KEO DLP

Версия 8.1.0

Руководство системного администратора

2025

Содержание

Список иллюстраций

Список таблиц

Перечень терминов и сокращений

АРМ	Автоматизированное рабочее место
БД	База данных
ИБ	Информационная безопасность
ИТ	Исключаемый текст
КА	Контентный анализ
МРД	Мандатное управление доступом
ОЕ	Организационная единица
ОС	Операционная система
ПО	Программное обеспечение
ПК	Программный комплекс
СХД	Система хранения данных
KEO DLP webProxy	Модуль контроля веб-трафика
СУБД	Система управления базами данных
УЗ	Учетная запись (пользователя)
УЦ	Удостоверяющий центр
ФХ	Файловое хранилище
ЦП	Центральный процессор – электронный блок либо интегральная схема, исполняющая машинные инструкции, главная часть аппаратного обеспечения компьютера или программируемого логического контроллера
ЭЦП	Электронная цифровая подпись
AD	Active Directory – служба каталогов для операционных систем семейства Windows. В каталоге хранятся сведения о различных объектах сетей, например, о компьютерах и учетных записях их пользователей. С помощью AD можно использовать групповые политики для единообразия настройки пользовательской рабочей среды и развертывания программного обеспечения на множестве компьютеров
CEF	Common Event Format – общий формат события
CLI	Command Line Interface – интерфейс командной строки
CRL	Certificate Revocation List – список отозванных сертификатов
DC	Domain controller — контроллер домена
DHCP	Dynamic Host Configuration Protocol – протокол динамической настройки узла
FQDN	Fully Qualified Domain Name – полное имя домена (имя домена, не имеющее неоднозначностей в определении)
GUI	Graphical User Interface – графический интерфейс пользователя
MD	Обозначение используется на рисунках и помечает элемент управления, отображаемый при наличии в системе модуля централизованного управления системой
MIME	Multipurpose Internet Mail Extension – многоцелевое расширение Интернет-почты

PID	Product Identifier – Идентификатор модели устройства
RFC	Request for Comments – спецификации и стандарты, применяемые в Интернет
SMB	Server Message Block – сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SMTP	Simple Mail Transfer Protocol – простой протокол передачи почты
TNEF	Transport Neutral Encapsulation Format – собственный формат вложений электронной почты, используемый Microsoft Outlook и Microsoft Exchange Server
TTS	Transportable Tablespaces – транспортируемые (перемещаемые) табличные пространства
VID	Vendor Identifier – Идентификатор производителя
Кластер	Совокупность серверов KEO DLP, соединенных между собой управляющими связями.
master-узел	Управляющий (главный) сервер кластера KEO DLP, непосредственно связанный с каждым из остальных.
slave-узел	Любой узел кластера KEO DLP, не являющийся управляющим.

Использование стилей

Шрифт без форматирования	Основной текст
Моноширинный шрифт	Пользовательский ввод
Рамка	Программный вывод на экран
Курсивный шрифт	Наименования документов
Полужирный подчеркнутый фиолетовый шрифт	Внутренняя ссылка
Полужирный шрифт	Наименование элементов интерфейса

1. Введение

1.1. Назначение документа

В настоящем руководстве описаны задачи, возникающие при эксплуатации и сопровождении ПК «KEO DLP» (далее – KEO DLP), а также способы и примеры их решения в ряде стандартных сценариев.

1.2. Аудитория

Документ предназначен для системных и сетевых администраторов, а также для сотрудников службы информационной безопасности компаний, обеспечивающих устойчивое функционирование KEO DLP.

2. О системе KEO DLP

Программный комплекс «KEO DLP» – это система контроля корпоративных коммуникаций класса Data Leak Prevention (DLP), с помощью которой можно выявлять и блокировать несанкционированную передачу данных с компьютеров, а также определять признаки корпоративного мошенничества.

К основным функциональным возможностям KEO DLP относятся:

- контроль каналов утечки данных (электронной почты, социальных сетей, мессенджеров и т. п.);
- контроль использования сетевых ресурсов сотрудниками;
- отслеживание и ограничение движения потоков информации;
- отслеживание и блокирование сетевых коммуникаций сотрудников;
- сбор, анализ и хранение сообщений о фактах передачи информации (при этом обеспечивается анализ содержимого сообщений и документов; выявление документов определённой структуры и содержания; сравнение текстовых, графических и табличных документов с заранее заданными эталонными документами; распознавание в текстах сообщений определенных последовательностей – ИНН, номеров паспортов и т. д.);
- сбор, систематизация и хранение данных о сотрудниках (ведение досье на каждого сотрудника);
- сбор, систематизация и хранение данных о местонахождении материалов, содержащих конфиденциальную информацию, и о сотрудниках, имеющих доступ к ним;
- поддержка процессов работы сотрудников службы безопасности (создание и настройка правил передачи и хранения информации; мониторинг событий и инцидентов; отслеживание действий сотрудников; назначение сотрудников, ответственных за разбор инцидентов; получение статистических отчетов);
- поддержка проведения расследований инцидентов информационной и экономической безопасности (поиск данных, выявление рабочих и личных контактов сотрудников; предоставление данных для анализа сетевой активности каждого сотрудника; подсказка следующих шагов в процессе расследования);
- учет и контроль рабочего времени сотрудников;
- мониторинг и анализ особенностей поведения персон и ресурсов на основе данных об их информационных коммуникациях.

3. Условия эксплуатации

3.1. Требования к квалификации персонала

Квалификация системного администратора KEO DLP должна быть достаточной для выполнения задач по обслуживанию системы, обеспечивающих бесперебойное функционирование всех её компонентов.

Требования к квалификации системного администратора KEO DLP:

- знания и навыки администрирования ОС Linux и СУБД PostgreSQL.
- знания и навыки администрирования системы мониторинга Zabbix.
- понимание особенностей работы KEO DLP.
- понимание работы сетевых протоколов.
- базовые знания языка PL/SQL.
- знания в области безопасности ОС класса UNIX.

В своей работе системные администраторы KEO DLP должны использовать документацию по обслуживанию KEO DLP и документацию по ОС Linux и СУБД PostgreSQL.

3.2. Требования к АРМ администратора

3.2.1. Аппаратное обеспечение

АРМ системного администратора KEO DLP должно быть оборудовано персональным компьютером с подключением к интернету. Минимально рекомендованные характеристики оборудования:

- Объем свободной оперативной памяти – не менее 4 ГБ после загрузки браузера.
- Разрешение экрана при работе с GUI от 1600x900.

АРМ системного администратора KEO DLP должно иметь терминальный доступ к master-узлу KEO DLP.

3.2.2. Программное обеспечение

В состав ПО компьютера для АРМ системного администратора KEO DLP должен входить браузер. Гарантируется корректная работа GUI KEO DLP в браузерах Google Chrome, Microsoft Edge, Mozilla Firefox, Yandex и Atom актуальных версий. В других браузерах корректная работа GUI KEO DLP невозможна.

Для корректной работы GUI KEO DLP настоятельно рекомендуется в настройках браузера разрешить выполнение **javascript** и сохранение файлов **cookies**. Кроме того, рекомендуется отключить сторонние расширения браузера, поскольку некоторые расширения могут негативно влиять на работу KEO DLP.

Внимание!

Рекомендуется использовать настройки размера шрифта и масштаба экрана по умолчанию, поскольку изменение этих настроек может привести к искажению дизайна и некорректной работе GUI KEO DLP.

4. Задачи планового администрирования системы KEO DLP

К задачам системного администратора KEO DLP относятся:

- управление доступом к учётным записям и группам пользователей (см. раздел 6.1);
- настройка параметров обработки пароля учётной записи пользователя (см. раздел 6.2);
- управление и мониторинг процессов системы (см. разделы 5.4, 6.4);
- управление и мониторинг ролей и сервисов на slave-узлах (см. разделы 5.3, 5.5.1, 6.10.1);
- просмотр и настройка журналов работы системы (см. разделы 5.5.2, 5.5.3, 6.11);
- контроль связи со структурой каталогов LDAP и диагностика проблем синхронизации (см. разделы 6.9, 6.19);
- сопровождение фильтра системы (см. разделы 6.16);
- управление и мониторинг БД системы (см. разделы 6.5, 6.12);
- управление архивом сообщений системы (см. раздел 6.13);
- управление и мониторинг спулов хранения сообщений системы (см. разделы 5.5.4, 6.17);
- сопровождение файлового хранилища (см. раздел 6.15);
- настройки ротации инцидентов системы (см. раздел 6.7);
- повышение точности определения кодировки сообщений (см. раздел 6.18);
- контроль работы модуля IDID (см. раздел 6.20);
- контроль работы модуля DIFI (см. раздел 6.21);
- контроль работы сервера действий (см. раздел 6.22);
- контроль целостности системы (см. раздел 6.28).

Для выполнения вышеуказанных задач системный администратор KEO DLP должен соответствовать требованиям, указанным в разделе 3.1.

5. Администрирование KEO DLP с помощью веб-интерфейса

5.1. Описание основных элементов интерфейса

После входа в систему открывается **Рабочий стол** (см. Рис.5.1).

Рис. 5.1. Рабочий стол

В левой части интерфейса расположено главное меню в свернутом виде. Главное меню предоставляет доступ к следующим разделам интерфейса (см. Рис.5.2):

- **Рабочий стол** – предназначен для отображения основных показателей информационной безопасности в компании.
- **События и инциденты** – предназначен для работы с инцидентами и событиями информационной безопасности.
- **Досье** – предназначен для работы с информацией о персонах.
- **Анализ поведения (UBA)** – предназначен для поиска персон, поведение которых соответствует определенному паттерну.
- **Расследование** – предназначен для работы с модулем расследования инцидентов ИБ.
- **Информационные объекты** – предназначен для управления информационными активами компании, нуждающимися в защите.
- **Поиск** – предназначен для поиска сообщений, персон, инцидентов и файлов.

- **Отчеты** – предназначен для формирования отчётов по различным показателям состояния информационной безопасности.
- **Политика** – предназначен для настройки политики фильтрации сообщений.
- **Агенты** – предназначен для настройки и мониторинга работы модуля контроля рабочих станций **Endpoint Agent**.
- **Краулер** – предназначен для настройки и мониторинга работы модуля мониторинга файловых ресурсов и средств защиты конфиденциальной информации **KEO DLP File Crawler**.
- **Пользователи** – предназначен для выполнения следующих действий:
  - управления учетными записями пользователей системы (создание, редактирование, блокировка, удаление);
  - настройки для пользователей прав доступа к различным объектам системы;
  - просмотра журнала действий пользователей системы;
  - настройки отправки сообщений, уведомляющих о действиях пользователей.
- **Справочники** – предназначен для работы с наборами (списками) элементов, сгруппированных по определенному признаку.
- **Система** – предназначен для администрирования KEO DLP. В этом разделе GUI системный администратор выполняет следующие действия:
  - настраивает параметры конфигурации;
  - назначает узлам роли;
  - отслеживает состояние различных ресурсов;
  - управляет функционированием KEO DLP.

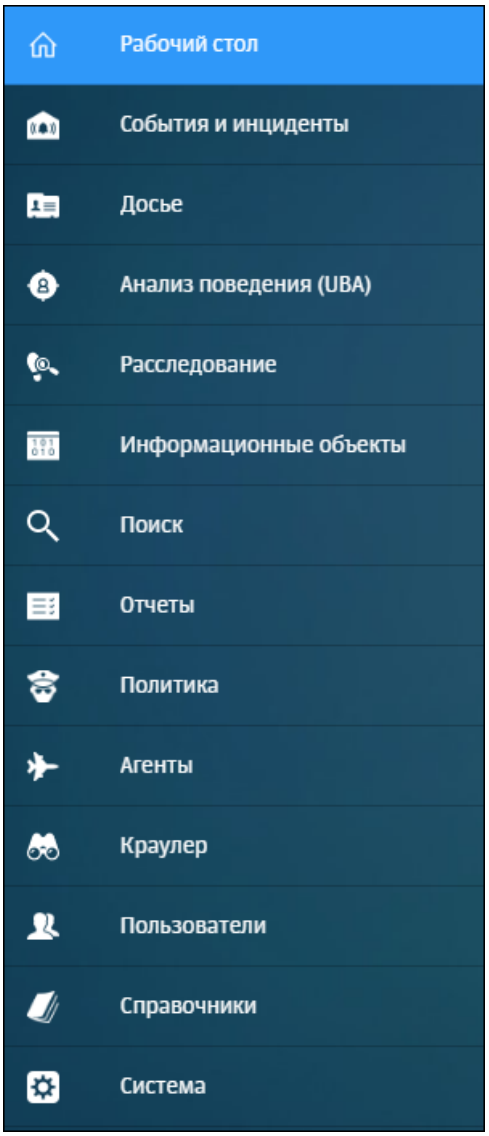


Рис. 5.2. Главное меню

При возникновении ошибок в верхней части интерфейса появляется всплывающее окно с сообщением об ошибке (см. Рис.5.3):

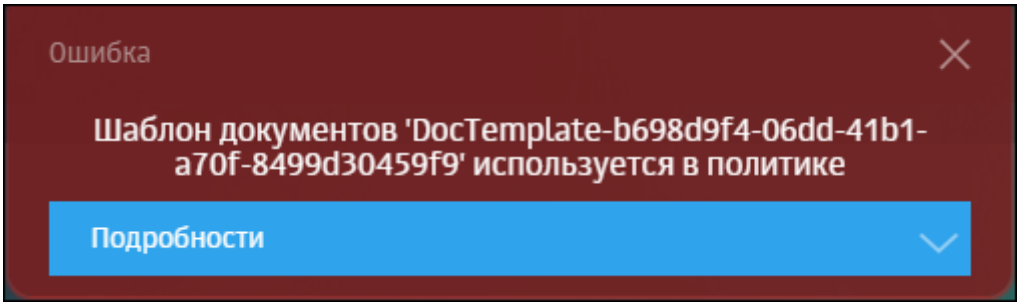


Рис. 5.3. Сообщение об ошибке

При нажатии на значок в правом верхнем углу веб-интерфейса, а затем на кнопку **Выход** в открывшемся окне завершается сеанс работы текущего пользователя и откры-

вается окно авторизации (описание первого входа в KEO DLP приведено в документе *Руководство по установке и настройке*).

5.2. Управление конфигурацией

Для управления конфигурацией KEO DLP предназначен раздел **Система** > **Конфигурация**. Он содержит два подраздела: **Основные настройки** и **Расширенные настройки** (см. Рис.5.4 и Рис.5.5).

