localhost:5432/komrad-preferences?sslmode...
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

5) Откройте файл ***pauth-server.yaml*** выполнив:

```
sudo nano /etc/echelon/komrad/pauth-server/pauth-server.yaml
```

Отредактируйте:

```
database: postgres://postgres:pass@localhost:5432/pauth-preferences?sslmode...
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

6) Откройте ***komrad-scanner-config.json***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-scanner/komrad-scanner-config.json
```

Отредактируйте:

```
"Main": {
      "Driver": "postgres",
      "Host": "localhost",
      "Port": 5432,
      "DBName": "scanner",
      "User": "postgres",
      "Password": "pass",
      "SSLMode": "disable"
            }
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

7) Откройте ***postgresql.conf***, выполнив:

```
sudo nano /etc/postgresql/11/main/postgresql.conf
```

8) Раскомментируйте и добавьте пути до сертификатов:

```
ssl = on
ssl_ca_file = '/var/lib/echelon/komrad/certs/ca.pem'
ssl_key_file = '/var/lib/echelon/komrad/certs/server-key.pem'
ssl_cert_file = '/var/lib/echelon/komrad/certs/server.pem'
```

9) Перезагрузите сервисы, выполнив команду в одну строчку:

```
sudo systemctl restart postgresql komrad-server komrad-processor komrad-scanner pauth-server correlation-dispatcher incident-manager
```

3.3.3.6. Шаг 6. Создание ролей администратора и пользователя с правами администратора

Создайте роль администратора и пользователя с правами администратора через команды в терминале.

Внимание! Каждая отдельная команда пишется одну строчку:

```
sudo pauthctl role add admin --migrate --conn "postgresql://postgres:pass@localhost:5432/pauth-preferences"
```

О успешном добавлении роли `admin` в строке сервиса будет строка:

```
INFO roles added {"role_names": ["admin"], "status": "success"}
```

```
sudo pauthctl role add user --conn "postgresql://postgres:pass@localhost:5432/pauth-preferences"
```

О успешном добавлении роли `user` в строке сервиса будет строка:

```
INFO roles added {"role_names": ["user"], "status": "success"}
```

```
sudo pauthctl user add --email name@domain.com --login admin --roles admin --password admin --conn "postgresql://postgres:pass@localhost:5432/pauth-preferences"
```

Где:

1) `pass` – укажите пароль пользователя postgres (PostgreSQL);

2) `--e-mail name@domain.com` – укажите свой e-mail адрес администратора;

3) `--login admin` – укажите свой логин администратора;

4) `--password admin` – укажите свой пароль администратора.

3.3.3.7. Шаг 7. Перенос лицензии

1) Удалите демо-лицензию из папки ***/etc/echelon/komrad/license*** командой в терминале:

```
sudo rm /etc/echelon/komrad/license/license.lic
```

2) Скопируйте в папку ***/etc/echelon/komrad/license*** файл лицензии с расширением (***.lic***).

3) Перезапустите сервисы komrad-server, komrad-processor, pauth-server командой в терминале:

```
sudo systemctl restart komrad-server komrad-processor pauth-server
```

3.3.3.8. Шаг 8. Создание сертификатов

Внимание! Дальнейшие действия желательно выполнять на отдельной ЭВМ, где в дальнейшем будут храниться корневые сертификаты, необходимые для корректной работы компонентов ПК «КОМРАД».

Создание сертификатов:

1) создайте на жестком диске папку ***/tls***;

Совет! Команда для создания папки:

```
mkdir tls
```

2) перейдите в папку ***/tls*** и выполните команду в терминале для создания корневого сертификата:

```
cd tls
echelontls ca --organization “Echelon”
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***ca.pem*** и ***ca-key.pem.***

3) создайте серверный сертификат командой в терминале:

```
echelontls cert --organization “Echelon” localhost 127.0.0.1 $(hostname -I) $(hostname)
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***server.pem*** и ***server-key.pem***

4) создайте клиентский сертификат командой в терминале:

```
echelontls cert --client
```

В папке ***/tls*** сгенерируются два файла ***client.pem*** и ***client-key.pem***

5) создайте сертификат для браузера командой в терминале:

```
echelontls browser
```

Внимание! При генерации сертификата для браузера, утилита komradtls попросит задать пароль. Этот пароль потребуется при добавлении сертификата в браузер, поэтому запомните этот пароль.

В папке ***/tls*** сгенерируется файл ***client-browser.p12***.

3.3.3.9. Шаг 9. Удаление сертификатов по умолчанию

Удалите все сертификаты из папки с сертификатами по умолчанию командой в терминале:

```
sudo rm /var/lib/echelon/komrad/certs/CAs/*
sudo rm /var/lib/echelon/komrad/certs/*
```

3.3.3.10. Шаг 10. Копирование сертификатов

Скопируйте сертификаты в следующие папки:

1) файлы ***ca.pem***, ***server.pem***, ***server-key.pem,*** ***client.pem,*** ***client-key.pem*** в ***/var/lib/echelon/komrad/komrad-server/certs/*** командой терминале:

```
sudo cp ca.pem server.pem server-key.pem client.pem client-key.pem /var/lib/echelon/komrad/certs/
```

Внимание! Команда выполняется в одну строчку.

2) файл ***ca.pem*** в ***/var/lib/echelon/komrad/certs/CAs/*** командой:

```
sudo cp ca.pem /var/lib/echelon/komrad/certs/CAs/
```

3.3.3.11. Шаг 11. Изменение владельца файлов на komrad:komrad и предоставление прав сертификатам

Введите команды в терминале:

```
sudo chown komrad:komrad  /etc/echelon/komrad/license/имя_лицензии.lic
sudo chown -R komrad:komrad  /var/lib/echelon/komrad/certs
sudo chmod -R 755 /var/lib/echelon/komrad/certs
sudo chmod 0640 /var/lib/echelon/komrad/certs/server-key.pem
sudo chown root:komrad /var/lib/echelon/komrad/certs/server-key.pem
sudo usermod -a -G komrad postgres
sudo chmod 755 client-browser.p12
```

Где в имя_лицензии – укажите наименование файла лицензии.

3.3.3.12. Шаг 12. Перезапуск сервисов

Перезагрузите систему.

3.3.3.13. Шаг 13. Установка корневого и браузерного сертификатов в браузере

Выполните следующие действия:

1) откройте **Firefox → Настройки → Приватность и защита → Сертификаты → Просмотр сертификатов**;

2) перейдите во вкладку **Ваши сертификаты** меню **Управления сертификатами;**

3) импортируйте сертификаты ***ca.pem*** в «Доверенные корневые центры сертификации» и ***client-browser.p12*** в «Личные», при этом потребуется указать пароль установленный, при генерации браузерного сертификата в Шаге 8;

4) перезагрузите браузер.

3.3.3.14. Шаг 14. Конец

ПК «КОМРАД» установлен и доступен по адресу https://localhost.

3.3.4. Установка компонентов ПК «КОМРАД» на одном узле, СУБД PostgreSQL и ClickHouse на другом

Поддерживаемые лицензии: Base, All-in-One, Enterprise.

Установка ПК «КОМРАД» будет состоять из двух этапов:

– на первом этапе установка и настройка PostgreSQL 11 и ClickHouse;

– на втором этапе установка и настройка ПК «КОМРАД».

Внимание! Для установки ПК «КОМРАД» на ОСОН «ОСнова» необходимы наличие:

– доступ к репозиторию;

– ОСОН «ОСнова», версия 2.

Установка ПК «КОМРАД» должна производиться без включённой (выключенной) функцией создания ЗПС.

Для работы ПК «КОМРАД» на ОСОН «ОСнова» в режиме замкнутой программной среды (ЗПС) после установки по основной инструкции нужно:

1) скопировать файл открытого ключа:

```
sudo cp echelon.der /etc/ima/certs/
```

2) включить политику ЗПС:

```
sudo rm /etc/ima/policy
sudo ln -s /etc/ima/policy.d/appraise /etc/ima/policy
sudo update-initramfs -u -k all
```

3) перезагрузить систему (после перезагрузки система загрузится уже в режиме ЗПС):

```
sudo reboot
```

Совет! Для выхода из режима ЗПС выполните команды:

```
sudo rm /etc/ima/policy
sudo ln -s /etc/ima/policy.d/empty /etc/ima/policy
sudo update-initramfs -u -k all
sudo reboot
```

3.3.4.1. Этап 1. Шаг 1. Установка и настройка PostgreSQL 11 и Clickhouse

На узле, где будут находиться PostgreSQL 11 и Clickhouse:

1) Установите и настройте PostgreSQL 11, выполнив команду в терминале:

```
sudo apt install postgresql -y
```

2) Перейдите в папку с дистрибутивом ***/osnova/db/clickhouse/*** и в терминале введите:

```
sudo dpkg -i ./*.deb
```

Укажите пароль для пользователя «default».

3) Запустите ClickHouse командой в терминале:

```
sudo service clickhouse-server start
```

4) Создайте пароль для ClickHouse командой в терминале, указав вместо `pass` ваш пароль:

Внимание! Команда пишется в одну строчку:

```
echo "pass"; echo -n "pass" | sha256sum | tr -d '-'
```

В первой строке результата – пароль (pass). Вторая строка – соответствующий ему хэш SHA256 (pass_SHA256).

5) Создайте и откройте на редактирование файл:

```
sudo nano /etc/clickhouse-server/users.d/komrad.xml
```

Заполните содержимое файла следующим фрагментом:

```
<yandex>
    <users>
        <komrad>
            <password remove='1' />
            <password_sha256_hex>pass_SHA256</password_sha256_hex>
        </komrad>
    </users>
</yandex>
```

Где вместо pass_SHA256 вставьте сгенерированный хэш, соответствующий вашему паролю.

6) Откройте файл, выполнив:

```
sudo nano /etc/clickhouse-server/users.xml
```

Добавьте пользователя komrad в группу пользователей, для чего приведите фрагмент файла к виду:

```
    <!-- Users and ACL. -->
    <users>
        <komrad>
                <access_management>1</access_management>
                <password></password>
        </komrad>
        <!-- If user name was not specified, 'default' user is used. -->
        <default>
```

7) Перезапустите сервер ClickHouse, выполнив:

```
sudo systemctl restart clickhouse-server.service
```

3.3.4.2. Этап1. Шаг 2. Задание прав пользователя на создание баз данных и создание базы данных

1) Чтобы создать нового пользователя, откройте аккаунт стандартного пользователя:

```
sudo su - postgres
```

2) Наделите пользователя правами на создание новых баз данных, где вместо `pass` – установите пароль для пользователя postgres:

```
psql -c "ALTER USER postgres WITH CREATEDB LOGIN PASSWORD 'pass';"
```

3) Установите расширение, выполнив:

```
psql -c "CREATE EXTENSION pg_trgm;"
```

4) Создайте базы данных, выполнив:

```
createdb -O postgres komrad-preferences
createdb -O postgres pauth-preferences
createdb -O postgres scanner
exit
```

5) Запустите клиент ClickHouse, используя данные пользователя komrad, где вместо `pass` – укажите пароль, заданный в шаге 1 при установке ClickHouse:

```
clickhouse-client --user=komrad --password=pass
```

6) Создайте базу данных, выполнив:

```
CREATE DATABASE komrad_events
exit
```

3.3.4.3. Этап 1. Шаг 3. Настройка подключения к базам данных с удаленных узлов

По умолчанию, серверы баз данных разрешают подключение только с локального компьютера. Для подключения с удаленных систем необходимо отредактировать три файла ***postgresql.conf***, ***pg_hba.conf*** и ***config.xml***.

1) Откройте для редактирования файл ***postgresql.conf***, выполнив:

```
sudo nano /etc/postgresql/11/main/postgresql.conf
```

Затем раскомментируйте строку, содержащую `# listen_addresses = `localhost``, убрав # перед строкой, и отредактируйте, чтобы получилось, как в следующем файле:

```
#------------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
```

```
#------------------------------------------------------------------

# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to listen on;
                                # comma-separated list of addresses;
                                # defaults to 'localhost'; use '*' for all
                                # (change requires restart)
```

Совет! В данном примере мы разрешили прослушивание запросов на всех IP-адресах (*), но, если требуется более безопасная настройка, можно перечислить последние через пробел.

Например: `listen_addresses = ` 192.168.0.15 10.10.0.16 `.`

Сохраните файл и закройте его.

2) Откройте для редактирования файл ***pg_hba.conf***, выполнив:

```
sudo nano /etc/postgresql/11/main/pg_hba.conf
```

После последней строки файла с новой строки добавить:

```
host    all     postgres    IP-адрес_ПК_КОМРАД/32    md5
```

Где IP-адрес_ПК_КОМРАД – IP-адрес хоста, с которого будет подключение.

Сохраните файл и закройте его, после чего перезапустите службу, выполнив:

```
sudo systemctl restart postgresql
```

3) Откройте для редактирования файл ***config.xml***, выполнив:

```
sudo nano /etc/clickhouse-server/config.xml
```

Затем раскомментируйте строку, содержащую <!-- <listen_host>0.0.0.0</listen_host> -->, как в следующем файле:

```
...
 <interserver_http_host>example.yandex.ru</interserver_http_host>
    -->

    <!-- Listen specified host. use :: (wildcard IPv6 address), if you want to
accept connections both with IPv4 and IPv6 from everywhere. -->
    <!-- <listen_host>::</listen_host> -->
    <!-- Same for hosts with disabled ipv6: -->
    <listen_host>0.0.0.0</listen_host>
```

```
    <!-- Default values - try listen localhost on ipv4 and ipv6: -->
    <!--
    <listen_host>::1</listen_host>
    <listen_host>127.0.0.1</listen_host>
    -->
...
```

Сохраните файл и закройте его. Для применения новой конфигурации перезапустите службу, выполнив:

```
sudo service clickhouse-server restart
```

Вы не увидите вывод этой команды. Сервер ClickHouse прослушивает порт 8123 для HTTP-соединений и порт 9000 для соединений из clickhouse-client. Разрешите доступ к обоим портам для IP-адреса вашего сервера, где будет установлен ПК «КОМРАД» с помощью следующих команд:

```
sudo ufw allow from IP_адрес_ПК_КОМРАД/32 to any port 8123
sudo ufw allow from IP_адрес_ПК_КОМРАД/32 to any port 9000
```

Вы увидите вывод о добавлении роли для обеих команд, который показывает, что вы включили доступ к обоим портам.

3.3.4.4. Этап 2. Шаг 1. Начало

Скопируйте папку ***/komrad/osnova*** с установочного носителя на узел, где будет работать ПК «КОМРАД».

3.3.4.5. Этап 2. Шаг 2. Установка Nmap

Перейдите в папку ***/tools*** и выполните команду**:**

```
sudo dpkg -i ./*.deb
```

3.3.4.6. Этап 2. Шаг 3. Установка ПК «КОМРАД»

Перейдите в папку с дистрибутивом ***/osnova/deb*** и через терминал выполните команду:

```
sudo dpkg -i ./*.deb
```

3.3.4.7. Этап 2. Шаг 4. Редактирование yaml-файлов

Для работы с удаленной базой данных, необходимо в yaml файлах указать информацию по подключению к ней:

1) Откройте файл ***komrad-server.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-server/komrad-server.yaml
```