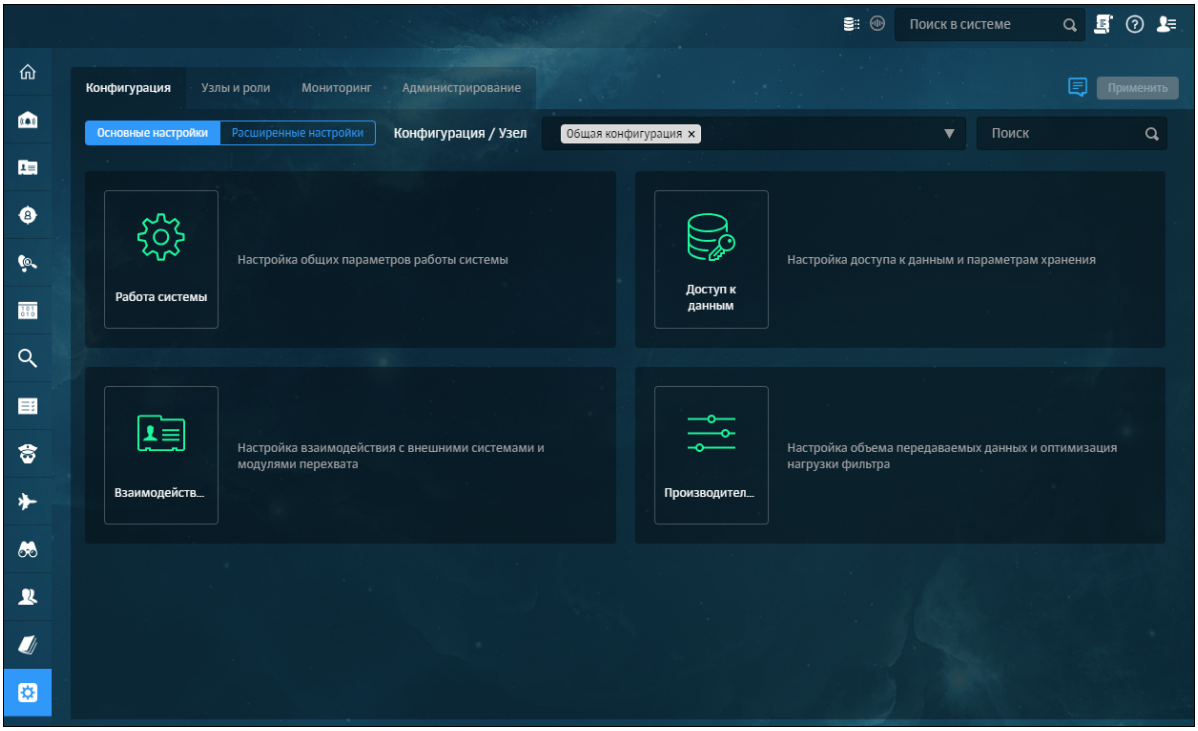


Рис. 5.4. Основные настройки конфигурации

В подразделе **Основные настройки** содержатся наиболее часто используемые параметры конфигурации KEO DLP. Они сгруппированы в следующие категории:

- **Работа системы** – основные параметры конфигурации.
- **Доступ к данным** – параметры соединения с БД и ФХ.
- **Взаимодействие** – параметры взаимодействия KEO DLP с источниками данных досье, модулями KEO DLP Endpoint Agent, KEO DLP File Crawler, KEO DLP Traffic Analyzer, а также параметры планировщика.
- **Производительность** – параметры, влияющие на производительность сервисов KEO DLP.

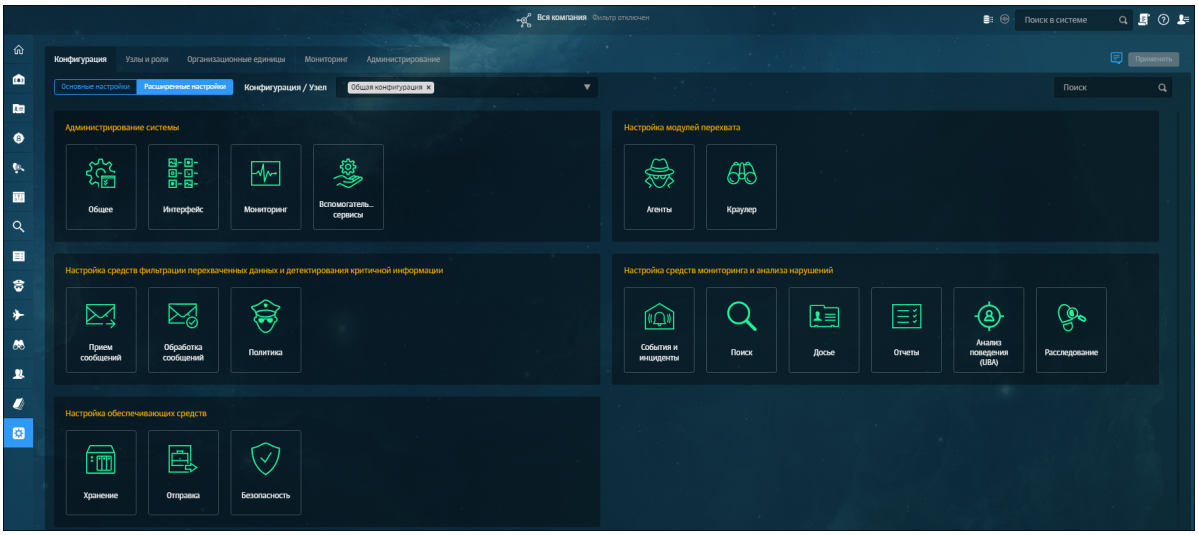


Рис. 5.5. Расширенные настройки конфигурации

В подразделе **Расширенные настройки** содержатся все параметры конфигурации KEO DLP, в том числе параметры из подраздела **Основные настройки**. Они сгруппированы в следующие категории:

- **Администрирование системы** – параметры соединения с БД и ФХ, использования модулей, настройки интерфейса, мониторинга и вспомогательных сервисов KEO DLP.
- **Настройка модулей перехвата** – параметры модулей KEO DLP Endpoint Agent, KEO DLP File Crawler и KEO DLP Traffic Analyzer.
- **Настройка средств фильтрации перехваченных данных и детектирования критичной информации** – параметры приёма и обработки сообщений, а также сервисов, используемых при фильтрации почтовых сообщений.
- **Настройка средств мониторинга и анализа нарушений** – параметры обнаружения событий ИБ / индексации и поиска / управления Досье / построения отчётов / модулей UBA и расследования инцидентов ИБ.
- **Настройка обеспечивающих средств** – параметры хранения, отправки, безопасности и интеграции.

Более подробное описание параметров конфигурации приведено в приложении (см. **Приложение А, *Параметры конфигурации KEO DLP***).

С помощью строки **Поиск** можно искать параметры конфигурации по их наименованию или значению. Чтобы воспользоваться поиском, следует ввести название искомого элемента или его часть в поле **Поиск**, расположенном в правой верхней части экрана (см. **Рис.5.6**).

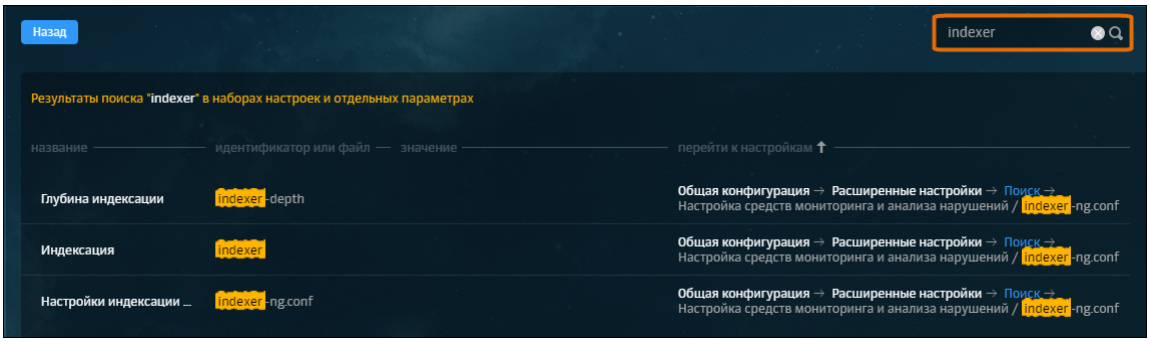


Рис. 5.6. Поиск по конфигурации

Чтобы перейти в раздел с искомым элементом, следует нажать на его имя (выделено синим).

После внесения изменений в значения параметров конфигурации их следует сохранить или отменить с помощью соответствующих кнопок (см. Рис.5.7).

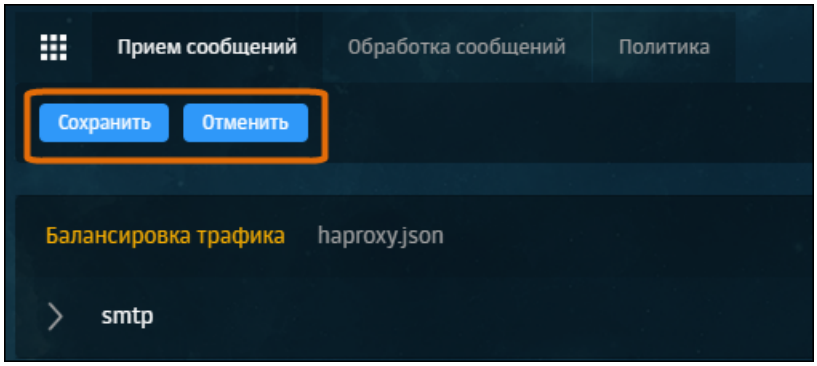


Рис. 5.7. Кнопки Сохранить и Отменить

Кнопка **Применить** служит для применения параметров конфигурации (см. Рис.5.8). При наведении курсора мыши на значок можно просмотреть сведения о последнем применении конфигурации: дата и время применения и комментарий системного администратора.

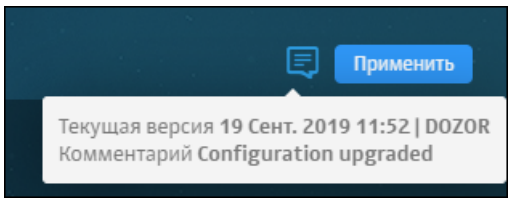


Рис. 5.8. Кнопка Применить

Примечание

*Помимо применения настроек конфигурации кнопка **Применить** служит для сохранения состава ролей на узлах (см. раздел 5.3).*

Раскрывающийся список **Конфигурация/Узел** используется для просмотра и задания параметров конфигурации всего кластера KEO DLP или локальных настроек для каждого узла кластера (см. Рис.5.9).

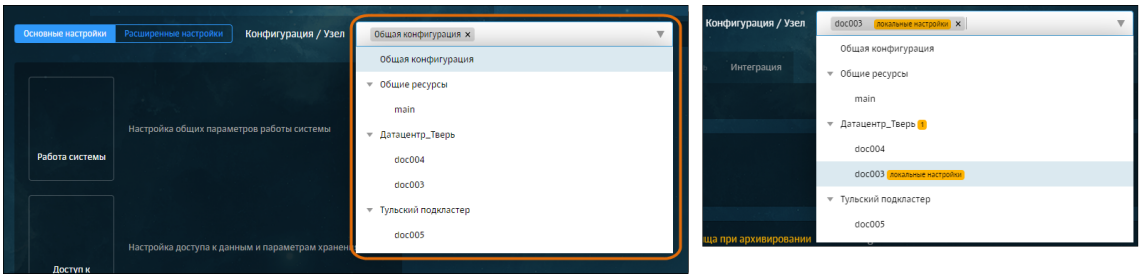


Рис. 5.9. Выбор узла

С помощью индикатора **Локальные настройки** можно определить наличие локальных настроек на узлах (см. Рис.5.9, Рис.5.10) или в параметрах/блоках параметров, связанных с такими узлами. Используя локальные настройки, системный администратор может настраивать определенные сервисы на отдельных узлах под конкретные задачи.

Системный администратор может выбрать из двух вариантов: задать локальные настройки для узла или вернуться к использованию общей конфигурации. Чтобы задать локальные настройки для узла, необходимо выполнить следующие действия:

1. Перейти в соответствующую секцию конфигурации (в примере ниже используется **Коннектор сервиса цифровых отпечатков**).

2. Установить переключатель **Использовать локальные настройки** напротив названия секции (конфигурационного файла) в положение **Включить** и задать для параметров соответствующие значения (см. Рис.5.10).

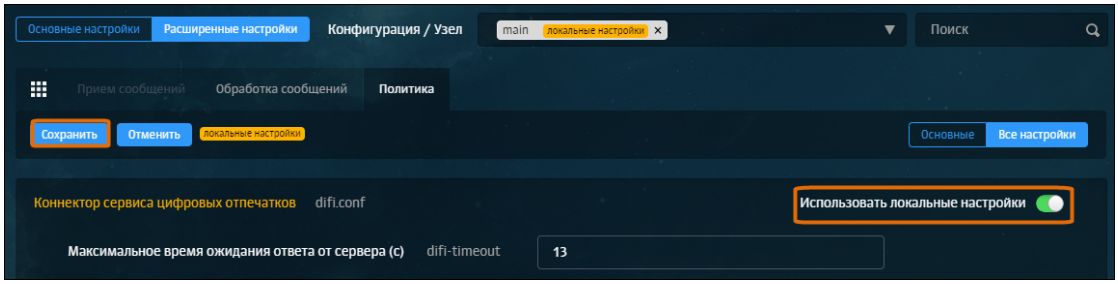


Рис. 5.10. Использование локальных настроек в секции конфигурации

3. Нажать кнопки **Сохранить** и **Применить** для сохранения и применения параметров конфигурации.

Примечание

Локальные настройки имеют преимущества перед настройками конфигурации по умолчанию в случае, если сервис настроен локально.

Чтобы вернуться к использованию общей конфигурации, следует выполнить действия:

1. Установить переключатель **Использовать локальные настройки** напротив названия секции в положение **Выключить**.

2. В открывшемся окне **Подтверждение изменений** нажать кнопку **Да** (см. Рис.5.11).

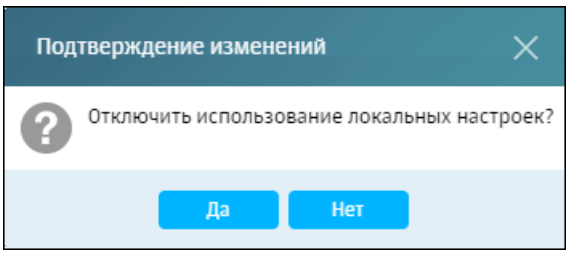


Рис. 5.11. Подтверждение отмены локальных настроек

3. Нажать кнопки **Сохранить** и **Применить** для сохранения и применения параметров конфигурации.

Примечание

После изменения параметров конфигурации и их применения перезапуск связанных с параметрами сервисов происходит на всех узлах.

Подробнее об управлении процессами см. разделы 6.4 и 5.5.1.

5.3. Назначение ролей узлам

Системный администратор может назначать роли узлам кластера KEO DLP в секции **Список узлов** раздела GUI **Система** > **Узлы и роли** (Рис.5.12).

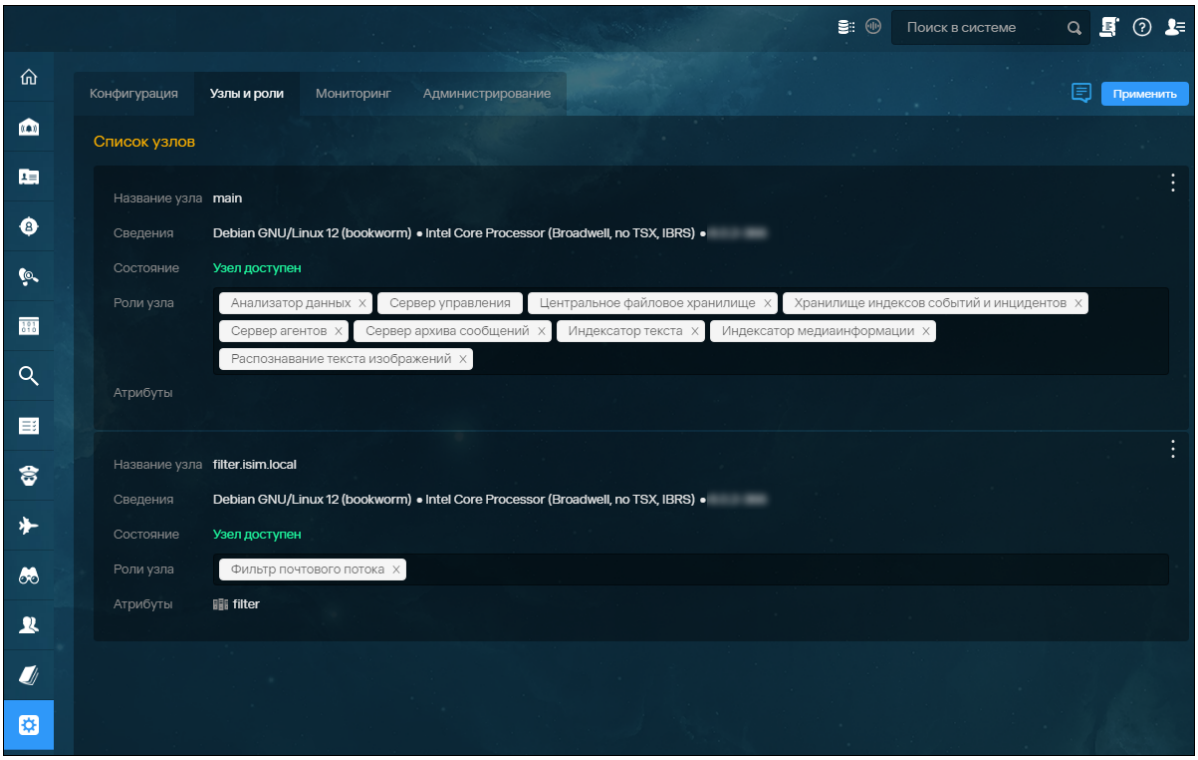


Рис. 5.12. Назначение ролей узлам

По каждому узлу предоставлена следующая информация:

- **Название узла** – имя узла, на котором установлен KEO DLP.
- **Сведения** – версия установленной на узле ОС; процессор; версия пакета KEO DLP.
- **Состояние** – показывает состояние узла. Принимает значения: **Узел доступен** или **Узел недоступен**.
- **Роли узла** – список ролей, которые выполняет данный узел. Роль выбирается из раскрывающегося списка. Подробное описание состава сервисов всех ролей приведено в документе *Руководство по установке и настройке*, приложение *Описание ролей и сервисов*. При наведении курсора мыши на роль можно просмотреть подсказку со списком разделов настроек для этой роли.
- **Атрибуты** – показывает атрибуты, которые относятся к узлу. На текущий момент можно указать два атрибута (Рис.5.13):
  - **Имя стойки, в которой расположен сервер** – атрибут, предназначенный для контроля распределения индексов OpenSearch по стойкам.
  - **Группа мониторинга** – атрибут для разбиения показателей по решаемым задачам, например: фильтрация, серверы агентов, и т.д.

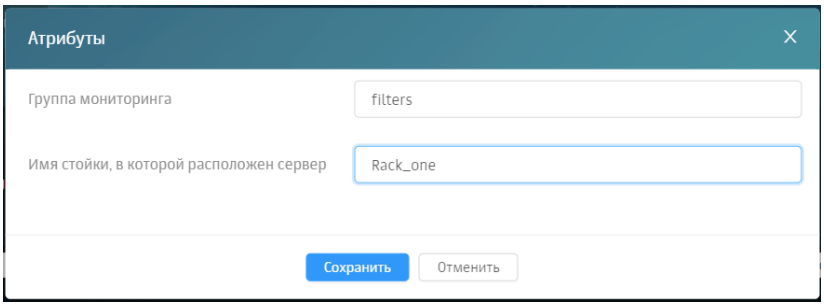


Рис. 5.13. Окно настройки атрибутов

- Индикатор локальных настроек узла – показывает, что для узлов/параметров/блоков параметров, связанных с такими узлами, заданы локальные настройки (Рис.5.14).

Примечание

Описание назначения локальных настроек приведено в разделе 5.2.

Рис. 5.14. Индикатор локальных настроек в списке узлов

Для отображения списка узлов используется пагинация, которая располагается в нижней части интерфейса. На одной странице может быть одновременно отображено не более пяти узлов.

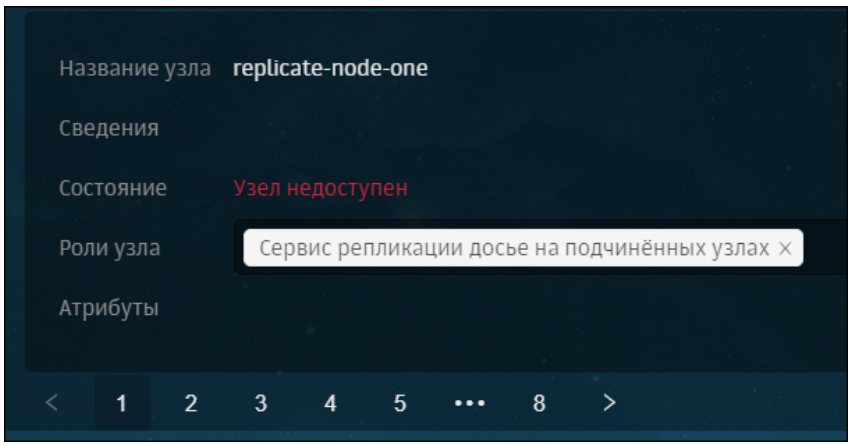


Рис. 5.15. Разбиение на страницы

Если в системе имеется более пяти узлов, в правой верхней части экрана отображается поле **Поиск по узлам** (Рис.5.16).

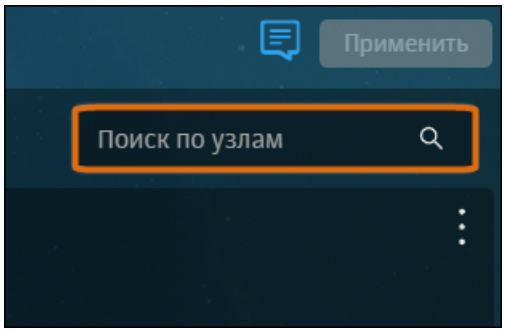


Рис. 5.16. Поиск узлов

Чтобы указать атрибуты для узла и просмотреть список доступных для выполнения на этом узле скриптов, следует вызвать меню действий с узлом системы и выбрать пункт **Атрибуты** (Рис.5.17, Рис.5.18).

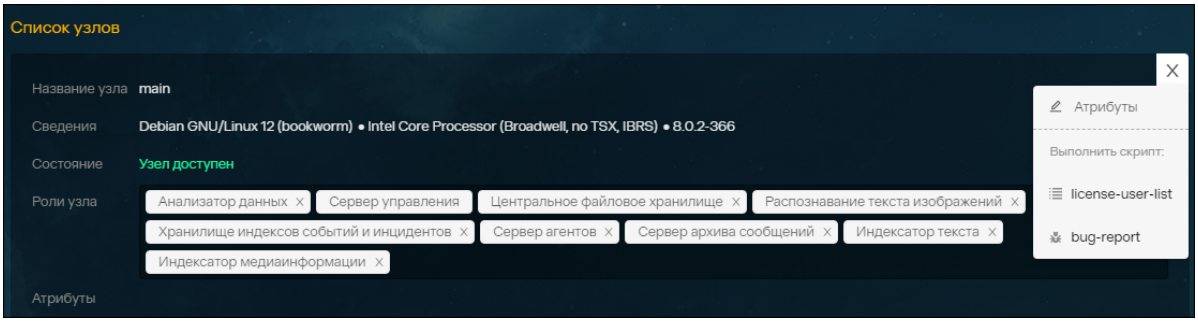


Рис. 5.17. Меню действий с master-узлом

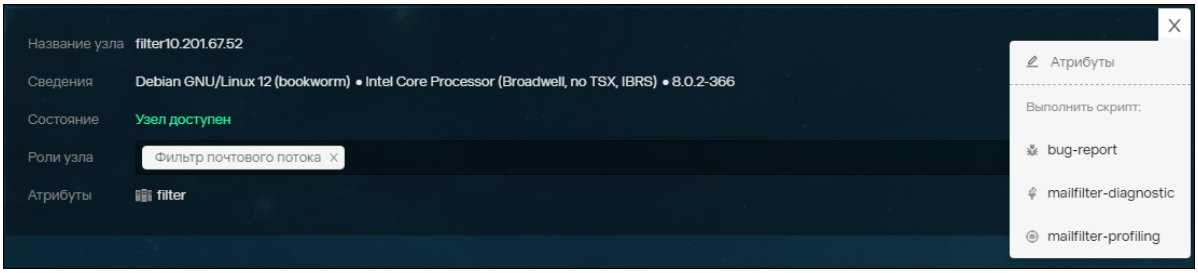


Рис. 5.18. Меню действий со slave-узлом

Далее в открывшемся окне необходимо внести соответствующие изменения и нажать кнопку **Сохранить**.

Примечание

Значение атрибута должно содержать только латинские буквы, цифры, а также символы минус и подчеркивание.

В системе можно выполнять следующие скрипты:

- **bug-report** – собирает и выводит информацию о системе, настройках и показателях работы ПО (при этом информация выводится в текстовый файл). Аналогичный скрипт

bug-report.sh можно выполнить в разделе GUI **Система > Администрирование > Скрипты** и в CLI (см. раздел 5.5.3).

- **license-user-list** – собирает и выводит информацию об активных адресах электронной почты. Для получения аналогичного результата можно запустить скрипт **license-tool** с ключами **-a**/**--active-addresses** и **-c**, **--active-addresses-count** (см. раздел 6.25.)
- **mailfilter-diagnostic** – собирает и выводит диагностическую информацию о работе почтового фильтра: журналы, политику и статистику очередей. Аналогичный скрипт можно запустить в CLI (см. раздел 6.16.3).
- **mailfilter-profiling** – собирает и выводит статистику работы **mailfilter**, содержит данные о временных затратах на проверку наиболее часто встречающихся типов файлов, типов сообщений, каналов коммуникаций и шаблонов документов. Аналогичный скрипт можно запустить в CLI (см. раздел 6.16.4).

Внимание!

*Скрипт **license-user-list** можно выполнить только на master-узле. Скрипты **mailfilter-diagnostic** и **mailfilter-profiling** выполняются для узлов с ролью **Фильтр почтового потока**.*

Для запуска скрипта необходимо нажать на имя скрипта. При успешном выполнении скрипта в верхней части экрана появится соответствующее сообщение (Рис.5.19). Для сохранения отчета следует перейти по соответствующей ссылке.

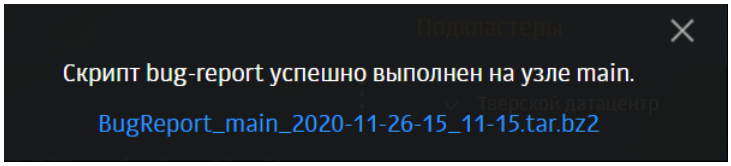


Рис. 5.19. Сообщение об успешном выполнении скрипта

Внимание!

*Перед запуском скрипта **mailfilter-profiling** необходимо включить вывод отладочной информации в журнал сервиса **mailfilter** согласно настройке параметра **Вывод отладочной информации** в секции **Настройки сервиса фильтрации сообщений** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений**). В противном случае после запуска скрипта появится сообщение об ошибке.*

Если версия пакета KEO DLP на slave-узле отличается от версии пакета на master-узле, она отображается желтым цветом. При наведении курсора мыши на версию пакета появляется всплывающая подсказка:

Версия системы отличается от версии master-узла. Применение конфигурации невозможно.

Внимание!

*При ошибках запуска сервисов на узлах системы следует получить все сведения с помощью скриптов **bug-report**, **bug-report.sh** и **bug-report-gzip.sh**. Файл с отчетом о работе скриптов необходимо предоставить в службу технической поддержки.*

Примечание

Информация об ошибках хранится в журналах сервисов. Описание журналов приведено в разделах 5.5.2 и 6.11.

Для каждого узла доступен выбор следующих ролей:

- Анализ поведения (UBA);
- Анализатор данных;
- Балансировщик;
- Вспомогательный индексатор исторических сообщений;
- Вспомогательный сервер OpenSearch;
- Вспомогательный сервер действий;
- Вспомогательный сервис индексации текста;
- Индексатор исторических сообщений;
- Индексатор медиаинформации;
- Индексатор текста;
- Контроль рабочего времени;
- Краулер: корпоративные мессенджеры;
- Краулер: файловые ресурсы и IMAP;
- Локальное файловое хранилище;
- Мониторинг локального почтового шлюза;
- Распознавание графических объектов;
- Распознавание речи;
- Расследование;
- Сервер агентов;
- Сервер архива сообщений;

- Сервер интеграции;
- Сервер категорий;
- Сервер управления;
- Сервер управления Краулером;
- Сервис перехвата и анализа сетевого трафика;
- Сервис распределённого хранения;
- Сервис репликации досье на подчинённых узлах;
- Фильтр почтового потока;
- Хранилище индексов исторических событий и инцидентов;
- Хранилище индексов событий и инцидентов;
- Центральное файловое хранилище.

Блоки параметров конфигурации отображаются в соответствии с запущенными на узле сервисами, которые связаны с назначенными узлу ролями. Для возможности редактирования таких блоков следует назначить узлам соответствующие роли.