Отредактируйте:

```
cors:
  enabled: true #– параметр true разрешает доступ только для устройств, внесённых в список allowedorigins, в случае, если ваше устройство не находится в списке allowedorigins, то можете внести его в этот список самостоятельно. Параметр false разрешает доступ для всех устройств, список allowedorigins при этом не создает ограничений.
    # При возникновении ошибок с CORS возможный выход - небезопасная настройка `allowedorigins: ["*"]`
    # allowedorigins: ["*"]
    allowedorigins:
      - https://IP-адрес_БД #– укажите IP-адрес сервера БД
      - https://localhost:443
      - https://localhost:3400
      - http://localhost:8080
      - https://localhost
      - https://localhost:3400
      # Сервис komrad-s3 раздаёт отчёты, изображения и должен быть упомянут в разрешённых источниках CORS
      - https://localhost:9050
      # - https://komrad-s3.enterprise.lan:9000
      # - https://komrad.enterprise.lan:443
secure:
   # Список FQDN от которых разрешены запросы, если список пустой - запросы со всех
   # хостов будут приниматься.
    AllowedHosts:
      - IP-адрес_БД #– укажите IP-адрес сервера БД
      - localhost
      - localhost:3400
      - localhost:443
      - localhost:8080
      - localhost
      - localhost:443
      - komrad.enterprise.lan
database:
pg:
  db: komrad-preferences
  host: IP-адрес_БД #– укажите IP-адрес сервера БД
```

```
  password: pass #– укажите пароль пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres
monitoring:
  http:
    dbpreferences:
      url: IP-адрес_БД:5432 #– укажите IP-адрес сервера БД
      interval: 10s
    dbevents:
      url: IP-адрес_БД:9000 #– укажите IP-адрес сервера БД
      interval: 10s
```

2) Откройте файл ***correlation-dispatcher.yaml***, выполнив***:***

```
sudo nano /etc/echelon/komrad/correlation-dispatcher/correlation-dispatcher.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@IP-адрес_БД:5432/komrad-preferences?sslmode...
CorrelatorController:
  # Настройка подключения к БД PostgreSQL в формате URL для коррелеторов.
  CorrelatorDB:postgres://postgres:pass@IP-адрес_БД:5432/komrad-
preferences?sslmode...
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

3) Откройте файл ***incident-manager.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/incident-manager/incident-manager.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@IP-адрес_БД:5432/komrad-preferences?sslmode...
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

4) Откройте файл ***komrad-processor.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-processor/komrad-processor.yaml
```

Отредактируйте:

```
# Настройки подключения к бд хранящей конфигурацию виджетов
widgetsdb:
  TLSCertPath: /var/lib/echelon/komrad/certs/client.pem
  TLSKeyPath: /var/lib/echelon/komrad/certs/client-key.pem
  TLSRootCAPath: /var/lib/echelon/komrad/certs/ca.pem
  db: komrad-preferences
  host: IP-адрес_БД
  password: pass # укажите пароль пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres
# Настройки хранилища событий информационной безопасности
storage:
  # Тип хранилища, в данной версии поддерживается только:
  # - timescale - PostgreSQL 12+ с плагином TimescaleDB 2.2.1+
  # - clickhouse - ClickHouse v21.7.8.58-stable
  # Для ОС "Основа" поддерживается PostgreSQL 11 с TimescaleDB 2.2.1
  kind: clickhouse
  clickhouse:
    # Название БД
    name: komrad_events
    user: komrad
    password: pass # укажите пароль пользователя komrad (ClickHouse)
    # Адрес хоста с ClickHouse-server
    host: IP-адрес_БД
    # Порт ClickHouse-server
    port: 9000
    # Режим работы - с TLS или без
    sslmode: disable
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароли.

5) Откройте файл ***pauth-server.yaml*** выполнив:

```
sudo nano /etc/echelon/komrad/pauth-server/pauth-server.yaml
```

Отредактируйте:

```
database: postgres://postgres:pass@IP-адрес_БД:5432/pauth-preferences?sslmode...
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

6) Откройте ***komrad-scanner-config.json***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-scanner/komrad-scanner-config.json
```

Отредактируйте:

```
"Main": {
      "Driver": "postgres",
      "Host": "IP-адрес_БД ",
      "Port": 5432,
      "DBName": "scanner",
      "User": "postgres",
      "Password": "pass",
      "SSLMode": "disable"
            }
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

3.3.4.8. Этап 2. Шаг 5. Перезапуск служб

Перезагрузите службы, выполнив:

```
sudo systemctl restart komrad-server komrad-processor komrad-scanner
pauth-server correlation-dispatcher incident-manager
```

3.3.4.9. Этап 2. Шаг 6. Создание ролей администратора и пользователя с правами администратора

Создайте роль администратора и пользователя с правами администратора.

Внимание! Все команды пишутся в одну строчку.

```
sudo pauthctl role add admin --conn postgresql://postgres:pass@IP-адрес_БД:5432/pauth-preferences
```

О успешном добавлении роли `admin` в строке сервиса будет строка:

```
INFO  roles added  {"role_names": ["admin"], "status": "success"}
```

```
sudo pauthctl role add user --conn postgresql://postgres:pass@IP-адрес_БД:5432/pauth-preferences
```

О успешном добавлении роли `user` в строке сервиса будет строка:

```
INFO  roles added  {"role_names": ["user"], "status": "success"}
```

```
sudo pauthctl user add --email name@domain.com --login admin --roles admin --password admin --conn postgresql://postgres:pass@IP-адрес_БД:5432/pauth-preferences
```

Где:

1) `IP-адрес_БД` – IP-адрес БД;

2) `pass` – укажите пароль пользователя postgres (PostgreSQL);

3) `--e-mail name@domain.com` – укажите свой e-mail адрес администратора;

4) `--login admin` – укажите свой логин администратора;

5) `--password admin` – укажите свой пароль администратора.

3.3.4.10. Этап 2. Шаг 7. Перенос лицензии

1) Удалите установочную demo-лицензию из папки ***/etc/echelon/komrad/license:***

```
sudo rm /etc/echelon/komrad/license/license.lic
```

2) Скопируйте в папку ***/etc/echelon/komrad/license*** файл лицензии с расширением (***.lic***).

3) Перезапустите сервисы komrad-server, komrad-processor, pauth-server:

```
sudo systemctl restart komrad-server komrad-processor pauth-server
```

3.3.4.11. Этап 2. Шаг 8. Создание сертификатов

Внимание! Дальнейшие действия желательно выполнять на отдельной ЭВМ, где в дальнейшем будут храниться корневые сертификаты, необходимые для корректной работы компонентов ПК «КОМРАД».

Создание сертификатов:

1) создайте на жестком диске папку ***tls***, выполнив:

```
mkdir tls
```

2) перейдите в папку ***/tls***:

```
cd tls
```

3) выполните команду для создания корневого сертификата:

```
echelontls ca --organization “Echelon”
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***ca.pem*** и ***ca-key.pem.***

4) создайте серверный сертификат, выполнив:

```
echelontls cert --organization “Echelon” localhost 127.0.0.1 $(hostname -I) $(hostname)
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***server.pem*** и ***server-key.pem***

5) создайте клиентский сертификат, выполнив:

```
echelontls cert --client
```

В папке ***/tls*** сгенерируются два файла ***client.pem*** и ***client-key.pem***

6) создайте сертификат для браузера, выполнив:

```
echelontls browser
```

В папке ***/tls*** сгенерируется файл ***client-browser.p12***.

Внимание! При генерации сертификата для браузера, утилита komradtls попросит задать пароль. Этот пароль потребуется при добавлении сертификата в браузер. Запомните этот пароль.

3.3.4.12. Этап 2. Шаг 9. Удаление сертификатов по умолчанию

Удалите все сертификаты из папки с сертификатами по умолчанию:

```
sudo rm /var/lib/echelon/komrad/certs/CAs/*
sudo rm /var/lib/echelon/komrad/certs/*
```

3.3.4.13. Этап 2. Шаг 10. Копирование сертификатов

Скопируйте сертификаты в следующие папки:

1) файлы ***ca.pem, server.pem, server-key.pem, client.pem, client-key.pem*** в ***/var/lib/echelon/komrad/certs/*** командой:

```
sudo cp ca.pem server.pem server-key.pem client.pem client-key.pem /var/lib/echelon/komrad/certs/
```

Внимание! Команда выполняется в одну строчку.

2) файл ***ca.pem*** в ***/var/lib/echelon/komrad/certs/CAs*** командой:

```
sudo cp ca.pem /var/lib/echelon/komrad/certs/CAs
```

3.3.4.14. Этап 2. Шаг 11. Изменение владельца файлов на komrad:komrad и предоставление прав сертификатам

На машине с ПК «КОМРАД» введите в терминале:

```
sudo chown komrad:komrad  /etc/echelon/komrad/license/имя_лицензии.lic
sudo chown -R komrad:komrad  /var/lib/echelon/komrad/certs
sudo chmod -R 755 /var/lib/echelon/komrad/certs
sudo chmod 0640 /var/lib/echelon/komrad/certs/server-key.pem
sudo chown root:komrad /var/lib/echelon/komrad/certs/server-key.pem
sudo usermod -a -G komrad postgres
sudo chmod 755 client-browser.p12
```

Где в имя_лицензии – укажите наименование файла лицензии.

3.3.4.15. Этап 2. Шаг 12. Изменение владельца файлов на postgres:postgres

На машине с БД создайте папку:

```
sudo mkdir -p /var/lib/echelon/komrad/certs
```

Далее перенесите сгенерированные сертификаты ***ca.pem***, ***server-key.pem***, ***server.pem*** в папку ***/var/lib/echelon/komrad/certs***.

На машине с БД введите в терминале:

```
sudo chown -R postgres:postgres /var/lib/echelon/komrad/certs
sudo chmod -R 755 /var/lib/echelon/komrad/certs
sudo chmod 0640 /var/lib/echelon/komrad/certs/server-key.pem
sudo chown root:postgres /var/lib/echelon/komrad/certs/server-key.pem
sudo usermod -a -G postgres postgres
sudo chmod 755 client-browser.p12
```

Проверьте наличие указанных путей до сертификатов в файле ***postgresql.conf***.

Для этого введите:

```
sudo nano /etc/postgresql/11/main/postgresql.conf
```

Раскомментируйте и добавьте пути до сертификатов:

```
ssl = on
ssl_ca_file = '/var/lib/echelon/komrad/certs/ca.pem'
ssl_key_file = '/var/lib/echelon/komrad/certs/server-key.pem'
ssl_cert_file = '/var/lib/echelon/komrad/certs/server.pem'
```

3.3.4.16. Этап 2. Шаг 13. Перезапуск сервисов

Перезагрузите системы.

3.3.4.17. Этап 2. Шаг 14. Установка корневых сертификатов в браузере

Выполните следующие действия:

1) откройте **Firefox → Настройки → Приватность и защита → Сертификаты → Просмотр сертификатов**;

2) перейдите во вкладку **Ваши сертификаты** меню **Управления сертификатами;**

3) импортируйте сертификаты ***ca.pem*** в «Доверенные корневые центры сертификации» и ***client-browser.p12*** в «Личные», при этом потребуется указать пароль установленный, при генерации браузерного сертификата в Шаге 8, этапа 2;

4) перезагрузите браузер.

3.3.4.18. Этап 2. Шаг 15. Конец

ПК «КОМРАД» установлен и доступен по адресу https://localhost.

Для работы ПК «КОМРАД» на ОСОН «ОСнова» в режиме замкнутой программной среды (ЗПС) после установки по основной инструкции нужно:

1) скопировать файл открытого ключа:

```
sudo cp *pub_key.gpg /etc/ima/certs/
```

2) скопировать файлы дампов:

```
sudo cp dumps/* /etc/dpkg/ima.d/
```

3) включить политику ЗПС:

```
sudo rm /etc/ima/policy
sudo ln -s /etc/ima/policy.d/appraise /etc/ima/policy
sudo update-initramfs -u -k all
```

4) перезагрузить систему (после перезагрузки система загрузится уже в режиме ЗПС).

3.4. Установка на Ubuntu, Debian

В ПК «КОМРАД» в зависимости от типа лицензии возможны следующие варианты установок:

– все компоненты на одном узел;

– компоненты ПК «КОМРАД» на одном узле, СУБД PostgreSQL на отдельном узле;

– территориально-распределенная установка (при выборе этого вида установки обратитесь в тех. поддержку).

3.4.1. Поставляемые компоненты

Дистрибутив ПК «КОМРАД» представлен в таблице 11.

Таблица 11 – Дистрибутив ПК «КОМРАД»

Название компонента	Папка	Описание
clickhouse-client_21.11.1_all_signed.deb clickhouse-client_21.11.1_all_signed.deb.asc clickhouse-common-static_21.11.1_amd64_signed.deb clickhouse-common-static_21.11.1_amd64_signed.deb.asc clickhouse-server_21.11.1_all_signed.deb clickhouse-server_21.11.1_all_signed.deb.asc	/ubuntu/db/clickhouse	СУБД Clickhouse
correlation-dispatcher_v4.1.33_amd64.deb correlation-dispatcher_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для управления коррелляторами
echelontls_v4.1.33_amd64.deb echelontls_v4.1.33_amd64.deb.asc	/ubuntu/deb	Утилита генерации сертификатов
file-collector_v4.1.33_amd64.deb file-collector_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для сбора событий из файлов
incident-manager_v4.1.33_amd64.deb incident-manager_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для управления инцидентами
komrad-backup_v4.1.33_amd64.deb komrad-backup_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для управления резервным копированием и восстановлением
komrad-bus_v4.1.33_amd64.deb komrad-bus_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для передачи событий и прочей информации

Название компонента	Папка	Описание
		между подсистемами ПК «КОМРАД»
komrad-cli_v4.1.33_amd64.deb komrad-cli_v4.1.33_amd64.deb.asc	/ubuntu/deb	Консольный интерфейс
komrad-correlator_v4.1.33_amd64.deb komrad-correlator_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для управления коррелляторами
komrad-processor_v4.1.33_amd64.deb komrad-processor_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для обогащения, фильтрации и индексации событий безопасности
komrad-reactor-cef_v4.1.33_amd64.deb komrad-reactor-cef_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для запуска скриптов реагирования на инцидент в формате CEF
komrad-reactor_v4.1.33_amd64.deb komrad-reactor_v4.1.33_amd64.deb	/ubuntu/deb	Модуль предназначен для запуска скриптов реагирования на инцидент
komrad-s3_v4.1.34_amd64.deb komrad-s3_v4.1.34_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для создания объектового хранилища системы резервного копирования и восстановления
komrad-scanner_v4.1.33_amd64.deb komrad-scanner_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для управления активами
komrad-server_v4.1.33_amd64.deb komrad-server_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для агрегирования действий других подсистем и маршрутизации уведомлений
komrad-vault_v4.1.33_amd64.deb	/ubuntu/deb	Подсистема

Название компонента	Папка	Описание
komrad-vault_v4.1.33_amd64.deb.asc		предназначена для управления выпущенными сертификатами
pauth-server_v4.1.33_amd64.deb pauth-server_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для управления доступом к функционалу программного комплекса
pauthctl_v4.1.33_amd64.deb pauthctl_v4.1.33_amd64.deb.asc	/ubuntu/deb	Утилита для работы с пользователями в командной строке
snmp-collector_v4.1.34_amd64.deb snmp-collector_v4.1.34_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для сбора событий по SNMP
sql-collector_v4.1.33_amd64.deb sql-collector_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для сбора событий из СУБД
sqlx-collector_v4.1.33_amd64.deb sqlx-collector_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для сбора событий из СУБД
syslog-collector_v4.1.33_amd64.deb syslog-collector_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для сбора событий по Syslog
xflow-collector_v4.1.33_amd64.deb xflow-collector_v4.1.33_amd64.deb.asc	/ubuntu/deb	Модуль предназначен для сбора событий sFlow и NetFlow
syslog_collector_root.sh	/ubuntu/scripts	Скрипт для syslog-collector
nmap.deb nmap.deb.asc	/ubuntu/tools	Сканер сети
komrad-cli.exe komrad-cli.exe.asc	/ubuntu/windows/gos-sopka	Консольный интерфейс
sql-collector.exe sql-collector.exe.asc sql-collector.yaml sql-collector.yaml.asc	/ubuntu/windows/sql-collector	Модуль предназначен для сбора событий из СУБД из Windows

Название компонента	Папка	Описание
wmi-agent.exe wmi-agent.exe.asc wmi-agent.yaml wmi-agent.yaml.asc	/ubuntu/windows/wmi-agent	Модуль предназначен для сбора событий по WMI

3.4.2. Аппаратные требования

В таблице 12 приведены ориентировочные значения технических данных аппаратной платформы.