Для назначения узлу какой-либо роли следует щелкнуть мышью в поле выбора роли и выбрать в раскрывающемся списке одну или несколько ролей для узла. В строках с назначенными узлу ролями установлены флажки синего цвета (Рис.5.20).

Примечание

Также можно ввести символы в поле выбора роли. По мере ввода система будет отображать список ролей, которые содержат вводимый набор символов.

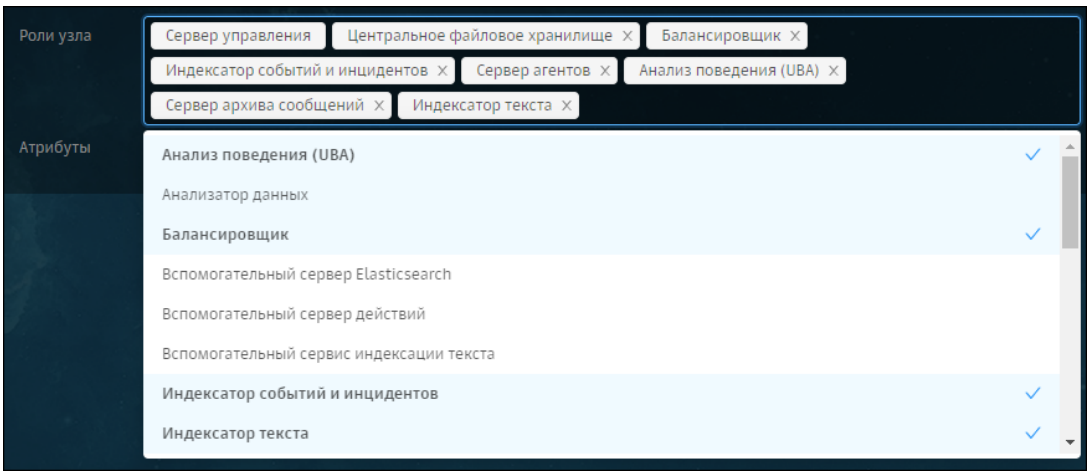


Рис. 5.20. Выбор ролей для узла

Для снятия с узла какой-либо роли следует щелкнуть мышью на этой роли в списке. Роль, назначенная узлу, определяет, какие сервисы будут работать на данном узле.

Рекомендации по назначению ролей узлам описаны в документе *Руководство по настройке производительности*. После назначения ролей следует сохранить изменения на всех узлах системы, нажав кнопку **Применить**.

Внимание!

Одновременно с сохранением состава ролей будут применены настройки конфигурации.

Примечание

Некоторые узлы при сохранении изменений могут быть недоступны. В этом случае изменения будут применены, когда узел станет доступным.

При сохранении изменений запуск сервисов на узле выполняется в соответствии с вновь назначенными узлу ролями. Кроме того, остановка сервисов выполняется в соответствии со снятыми для узла ролями.

Примечание

После назначения узлу роли станет доступен для редактирования блок параметров, связанных с такой ролью.

5.4. Мониторинг системы

В KEO DLP реализована подсистема мониторинга на основе Zabbix. Для Zabbix используются стандартные пути к каталогам файловой системы.

В разделе GUI **Система > Мониторинг** системный администратор может выполнять:

- диагностику проблем на узлах кластера KEO DLP (см. раздел 5.4.2),
- мониторинг работы KEO DLP (см. раздел 5.4.3) и показателей, полученных средствами ОС (см. раздел 5.4.4);
- построение отчетов по сводным статистическим показателям (см. раздел 5.4.5).

В верхней части всех подразделов раздела GUI **Система > Мониторинг** расположены списки групп серверов и узлов для отображения. По умолчанию отображаются все узлы и группа **Общая группа**. Для возможности выбора других групп мониторинга следует создать их в разделе GUI **Система > Узлы и роли**. Для отображения определенного набора узлов следует открыть список узлов и выделить курсором все требуемые узлы. Для групп серверов необходимо выполнить аналогичные действия. Сбросить группировку можно нажатием на значок  .

С помощью набора статистических показателей **Наличие проблем на узлах (средние и выше)** (Рис.5.21) на каждом узле кластера KEO DLP можно определить количество проблем с разными уровнями критичности (описание проблем на узлах приведено в разделе 5.4.2). Если на узле есть проблемы с уровнем критичности **Средняя и выше**,

индикатор состояния узла отображается красным цветом. Если на узле имеются проблемы с низким уровнем критичности, индикатор состояния узла отображается желтым цветом. Если на узле нет проблем, в прямоугольном блоке отображается **ОК**.

Рис. 5.21. Отображение состояния узла

5.4.1. Изменение периода времени и редактирование графика

В подразделах **Показатели системы**, **Показатели ОС** и **Подробные данные** можно изменить период времени, за который отображается информация по показателям. Для этого следует в соответствующем списке выбрать или задать требуемое значение (Рис.5.22).

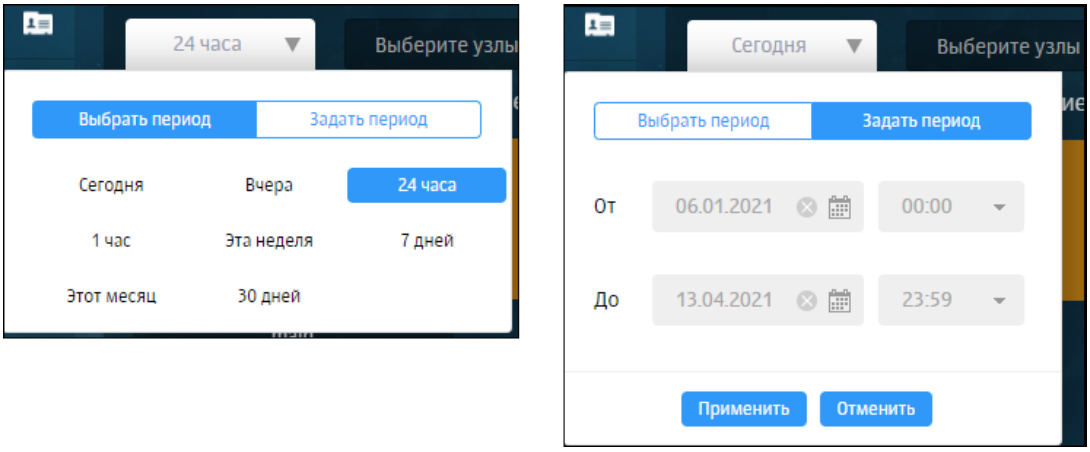


Рис. 5.22. Выбор/задание периода времени

Пример: необходимо проанализировать сетевой трафик узла за 8-часовой рабочий день. Для этого в списке следует задать диапазон и нажать кнопку **Применить**. В результате будут отображены данные за последние 8 часов (Рис.5.23).

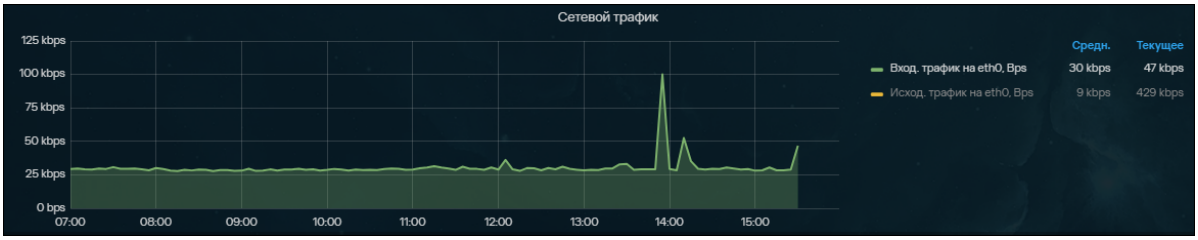


Рис. 5.23. Пример отображения данных за 8 часов

Область с построенным графиком включает график и поясняющую информацию:

- строку заголовка,
- легенду от графика. Может располагаться справа или снизу от графика.

Чтобы увеличить масштаб графика, следует выполнить действия:

1. Навести курсор мыши на нужную область графика.
2. Щелкнуть левой кнопкой мыши, и не отпуская ее, двигать курсор в необходимом направлении.

   В результате система автоматически поменяет масштаб графика.

Системный администратор может просмотреть информацию по определенному показателю. Например, можно определить максимальную и минимальную скорости входящего и исходящего трафика на узле (см. **Рис.5.23**).

Цвет графика выбирается из раскрывающегося списка. Для этого необходимо нажать на цвет линии в легенде.

На каждом графике отображается один или несколько показателей работы системы, их выбор доступен в процессе редактирования графика.

Разные показатели на графике обозначены линиями соответствующего цвета. При наведении курсора мыши на конкретную точку графика появляется подсказка (**Рис.5.24**), показывающая значение в определенный момент времени.

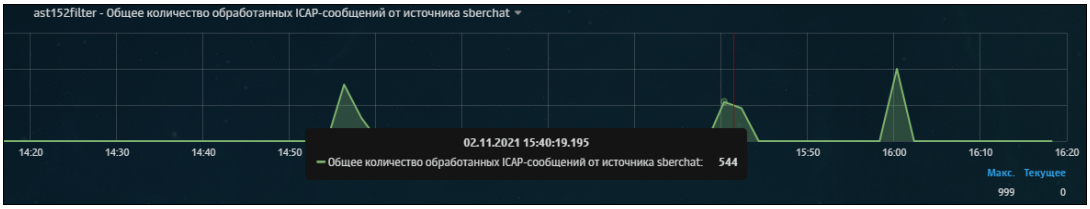


Рис. 5.24. Просмотр значения показателя в конкретный момент времени

Для отображения графика одного из показателей следует щелкнуть по его легенде левой кнопкой мыши. При повторном нажатии вновь отобразятся все графики.

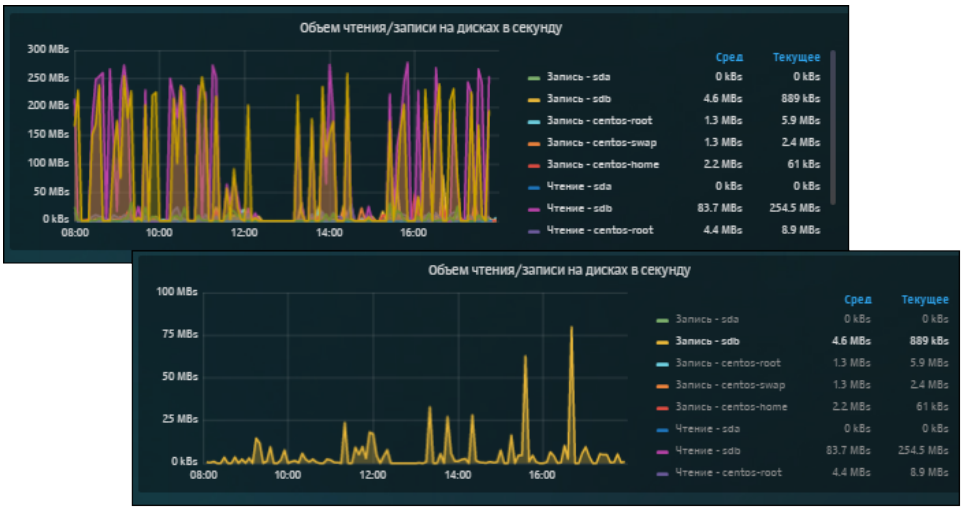


Рис. 5.25. Выбор показателей для отображения

5.4.2. Диагностика проблем на узлах KEO DLP

В разделе **Система > Мониторинг > Состояние системы** системный администратор может просмотреть состояние всех узлов кластера KEO DLP (Рис.5.26).

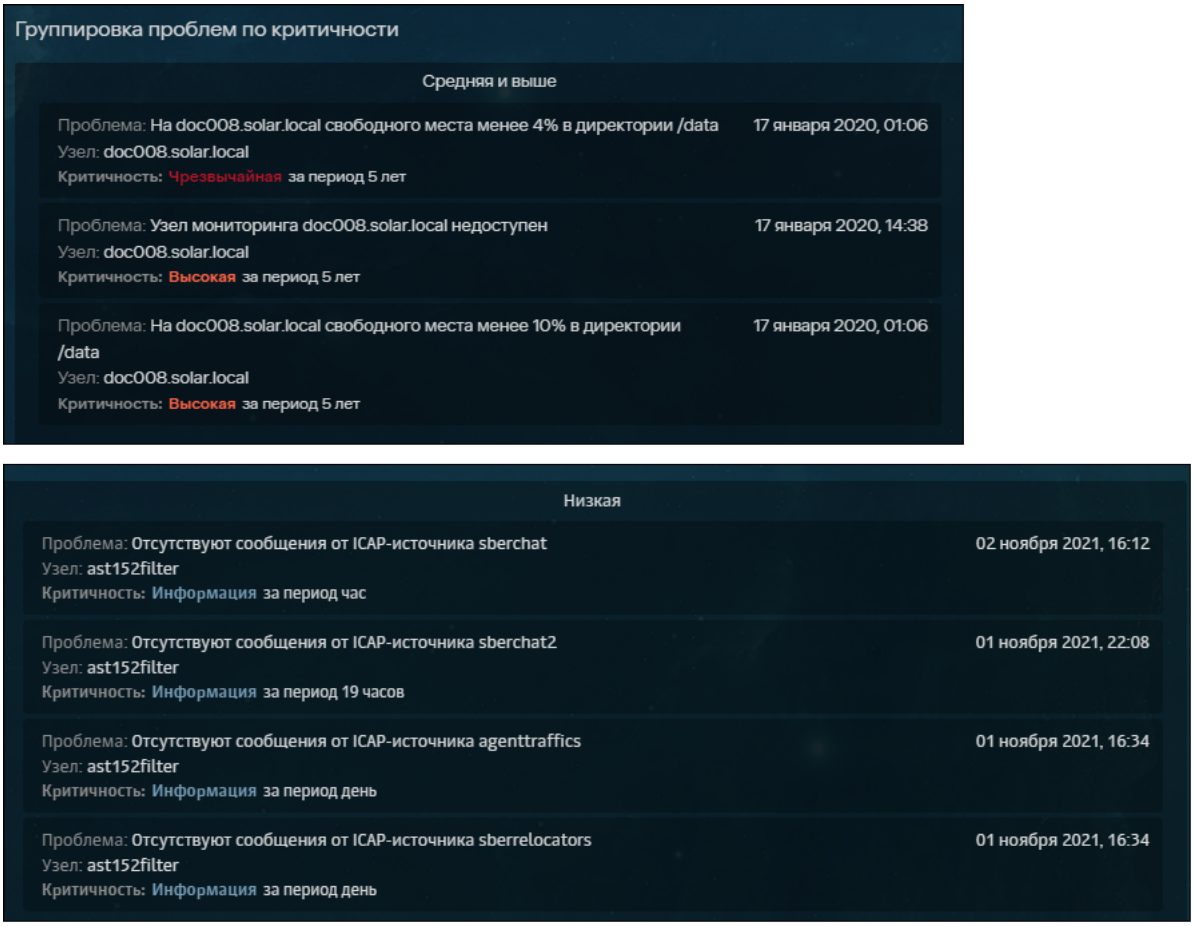


Рис. 5.26. Диагностика проблем KEO DLP

В интерфейсе KEO DLP можно просмотреть проблемы, сгруппированные по уровню критичности. Уровень критичности характеризует серьезность проблемы. В нижней части интерфейса расположены следующие списки проблем:

- **Средняя и выше** – проблемы с уровнями критичности **Средняя**, **Высокая** и **Чрезвычайная**. Проблемы с уровнями критичности **Средняя** и **Высокая** следует решить, как можно скорее. В противном случае системе будет причинен ущерб.

  Проблемы с уровнем критичности **Чрезвычайная** необходимо незамедлительно устранить. В противном случае это может привести к выходу из строя узла кластера.

- **Низкая** – проблемы с меньшей критичностью, но также требующие решения.

Примечание

*Описание набора статистических показателей **Наличие проблем на узлах (средние и выше)** приведено в разделе 5.4.*

Секция **Сервер мониторинга** (раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование системы > Мониторинг**) содержит настройки работы монитора ресурсов, величины порогов состояния некоторых ресурсов и варианты реакции системы на смену состояния некоторых ресурсов. При появлении проблем система отправляет письмо с уведомлением об этом. Адреса отправителя и получателей задаются в группе параметров **Настройки оповещения**.

5.4.3. Показатели системы

В разделе **Система > Мониторинг > Показатели системы** системный администратор может просмотреть статистическую информацию о системных показателях работы KEO DLP.

В верхней части расположен список узлов для отображения и инструмент для выбора временного отрезка, за который необходимо получить данные.

Ниже расположены блоки с названиями узлов. Принцип их отображения такой же, как и в разделе GUI **Система > Мониторинг > Состояние системы**.

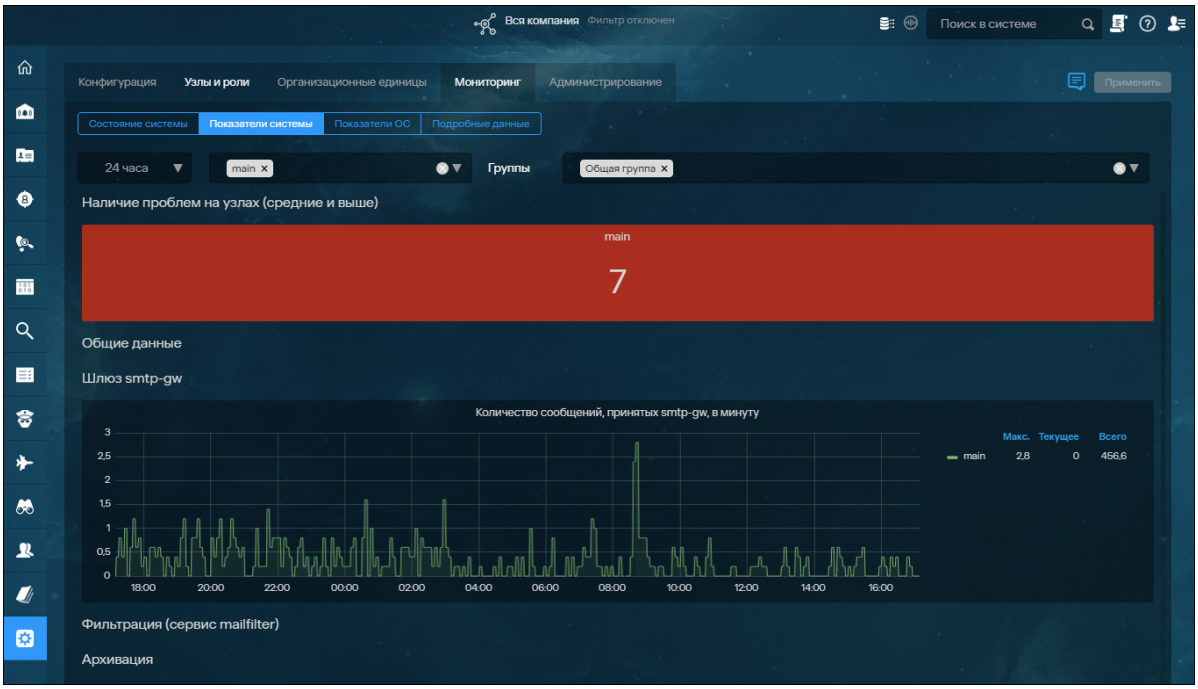


Рис. 5.27. Информация о показателях системы

Ниже расположена группа графиков для каждого выбранного узла, отображающих следующие данные:

- **Общие данные** – количество сообщений в спулах **archiver**, **mailfilter** и **sender**.
- **Шлюз smtp-gw** – количество сообщений, обработанных шлюзом **smtp-gw**.
- **Фильтрация (сервис mailfilter)** – количество сообщений, обработанных системой фильтрации: включает в себя статистику по входящему трафику от внешних ICAP-источников и типам сообщений, определяемым в KEO DLP (более подробное описание типов сообщений см. в документе *Справочник пользователя*).

- **Архивация** – статистика использования дискового пространства базами данных архива.
- **Индексация** – количество сообщений, проиндексированных модулем OpenSearch.
- **Агенты** – количество агентов в зависимости от версии и число рабочих станций в зависимости от статуса и подстатуса Агента;
- **Базы данных** – размеры разделов и свободное/занятое место в следующих БД, использующихся в KEO DLP:
  - БД политики фильтрации;
  - БД событий и инцидентов ИБ;
  - БД модуля KEO DLP File Crawler;
  - БД архива сообщений.

Примечание

Описание работы с графиками приведено в разделе 5.4.

5.4.4. Показатели ОС

В разделе **Система > Мониторинг > Показатели ОС** (Рис.5.28) системный администратор может просмотреть информацию по статистическим показателям, которые были получены средствами ОС. К таким показателям, например, относятся размер доступной оперативной памяти, загрузка центрального процессора и т.д.

В верхней части расположен список узлов для отображения и инструмент для выбора временного отрезка, за который необходимо получить данные. Для просмотра подробных сведений необходимо навести курсор мыши на имя показателя и щелкнуть по нему левой кнопкой мыши. При повторном нажатии информация по узлу будет скрыта.

Рис. 5.28. Информация о показателях ОС

Ниже отображается информация:

- **Время работы** – продолжительность непрерывной работы системы.
- **Средняя загрузка (LA)** – средняя загрузка системы за последнюю минуту.
- **Количество ядер ЦПУ** – количество ядер процессора.
- **Доступно памяти** – размер доступной оперативной памяти.
- **ЦПУ** – загрузка центрального процессора.
- **Память** – размер свободной оперативной памяти.
- **Свободное место для разделов** – процент использования разделов **/** и **/boot**.
- **Свободные индексные дескрипторы для разделов** – процент использования индексных узлов.
- **Свободное место для разделов** – свободное место на диске в Гб.
- **Активное время дисков** – степень загрузки разделов диска, выраженная в процентах.

- **Количество операций чтения/записи на дисках в секунду** – величина операций чтения/записи в секунду.
- **Время ожидания чтения/записи дисков** – время на обработку центральным процессором операций чтения/записи дисков.
- **Объем чтения/записи на дисках в секунду** – объем операций чтения/записи в Кб.
- **Сетевой трафик** – объем входящего и исходящего сетевого трафика.

Внимание!

*Первоначальная информация по дисковой подсистеме и сетевому трафику в разделе **Система > Мониторинг > Показатели ОС** появляется не раньше, чем через час после установки KEO DLP.*

Примечание

Описание работы с графиками приведено в разделе 5.4.

5.4.5. Подробные данные

В разделе **Система** > **Мониторинг** > **Подробные данные** системный администратор может построить отчеты по необходимым статистическим показателям, выбрав определенный набор узлов.

Для построения отчетов по конкретным показателям следует в выпадающем списке выделить курсором необходимые показатели. Сбросить группировку можно нажатием на значок  .

Принципы отображения узлов и групп мониторинга и инструмент для выбора временного отрезка, за который необходимо получить данные, описаны в разделе 5.4.

Примечание

*На вкладке **Подробные данные** не будут строиться отчеты по некоторым показателям из-за особенностей вывода команды **iostat** в ОС. В этом случае появится сообщение **Нет данных для отображения**.*

Рис. 5.29. Подробные данные

Примечание

Если выбрано более трех показателей, то нажав на число в конце списка, отобразится полный список выбранных показателей.

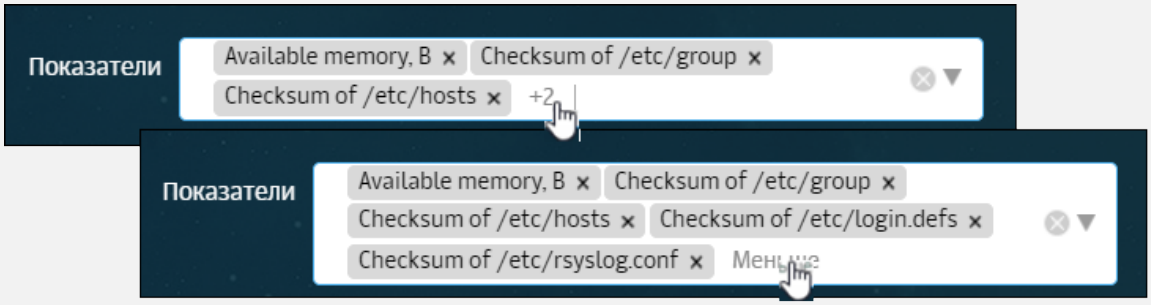


Рис. 5.30. Отображение показателей

5.5. Администрирование системы

Работа системного администратора с GUI выполняется в разделе главного меню **Система** > **Администрирование**. В левой части раздела расположено дерево объектов для управления функционированием KEO DLP (см. Рис.5.31):

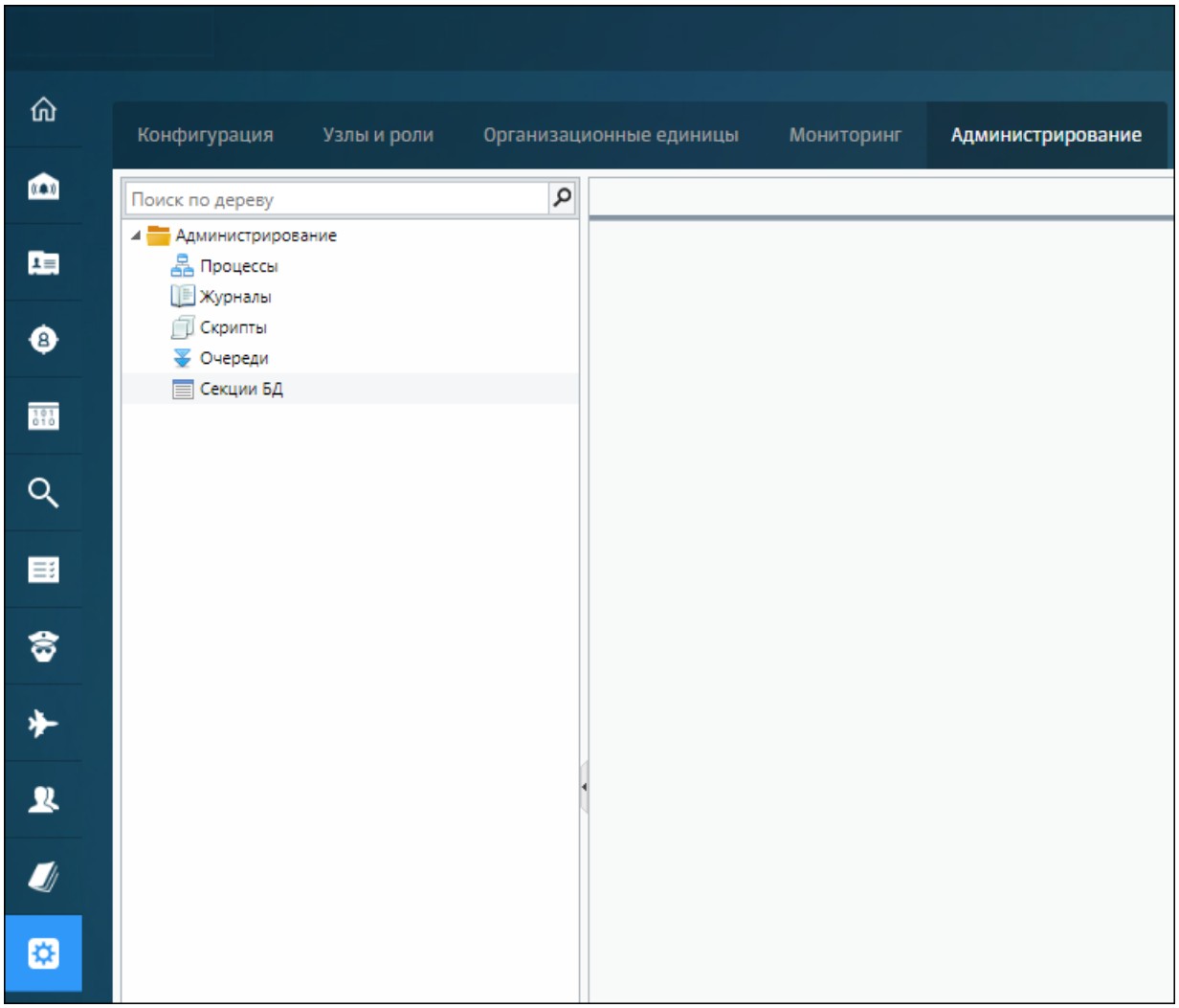


Рис. 5.31. Дерево объектов раздела Система > Администрирование

Дерево объектов содержит раздел **Администрирование**. Раздел **Администрирование** содержит следующие подразделы:

- **Процессы** – предназначен для управления процессами системы, запуска, перезапуска, остановки и т.д. (см. раздел 5.5.1).
- **Журналы** – предназначен для просмотра записей в журнальных файлах (см. раздел 5.5.2).
- **Скрипты** – предназначен для запуска служебных скриптов (см. раздел 5.5.3).
- **Очереди** – предназначен для работы с очередями сообщений, обрабатываемых различными сервисами (см. раздел 5.5.4).
- **Секции БД** – предназначен для управления секциями БД Oracle и/или PostgreSQL (см. 5.5.5).