Таблица 12 – Требования к аппаратной платформе

Тип лицензии	CPU	RAM	SSD\HDD
Base	Минимум – 2 ядра Рекомендовано – от 2-х ядер	Минимум – 2 Гб Рекомендовано – 4 Гб	От 100 Гб
All-in-One	Минимум – 2 ядра Рекомендовано – 4 ядра	Минимум – 8 Гб Рекомендовано – 16 Гб	От 1 Тб
Enterprise	Минимум – 4 ядра Рекомендовано – 8 ядра	Минимум – 32 Гб Рекомендовано – 128 Гб	От 10 Тб

При выборе аппаратной части необходимо провести консультацию с техническим специалистом для предварительной оценки и рекомендаций при выборе аппаратной части.

Увеличение количества источников и\или увеличение количества событий от существующих источников повлечёт за собой увеличение ресурсов.

3.4.3. Установка всех компонентов на один узел

Поддерживаемые лицензии: Base, All-in-One, Enterprise.

Для проверки верификации подлинности пакетов необходимо:

1) Импортировать публичный ключ:

```
gpg --keyserver keyserver.ubuntu.com --recv 532C05AF2562570A
```

2) Проверить дистрибутив, например, syslog-collector:

```
gpg --verify syslog-collector_v4.1.33_amd64.deb.asc
```

Внимание! Для установки ПК «КОМРАД» на Ubuntu, Debian необходимы наличие:

– доступ к репозиторию;

– версия Ubuntu не ниже 20, либо Debian не ниже 7;

– СУБД Postgres из официального репозитория Ubuntu или Debian.

3.4.3.1. Шаг 1. Установка и настройка PostgreSQL и Clickhouse

1) Установите и настройте PostgreSQL, выполнив команду в терминале:

```
sudo apt update
sudo apt install postgresql -y
```

2) Перейдите в папку с дистрибутивом ***/ubuntu/db/clickhouse/*** и в терминале введите:

```
sudo dpkg -i ./*.deb
```

Укажите пароль для пользователя «default».

3) Запустите ClickHouse командой в терминале:

```
sudo service clickhouse-server start
```

4) Создайте пароль для ClickHouse командой в терминале, указав вместо `pass` ваш пароль:

Внимание! Команда пишется в одну строчку:

```
echo "pass"; echo -n "pass" | sha256sum | tr -d '-'
```

В первой строке результата – пароль (`pass`). Вторая строка – соответствующий ему хэш SHA256 (`pass_SHA256`).

5) Создайте и откройте на редактирование файл:

```
sudo nano /etc/clickhouse-server/users.d/komrad.xml
```

Заполните содержимое файла следующим фрагментом:

```
<yandex>
    <users>
        <komrad>
            <password remove='1' />
            <password_sha256_hex>pass_SHA256</password_sha256_hex>
        </komrad>
    </users>
</yandex>
```

Где вместо `pass_SHA256` вставьте сгенерированный хэш, соответствующий вашему паролю.

6) Откройте файл, выполнив:

```
sudo nano /etc/clickhouse-server/users.xml
```

Добавьте пользователя komrad в группу пользователей, для чего приведите фрагмент файла к виду:

```
<!-- Users and ACL. -->
<users>
    <komrad>
            <access_management>1</access_management>
            <password></password>
    </komrad>
    <!-- If user name was not specified, 'default' user is used. -->
    <default>
```

7) Перезапустите сервер ClickHouse, выполнив:

```
sudo systemctl restart clickhouse-server.service
```

3.4.3.2. Шаг 2. Задание прав пользователя на создание баз данных и создание базы данных

1) Чтобы создать нового пользователя, откройте аккаунт стандартного пользователя:

```
sudo su - postgres
```

2) Наделите пользователя правами на создание новых баз данных, где вместо `pass` – установите пароль для пользователя postgres:

```
psql -c "ALTER USER postgres WITH CREATEDB LOGIN PASSWORD 'pass';"
```

3) Установите расширение, выполнив:

```
psql -c "CREATE EXTENSION pg_trgm;"
```

4) Создайте базы данных, выполнив:

```
createdb -O postgres komrad-preferences
createdb -O postgres pauth-preferences
createdb -O postgres scanner
exit
```

5) Запустите клиент ClickHouse, используя данные пользователя komrad, где вместо `pass` – укажите пароль, заданный в шаге 1 при установке ClickHouse:

```
clickhouse-client --user=komrad --password=pass
```

6) Создайте базу данных, выполнив:

```
CREATE DATABASE komrad_events
exit
```

3.4.3.3. Шаг 3. Установка модуль сканирования сети Nmap

Перейдите в папку с утилитами ***/ubuntu/tools*** и через терминал выполните команду:

```
sudo dpkg -i ./*.deb
```

3.4.3.4. Шаг 4. Установка ПК «КОМРАД»

Перейдите в папку с дистрибутивом ***/ubuntu/deb*** и через терминал выполните команду:

```
sudo dpkg -i ./*.deb
```

3.4.3.5. Шаг 5. Редактирование yaml-файлов

1) Откройте файл ***komrad-processor.yaml***, выполнив через команду в терминале:

```
sudo nano /etc/echelon/komrad/komrad-processor/komrad-processor.yaml
```

Приведите фрагмент файла к данному виду:

```
# Настройки подключения к бд хранящей конфигурацию виджетов
widgetsdb:
  TLSCertPath: /var/lib/echelon/komrad/certs/client.pem
  TLSKeyPath: /var/lib/echelon/komrad/certs/client-key.pem
  TLSRootCAPath: /var/lib/echelon/komrad/certs/ca.pem
  db: komrad-preferences
  host: localhost
  password: pass # укажите пароль для пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres

# Настройки хранилища событий информационной безопасности
storage:
  # Тип хранилища, в данной версии поддерживается только:
  # - timescale - PostgreSQL 12+ с плагином TimescaleDB 2.2.1+
  # - clickhouse - ClickHouse v21.7.8.58-stable
  # Для ОС "Основа" поддерживается PostgreSQL 11 с TimescaleDB 2.2.1
  kind: clickhouse
```

```
clickhouse:
  # Название БД
  name: komrad_events
  user: komrad
  password: pass # укажите пароль для пользователя komrad (ClickHouse)
  # Адрес хоста с ClickHouse-server
  host: localhost
  # Порт ClickHouse-server
  port: 9000
  # Режим работы - с TLS или без
  sslmode: disable
```

2) Откройте файл ***komrad-server.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-server/komrad-server.yaml
```

Отредактируйте:

```
database:
pg:
  db: komrad-preferences
  host: localhost
  password: pass # укажите пароль для пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres
```

3) Откройте файл ***correlation-dispatcher.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/correlation-dispatcher/correlation-dispatcher.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@localhost:5432/komrad-preferences?sslmode...
CorrelatorController:
  # Настройка подключения к БД PostgreSQL в формате URL для коррелляторов.
  CorrelatorDB:postgres://postgres:pass@localhost:5432/komrad-preferences?sslmode...
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

4) Откройте файл ***incident-manager.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/incident-manager/incident-manager.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@localhost:5432/komrad-preferences?sslmode...
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

5) Откройте файл ***pauth-server.yaml*** выполнив:

```
sudo nano /etc/echelon/komrad/pauth-server/pauth-server.yaml
```

Отредактируйте:

```
database: postgres://postgres:pass@localhost:5432/pauth-preferences?sslmode...
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

6) Откройте ***komrad-scanner-config.json***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-scanner/komrad-scanner-config.json
```

Отредактируйте:

```
"Main": {
      "Driver": "postgres",
      "Host": "localhost",
      "Port": 5432,
      "DBName": "scanner",
      "User": "postgres",
      "Password": "pass",
      "SSLMode": "disable"
            }
```

Где в `pass` – укажите пароль пользователя postgres (PostgreSQL).

7) Откройте ***postgresql.conf***, выполнив:

```
sudo nano /etc/postgresql/*/main/postgresql.conf
```

8) Раскомментируйте и добавьте пути до сертификатов:

```
ssl = on
ssl_ca_file = '/var/lib/echelon/komrad/certs/ca.pem'
ssl_key_file = '/var/lib/echelon/komrad/certs/server-key.pem'
ssl_cert_file = '/var/lib/echelon/komrad/certs/server.pem'
```

9) Перезагрузите сервисы, выполнив команду в одну строчку:

```
sudo systemctl restart postgresql komrad-server komrad-processor komrad-scanner pauth-server correlation-dispatcher incident-manager
```

3.4.3.6. Шаг 6. Создание ролей администратора и пользователя с правами администратора

Создайте роль администратора и пользователя с правами администратора через команды в терминале.

Внимание! Каждая отдельная команда пишется одну строчку:

```
sudo pauthctl role add admin --migrate --conn "postgresql://postgres:pass@localhost:5432/pauth-preferences"
```

О успешном добавлении роли `admin` в строке сервиса будет строка:

INFO roles added {"role_names": ["admin"], "status": "success"}

```
sudo pauthctl role add user --conn "postgresql://postgres:pass@localhost:5432/pauth-preferences"
```

О успешном добавлении роли `user` в строке сервиса будет строка:

INFO roles added {"role_names": ["user"], "status": "success"}

```
pauthctl user add --email name@domain.com --login admin --roles admin --password admin --conn "postgresql://postgres:pass@localhost:5432/pauth-preferences"
```

Где:

1) `pass` – укажите пароль пользователя postgres (PostgreSQL);

2) `--e-mail name@domain.com` – укажите свой e-mail адрес администратора;

3) `--login admin` – укажите свой логин администратора;

4) `--password admin` – укажите свой пароль администратора.

3.4.3.7. Шаг 7. Перенос лицензии

1) Удалите демо-лицензию из папки ***/etc/echelon/komrad/license*** командой в терминале:

```
sudo rm /etc/echelon/komrad/license/license.lic
```

2) Скопируйте в папку ***/etc/echelon/komrad/license*** файл лицензии с расширением (***.lic***).

3) Перезапустите сервисы komrad-server, komrad-processor, pauth-server командой в терминале:

```
sudo systemctl restart komrad-server komrad-processor pauth-server
```

3.4.3.8. Шаг 8. Создание сертификатов

Внимание! Дальнейшие действия желательно выполнять на отдельной ЭВМ, где в дальнейшем будут храниться корневые сертификаты, необходимые для корректной работы компонентов ПК «КОМРАД».

Создание сертификатов:

1) создайте на жестком диске папку ***/tls***;

Совет! Команда для создания папки:

```
mkdir tls
```

2) перейдите в папку ***/tls*** и выполните команду в терминале для создания корневого сертификата:

```
cd tls
echelontls ca --organization “Echelon”
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***ca.pem*** и ***ca-key.pem.***

3) создайте серверный сертификат командой в терминале:

```
echelontls cert --organization “Echelon” localhost 127.0.0.1 $(hostname -I) $(hostname)
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***server.pem*** и ***server-key.pem***

4) создайте клиентский сертификат командой в терминале:

```
echelontls cert --client
```

В папке ***/tls*** сгенерируются два файла ***client.pem*** и ***client-key.pem***

5) создайте сертификат для браузера командой в терминале:

```
echelontls browser
```

Внимание! При генерации сертификата для браузера, утилита komradtls попросит задать пароль. Этот пароль потребуется при добавлении сертификата в браузер, поэтому запомните этот пароль.

В папке ***/tls*** сгенерируется файл ***client-browser.p12***.

3.4.3.9. Шаг 9. Удаление сертификатов по умолчанию

Удалите все сертификаты из папки с сертификатами по умолчанию командой в терминале:

```
sudo rm /var/lib/echelon/komrad/certs/CAs/*
sudo rm /var/lib/echelon/komrad/certs/*
```

3.4.3.10. Шаг 10. Копирование сертификатов

Скопируйте сертификаты в следующие папки:

1) файлы ***ca.pem***, ***server.pem***, ***server-key.pem,*** ***client.pem,*** ***client-key.pem*** в ***/var/lib/echelon/komrad/komrad-server/certs/*** командой терминале:

```
sudo cp ca.pem server.pem server-key.pem client.pem client-key.pem
/var/lib/echelon/komrad/certs/
```

Внимание! Команда выполняется в одну строчку.

2) файл ***ca.pem*** в ***/var/lib/echelon/komrad/certs/CAs/*** командой:

```
sudo cp ca.pem /var/lib/echelon/komrad/certs/CAs/
```

3.4.3.11. Шаг 11. Изменение владельца файлов на komrad:komrad и предоставление прав сертификатам

Введите команды в терминале:

```
sudo chown komrad:komrad  /etc/echelon/komrad/license/имя_лицензии.lic
sudo chown -R komrad:komrad  /var/lib/echelon/komrad/certs
sudo chmod -R 755 /var/lib/echelon/komrad/certs
sudo chmod 0640 /var/lib/echelon/komrad/certs/server-key.pem
sudo chown root:komrad /var/lib/echelon/komrad/certs/server-key.pem
sudo usermod -a -G komrad postgres
sudo chmod 755 client-browser.p12
```

Где в имя_лицензии – укажите наименование файла лицензии.

3.4.3.12. Шаг 12. Перезапуск сервисов

Перезагрузите систему.

3.4.3.13. Шаг 13. Установка корневого и браузерного сертификатов в браузере

Выполните следующие действия:

1) откройте **Firefox → Настройки → Приватность и защита → Сертификаты → Просмотр сертификатов**;

2) перейдите во вкладку **Ваши сертификаты** меню **Управления сертификатами;**

3) импортируйте сертификаты ***ca.pem*** в «Доверенные корневые центры сертификации» и ***client-browser.p12*** в «Личные», при этом потребуется указать пароль установленный, при генерации браузерного сертификата в Шаге 8;

4) перезагрузите браузер.

3.4.3.14. Шаг 14. Конец

ПК «КОМРАД» установлен и доступен по адресу https://localhost.

3.4.4. Установка компонентов ПК «КОМРАД» на одном узле, СУБД PostgreSQL и ClickHouse на другом

Поддерживаемые лицензии: Base, All-in-One, Enterprise.

Установка ПК «КОМРАД» будет состоять из двух этапов:

– на первом этапе установка и настройка PostgreSQL;

– на втором этапе установка и настройка ПК «КОМРАД»

3.4.4.1. Этап 1. Шаг 1. Установка и настройка PostgreSQL и Clickhouse

1) Установите и настройте PostgreSQL, выполнив команду в терминале:

```
sudo apt update
sudo apt install postgresql -y
```

2) Перейдите в папку с дистрибутивом ***/ubuntu/db/clickhouse/*** и в терминале введите:

```
sudo dpkg -i ./*.deb
```

Укажите пароль для пользователя «default».

3) Запустите ClickHouse командой в терминале:

```
sudo service clickhouse-server start
```

4) Создайте пароль для ClickHouse командой в терминале, указав вместо `pass` ваш пароль:

Внимание! Команда пишется в одну строчку:

```
echo "pass"; echo -n "pass" | sha256sum | tr -d '-'
```

В первой строке результата – пароль (`pass`). Вторая строка – соответствующий ему хэш SHA256 (`pass_SHA256`).

5) Создайте и откройте на редактирование файл:

```
sudo nano /etc/clickhouse-server/users.d/komrad.xml
```

Заполните содержимое файла следующим фрагментом:

```
<yandex>
    <users>
        <komrad>
            <password remove='1' />
            <password_sha256_hex>pass_SHA256</password_sha256_hex>
        </komrad>
    </users>
</yandex>
```

Где вместо `pass_SHA256` вставьте сгенерированный хэш, соответствующий вашему паролю.

6) Откройте файл, выполнив:

```
sudo nano /etc/clickhouse-server/users.xml
```

Добавьте пользователя komrad в группу пользователей, для чего приведите фрагмент файла к виду:

```
<!-- Users and ACL. -->
<users>
    <komrad>
            <access_management>1</access_management>
            <password></password>
    </komrad>
    <!-- If user name was not specified, 'default' user is used. -->
    <default>
```

7) Перезапустите сервер ClickHouse, выполнив:

```
sudo systemctl restart clickhouse-server.service
```

3.4.4.2. Этап 1. Шаг 2. Задание прав пользователя на создание баз данных и создание базы данных

1) Чтобы создать нового пользователя, откройте аккаунт стандартного пользователя:

```
sudo su - postgres
```

2) Наделите пользователя правами на создание новых баз данных, где вместо `pass` – установите пароль для пользователя postgres:

```
psql -c "ALTER USER postgres WITH CREATEDB LOGIN PASSWORD 'pass';"
```

3) Установите расширение, выполнив:

```
psql -c "CREATE EXTENSION pg_trgm;"
```

4) Создайте базы данных, выполнив:

```
createdb -O postgres komrad-preferences
createdb -O postgres pauth-preferences
createdb -O postgres scanner
exit
```

5) Запустите клиент ClickHouse, используя данные пользователя komrad, где вместо `pass` – укажите пароль, заданный в шаге 1 при установке ClickHouse:

```
clickhouse-client --user=komrad --password=pass
```

6) Создайте базу данных, выполнив:

```
CREATE DATABASE komrad_events
exit
```

3.4.4.3. Этап 1. Шаг 3. Настройка подключения к базам данных с удаленных узлов

По умолчанию, серверы баз данных разрешают подключение только с локального компьютера. Для подключения с удаленных систем необходимо отредактировать три файла ***postgresql.conf***, ***pg_hba.conf*** и ***config.xml***.

1) Откройте для редактирования файл ***postgresql.conf***, выполнив:

```
sudo nano /etc/postgresql/*/main/postgresql.conf
```

Затем раскомментируйте строку, содержащую `# listen_addresses = `localhost``, убрав # перед строкой, и отредактируйте, чтобы получилось, как в следующем файле:

```
#------------------------------------------------------------------
# CONNECTIONS AND AUTHENTICATION
#------------------------------------------------------------------

# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to listen on;
                                # comma-separated list of addresses;
                                # defaults to 'localhost'; use '*' for all
                                # (change requires restart)
```

Совет! В данном примере мы разрешили прослушивание запросов на всех IP-адресах (*), но, если требуется более безопасная настройка, можно перечислить последние через пробел.

Например: `listen_addresses = ` 192.168.0.15 10.10.0.16 `.`

Сохраните файл и закройте его.

2) Откройте для редактирования файл ***pg_hba.conf***, выполнив:

```
sudo nano /etc/postgresql/*/main/pg_hba.conf
```

После последней строки файла с новой строки добавить:

```
host    all     postgres    IP-адрес_ПК_КОМРАД/32    md5
```

Где IP-адрес_ПК_КОМРАД – IP-адрес хоста, с которого будет подключение.

Сохраните файл и закройте его, после чего перезапустите службу, выполнив:

```
sudo systemctl restart postgresql
```

3) Откройте для редактирования файл ***config.xml***, выполнив:

```
sudo nano /etc/clickhouse-server/config.xml
```

Затем раскомментируйте строку, содержащую `<!-- <listen_host>0.0.0.0</listen_host> -->`, как в следующем файле:

```
...
 <interserver_http_host>example.yandex.ru</interserver_http_host>
    -->
    <!-- Listen specified host. use :: (wildcard IPv6 address), if you want to
accept connections both with IPv4 and IPv6 from everywhere. -->
    <!-- <listen_host>::</listen_host> -->
    <!-- Same for hosts with disabled ipv6: -->
    <listen_host>0.0.0.0</listen_host>

    <!-- Default values - try listen localhost on ipv4 and ipv6: -->
    <!--
    <listen_host>::1</listen_host>
    <listen_host>127.0.0.1</listen_host>
    -->
...
```

Сохраните файл и закройте его. Для применения новой конфигурации перезапустите службу, выполнив:

```
sudo service clickhouse-server restart
```

Вы не увидите вывод этой команды. Сервер ClickHouse прослушивает порт 8123 для HTTP-соединений и порт 9000 для соединений из clickhouse-client. Разрешите доступ к обоим портам для IP-адреса вашего сервера, где будет установлен ПК «КОМРАД» с помощью следующих команд:

```
sudo ufw allow from IP_адрес_ПК_КОМРАД/32 to any port 8123
sudo ufw allow from IP_адрес_ПК_КОМРАД/32 to any port 9000
```

Вы увидите вывод о добавлении роли для обеих команд, который показывает, что вы включили доступ к обоим портам.

3.4.4.4. Этап 2. Шаг 1. Начало

Скопируйте папку ***/komrad/ubuntu*** с установочного носителя на узел, где будет работать ПК «КОМРАД».

3.4.4.5. Этап 2. Шаг 2. Установка Nmap

Перейдите в папку ***/tools*** и выполните команду**:**

```
sudo dpkg -i ./*.deb
```

3.4.4.6. Этап 2. Шаг 3. Установка ПК «КОМРАД»

Перейдите в папку с дистрибутивом ***/ubuntu/deb*** и через терминал выполните команду:

```
sudo dpkg -i ./*.deb
```

3.4.4.7. Этап 2. Шаг 4. Редактирование yaml-файлов

Для работы с удаленной базой данных, необходимо в yaml файлах указать информацию по подключению к ней:

1) Откройте файл ***komrad-server.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-server/komrad-server.yaml
```

Отредактируйте:

```
cors:
  enabled: true #– параметр true разрешает доступ только для устройств, внесённых в список allowedorigins, в случае, если ваше устройство не находится в списке allowedorigins, то можете внести его в этот список самостоятельно. Параметр false разрешает доступ для всех устройств, список allowedorigins при этом не создает ограничений.
    # При возникновении ошибок с CORS возможный выход - небезопасная настройка `allowedorigins: ["*"]`
    # allowedorigins: ["*"]
    allowedorigins:
      - https://IP-адрес_БД #– укажите IP-адрес сервера БД
      - https://localhost:443
      - https://localhost:3400
      - http://localhost:8080
      - https://localhost
      - https://localhost:3400
      # Сервис komrad-s3 раздаёт отчёты, изображения и должен быть упомянут в разрешённых источниках CORS
      - https://localhost:9050
      # - https://komrad-s3.enterprise.lan:9000
      # - https://komrad.enterprise.lan:443
secure:
    # Список FQDN от которых разрешены запросы, если список пустой - запросы со всех
    # хостов будут приниматься.
```

```
    AllowedHosts:
      - IP-адрес_БД #– укажите IP-адрес сервера БД
      - localhost
      - localhost:3400
      - localhost:443
      - localhost:8080
      - localhost
      - localhost:443
      - komrad.enterprise.lan

database:
pg:
  db: komrad-preferences
  host: IP-адрес_БД #– укажите IP-адрес сервера БД
  password: pass #– укажите пароль пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres

monitoring:
  http:
    dbpreferences:
      url: IP-адрес_БД:5432 #– укажите IP-адрес сервера БД
      interval: 10s
    dbevents:
      url: IP-адрес_БД:9000 #– укажите IP-адрес сервера БД
      interval: 10s
```

2) Откройте файл ***correlation-dispatcher.yaml***, выполнив***:***

```
sudo nano /etc/echelon/komrad/correlation-dispatcher/correlation-dispatcher.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@IP-адрес_БД:5432/komrad-preferences?sslmode...

CorrelatorController:
  # Настройка подключения к БД PostgreSQL в формате URL для коррелляторов.
  CorrelatorDB:postgres://postgres:pass@IP-адрес_БД:5432/komrad-
preferences?sslmode...
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

3) Откройте файл ***incident-manager.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/incident-manager/incident-manager.yaml
```

Отредактируйте:

```
# Настройка подключения к БД PostgreSQL в формате URL.
DB: postgres://postgres:pass@IP-адрес_БД:5432/komrad-preferences?sslmode...
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

4) Откройте файл ***komrad-processor.yaml***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-processor/komrad-processor.yaml
```

Отредактируйте:

```
# Настройки подключения к бд хранящей конфигурацию виджетов
widgetsdb:
  TLSCertPath: /var/lib/echelon/komrad/certs/client.pem
  TLSKeyPath: /var/lib/echelon/komrad/certs/client-key.pem
  TLSRootCAPath: /var/lib/echelon/komrad/certs/ca.pem
  db: komrad-preferences
  host: IP-адрес_БД
  password: pass # укажите пароль пользователя postgres (PostgreSQL)
  port: 5432
  tlsmode: verify-full
  user: postgres

# Настройки хранилища событий информационной безопасности
storage:
  # Тип хранилища, в данной версии поддерживается только:
  # - timescale - PostgreSQL 12+ с плагином TimescaleDB 2.2.1+
  # - clickhouse - ClickHouse v21.7.8.58-stable
  # Для ОС "Основа" поддерживается PostgreSQL 11 с TimescaleDB 2.2.1
```

```
kind: clickhouse
clickhouse:
  # Название БД
  name: komrad_events
  user: komrad
  password: pass # укажите пароль пользователя komrad (ClickHouse)
  # Адрес хоста с ClickHouse-server
  host: IP-адрес_БД
  # Порт ClickHouse-server
  port: 9000
  # Режим работы - с TLS или без
  sslmode: disable
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароли.

5) Откройте файл ***pauth-server.yaml*** выполнив:

```
sudo nano /etc/echelon/komrad/pauth-server/pauth-server.yaml
```

Отредактируйте:

```
database: postgres://postgres:pass@IP-адрес_БД:5432/pauth-preferences?sslmode...
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

6) Откройте ***komrad-scanner-config.json***, выполнив:

```
sudo nano /etc/echelon/komrad/komrad-scanner/komrad-scanner-config.json
```

Отредактируйте:

```
"Main": {
      "Driver": "postgres",
      "Host": "IP-адрес_БД ",
      "Port": 5432,
      "DBName": "scanner",
      "User": "postgres",
```

```
"Password": "pass",
"SSLMode": "disable"
        }
```

Где:

– IP-адрес_БД – укажите IP-адрес сервера БД;

– pass – укажите пароль пользователя postgres (PostgreSQL).

3.4.4.8. Этап 2. Шаг 5. Перезапуск служб

Перезагрузите службы, выполнив:

```
sudo systemctl restart komrad-server komrad-processor komrad-scanner pauth-server correlation-dispatcher incident-manager
```

3.4.4.9. Этап 2. Шаг 6. Создание ролей администратора и пользователя с правами администратора

Создайте роль администратора и пользователя с правами администратора.

Внимание! Все команды пишутся в одну строчку.

```
sudo pauthctl role add admin --conn postgresql://postgres:pass@IP-адрес_БД:5432/pauth-preferences
```

О успешном добавлении роли admin в строке сервиса будет строка:

```
INFO   roles added     {"role_names": ["admin"], "status": "success"}
```

```
sudo pauthctl role add user --conn postgresql://postgres:pass@IP-адрес_БД:5432/pauth-preferences
```

О успешном добавлении роли user в строке сервиса будет строка:

```
INFO   roles added     {"role_names": ["user"], "status": "success"}
```

```
sudo pauthctl user add --email name@domain.com --login admin --roles admin --password admin --conn postgresql://postgres:pass@IP-адрес_БД:5432/pauth-preferences
```

Где:

1) IP-адрес_БД – IP-адрес БД;

2) pass – укажите пароль пользователя postgres (PostgreSQL);

3) --e-mail name@domain.com – укажите свой e-mail адрес администратора;

4) --login admin – укажите свой логин администратора;

5) --password admin – укажите свой пароль администратора.

3.4.4.10. Этап 2. Шаг 7. Перенос лицензии

1) Удалите установочную demo-лицензию из папки ***/etc/echelon/komrad/license:***

```
sudo rm /etc/echelon/komrad/license/license.lic
```

2) Скопируйте в папку ***/etc/echelon/komrad/license*** файл лицензии с расширением (***.lic***).

3) Перезапустите сервисы komrad-server, komrad-processor, pauth-server:

```
sudo systemctl restart komrad-server komrad-processor pauth-server
```

3.4.4.11. Этап 2. Шаг 8. Создание сертификатов

Внимание! Дальнейшие действия желательно выполнять на отдельной ЭВМ, где в дальнейшем будут храниться корневые сертификаты, необходимые для корректной работы компонентов ПК «КОМРАД».

Создание сертификатов:

1) создайте на жестком диске папку ***tls***, выполнив:

```
mkdir tls
```

2) перейдите в папку ***/tls***:

```
cd tls
```

3) выполните команду для создания корневого сертификата:

```
echelontls ca --organization “Echelon”
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***ca.pem*** и ***ca-key.pem.***

4) создайте серверный сертификат, выполнив:

```
echelontls cert --organization “Echelon” localhost 127.0.0.1 $(hostname -I) $(hostname)
```

Где вместо `Echelon` укажите название своей организации.

В папке ***/tls*** сгенерируются два файла ***server.pem*** и ***server-key.pem***

5) создайте клиентский сертификат, выполнив:

```
echelontls cert --client
```

В папке ***/tls*** сгенерируются два файла ***client.pem*** и ***client-key.pem***

6) создайте сертификат для браузера, выполнив:

```
echelontls browser
```

В папке ***/tls*** сгенерируется файл ***client-browser.p12***.

Внимание! При генерации сертификата для браузера, утилита komradtls попросит задать пароль. Этот пароль потребуется при добавлении сертификата в браузер. Запомните этот пароль.

3.4.4.12. Этап 2. Шаг 9. Удаление сертификатов по умолчанию

Удалите все сертификаты из папки с сертификатами по умолчанию:

```
sudo rm /var/lib/echelon/komrad/certs/CAs/*
sudo rm /var/lib/echelon/komrad/certs/*
```

3.4.4.13. Этап 2. Шаг 10. Копирование сертификатов

Скопируйте сертификаты в следующие папки:

1) файлы ***ca.pem, server.pem, server-key.pem, client.pem, client-key.pem*** в ***/var/lib/echelon/komrad/certs/*** командой:

```
sudo cp ca.pem server.pem server-key.pem client.pem client-key.pem /var/lib/echelon/komrad/certs/
```

Внимание! Команда выполняется в одну строчку.

2) файл ***ca.pem*** в ***/var/lib/echelon/komrad/certs/CAs*** командой:

```
sudo cp ca.pem /var/lib/echelon/komrad/certs/CAs
```

3.4.4.14. Этап 2. Шаг 11. Изменение владельца файлов на komrad:komrad и предоставление прав сертификатам

На машине с ПК «КОМРАД» введите в терминале:

```
sudo chown komrad:komrad  /etc/echelon/komrad/license/имя_лицензии.lic
sudo chown -R komrad:komrad  /var/lib/echelon/komrad/certs
sudo chmod -R 755 /var/lib/echelon/komrad/certs
sudo chmod 0640 /var/lib/echelon/komrad/certs/server-key.pem
sudo chown root:komrad /var/lib/echelon/komrad/certs/server-key.pem
sudo usermod -a -G komrad postgres
sudo chmod 755 client-browser.p12
```

Где в имя_лицензии – укажите наименование файла лицензии.

3.4.4.15. Этап 2. Шаг 12. Изменение владельца файлов на postgres:postgres

На машине с БД создайте папку:

```
sudo mkdir -p /var/lib/echelon/komrad/certs
```

Далее перенесите сгенерированные сертификаты ***ca.pem***, ***server-key.pem***, ***server.pem*** в папку ***/var/lib/echelon/komrad/certs***.

На машине с БД введите в терминале:

```
sudo chown -R postgres:postgres /var/lib/echelon/komrad/certs
sudo chmod -R 755 /var/lib/echelon/komrad/certs
sudo chmod 0640 /var/lib/echelon/komrad/certs/server-key.pem
sudo chown root:postgres /var/lib/echelon/komrad/certs/server-key.pem
sudo usermod -a -G postgres postgres
sudo chmod 755 client-browser.p12
```

Проверьте наличие указанных путей до сертификатов в файле ***postgresql.conf***.

Для этого введите:

```
sudo nano /etc/postgresql/*/main/postgresql.conf
```

Раскомментируйте и добавьте пути до сертификатов:

```
ssl = on
ssl_ca_file = '/var/lib/echelon/komrad/certs/ca.pem'
ssl_key_file = '/var/lib/echelon/komrad/certs/server-key.pem'
ssl_cert_file = '/var/lib/echelon/komrad/certs/server.pem'
```

3.4.4.16. Этап 2. Шаг 13. Перезапуск сервисов

Перезагрузите системы.

3.4.4.17. Этап 2. Шаг 14. Установка корневых сертификатов в браузере

Выполните следующие действия:

1) откройте **Firefox → Настройки → Приватность и защита → Сертификаты → Просмотр сертификатов**;

2) перейдите во вкладку **Ваши сертификаты** меню **Управления сертификатами;**

3) импортируйте сертификаты ***ca.pem*** в «Доверенные корневые центры сертификации» и ***client-browser.p12*** в «Личные», при этом потребуется указать пароль установленный, при генерации браузерного сертификата в Шаге 8, этапа 2;

4) перезагрузите браузер.

3.4.4.18. Этап 2. Шаг 15. Конец

ПК «КОМРАД» установлен и доступен по адресу https://localhost.

3.5. Работа со службами и проверка корректности установки служб

Службы — это вид программ, которые работают в фоне и не требуют действий пользователя.

3.5.1. Службы в Windows

Службы могут как относиться к операционной системе Windows, так и быть сторонними приложениями. Примеры служб, которые может установить сам пользователь: веб-сервер, сервер удалённого рабочего стола VNC, SSH сервер, сервер СУБД MySQL.

Управлять службами можно:

– в графическом интерфейсе;

– командной строке;

– в PowerShell.

Для получения общего списка служб в Windows необходимо перейти в интерфейс «Службы»:

– средства администрирования Windows → Службы;

– или запустить сервис Службы в командной строке (**`Win + R`**) командой services.msc.

Здесь, в столбце «Имя», вы увидите список служб, работающих в вашей системе, вместе с их Описанием. Вы также сможете увидеть их Статус — независимо от того, запущены они или остановлены, а также Типы запуска и Вход от имени.

Windows предлагает следующие типы запуска:

– автоматически;

– автоматически (отложенный запуск);

– вручную;

– вручную (запуск по триггеру);

– отключена.

3.5.1.1. Работа со службами

Чтобы запустить, остановить, приостановить, возобновить или перезапустить службу Windows, выберите службу и щёлкните её правой кнопкой мыши. Вам будут предложены эти варианты.

Если вы хотите управлять дополнительными опциями, дважды щёлкните Сервис, чтобы открыть окно его свойств.

Здесь, в раскрывающемся меню **Тип запуска**, вы сможете выбрать тип запуска для Сервиса.

В разделе «**Состояние службы**» вы увидите кнопки «**Запустить**», «**Остановить**», «**Приостановить**», «**Продолжить**».

В окне «**Свойства**» вы также увидите другие вкладки, такие как «**Вход в систему**», «**Восстановление**» и «**Зависимости**», которые предлагают дополнительные параметры и информацию.

После внесения изменений вам нужно будет нажать «**Применить**».

Пример работы со службами представлен в таблице 13.

Таблица 13 – Пример работы со службами Windows

Наименование	Пример работы
Остановка службы	**Средства администрирования Windows → Службы** Далее правой кнопкой мыши на сервисе «**НАЗВАНИЕ СЕРВИСА**» выбрать пункт «**Остановить**»
Запуск службы	**Средства администрирования Windows → Службы** Далее правой кнопкой мыши на сервисе «**НАЗВАНИЕ СЕРВИСА**» выбрать пункт «**Запустить**»
Перезагрузка службы	**Средства администрирования Windows → Службы** Далее правой кнопкой мыши на сервисе «**НАЗВАНИЕ СЕРВИСА**» выбрать пункт «**Перезапустить**»
Удаление службы	Осуществляется в соответствии с разделом «Удаление SIEM ПК «КОМРАД»

3.5.1.2. Управление службами с помощью командной строки

Вы также можете использовать командную строку для запуска, остановки, приостановки, возобновления обслуживания. Чтобы использовать консоль, откройте командную строку или PowerShell с правами администратора и выполните одну из следующих команд.

Существует восемь основных командлетов Service, предназначенных для просмотра состояния и управления службами Windows.

Чтобы получить весь список командлетов Service, введите команду:

```
Get-Help \*-Service
```

Описания командлетов представлены в таблице 14.

Таблица 14 – Описание командлетов Service

Командлет	Описание
Get-Service	Позволяет получить службы на локальном или удаленном компьютере, как запущенные, так и остановленные
New-Service	Создает службу. Создает в реестре и базе данных служб новую запись для

Командлет	Описание
	службы Windows
Restart-Service	Перезапускает службу. Передает сообщение об перезапуске службы через Windows Service Controller
Resume-Service	Возобновляет службы. Отсылает сообщение о возобновлении работы диспетчеру служб Windows
Set-Service	Изменяет параметры локальной или удаленной службы, включая состояние, описание, отображаемое имя и режим запуска. Этот командлет также можно использовать для запуска, остановки или приостановки службы
Start-Service	Запускает службу
Stop-Service	Останавливает службу (отсылает сообщение об остановке диспетчеру служб Windows)
Suspend-Service	Приостанавливает службу. Приостановленная служба по-прежнему выполняется, однако ее работа прекращается до возобновления работы службы, например с помощью командлета Resume-Service.

Получить подробное описание и примеры использования конкретного командлета можно через Get-help:

```
Get-Help Start-Service
```

Для просмотра списка служб ПК «КОМРАД» введите:

```
Get-Service -name komrad*
```

Список используемых служб приведён в таблице 15.

Таблица 15 – Список служб ПК «КОМРАД» на Windows

Служба	Описание	Состояние	Тип запуска
Komrad WMI Agent	Monitors Windows events from event logs and local text-like files.	Выполняется	Автоматически

3.5.2. Службы в Linux

Дистрибутивы Linux в которых функционирует ПК «КОМРАД» используют systemd в качестве системы инициализации и диспетчера служб по умолчанию.

Systemd — это набор инструментов для управления системами Linux. Он используется для загрузки машины, управления службами, автоматического монтирования файловых систем, регистрации событий, настройки имени хоста и других системных задач.

Внимание! Если в строке состояния работы служб указано «failed» или «inactive», то необходимо перезапустить службу. Или если служба не запускается в ручном режиме, то обратитесь в раздел «Диагностика и решение проблем».

3.5.2.1. Команды для работы со службами

Команды для работы со службами представлен в таблице 16.

Таблица 16 – Список команд

Команда	Описание
Список всех загруженных служб	В терминале выполнить команду: `sudo systemctl list-units --type service`
Список всех работающих служб	В терминале выполнить команду: `sudo systemctl list-units --type service --state running`
Остановка службы	В терминале выполнить команду: `sudo systemctl stop название-сервиса.service`
Запуск службы	В терминале выполнить команду: `sudo systemctl start название-сервиса.service`
Перезагрузка службы	В терминале выполнить команду: `sudo systemctl restart название-сервиса.service`
Удаление службы	Осуществляется в соответствии с разделом «Удаление ПК «КОМРАД»
Просмотр журнала	В терминале выполнить команду: `sudo journalctl -u название-сервиса`

Службы, которые должны быть в статусе running представлены в таблице 17.

Таблица 17 – Список служб

Служба	Статус
correlation-dispatcher.service	loaded active running correlation-dispatcher
file-collector.service	loaded active running file-collector
incident-manager.service	loaded active running incident-manager
komrad-bus.service	loaded active running komrad-bus
komrad-processor.service	loaded active running komrad-processor
komrad-reactor.service	loaded active running komrad-reactor
komrad-s3.service	loaded active running komrad-s3

Служба	Статус
komrad-scanner.service	loaded active running komrad-scanner
komrad-server.service	loaded active running komrad-server
pauth-server.service	loaded active running pauth-server
postgresql.service	loaded active exited PostgreSQL RDBMS
postgresql@«version»-main.service	loaded active running PostgreSQL «version»
snmp-collector.service	loaded active running snmp-collector
sql-collector.service	loaded active running sql-collector
syslog-collector.service	loaded active running syslog-collector
xflow-collector.service	loaded active running xflow-collector

3.6. Рекомендации по установке SIEM ПК «КОМРАД» в виртуальной среде

ПК «КОМРАД» может устанавливаться на следующие виды виртуальных сред:

– VmWare;

– VirtualBox;

– ProxMox;

– KVM;

– Hyper-V.

3.6.1. Настройка работы процессора

Предъявляемые аппаратные требования к дистрибутивам ПК «КОМРАД»:

– Для Astra Linux аппаратные требования указаны в пункте 3.2.2. «Аппаратные требования»;

– Для ОСОН «ОСнова» аппаратные требования указаны в пункте 3.3.2. «Аппаратные требования»;

– Для Ubuntu, Debian аппаратные требования указаны в пункте 3.4.2 «Аппаратные требования».

В виртуальных средах, где не используется режим Hyperthreading, количество физических ядер должно быть равно количеству логических.

При наличии и включении технологии Hyperthreading для ПК «КОМРАД» достаточно выделить вдвое меньше физических ядер.

3.6.2. Настройка оперативной памяти

Объем оперативной памяти выделяемой виртуальной среде должно быть не менее значения, указанного в требованиях к аппаратным средствам. Рекомендуется устанавливать на 10-15% больше объема оперативной памяти от рекомендуемого, т.к. часть этого объема используется для работы самой виртуальной среды.

3.6.3. Настройка жесткий дисков

Объем жестких дисков выделяемой виртуальной среде должно быть не менее значения, указанного в требованиях к аппаратным средствам.

Рекомендуем использовать технологию Storage I/O Control при обмене данных между виртуальной средой и сервером баз данных.

3.7. Настройка времени хранения данных о событиях ИБ

Для оптимизации дискового пространства в ПК «КОМРАД» реализована возможность управления временем, по прошествии которого данные из таблицы events базы данных komrad-events будут удаляться.

Данная возможность реализована с помощью утилиты komrad-cli.

Внимание! Команда пишется в одну строчку.

Например:

```
komrad-cli db clickhouse events-ttl --host  localhost --user komrad --
pass $CLIKHOUSE_PASS --duration 6m14d
```

Здесь устанавливается или изменяется TTL (время жизни) на таблицу events при помощи ключа `--duration` на промежуток времени 6 месяцев и 14 дней. Общий формат для ключа duration: n1[Year, year, Y, y]n2[Month, month, M, m]n3[Day, day, D, d], где: n1 – количество (натуральное число) лет, n2 – количество (натуральное число) месяцев, n3 – количество (натуральное число) дней.

В позиции `pass  $CLIKHOUSE_PASS`, вместо `$CLIKHOUSE_PASS` укажите пароль для пользователя komrad.

4. ПОЛЬЗОВАТЕЛИ И РОЛИ В SIEM ПК «КОМРАД»

В ПК «КОМРАД» реализована ролевая модель управления доступом. Пользователю могут быть назначены определенные роли. Каждая роль содержит набор привилегий, которые определяют доступные для пользователя разделы интерфейса и операции в ПК «КОМРАД».

4.1. Управление учётными записями

В момент установки ПК «КОМРАД» создаётся учётная запись администратора системы. После входа в систему необходимо заполнить поля карточки администратора.

Управление учётными данными пользователей системы происходит в веб интерфейс ПК «КОМРАД», расположенного в **Меню → Администрирование → Пользователи**.

В карточке пользователя заполняются следующие поля:

– фамилия;

– имя;

– отчество;

– логин;

– телефон;

– e-mail;

– пароль.

Для добавления второго администратора системы необходимо выполнить следующую команду:

```
pauthctl user add --email name2@domain.com --login admin2 --roles admin --password admin2
```

Укажите:

1) `--email name2@domain.com` – свой e-mail адрес;

2) `--login admin2` – свой логин;

3) `--password admin2` – свой пароль.

4.2. Роли

В ПК «КОМРАД» реализовано две роли:

– Администратор системы;

– Пользователь.

Пользователь получает доступ к следующему функционалу ПК «КОМРАД»:

1) **Меню → Виджеты → Статус компонентов**;

2) **Меню → Активы → Задачи → Дашборды**;

3) **Меню → События в реальном времени → Поиск по событиям → Фильтры**;

4) **Меню → Инциденты → Статистика инцидентов → Директивы**.

Администратор системы получает доступ ко всем функциям ПК «КОМРАД».

5. ОБНОВЛЕНИЕ SIEM ПК «КОМРАД»

5.1. Проверка наличия новой версии

Информация о новых версиях ПК «КОМРАД» будет приходить на электронный адрес, указанный в лицензионном договоре. Также информация будет размещена на сайте производителя ПК «КОМРАД».

5.2. Загрузка новой версии

Механизм получения новой версии указан в лицензионном договоре.

5.3. Обновление ПК «КОМРАД»

Для обновления необходимо:

1) скопировать дистрибутив на ЭВМ, где установлен ПК «КОМРАД»;

2) сделать резервные копии всех конфигурационных файлов. Пути расположения указаны; п. 2.15 «Структура директорий» настоящего документа;

3) каждый deb-пакет из состава дистрибутива имеет с собой закодированный файл формата .asc, который можно использовать для верификации подлинности и целостности, также в составе дистрибутива для Astra Special Edition и для ОСОН «ОСнова» есть файлы открытых ключей для проверки электронной цифровой подписи в режиме ЗПС, для ОС Ubuntu и Debian файл открытого ключа необходимо скачать с официального сервера Ubuntu (см. п. 3.4.3).

4) провести расчет контрольных сумм файлов обновлений с использованием утилиты «Инспектор» программного комплекса «Средство анализа защищенности «Сканер-ВС» (Сертификат ФСТЭК № 2204 от 13.11.2010, срок действия до 13.11.2024) по алгоритму «ФИКС (уровень 1)» и сравненить их со значениями, указанными в формуляре НПЕШ.60010-03 30. При расхождении контрольных сумм с эталонными значениями необходимо обратиться в службу поддержки предприятия-изготовителя;

5) выполните установку всех пакетов:

```
sudo dpkg -i ./*.deb
```

6) выполните настройку конфигурационных файлов, если они были ранее изменены;

7) перезапустите сервисы, конфигурационные файлы которых были изменены;

8) замените сертификаты для работы сервисов на свои, созданные при установке ПК «КОМРАД».

6. УДАЛЕНИЕ SIEM ПК «КОМРАД»

6.1. Удаление в Linux

При необходимости сделайте резервные копии ПК «КОМРАД».

Для удаления SIEM ПК «КОМРАД»:

1) в командной строке выполните команду:

```
sudo apt purge komrad-processor pauth-server komrad-server komrad-reactor komrad-s3 incident-manager correlation-dispatcher komrad-bus komrad-scanner {file,snmp,xflow,syslog,sql}-collector
```

Затем удалите каталог:

```
sudo rm -rf /etc/echelon
```

2) при необходимости удалите базу данных PostgreSQL:

Выведет список всех пакетов, связанных с postgres:

```
dpkg -l | grep postgres
```

Удалите все перечисленные выше пакеты с помощью команды

```
sudo apt purge package1 package2...
```

7. РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

7.1. Методы резервного копирования

Существует два фундаментально разных подхода к резервному копированию данных в ПК «КОМРАД»:

– с применением программы pgAdmin;

– сохранение резервных копий в объектное хранилище Komrad-S3.

7.2. Резервное копирование в программе pgAdmin

1) запустите pgAdmin;

2) найдите меню **Browser** (Браузер) с левой стороны. Нажмите правой кнопкой мыши на пункт **Servers** (Серверы), чтобы открыть контекстное меню, наведите курсор мыши на пункт **Create** (Создать) и нажмите **Server…** (Сервер…). В результате в браузере появится окно, в котором вы должны ввести информацию о вашем сервере, роли и базе данных;

3) на вкладке **General** (Общее) введите имя сервера;

4) на вкладке **Connection** (Подключение), в поле **Host name/address** (Имя хоста/адрес) введите localhost. В поле **Port** (Порт) необходимо задать значение 5432 по умолчанию, которое будет работать для этой настройки, поскольку это порт, используемый для PostgreSQL по умолчанию;

5) в поле **Maintenance database** (Поддержание базы данных) введите имя базы данных, к которой вы хотите подключиться. Обратите внимание, что эта база данных должна быть уже создана на вашем сервере. Затем введите имя пользователя и пароль PostgreSQL, которые вы настроили ранее в полях **Username** (Имя пользователя) и **Password** (Пароль);

6) пустые поля в других вкладках являются опциональными, их необходимо заполнять, если у вас есть конкретные требования для установки, где они могут потребоваться. Нажмите кнопку **Save** (Сохранить), после чего база данных появится в списке **Servers** (Серверы) в меню **Browser** (Браузер);

7) правый клик мышкой по базе данных, которой необходимо сделать резервное копирование и выбрать пункт **Backup** (Резервная копия):

– укажите имя файла и путь для сохранения файла;

– укажите формат:

В pgAdmin 4 есть несколько форматов выгрузки базы в дамп:

– **Custom** (Специальный) - формат архива рекомендуется для средних и больших баз данных, поскольку он по умолчанию сжимается;

– **Tar** - формат рекомендуется выбирать для малых баз. (Для коэффициента сжатия в таком случаи оставляем пустое значение, так как **Tar** не поддерживает сжатие);

– **Plain** (Простой) - формат нужен, чтоб создать файл сценария с открытым текстом. Будет создан файл сценария с открытым текстом, который содержит инструкции и команды SQL. Файл резервной копии в “Простом” формате можно отредактировать в текстовом редакторе при необходимости;

– **Directory** (Каталог) - этот формат предназначен, чтобы создать архив в формате каталога. Этот формат файла создает каталог с одним файлом для каждой таблицы и сбрасывается blob! (blob – крупные объекты в резервной копии.), а также файл оглавления, описывающий сбрасываемые объекты в машиночитаемом формате, который может читать pg_restore.

– **Compression ratio** (коэффициент сжатия) - здесь можно указать значение коэффициента от 0 до 9, или оставить поле пустым (кроме **Tar**);

– **Encoding** (Кодировка) - указывать не нужно;

– **Number of jobs** (Число заданий) - указывать не нужно;

Число заданий - настройка позволяет указать количество таблиц, которые будут сбрасывать одновременно в параллельной резервной копии.

– **Role name** (Имя роли) - указать нужно рута «postgres».

8) вкладку **Dump options** (Параметры выгрузки) оставляем без изменений.

9) после того, как все нужные поля заполнены, то выполните клик по кнопке **Backup** (Резервная копия).

7.3. Резервное восстановление в программе pgAdmin

1) запустите pgAdmin;

2) найдите меню **Browser** (Браузер) с левой стороны. Нажмите правой кнопкой мыши на пункт **Servers** (Серверы), чтобы открыть контекстное меню, наведите курсор мыши на пункт **Create** (Создать) и нажмите **Server**… (Сервер…). В результате в браузере появится окно, в котором вы должны ввести информацию о вашем сервере, роли и базе данных.

3) на вкладке **General** (Общее) введите имя сервера.

4) на вкладке **Connection** (Подключение), в поле **Host name/address** (Имя хоста/адрес) введите localhost. В поле **Port** (Порт) необходимо задать значение 5432 по умолчанию, которое будет работать для этой настройки, поскольку это порт, используемый для PostgreSQL по умолчанию.

5) в поле **Maintenance database** (Поддержание базы данных) введите имя базы данных, к которой вы хотите подключиться. Введите имя пользователя и пароль PostgreSQL, которые вы настроили ранее в полях **Username** (Имя пользователя) и **Password** (Пароль).

6) пустые поля в других вкладках являются опциональными, их необходимо заполнять, если у вас есть конкретные требования для установки, где они могут потребоваться. Нажмите кнопку **Save** (Сохранить), после чего база данных появится в списке **Servers** (Серверы) в меню **Browser** (Браузер).

7) создайте базы данных. На Database кликните правой кнопкой мыши, далее **Create → Database**:

– komrad-preferences;

– pauth-preferences;

– scanner;

– komrad-events.

8) выбираем базу данных **KOMRAD-EVENTS**, далее выбираем **Menu → Tools → Restore...** В появившимся окне выберете пункт меню Filename и укажите файл резервной копии базы данных, которую необходимо восстановить:

– komrad-preferences-backup;

– pauth-preferences-backup;

– scanner-backup;

– komrad-events-backup.

Нажмите на кнопку **RESTORE** и дождитесь процесса восстановления. Восстановите оставшиеся базы данных.

7.4. Объектовое хранилище Komrad-S3

7.4.1. Архитектура хранилища

Komrad-S3 – это высокопроизводительное объектное хранилище для хранения неструктурированных данных большого объема, таких как изображения, видео, файлы журналов, образы виртуальных машин, а также системы резервного копирования и восстановления ПК «КОМРАД».

7.4.1.1. Объектное хранилище Komrad-S3

Объект – это двоичные данные, иногда называемые большим двоичным объектом (BLOB). BLOB-объекты могут быть большими архивами, изображениями, аудиофайлами, электронными таблицами и т.д.

Komrad-S3 использует корзины для организации объектов. Корзина похожа на папку или каталог в файловой системе, где каждая корзина может содержать произвольное количество объектов.

7.4.1.2. Архитектура системы Komrad-S3

1) Режим локального хранилища. Данный режим подразумевает создание отдельной папки, где будут храниться все данные на одном сервере. В этой конфигурации потеря информации крайне высока. Крайне не рекомендуется создание на одном жёстком диске несколько логических дисков, так как при поломке жесткого диска возможна потеря всей информации.

2) Режим дискового массива. Набор дисков на одном сервере с поддержкой алгоритма восстановления потерянных и поврежденных данных, что обеспечивает высокую доступность, надежность и целостность данных. Komrad-S3 делит объекты на части и равномерно распределяет их по каждому диску. Komrad-S3 может продолжать беспрепятственно обслуживать запросы на чтение и запись, несмотря на потерю до половины дисков.

3) Режим серверной группировки. Набор сервером с установленным на каждом сервисом (сервером) Komrad-S3, которые объединяют свои диски и ресурсы для поддержки запросов на хранение и извлечение объектов. При развёртывании сервиса (сервера) Komrad-S3 необходимо обеспечить одни и те же настройки на всех узлов.

7.4.1.3. Рекомендации по работе Komrad-S3

Для гарантированного восстановления данных рекомендуется не менее 4 узлов на кластер, или 4-х жестких дисков в одном сервере. Это позволит перенести потерю до половины узлов или половины дисков с обеспечением целостности информации.

7.4.1.4. Возможности Komrad-S3

1) уведомления корзины, когда в корзине происходят определенные события.

2) управление версиями поддерживает хранение нескольких «версий» объекта в одной корзине. Операции записи, которые обычно перезаписывают существующий объект, вместо этого приводят к созданию нового объекта с версией.

Внимание! Данный режим включается только в момент создания корзин.

3) коды избыточности – это функция избыточности и доступности данных, которая позволяет автоматически восстанавливать объекты на лету, несмотря на потерю нескольких дисков или узлов в кластере. Коды избыточности обеспечивают восстановление на уровне объекта с меньшими накладными расходами, чем смежные технологии, такие как RAID или репликация.

4) репликация сегментов – это автоматическая конфигурация на уровне сегментов, которая синхронизирует объекты между кластерами и поддерживает одностороннюю «активно-пассивную» и двустороннюю «активно-активную» конфигурации.

7.5. Установка сервера Komrad-S3

Установка Komrad-S3 разделена на 3 этапа:

– подготовка к установке;

– запуск сервера в одном из 2-х конфигураций;

– создание корзин.

7.5.1. Этап 1. Подготовка к установке

1) Создайте на сервере, где будет размещаться объектовое хранилище Komrad-S3, папку ***komrad***.

2) Скопируйте из дистрибутива ПК «КОМРАД» на сервер в папку ***komrad*** файл ***komrad-s3_v4.1.33_amd64.deb***.

7.5.2. Этап 2. Запуск Komrad-S3

Запуск сервиса (сервера) Komrad-S3 возможен в 2 конфигурациях:

1) Локальное хранилище;

2) Дисковый массив.

7.5.2.1. Локальное хранилище

Конфигурация локального хранилища состоит из одного сервиса (сервера) Komrad-S3 с одним диском и папкой для хранения данных.

7.5.2.2. Локальное хранилище. Шаг 1. Создание папки

Внимание! Объем диска, в котором создается папка ***Data*** должен быть не менее 100Гб. Производите мониторинг места на жестком диске. Если места на диске будет недостаточно, то система резервного копирования и восстановления будет работать некорректно. В этой конфигурации потеря информации крайне высока, т. к. все данные находятся на одном жестком, в одной папке.

Создайте папку в директории пользователя, работающего с ПК «КОМРАД», где будут храниться файлы с данными резервного копирования.

```
mkdir Data
```

Где `Data` название папки.

7.5.2.3. Локальное хранилище. Шаг 2. Установка Komrad-S3

Перейдите в папку с файлом ***komrad-s3_v4.1.33_amd64.deb*** и установите Komrad-S3 выполнив команду в терминале:

```
sudo dpkg -i ./*.deb
```

Скопируйте в папку ***/var/lib/echelon/komrad/komrad-s3/.s3/certs*** файлы ***server.pem*** и ***server-key.pem***, которые были сгенерированы на отдельной ЭВМ. Инструкция по установке и генерации ключей описаны в соответствующих пунктах по установке ПК «КОМРАД» на операционные системы.

Скопируйте в папку ***/var/lib/echelon/komrad/komrad-s3/.s3/certs/CAs*** файл ***ca.pem,*** который был сгенерирован на отдельной ЭВМ. Инструкция по установке и генерации ключей описаны в соответствующих пунктах по установке ПК «КОМРАД» на операционные системы.

7.5.2.4. Локальное хранилище. Шаг 2. Доступ к сервису

Доступ к сервису (серверу) Komrad-S3 осуществляется при помощи веб-интерфейса по адресу https://IP-адрес_сервера:9050/ или https://localhost:9050, имя пользователя и пароль: komradadmin.

Для работы с сервисом (сервером) используется инструмент командной строки Komrad-S3 Client mc, описанный в соответствующем разделе.

Процесс создание корзин описан в Этапе 3.

7.5.2.5. Дисковый массив

Конфигурация в режиме дискового хранилища состоит из одного сервиса (сервера) Komrad-S3 установленного на сервер с не менее чем с 4 жесткими дисками.

Для Linux:

– убедитесь, что все жесткие диски имеют одинаковый размер. Желательно использовать жесткие диски из одной партии.

– убедитесь, что все жесткие диски примонтированы в ***/mnt*** и имеют системное название Disk1, Disk2, Disk3, Disk4.

7.5.2.6. Дисковый массив. Шаг 1. Установка и копирование файлов

Для Linux:

1) Установите Komrad-S3 выполнив команду в терминале:

```
sudo dpkg -i ./komrad-s3_v4.1.33_amd64.deb -y
```

2) Скопируйте в папку ***/var/lib/echelon/komrad/komrad-s3/.s3/certs*** файлы ***server.pem*** и ***server-key.pem***, которые были сгенерированы на отдельной ЭВМ. Инструкция по установке и генерации ключей описаны в соответствующих пунктах по установке ПК «КОМРАД» на операционные системы;

3) Скопируйте в папку ***/var/lib/echelon/komrad/komrad-s3/.s3/certs/CAs*** файл ***ca.pem***, который был сгенерирован на отдельной ЭВМ. Инструкция по установке и генерации ключей описаны в соответствующих пунктах по установке ПК «КОМРАД» на операционные системы.

7.5.2.7. Дисковый массив. Шаг 2. Запуск Komrad-S3 сервис (сервер)

В терминале выполните команду:

```
komrad-s3 server /mnt/disk{1...4}/data
```

Дескрипторы { } обозначают последовательность и количества дисков.

Результатом выполнения команды будет:

– ***/mnt/disk1/data***;

– ***/mnt/disk2/data***;

– ***/mnt/disk3/data***;

– ***/mnt/disk4/data***.

7.5.2.8. Дисковый массив. Шаг 3. Доступ к сервису (серверу) Komrad-S3

Доступ к сервису (серверу) Komrad-S3 осуществляется при помощи веб-интерфейса по адресу: http://IP-адрес_сервера:9050 или https://localhost:9050.

Для работы с сервисом (сервером) используется инструмент командной строки Komrad-S3 Client mc, описанный в соответствующем разделе.

Создание корзин описаны в Этапе 3.

7.5.3. Этап 3. Создание корзины

Клиент Komrad-S3-admin позволяет управлять объектным хранилищем из командной строки и представляет альтернативу командам Linux по просмотру файлов, работой с файловой системой и управлению корзинами.

komrad-s3-admin имеет следующий синтаксис:

```
komrad-s3-admin [флаг] КОМАНДА [АРГУМЕНТЫ...] [ФЛАГ КОМАНД | -h]
```

7.5.3.1. Подключение к серверу Komrad-S3

Для удобства подключения создайте алиас подключения:

```
komrad-s3-admin alias set komrads3 http://192.168.1.1:9050 login password
```

Где:

1) komrads3 – укажите своё название сервиса (сервера);

2) 192.168.1.1 – IP-адрес, где установлен сервис Komrad-S3;

3) login\password – аутентификационные данные указанные в шаге установки сервиса.

7.5.3.2. Просмотр списка алиасов

Синтаксис команды:

```
komrad-s3-admin alias list
```

7.5.3.3. Удаление алиаса подключения

Синтаксис команды:

```
komrad-s3-admin alias remove НАЗВАНИЕ АЛИАСА
```

Пример:

```
komrad-s3-admin alias remove komrads3 - удаляет алиас подключения komrads3
```

7.5.3.4. Тестирование подключения к серверу

Для тестирования подключения к серверу Komrad-S3, используйте следующую команду:

```
komrad-s3-admin admin info komrads3
```

где komrads3 – название сервера при установке алиаса.

7.5.3.5. Создание корзины

Команда `komrad-s3-admin mb` создает новую корзину или каталог по указанному пути.

Синтаксис команды:

```
komrad-s3-admin mb [флаг] путь до сервиса/название корзины
```

Пример:

```
komrad-s3-admin mb -l komrads3/komrad-backup
```

команда создаст корзину komrad-backup на сервере komrads3.

Флаги:

1) `--p` - игнорирует, если корзина или папка уже созданы;

2) `--l` - включает блокировку объекта в указанном сегменте.

7.5.3.6. Копирование файлов в корзину

Команда `komrad-s3-admin cp` копирует данные из одного или нескольких источников в Komrad-S3.

Синтаксис команды:

```
komrad-s3-admin cp [флаг] путь до сервиса/название корзины
```

Пример:

```
komrad-s3-admin cp название файла komrads3/komrad-backup
komrad-s3-admin cp -r c:\название папки komrads3/komrad-backup
```

Первая команда скопирует указанный файл, вторая команда скопирует всю указанную папку.

Флаги:

1) --vid – копирует только указанные версии объектов;

2) --r – рекурсивное копирование файлов из директории.

7.5.3.7. Вывод списка объектов в объектовом хранилище

Команда выводит список всех корзин и список всех файлов, находящихся в корзинах.

Синтаксис команды:

```
komrad-s3-admin ls [флаг] путь до сервиса/название корзины
```

Примеры:

1) Покажет все корзины:

```
komrad-s3-admin ls komrads3
```

2) Покажет все корзины и файлы, находящиеся в них:

```
komrad-s3-admin ls -r komrads3
```

Флаги:

1) -r – рекурсивно перечисляет содержимое каждой корзины или каталога;

2) --versions – показывает версию объектов при условии включения функции управления версиями корзины;

3) -- incomplete – возвращает все незавершенные загрузки.

7.5.3.8. Удаление корзины

Удаление корзины с помощью `komrad-s3-admin rb` также удаляет все конфигурации, связанные с этой корзиной. Чтобы удалить только содержимое корзины, используйте вместо этого `komrad-s3-admin rm`.

Синтаксис:

```
komrad-s3-admin rb [флаг] путь до сервиса/название корзины
```

Пример:

Команда удалит из сервера komrads3 корзину komrad-backup:

```
komrad-s3-admin rb –force komrads3/komrad-backup
```

Флаги:

1) --force – позволяет запускать mc rb в корзине с включенным управлением версиями;

2) --dangerous – удаление корня объектового хранилища.

7.5.3.9. Удаление содержимого корзины

Команда `komrad-s3-admin rm -r –force` удаляет файлы из указанной корзины.

Синтаксис:

```
komrad-s3-admin rm -r -- force путь до сервиса/название корзины
```

Пример:

Команда удалит из корзины komrad-backup все файлы:

```
komrad-s3-admin rm -r -- force komrads3/komrad-backup
```

Флаг --r – рекурсивное удаление всех файлов и папок.

7.5.3.10. Перемещение файлов в корзины

Команда `komrad-s3-admin mv` переместит с удалением файлы и папки.

Синтаксис:

```
komrad-s3-admin mv название файла путь до сервиса/название корзины
komrad-s3-admin mv -r название папки путь до сервиса/название корзины
```

Пример:

```
komrad-s3-admin mv название файла komrads3/komrad-backup
komrad-s3-admin mv -r название папки komrads3/komrad-backup
komrad-s3-admin mv -r komrad1/backup komrads3/komrad-backup
```

В первом примере переместиться файл, во втором примере переместиться папка, в третьем примере переместиться папка ***/backup*** с сервера Komrad-S3 под именем ***komrad1*** в папку ***/komrad-back-up*** сервера komrads3.

7.5.3.11. Просмотр файлов и папок в виде дерева

Команда `komrad-s3-admin tree` покажет древовидную структура папок и файлов.

Синтаксис:

```
komrad-s3-admin tree название сервиса
```

Пример:

```
komrad-s3-admin tree komrads3
komrad-s3-admin tree -- file komrads3
```

Первая команда выведет список корзин и папок, вторая команда выведет список файлов в корзинах и папках.

7.5.3.12. Работа с пользователями

Команда добавление пользователя:

```
komrad-s3-admin admin user add ALIAS ACCESSKEY SECRETKEY
```

Пример команды добавления пользователя:

```
komrad-s3-admin admin user add komrads3 komradadmin komradadmin
```

Команда удаления пользователя:

```
komrad-s3-admin admin remove alias username
```

Пример команды удаления пользователя:

```
komrad-s3-admin admin remove komrads3 komradadmin
```

Команда просмотра списка пользователей:

```
komrad-s3-admin user list alias
komrad-s3-admin user info alias username
```

Пример команды просмотра списка пользователей:

```
komrad-s3-admin user list komrads3
komrad-s3-admin user info komrads3 komradadmin
```

В первом примере выведутся все пользователи, во втором подробная информация о пользователе.

Команды блокировки и разблокировки пользователей:

```
komrad-s3-admin admin user disable alias username
komrad-s3-admin admin user enable alias username
```

Примеры команд блокировки и разблокировки пользователей:

```
komrad-s3-admin admin user disable komrads3 komradadmin
komrad-s3-admin admin user enable komrads3 komradadmin
```

В первом примере пользователь будет заблокирован, аутентификация будет невозможна, но данные пользователя останутся в системе. Во втором примере пользователь разблокируется.

7.6. Резервное копирование в объектное хранилище Komrad-S3

Для резервного копирования и восстановления необходимо наличие объектового хранилища Komrad-S3. Создание объектного хранилища описана в п.7.5 настоящего руководства.

Вся процедура резервного копирования сводится к нескольким этапам:

1) Подготовка объектного хранилища Komrad-S3;

2) Создание конфигурационного файла для подключения к Komrad-S3;

3) Настройка PostgreSQL к резервному копированию;

4) Создание первого снимка базы;

5) Резервное копирование.

7.6.1. Этап 1. Подготовка объектного хранилища Komrad-S3

7.6.1.1. Шаг 1. Создание корзины в Komrad-S3

7.6.1.1.1. Создание корзины в Komrad-S3 сервисе через web-интерфейс

Внимание! Далее название корзины в примерах будет komrad-backup.

Веб-интерфейс доступен по адресу https://IP-адрес_KOMRAD-S3:9050.

– Нажмите на «Корзины» в левом столбце и «+ Создать корзину» (create backet);

– Введите название корзины ***komrad-backup;***

Внимание! Название корзин должно быть с маленьких букв.

– Созданная корзина появится в списке корзин слева.

7.6.1.1.2. Создание корзины при помощи консольной утилиты komrad-s3-admin

1) В Linux создайте алиас подключения к серверу Komrad-S3 следующей командой:

```
komrad-s3-admin alias set --insecure komrads3 https://localhost:9050 login password
```

Где:

– `komrads3` – укажите своё название сервиса (сервера);

– `localhost` – IP-адрес, где установлен сервис Komrad-S3;

– `login\password` – аутентификационные данные указанные в шаге установки сервиса.

2) Создайте корзину следующей командой:

```
komrad-s3-admin mb komrads3/komrad-backup
```

Где:

– `komrads3` – название алиаса подключения к Komrad-S3 серверу;

– komrad-backup – название корзины, где будут храниться данные.

7.6.1.2. Шаг 2. Добавление переменной S3_CA_CERT_FILE в систему переменных сред

Добавьте переменную S3_CA_CERT_FILE в систему переменных сред с указанием пути и файла, где лежит корневой сертификат ***ca.pem***:

В Linux путь: ***/var/lib/echelon/komrad/certs/ca.pem***

Отредактируйте файл:

```
sudo nano /etc/environment
```

задав переменную:

```
S3_CA_CERT_FILE=”/var/lib/echelon/komrad/certs/ca.pem”
```

7.6.2. Этап 2. Создание конфигурационного файла для подключения к Komrad-S3

В Linux:

1) Создайте папку ***komrad-data***;

2) Создайте в ***/komrad-data*** подпапку ***/data***;

3) Создайте в ***/komrad-data*** подпапку ***/wal*** для временного хранения файлов бэкапирования.

Совет! Введите:

```
mkdir komrad-data komrad-data/data komrad-data/wal
```

4) Скопируйте из ***/etc/echelon/komrad/komrad-backup*** файл ***komrad-backup.toml*** в папку ***/komrad-data***;

Совет! Команда выполняется в одну строчку:

```
sudo cp /etc/echelon/komrad/komrad-backup/komrad-backup.toml /home/путь_до_файла/komrad-data/
```

5) Отредактируйте файл ***komrad-backup.toml***;

Совет! Путь: ***/home/путь_до_файла/komrad-data/komrad-backup.toml***

```
######### Общие настройки ###############

# WALG_PREFETCH_DIR - папка для скачивания WAL файлов, в PostgreSQL 13+ необходимо хранить
# их вне основной папки pg_wal
WALG_PREFETCH_DIR="/home/имя_пользователя/komrad-data/wal"          #-укажите путь к папке для временного хранения файлов бэкапирования
```

```
S3_CA_CERT_FILE="/var/lib/echelon/komrad/certs/ca.pem"

PGDATA="/var/lib/postgresql/13/main"  #- укажите путь до папки с данными
PGHOST="/var/run/postgresql"
PGUSER="postgres"
PGDATABASE="komrad-preferences"

######### 1. Хранение в KOMRAD-S3/Minio ###############

WALG_S3_PREFIX="s3://komrad-backup"  #- укажите название корзины, созданной в KOMRAD-S3
AWS_ACCESS_KEY_ID="minioadmin" #- укажите логин
AWS_SECRET_ACCESS_KEY="minioadmin" #- укажите пароль
AWS_ENDPOINT="192.168.6.139:9050"  #- укажите адрес и порт, где установлен KOMRAD-S3
AWS_S3_FORCE_PATH_STYLE="true"
```

7.6.3. Этап 3. Настройка PostgreSQL к резервному копированию

7.6.3.1. Шаг 1. Редактирование файла postgresql.conf

1) В блоке директив файла раскомментируйте:

Совет! Введите для открытия:

```
sudo nano /etc/postgresql/version/main/postgresql.conf
```

Где вместо `version` укажите версию PostgreSQL.

```
# WRITE-AHEAD LOG
wal_level = replica
archive_mode = on
```

2) Для Linux укажите путь, где лежит ***komrad-backup.exe*** и ***komrad-backup.toml***:

```
archive_command = 'komrad-backup wal-push %p --config /home/имя_пользователя/komrad-data/komrad-backup.toml --s3-ca-cert-file /var/lib/echelon/komrad/certs/ca.pem'
restore_command = 'komrad-backup wal-fetch %f %p --config /home/имя_пользователя/komrad-data/komrad-backup.toml --s3-ca-cert-file /var/lib/echelon/komrad/certs/ca.pem'
archive_timeout = 60  //время в секундах, через которое будет производиться архивирование
```

7.6.3.2. Шаг 2. Создание файла .pspass

Создайте в папке ***komrad-data*** файл ***.pgpass*:**

```
127.0.0.1:5432:komrad-preferences:postgres:pass
127.0.0.1:5432:komrad-events:postgres:pass
127.0.0.1:5432:pauth-preferences:postgres:pass
127.0.0.1:5432:scanner:postgres:pass
```

7.6.3.3. Шаг 3. Перезапуск PostgreSQL

Перезапустите PostgreSQL

7.6.4. Этап 4. Создание первого снимка базы

Сделайте первоначальную резервную копию:

1) Для Linux в терминале выполните команду:

```
komrad-backup backup-push --config /home/имя_пользователя/komrad-data/komrad-backup.toml --pgpassfile /home/имя_пользователя/komrad-data/.pgpass
```

2) Дождитесь окончания резервного копирования.

7.7. Резервное восстановление из объектного хранилища Komrad-S3

В случае, если ПК «КОМРАД» и СУБД функционируют на одном узле, то установите ПК «КОМРАД» в соответствии с руководством по установке.

Если СУБД находится на отдельном сервере, то достаточно установить PostgreSQL, TimescaleDB.

Совет! Если СУБД переноситься на другой сервер с изменением IP-адреса, то необходимо в конфигурационных файлах отредактировать путь к СУБД и перевыпустить сертификат на ЭВМ с СУБД.

Более подробная информация представлена в разделах по установке ПК «КОМРАД» на отдельных узлах.

7.7.1. Шаг 1. Перенос сертификатов

Перенесите новые сертификаты: ***server.pem***, ***server-key.pem*** на сервер Komrad-S3.

В папку ***komrad/komrad-s3/.s3/certs*** и ***ca.pem*** в папку ***komrad/komrad-s3/.s3/certs/CAs/.***

Удалите старые сертификаты и установите новые сертификаты в браузер.

7.7.2. Шаг 2. Остановка PostgreSQL

Остановите PostgreSQL.

7.7.3. Шаг 3. Удаление содержимого папки

Удалите все из папки выполнив:

```
sudo su
rm -f /var/lib/postgresql/13/main/*
```

7.7.4. Шаг 4. Повторение Этапа 2

Произведите действия пункта 7.6.2. «Этап 2. Создание конфигурационного файла для подключения к Komrad-S3» или скопируйте файлы ***komrad-backup.toml*** и ***.pgpass*** с ЭВМ, где ранее был настроена система резервного копирования, в папку ***komrad-data/***.

7.7.5. Шаг 5. Скачивание резервной копии

Выполните команду:

```
komrad-backup backup-fetch /var/lib/postgresql/13/main LATEST --config /home/имя_пользователя/komrad-data/komrad-backup.toml
```

7.7.6. Шаг 6. Создаем пустой файл recovery.signal

Создаём пустой файл ***recovery.signal*** и размещаем в ***var/lib/postgresql/*v/main***

Файл должен быть создан от пользователя postgres.

7.7.7. Шаг 7. Запуск базы данных

Запускаем базу данных, чтобы она инициализировала процесс восстановления.

```
sudo systemctl start postgresql
```

Процесс восстановления закончится после того, как сигнальный файл ***recovery.signal*** пропадёт из папки ***/var/lib/postgresql/*v/main***

8. ИНТЕГРАЦИЯ С ВНЕШНИМИ СИСТЕМАМИ

8.1. Настройка отправки уведомлений по SMTP

Для обеспечения возможности отправки уведомлений об инцидентах по электронной почте в конфигурационном файле ***komrad-server.yaml*** задайте параметры отправителя и подключения к почтовому серверу в блоке директив:

```
notificationtransport:
senderaddress: sender@localhost      //адрес от кого будет приходить
                                     сообщения
  emailtransports:
      name: SMTP Service
      client:
        host: email.server.lan       //IP адрес или имя почтового
        idletimeout: 30s             сервера
        noverify: true
        password: password
        port: 25                     //пароль пользователя
        username:                    //порт почтового сервера
username@localhost                   //пользователь почтового сервера
```

В состав сообщения можно включать предустановленные поля с информацией инцидента при помощи встроенного языка запросов.

8.1.1. Язык запросов

Язык запросов разделён на объекты и теги.

8.1.1.1. Объекты

Объекты сообщают, где показывать информацию из полей в тексте сообщении.

Имена объектов и переменных обозначаются двойными фигурными скобками:

```
{{   Предустановленное поле  }}
```

Пример:

```
Тип инцидента: {{  GosSOPKAIncidentType  }}
```

В этом случае в тексте сообщения содержимое объекта с именем `GosSOPKAIncidentType`, будет содержать текст о типе инцидента:

```
Тип инцидента: Компрометация учётной записи.
```

8.1.1.2. Теги

Теги создают логику и поток управления для вывода информации. Фигурные скобки, разделители процентов `{%  теги и текс  %}` который они окружают, не производят видимого

вывода при выводе сообщений. Это позволяет вам назначать переменные и создавать условия или циклы, не отображая на странице какую-либо логику.

Теги разделяются на несколько типов:

1) Логические операторы (if, unless, elsif/else, case/when);

2) Циклы (for, else, break, continue, limit, offset, range, reversed, cycle, tablerow);

3) Работа с шаблоном вывода (comment, raw, liquid, echo, render, include);

4) Работа с переменными (assign, capture, increment, decriment).

Пример:

```
{% if incident.EventKeys != null %}
{% for key in incident.EventKeys %}
{{ key }}{% endfor %}
{% else %}Событий не найдено, возможно ошибка в директиве корреляции.
{% endif %}
```

8.1.2. Пример электронного сообщения

```
Внимание!