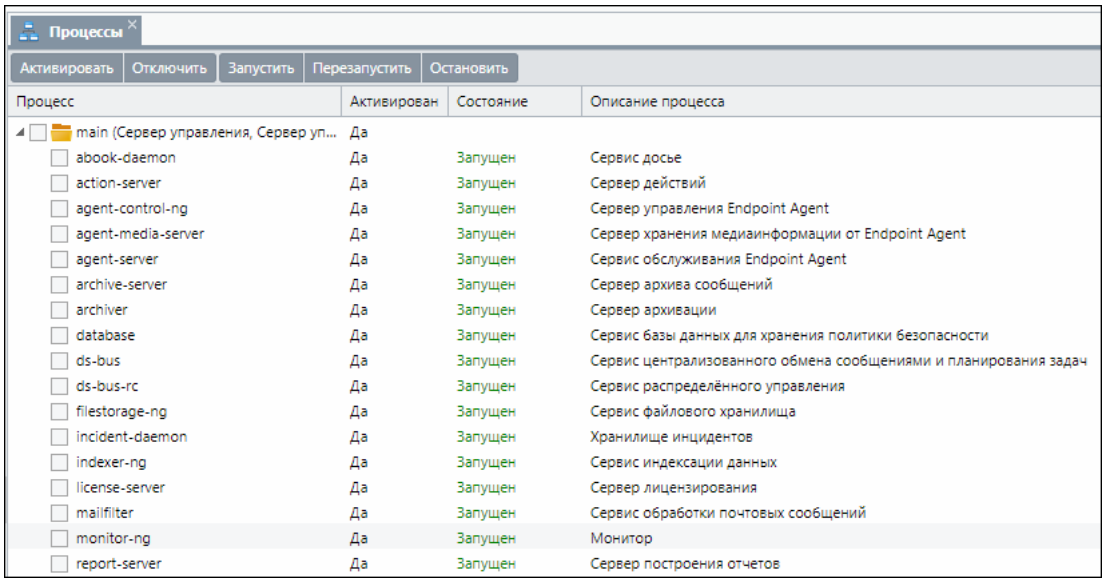
Чтобы найти необходимый подраздел, в поле для поиска необходимо ввести часть имени подраздела и нажать кнопку .

5.5.1. Управление процессами

Для управления запуском, остановкой и перезапуском процессов предназначен раздел дерева объектов **Администрирование > Процессы**. При выборе данного раздела в основном окне открывается вкладка **Процессы**, на которой приведён список всех процессов для каждого узла (см. Рис.5.32).

Примечание

*В случае распределённой системы в списке процессов появляется дополнительный раздел с именем **Все хосты**. Здесь представлены все процессы для всех узлов. Этот раздел предназначен для выполнения массовых действий над процессами на всех имеющихся узлах. Выбор какого-либо процесса в разделе **Все хосты** аналогичен выбору одноимённого процесса на каждом узле, где он запущен или может быть запущен.*



Процесс	Активирован	Состояние	Описание процесса
main (Сервер управления, Сервер уп...	Да		
abook-daemon	Да	Запущен	Сервис досье
action-server	Да	Запущен	Сервер действий
agent-control-ng	Да	Запущен	Сервер управления Endpoint Agent
agent-media-server	Да	Запущен	Сервер хранения медиаинформации от Endpoint Agent
agent-server	Да	Запущен	Сервис обслуживания Endpoint Agent
archive-server	Да	Запущен	Сервер архива сообщений
archiver	Да	Запущен	Сервер архивации
database	Да	Запущен	Сервис базы данных для хранения политики безопасности
ds-bus	Да	Запущен	Сервис централизованного обмена сообщениями и планирования задач
ds-bus-rc	Да	Запущен	Сервис распределённого управления
filestorage-ng	Да	Запущен	Сервис файлового хранилища
incident-daemon	Да	Запущен	Хранилище инцидентов
indexer-ng	Да	Запущен	Сервис индексации данных
license-server	Да	Запущен	Сервер лицензирования
mailfilter	Да	Запущен	Сервис обработки почтовых сообщений
monitor-ng	Да	Запущен	Монитор
report-server	Да	Запущен	Сервер построения отчетов

Рис. 5.32. Вкладка Процессы

Таблица со списком процессов состоит из четырёх столбцов.

В столбце **Процесс** отображаются названия процессов KEO DLP, а в столбце **Описание процесса** – более подробное описание процесса и его назначения. Процессы сгруппированы по узлам. Чтобы свернуть/развернуть список процессов, работающих на каждом узле, необходимо щелкнуть мышью на значок ▷ в строке с именем узла.

В зависимости от роли, выбранной для узла, на нём могут работать процессы из определённого перечня. Список соответствия ролей и активируемых процессов приведён в разделе 5.3.

В столбце **Активирован** указан статус активности процесса: **Да** – процесс активирован или **Нет** – процесс не активирован. Если процесс не активирован, это значит, что его работа полностью остановлена. При этом удаляется журнальный файл процесса и его рабочий каталог на файловой системе. Для активации процесса необходимо выбрать его в списке процессов, установив флажок слева от названия процесса, и нажать кнопку **Активировать** в меню сверху над списком процессов. Чтобы полностью выключить активный процесс, необходимо выбрать его и нажать кнопку **Отключить**. Установка статуса

активности процесса в веб-интерфейсе аналогична выполнению скрипта **config cluster** с параметром **enable-services** или **disable-services** с помощью CLI (см. раздел 6.10.1).

Активированный процесс может находится в состоянии **Запущен**, **Не запущен**, **Запускается**, соответствующая запись отображается в столбце **Состояние**. Кроме того, предусмотрено цветовое выделение для процессов, находящихся в разных состояниях: зеленым цветом показано состояние запущенных процессов, красным – не запущенных, черным – в состоянии запуска.

Системный администратор может управлять состоянием процессов с помощью кнопок **Запустить**, **Остановить**, **Перезапустить** в меню сверху над списком процессов.

Чтобы запустить, остановить или перезапустить один или несколько процессов, необходимо:

1. Выбрать нужные процессы, установив флажки рядом с названием. Если требуется произвести какое-либо действие одновременно со всеми процессами на каком-то узле, то необходимо установить флажок рядом с именем узла.

2. Нажать в меню кнопку, соответствующую выполняемому действию.

Примечание

*Сразу после запуска процесса, в течении 10 секунд, его статус отображается как **Загрузка**. Это относится как к тем процессам, которые были преднамеренно остановлены системным администратором, так и к тем, которые могли завершиться (а потом быть перезапущены) из-за внутренней ошибки.*

Операции запуска, перезапуска, остановки процессов с помощью веб-интерфейса аналогичны выполнению скрипта **dsctl** с ключами **start**, **stop**, **restart** с помощью интерфейса командной строки (см. раздел 6.4).

5.5.2. Просмотр журнальных файлов

Журнальные файлы содержат записи о работе процессов и сервисов KEO DLP. Для просмотр журнальных файлов, формируемых KEO DLP, необходимо выбрать раздел **Система > Администрирование > Журналы** в дереве объектов (см. Рис.5.33):

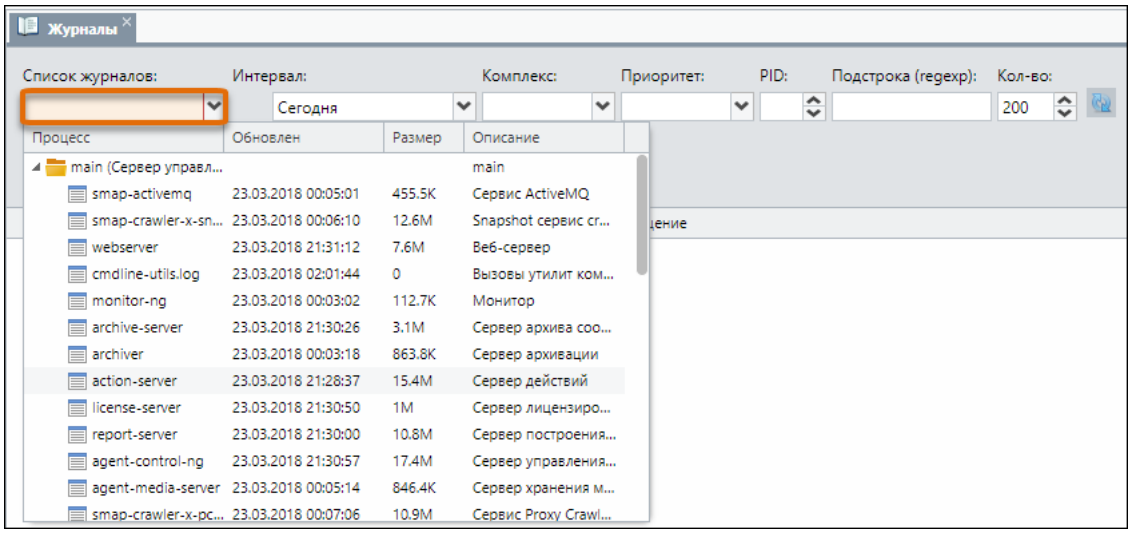


Рис. 5.33. Основное окно просмотра журнальных файлов

Настройка общих параметров журналирования выполняется в секции **Общие настройки системы** (раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование системы > Общее**).

Для занесения в журнал отладочной информации необходимо установить флажок **Вывод отладочной информации** (Рис.5.34). Далее необходимо настроить параметры **Уровень журналирования** и **Использование syslog**.

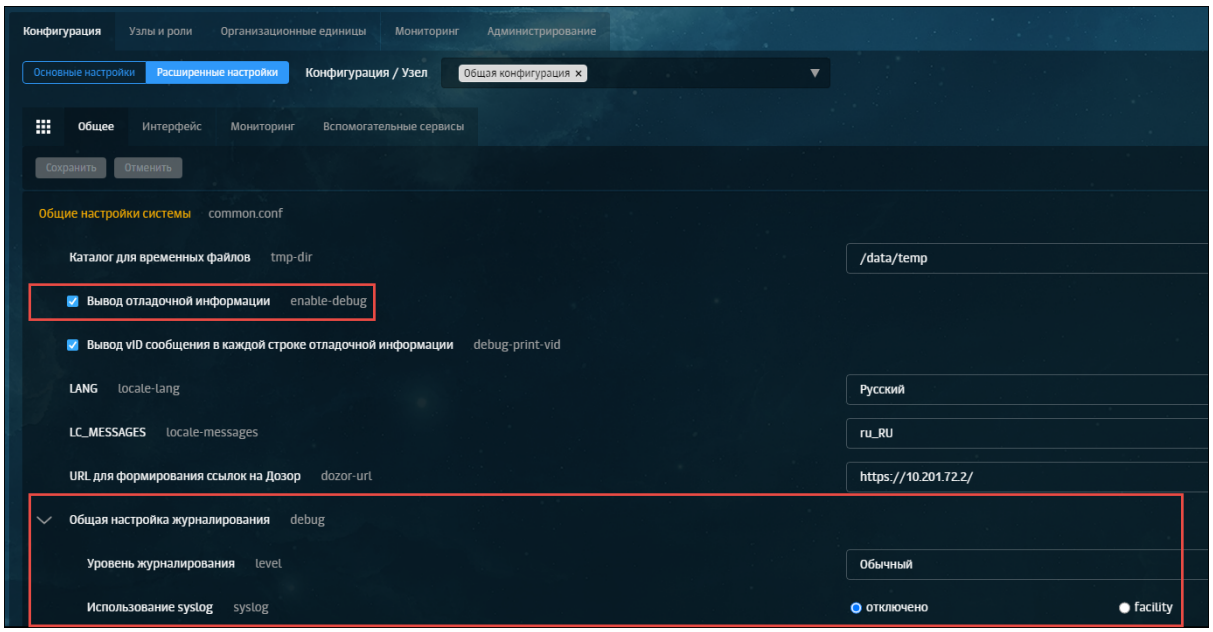


Рис. 5.34. Настройка общих параметров журналирования

Кроме того, для процессов, работа которых журналируется, существуют конфигурационные файлы с именами вида **<имя процесса>.debug** или параметры с именем **debug**, в которых выполняются настройки журналирования для каждого отдельного процесса. Получить список таких конфигурационных файлов можно, указав в поле для поиска в дереве объектов ключевое слово **debug** и нажав кнопку  (Рис.5.35).

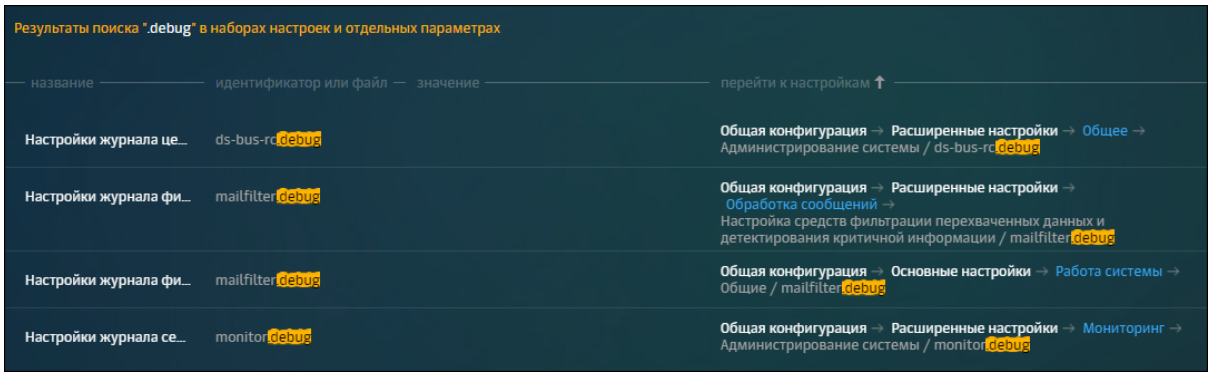


Рис. 5.35. Поиск конфигурационных файлов для настроек журналирования

В каждом из этих файлов есть возможность настройки общих параметров процессов и, при необходимости, настройки параметров журналирования для различных модулей KEO DLP (более подробно описано в разделе 6.11).

Строка настройки фильтра для просмотра журнальных файлов содержит следующие поля (см. Рис.5.33):

- **Список журналов** – раскрывающийся список журнальных файлов, доступных для отображения (см. Рис.5.36). В списке представлены журналы процессов, запущенных на каждом из имеющихся узлов (в зависимости от роли, назначенной узлу, список работающих процессов, а соответственно и список доступных журналов может различаться для разных узлов). Помимо названия журнального файла в списке приводятся: дата последнего обновления, его размер и описание.

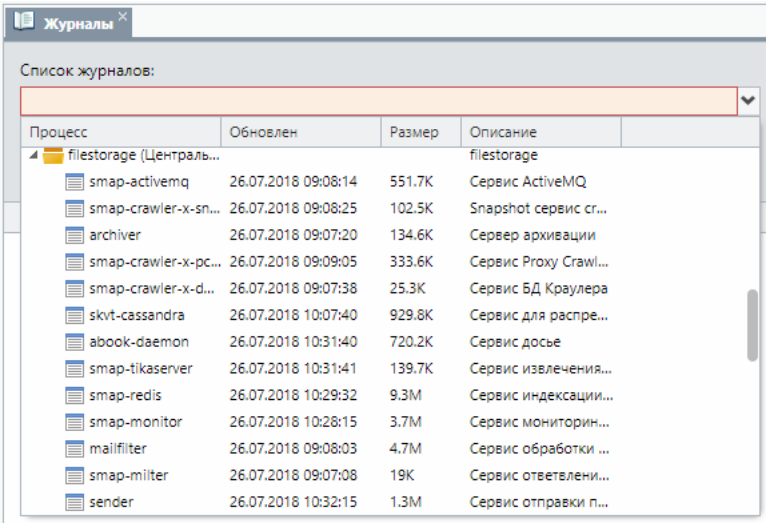


Рис. 5.36. Выбор журнального файла

После выбора журнального файла в основном окне отображается таблица со списком записей этого журнального файла (см. Рис.5.37):

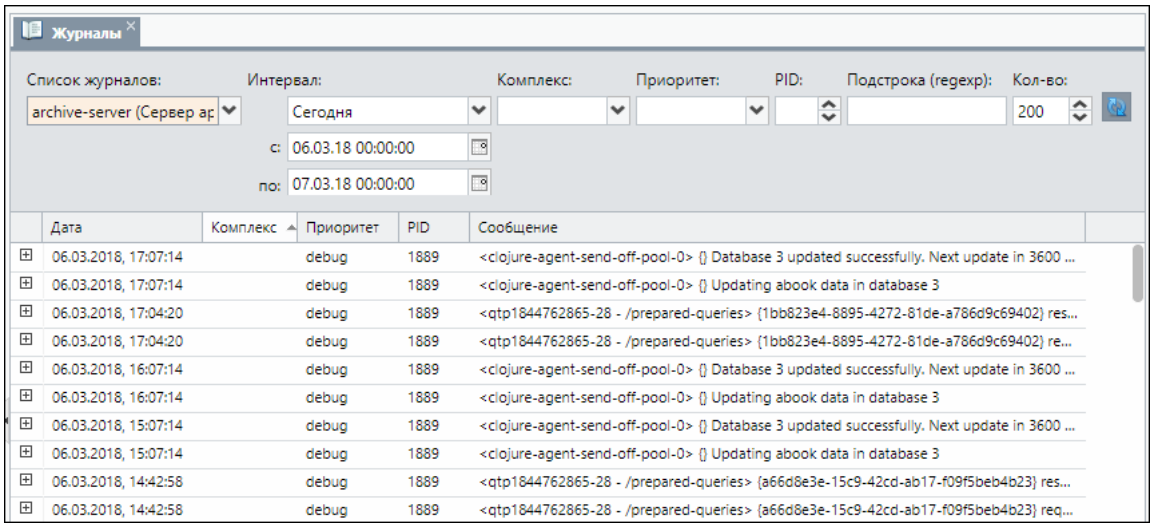


Рис. 5.37. Вкладка Журналы

Таблица имеет следующие столбцы:

- **Дата** – дата и время записи.
- **Комплекс** – имя модуля (или процесса), создавшего запись.
- **Приоритет** – тип журнальной записи.
- **PID** – идентификатор процесса.
- **Сообщение** – текст журнальной записи.

- **Интервал** – поле для задания интервала отображения информации. Имеются следующие возможности задания интервала:
  - Раскрывающийся список, позволяющий задать следующие интервалы: **Час, Три часа, Сегодня, Вчера, За последние три дня, С начала недели, За прошлую неделю, С начала месяца, За прошлый месяц, За последние 30 дней, С начала года** (Рис.5.38). Значение по умолчанию: **Сегодня**.

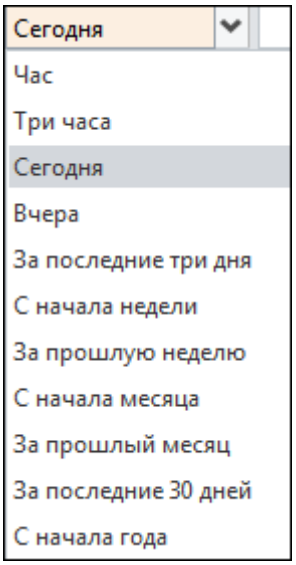


Рис. 5.38. Раскрывающийся список интервалов

- **с:** – открывает календарь для задания конкретной даты и времени начала вывода информации (см. Рис.5.39); При нажатии кнопки **Сейчас** будет выведена текущая информация.

- **по:** – открывает календарь для задания конкретной даты и времени завершения вывода информации.

В результате выбора интервала будут показаны журнальные записи именно за этот интервал.

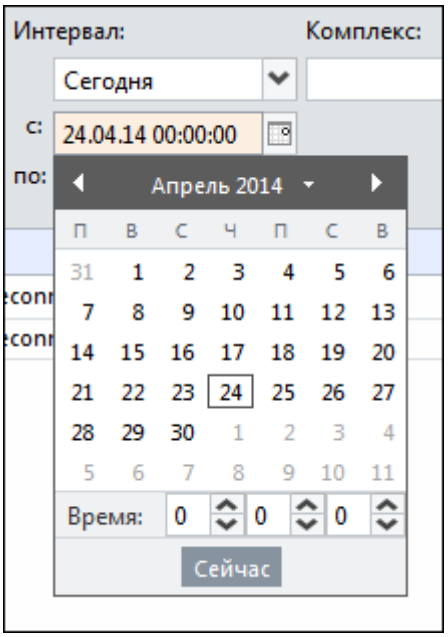


Рис. 5.39. Выбор интервала

- **Комплекс** – раскрывающийся список для выбора модуля (или подсистемы) KEO DLP для отображения его журнальных записей (Рис.5.40):

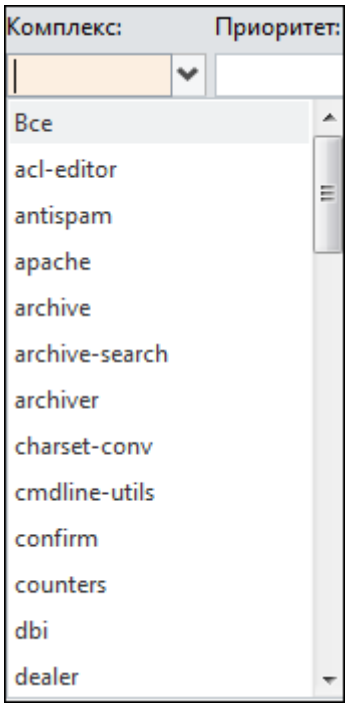


Рис. 5.40. Выбор комплекса из раскрывающегося списка

- **Приоритет** – тип записи в журнальном файле. В зависимости от установленного в настройках уровня (**Обычный**, **Повышенный** или **Отладочный**) в файлы журналирования выводятся различные типы записей (более подробно описано в разделе 6.11). Приоритеты в KEO DLP имеют следующий порядок:
  - **info** – информационное сообщение;
  - **debug** – отладочная информация;
  - **fatal** – сообщение о критической ошибке, препятствующей дальнейшей работе подсистемы;
  - **error** – сообщение об ошибке, позволяющей продолжить нормальное функционирование подсистемы;
  - **emerg** – сообщение об аварийной ситуации, препятствующей дальнейшей работе подсистемы;
  - **alert** – сообщение о критической ошибке, позволяющей продолжить нормальное функционирование подсистемы, но требующей немедленного устранения;
  - **crit** – сообщение о критической ошибке, препятствующей дальнейшей работе подсистемы;
  - **warn** – предупреждение, выводится в том случае, если обнаружено некое несоответствие ожидаемому поведению;
  - **warning** – предупреждение, выводится в том случае, если обнаружено некое несоответствие ожидаемому поведению;
  - **notice** – информационное сообщение.

- **PID** – поле, позволяющее отфильтровать записи журнала по идентификатору процесса. При указании значения PID в журнале останутся только записи для процесса с данным значением идентификатора.

- **Подстрока (regexp)** – поле, позволяющее отфильтровать записи журнала по значению подстроки. В результате ввода в поле какой-нибудь строки символов будут показаны только те записи журнала, в которых такая строка встречается. Данный параметр является регистрозависимым – значения «строка для поиска» и «СТРОКА ДЛЯ ПОИСКА» считаются разными. Строку для поиска можно формировать с использованием регулярных выражений, подробнее о работе с ними написано в документе *Справочник администратора безопасности*.

- **Кол-во** – с помощью данного пункта меню можно ограничить количество выводимых записей журнала. При вводе в данное поле числа N будет показано N последних записей журнала.

При задании какого-либо значения фильтра данные в таблице журнала автоматически обновляются. Если этого не произошло, то можно обновить данные, нажав на значок в строке параметров фильтрации.

5.5.3. Запуск скриптов для получения информации о работе KEO DLP

Для получения информации о работе системы предназначен раздел **Администрирование > Скрипты** дерева объектов. Эта информация необходима, например, инженерам поддержки KEO DLP в случае сбоев в работе системы. При выборе данного раздела в основном окне открывается вкладка **Скрипты** со списком имеющихся узлов (Рис.5.41). При нажатии на значок рядом с именем узла раскрывается список доступных для выполнения на этом узле скриптов:

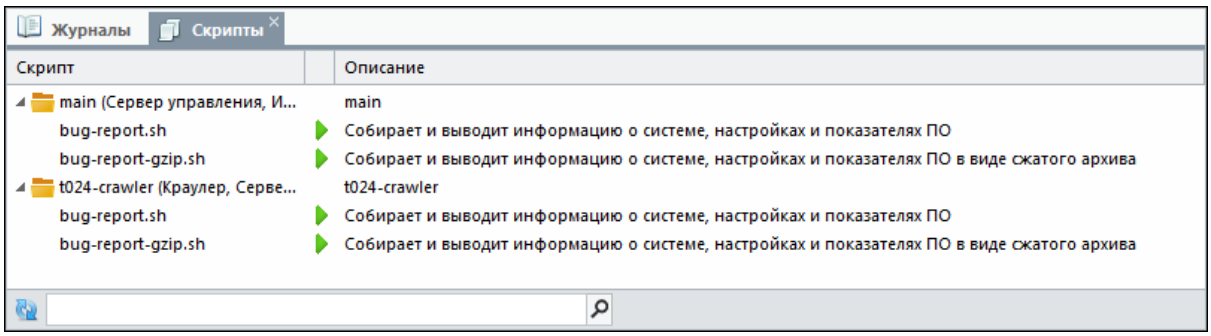


Рис. 5.41. Вкладка Скрипты

Для каждого узла можно выполнить один из следующих скриптов:

- **bug-report.sh** – собирает и выводит информацию о системе, настройках и показателях работы ПО (при этом информация выводится в текстовый файл);

- **bug-report-gzip.sh** – собирает и выводит информацию о системе, настройках и показателях работы ПО (при этом информация выводится в архив **gzip**).

Для запуска скрипта необходимо нажать на значок справа от имени скрипта. По окончании работы скрипта информация либо будет выведена в текстовом виде на отдельной вкладке браузера, либо откроется стандартное окно для сохранения файла с отчётом на жёстком диске.

Скрипт **bug-report-full.sh** можно запустить с помощью CLI. Перед выполнением скрипта следует запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта:

 # bug-report-full.sh [-f] [-a] [-d <YYYY-MM-DD>]

Доступны следующие ключи:

- **-f** – вывести всю информацию о системе. Если не указывать, будут отображаться последние 3000 строк журнала.
- **-a** – включить в отчет информацию о последних 4 файлах, которые содержат вывод команды **atop**. При использовании с ключом **-d** в отчет будет включена информация о последнем файле с выводом команды **atop** за дату **YYYY-MM-DD**.
- **-d** – вывести отчет за дату, указанную в формате **YYYY-MM-DD**.
- **-h** – вывести справку по работе со скриптом.

Пример вывода при успешном выполнении скрипта:

```
Packed to /data/temp/bug-report-vrogov.isim.local-2021-04-14_17-17-17.tar.bz2
```

В результате выполнения скрипта будет создан отчет об ошибках со следующей информацией:

- дата формирования отчета;
- информация об используемой ОС и ее ресурсах;
- текущая версия и номер сборки ПК;
- список пакетных файлов в составе дистрибутива системы;
- список установленных обновлений системы;
- информация о состоянии лицензии;

Примечание

Более подробно о license-tool см. раздел 6.25.

- таблица маршрутизации;
- настройки сетевых интерфейсов;
- настройки DNS;
- содержимое спулов;
- содержимое журнальных файлов;

- настройки журналирования;
- конфигурационные файлы узлов кластера;

Примечание

*Сбор конфигурационных файлов выполняется при запуске скрипта **bug-report-full.sh** на master-узле.*

- содержимое набора правил фильтрации;
- данные планировщика **cron**;
- информация о ролях, назначенных кластеру/узлу кластера KEO DLP;
- информация о файловой системе;
- результаты выполнения команд **last** и **history** (для пользователей **root** и **dozor**);
- данные о событиях ядра Linux с уровнем важности **3: errors (ошибки)**;
- информация о количестве и суммарном размере сообщений по каналам коммуникации и дате в активной БД архива;
- сведения о секциях активной БД архива;
- информация о сессиях пользователя **dozor**, подключенного к активной БД архива;
- информация о процессах системы и используемой виртуальной памяти;
- параметры конфигурации системы (данные аналогичны выводу скрипта **get-config**);
- сведения о состоянии кластеров Cassandra и OpenSearch;
- триггеры Zabbix, отражающие текущее состояние системы.

  Пример записи:

```
----------------------------------------------------------------
Zabbix triggers:

Сервис DIFI не доступен на tn733.isim.local:9301

Сервис IDID не доступен на tn735.isim.local:9302
----------------------------------------------------------------
```

5.5.4. Работа с очередями сообщений

На вкладке **Очереди** (см. Рис.5.42) выполняется работа с очередями сообщений. Для каждого узла выводится информация о количестве сообщений, количестве файлов и объеме сообщений, находящихся в очередях фильтра, сервиса архивации и сервиса отправки.

В распределённой системе суммарные данные очередей по всем узлам отображаются в разделе **Все хосты**. Этот раздел предназначен для выполнения массовых действий над очередями: выбор какой-либо очереди в разделе **Все хосты** аналогичен выбору одноимённых очередей для всех имеющихся узлов.

При этом очереди сообщений также разделяются по слотам хранения: **norm** – сообщения из обычных слотов, **high** – сообщения с высоким приоритетом, **err** – сообщения, обработка которых завершилась с ошибкой.

Примечание

Подробнее о хранении сообщений на файловой системе и структуре спулов см. раздел 6.17.1.