В {{ incident.InitialTime | date: "%H:%M %d-%m-%Y" }}
сработала директива {{ incident.DirectiveName }}
на активе {% for ip in incident.Assets %} {{ ip | IPToString}} {% endfor %}, установленном
в {{ incident.TenantID }}.

Степень важности инцидента - {{ incident.Severity | ru }}
Тип инцидента – {{ incident.GosSOPKAIncidentType }}

Ответственным за инцидент назначен -  {{ incident.AssignedTo }}
По данному инциденту необходимо выполнить следующие рекомендации:
{{ incident.Recommendations }}

Справочно:
Номер инцидента: {{ incident.ID }}
Номер директивы: {{ incident.DirectiveID }}
События, благодаря которым был сгенерирован инцидент:
=====
{% if incident.EventKeys != null %}
{% for key in incident.EventKeys %}
{{ key }}{% endfor %}
{% else %}Событий не найдено, возможно ошибка в директиве корреляции.
{% endif %}
=====
```

Предустановленные поля с информацией из инцидента представлены в таблице 18.

Таблица 18 – Поля в ПК «КОМРАД», которые используются при отправке сообщений

Название поля	Описание

Название поля	Описание
incident.ID	Номер инцидента
incident.DirectiveID	Номер директивы
incident.AssignedTo	Ответственный за инцидент
incident.InitialTime	Время первого события, из числа всех событий выявленного инцидента
incident.Severity	Уровень инцидента (несущественный, низкий, средний, высокий)
incident.Recommendations	Рекомендации из директивы
incident.TenantID	Идентификатор места установки коллектора
incident.Assets	IP адрес актива
incident.HasErrors	Возможно ложное срабатывание или неправильно написано правило корреляции
incident.DirectiveName	Имя директивы
incident.GosSOPKAIncidentType	Тип инцидента из справочника

8.2. Настройка отправки инцидентов по протоколу Syslog в формате CEF

Для обеспечения возможности отправки инцидента по Syslog в формате CEF:

1) в конфигурационном файле ***komrad-server.yaml*** задайте следующие параметры раскомментируйте все поля блока cef, убрав «#» перед строками:

```
cef:
 recipient:
 - "tcp://192.168.6.156:49000"  #– укажите IP-адрес и порт куда отправлять данные
 - "utp://192.168.6.156:49050" #– укажите IP-адрес и порт куда отправлять данные
 hostname: komrad-node #– укажите название ЭВМ, где установлен ПК КОМРАД
 version: 0
 devicevendor: NPOECHELON
 deviceproduct: KOMRAD-SIEM
 deviceversion: v4.0.10
 deviceeventclassid: SIEM
 name: komrad-server Moskwa Elektrozavodskaya 24 #– можно указать адрес установки
```

```
 severity: 0
mapping: "/etc/echelon/komrad/komrad-server/komrad-server-notification-mapping-syslog-cef.yaml
```

2) в файле ***komrad-server-notification-mapping-syslog-cef.yaml*** раскомментируйте или закомментируйте поля те поля событий, которые необходимо передавать в событии. Список полей с описанием представлен в таблице 19.

Таблица 19 – Список полей файла ***komrad-server-notification-mapping-syslog-cef.yaml***

Название поля	**CEF**	**Описание**
incident.ID	ECS.Event.ID	Номер инцидента
incident.DirectiveID	ECS.Rule.ID	Номер директивы
incident.AssignedTo	ECS.Rule.Author	Ответственный за инцидент
incident.InitialTime	ECS.Event.Start	Время первого события, из числа всех событий выявленного инцидента
incident.Severity	ECS.Event.Severity	Уровень инцидента (несущественный, низкий, средний, высокий)
incident.Recommendations	ECS.Threat.TechniqueReference	Рекомендации из директивы
incident.TenantID	ECS.Organization.ID	Идентификатор места установки коллектора
incident.Assets	ECS.Related.IP	IP адрес актива
incident.HasErrors	ECS.Error.Message	Возможно ложное срабатывание или неправильно написано правило корреляции
incident.DirectiveName	ECS.Rule.Name	Имя директивы
incident.*GosSOPKAIncidentType*	ECS.Rule.Category	Тип инцидента из справочника
incident.RegistrationTime	ECS.Event.Ingested	Время регистрации инцидента менеджером инцидентов.
incident.CloseTime	ECS.Event.End	Время закрытия инцидента.
incident.StatusReason – характерен для IRP систем, в ECS нет подходящего поля	reason	Причина (пояснение) установки того или иного статуса.
incident.Description	ECS.Rule.Description	Описание инцидента, задаётся пользователем.
incident.EventKeys	ECS.Related.Hash	События, благодаря которым был

Название поля	CEF	Описание
		сгенерирован инцидент.

9. АКТИВАЦИЯ ЛИЦЕНЗИИ SIEM ПК «КОМРАД»

При поставке ПК «КОМРАД» будет предоставлен файл лицензии формата:

1) komrad-base.lic – возможный вариант наименования файла лицензии Base;
2) komrad-aio.lic – возможный вариант наименования файла лицензии All-in-One;
3) komrad-ent.lic – возможный вариант наименования файла лицензии Enterprise.

9.1. Активация лицензии

Для активации лицензии скопируйте файл лицензии в папку ***/etc/echelon/komrad/license***.

Перезапустите сервисы komrad-server и komrad-processor.

9.2. Информация о лицензии

Информацию о версии ПК «КОМРАД», сроке и виде лицензии, номер лицензии, на какую организацию оформлена лицензия, количество EPS - возможно в веб-интерфейсе ПК «КОМРАД», описанном в документе НПЕШ.60010-03 34 «Руководство оператора».

9.3. Удаление лицензии

Удалите файл лицензии komrad с расширением (***.lic***) из папки ***/etc/echelon/komrad/license***.

9.4. Смена типа лицензии

В случае, когда необходимо сменить тип лицензии, сделайте следующие действия:

9.4.1. Шаг 1. Удаление файла лицензии

Удалите файл лицензии из папки ***/etc/echelon/komrad/license.***

9.4.2. Шаг 2. Копирование новой лицензии

Скопируйте новый файл лицензии в папку с лицензией.

9.4.3. Шаг 3. Перезапуск сервисов

Перезапустите сервисы komrad-server и komrad-processor:

```
sudo systemctl restart komrad-server
sudo systemctl restart komrad-processor
```

10. ДИАГНОСТИКА И РЕШЕНИЕ ПРОБЛЕМ

При возникновении проблем в процессе функционирования ПК «КОМРАД» диагностические сообщения выводятся в журналы системы.

10.1. Уведомления о состоянии системы

В ПК «КОМРАД» заложена функции уведомления о состоянии системы в виде сигнализатора/светофора в верхнем правом углу экрана. Каждый цвет сигнализирует об определённом состоянии:

1) Зеленый цвет сигнализирует об отсутствии каких-либо препятствий для функционирования всех сервисов;
2) Оранжевый цвет сигнализирует об удовлетворительном состоянии системы, что означает, что какие-то сервисы не работают;
3) Красный цвет сигнализирует об серьезных ошибках в процессе функционирования сервисов ПК «КОМРАД».

10.2. Ошибки и пути их решения

Описания возможных ошибок приведены в таблице 20.

Таблица 20 – Типы ошибок

Ошибка	Описание
got a panic; recovered, but please, report to Echelon support team	Сообщить текст ошибки с полным выводом лога в службу технической поддержки изготовителя.
failed to read WAL	Произошла ошибка чтения write-ahead-log коллектора. Возможная причина - повреждение данных в результате сбоя диска. Вероятна потеря накопленных пакетов событий. Если восстановление событий критически важно - обратитесь в службу технической поддержки изготовителя. В некритичных случаях рекомендуется удалить всю папку указанную в разделе `wal.path` коллектора, в котором обнаружен сбой, и перезагрузить сервис коллектора из консоли.

10.2.1. Ошибки komrad-processor

Описания возможных ошибок komrad-processor приведены в таблице 21.

Таблица 21 – Типы ошибок komrad-processor

Ошибка	Описание
flat keys query failed	Ошибка работы с БД komrad-events. Сообщить текст ошибки с полным выводом лога в службу технической поддержки изготовителя.
failed to set_chunk_time_interval in TimescaleDB events table with value from configuration file	Параметр set_chunk_time_interval регулирует производительность БД “События” и БД “Индексы” в зависимости от интенсивности потока данных. Рекомендуется использовать параметры по умолчанию. Ошибка обычно возникает при ручной установке параметра через конфигурационный файл komrad-processor.yaml - рекомендуется обратиться в службу технической поддержки изготовителя либо обратиться к документации TimescaleDB 2.0+.
failed to add_compress_chunks_policy in TimescaleDB events table	Параметр set_chunk_time_interval регулирует интенсивность сжатия исторических данных в БД “События” и БД “Индексы” в зависимости от интенсивности потока данных. Рекомендуется использовать параметры по умолчанию. Ошибка обычно возникает при ручной установке параметра через конфигурационный файл komrad-processor.yaml - рекомендуется обратиться в службу технической поддержки изготовителя либо обратиться к документации TimescaleDB 2.0+.
failed to decompress batch of events	Произошла ошибка распаковки пакета событий, полученного из брокера komrad-bus. Ошибка может связана с несовместимостью версий ПО после получения обновления. Рекомендуется проверить версии коллектора, брокера komrad-bus и komrad-processor.
failed to unmarshal batch of events	Произошла ошибка десериализации пакета событий, полученного из брокера komrad-bus. Ошибка может быть связана с несовместимостью версий ПО после получения обновления. Рекомендуется проверить версии коллектора, брокера komrad-bus и komrad-processor.

Ошибка	Описание
can't setup notification broker	Произошла ошибка во время попытки создать подписку на очередь изменения данных ПК «КОМРАД» (новые инциденты, изменения в инцидентах, новые отчёты, новые уведомления). ПК «КОМРАД» сможет продолжать работу, но функциональность оповещения внешних систем будет отключена. Рекомендуется изучить логи, связаться со службой технической поддержки изготовителя.

10.2.2. Ошибки komrad-server

Описания возможных ошибок komrad -server приведены в таблице 22.

Таблица 22 – Типы ошибок komrad -server

Ошибка	Описание
failed to subscribe to CDC Queue	Произошла ошибка во время попытки создать подписку на очередь изменения данных ПК «КОМРАД» (новые инциденты, изменения в инцидентах, новые отчёты, новые уведомления). ПК «КОМРАД» сможет продолжать работу, но функциональность оповещения внешних систем будет отключена. Рекомендуется изучить логи, связаться со службой поддержки изготовителя.

10.2.3. Ошибки komrad-processor и komrad-server

Описания возможных ошибок komrad-processor и komrad-server приведены в таблице 23.

Таблица 23 – Типы ошибок komrad-processor и komrad-server

Ошибка	Описание
filter does not exist	Данные по выбранному фильтру не валидны, либо потеряли актуальность - либо есть запись о фильтре в БД настроек, но нет индексов по нему, либо есть индексы по фильтру, записи о котором нет в БД настроек. Необходимо удалить проблемный фильтр и создать его заново, после обновить все зависящие от него правила корреляции, отчёты и дашборды.
failed to init filter	Фильтр не валиден. Если фильтр создан недавно – возможно, ошибка в синтаксисе, рекомендуется проверить фильтр и сохранить заново. Если ошибка возникает во время

Ошибка	Описание
	регулярной работы после рестарта ПК «КОМРАД» - рекомендуется проверить ошибочные фильтры, возможно, требуется чистка БД komrad-core. В крайнем случае попробуйте удалить ошибочный фильтр и создать его заново (данные исторической

10.2.4. Ошибки komrad-correlator

Описания возможных ошибок komrad-correlator приведены в таблице 24.

Таблица 24 – Типы ошибок komrad-correlator

Ошибка	Описание
failed to send SIGINT to a stc process, will try to kill	Неудачная попытка остановки коррелятора, работающего по директиве. Коррелятор был завершён с жёсткой терминацией (kill), возможна потеря инцидентов. Обычно такое происходит при дефиците ресурсов на узле корреляции. Рекомендуется изучить параметры узла, на котором работает коррелятор - объём доступной памяти, диска, загрузка процессора.

10.2.5. Ошибки komrad-collector

Описания возможных ошибок komrad-collector приведены в таблице 25.

Таблица 25 – Типы ошибок komrad-collector

Ошибка	Описание
failed to connect to message broke	Ошибка при подключении к брокеру сообщений Комрад. Необходимо проверить запущен ли брокер komrad-bus, достаточно ли ресурсов на узле брокера, проверить логи сообщений брокера, проверить доступность узла komrad-bus с узла, на котором произошла ошибка, порт брокера по умолчанию – 3490.
failed to send event batch	Возникла ошибка при отправке пакета событий ИБ из коллектора в брокер сообщений komrad-bus. В этом случае коллектор переходит в режим накопления сжатых пакетов событий на диске в write-ahead-log (WAL). После восстановления связи с komrad-bus должна произойти передача накопленных за период отсутствия связи пакетов

Ошибка	Описание
	событий. Рекомендуется наблюдать за потоком событий после устранения проблем в сети либо дефицита мощности оборудования.

10.2.6. Ошибки correlation-dispatcher

Описания возможных ошибок correlation-dispatcher приведены в таблице 26.

Таблица 26 – Типы ошибок correlation-dispatcher

Ошибка	Описание
failed to start a correlator	Не получилось запустить коррелятор по выбранной директиве. Рекомендуется ознакомиться с логом коррелятора.

10.2.7. Ошибки single-tasking-correlator

Описания возможных ошибок single-tasking-correlator приведены в таблице 27.

Таблица 27 – Типы ошибок single-tasking-correlator

Ошибка	Описание
failed to run a reaction	Неудачная попытка произвести реакцию на обнаруженный инцидент. Рекомендуется проверить логи сервиса komrad-reactor.

11. ОБРАЩЕНИЕ В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

11.1. Виды вопросов в техническую поддержку

Служба технической поддержки оказывает консультационную поддержку по вопросам:

– установки и настройки ПК «КОМРАД» в рамках эксплуатационной документации;

– моделированию проблемных ситуаций на собственном тестовом стенде;

– решению вопросов связанных подключением источников и работы коллекторов;

– помощь в написании директив безопасности;

– вопросы по администрированию продукта;

– восстановлению работоспособности продукта;

– вопросы, связанные с обновлением продукта;

– ответы по текущим обращениям и стадиям их решений.

11.2. Техническая поддержка по телефону и e-mail

На сайте www.npo-echelon.ru указаны актуальные телефоны, e-mail и время работы технической поддержки.

11.3. Необходимая информация при обращении в службу технической поддержки

При обращении в службу технической поддержки необходимо предоставить следующую информацию:

1) номер лицензии на ПК «КОМРАД»;

2) файлы журналов;

3) по возможности снимки экранов;

4) по взаимному согласию возможность предоставить средства удаленного доступа.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ	–	автоматизированное рабочее место
БД	–	база данных
ИАФ	–	идентификация и аутентификация субъектов доступа и объектов доступа
ИБ	–	информационная безопасность
«КОМРАД»	–	комплекс оперативного мониторинга, реагирования и анализа данных
ОС	–	операционная система
ОЦЛ	–	обеспечение целостности информационной системы и персональных данных
ПО	–	программное обеспечение
РСБ	–	регистрация событий безопасности
СЗИ	–	средства защиты информации
СОВ	–	система обнаружения вторжений
СУБД	–	система управления базами данных
УПД	–	управление доступом субъектов доступа к объектам доступа
ЭВМ	–	электронная вычислительная машина

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	изме-ненных	заме-ненных	новых	аннулиро-ванных					