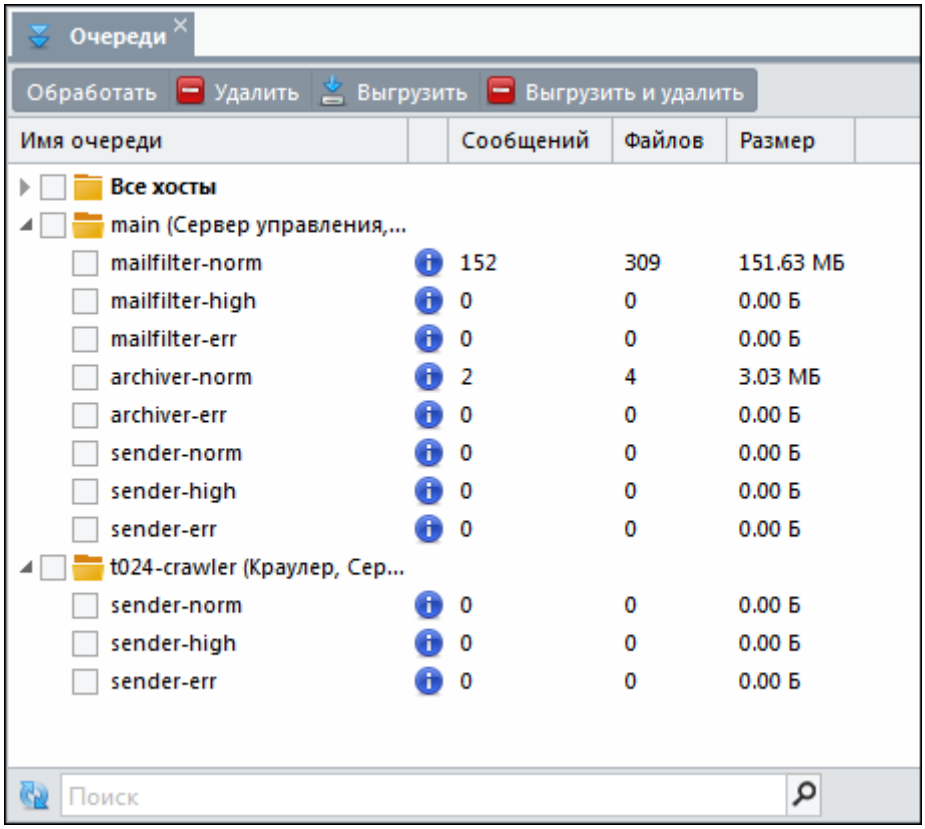


Рис. 5.42. Вкладка Очереди

5.5.4.1. Просмотр очереди сообщений

Чтобы открыть для просмотра очередь сообщений, необходимо нажать на значок в нужной строке таблицы. Например, чтобы просмотреть очередь сообщений сервиса фильтрации, следует выбрать строку **mailfilter-norm** (см. Рис.5.43):

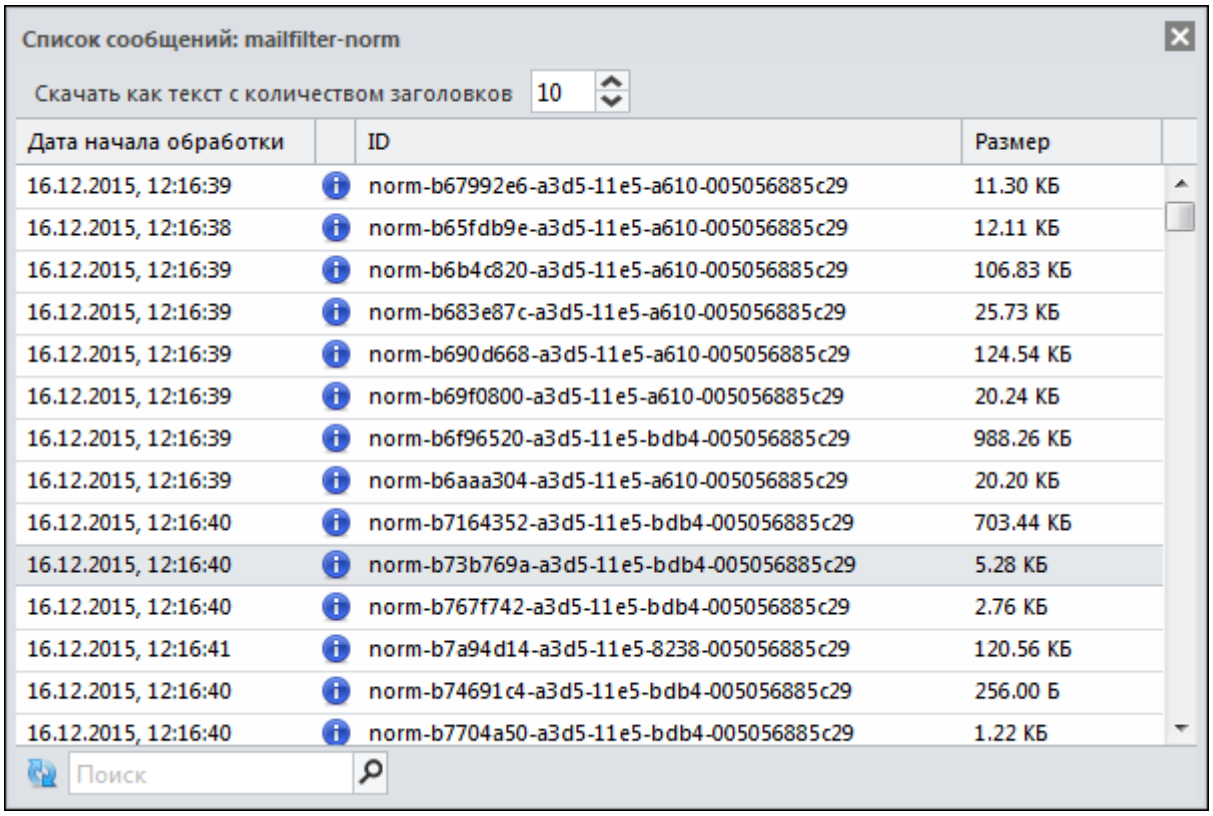


Рис. 5.43. Очередь сообщений сервиса фильтрации

В таблице со списком сообщений для каждого сообщения указывается дата и время начала обработки сообщения, его размер и идентификатор ID.

Список очереди сообщений можно открыть в текстовом виде. Для этого следует нажать кнопку **Скачать как текст с количеством заголовков** (см. Рис.5.43), указав предварительно в поле ввода рядом количество выводимых заголовков. Будет сформирован файл в формате .txt, который можно либо сразу открыть в текстовом редакторе, либо сохранить на жёсткий диск – при нажатии на кнопку **Скачать как текст с количеством заголовков** появится стандартное окно для выбора нужного варианта. Примерный вид такого файла показан на рисунке ниже (см. Рис.5.44):

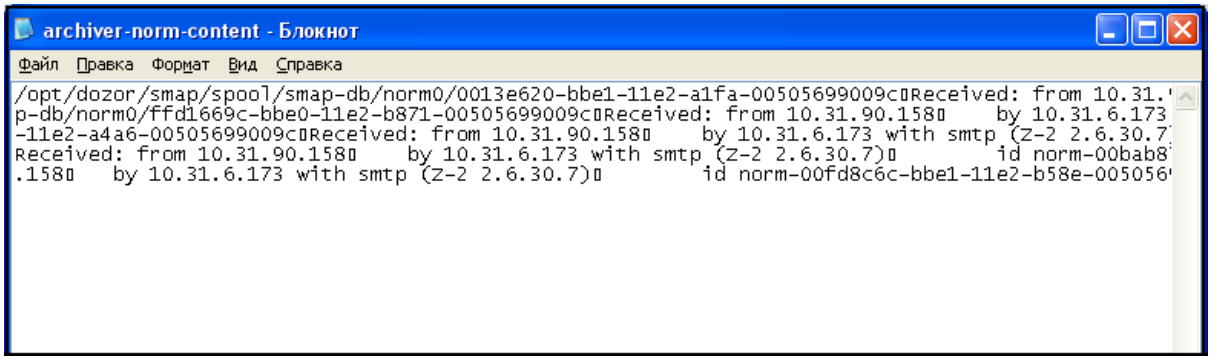


Рис. 5.44. Очередь сообщений в текстовом виде

5.5.4.2. Действия над очередями сообщений

Для каждой очереди сообщений доступны следующие действия:

- обработать (для сообщений, обработка которых завершилась с ошибкой);
- удалить;
- выгрузить;
- выгрузить и удалить.

Для выполнения этих действий используются одноимённые кнопки меню в верхней части вкладки **Очереди** (см. Рис.5.42). Выполняемые действия относятся только к тем очередям, для которых установлены флажки рядом с их именами.

При выполнении действия **Обработать** сообщения из очереди, то есть сообщения хранящиеся в спуле **spool/smap/err0**, передаются на обработку, то есть перемещаются в спул **spool/smap/norm**. При этом на экране появляется сообщение о результате обработки. Если выполнить действие **Обработать** над очередью сообщений в спуле, отличном от err-спула, то появится сообщение об ошибке.

При выполнении действия **Выгрузить** над выбранной очередью сообщений формируется архив формата .tar, содержащий файлы с журнальными записями обработки сообщений. Откроется стандартное окно для выбора варианта загрузить архив на жёсткий диск компьютера или сразу открыть его для просмотра.

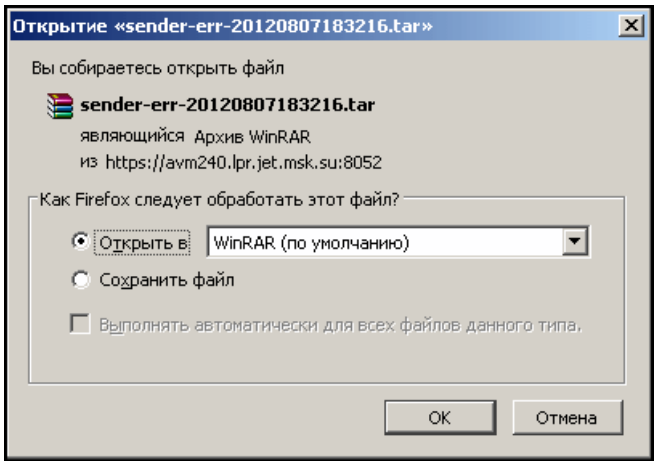


Рис. 5.45. Выгрузка очереди сообщений

При выполнении действия **Удалить** удаляются сообщения из выбранной очереди, то есть удаляются все файлы сообщений из каталога соответствующего спула.

При выполнении действия **Выгрузить и удалить** формируется архив очереди сообщений и происходит выгрузка, как описано выше, после чего сообщения из очереди сообщений удаляются.

5.5.5. Управление секциями БД

Раздел **Секции БД** дает возможность подключать, отключать, перемещать на хранение и удалять секции баз данных Oracle и/или PostgreSQL с помощью веб-интерфейса. При этом остановка каких-либо сервисов не требуется.

В интерфейсе управления секциями БД доступна следующая информация (Рис.5.46):

- **База данных** – имя схемы соединения с базой данных или название секции.
- **Дата** – дата окончания секции, т.е. момент времени, в который была или будет прекращена запись данных в секцию.
- **Объем** – объем данных в секции.
- **Статус** – состояние секции в текущий момент.
- **Действия** – список действий, доступных для конкретной секции.

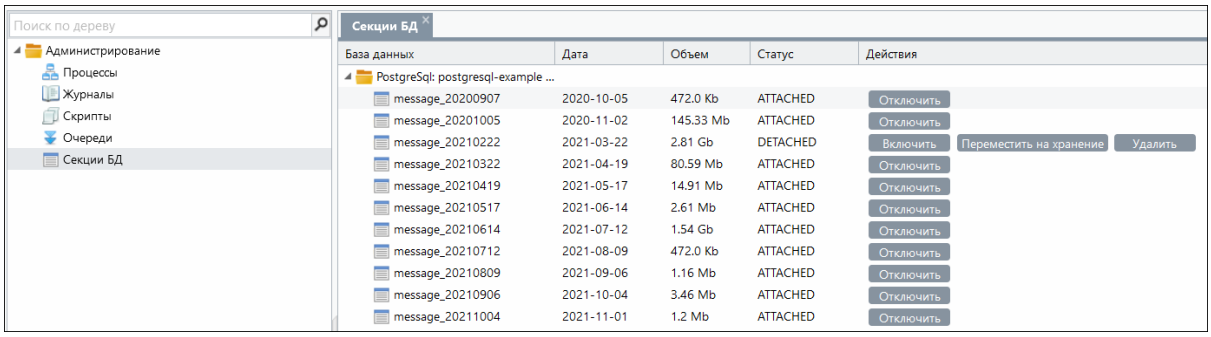


Рис. 5.46. Вкладка Секции БД

В нижней части окна расположена строка меню со значком обновления информации вкладки и полем поиска (Рис.5.46).

Чтобы получить список секций БД, следует нажать на значок в строке этой БД.

Действия, доступные для секции, зависят от её состояния. Ниже приведена таблица соответствия состояний секций и доступных для них действий:

Табл. 5.1. Соответствие состояний секций и доступных действий

Статус	Расшифровка статуса	Доступные действия
ATTACHED	Секция подключена и доступна для записи	Отключить
DETACHED	Секция отключена	Включить, Переместить на хранение, Удалить

Действия над секциями:

- **Отключить** – отключение включенной секции.
- **Включить** – включение ранее отключенной секции.
- **Переместить на хранение** – перемещение секции в указанный каталог на сервере базы данных, к которой принадлежит перемещаемая секция. Файлы данных при этом не переименовываются.
- **Удалить** – удаление секции.

Для подключения секции, ранее перемещённой на хранение с помощью веб-интерфейса, необходимо предварительно скопировать её файлы данных в прежний каталог.

6. Сопровождение KEO DLP

Для сопровождения системы предусмотрены следующие специальные скрипты:

- **bug-report.sh**, **bug-report-gzip.sh** – построение статистических отчетов о ходе работы системы (см. раздел 5.5.3). Данная информация необходима для инженеров поддержки в случае сбоев;
- **user-tool.py** – управление учётными записями и группами пользователей (см. раздел 6.1);
- **config-protection** – шифрование и расшифровка паролей (см. раздел 6.3);
- **dsctl** – управление сервисами KEO DLP (см. раздел 6.4);
- **db-conn.py** – просмотр информации о настроенных соединениях с БД в виде, удобном для использования в sh-скриптах (см. раздел 6.5);
- **incident-tool** – управление ротацией инцидентов (см. раздел 6.7);
- **ldap-tool** – получение списка групп LDAP (см. раздел 6.9);
- **config** – управление конфигурацией кластера KEO DLP (см. раздел 6.10);
- **part-control** – для автоматического отключения, архивации и удаления секций БД архива (см. раздел 6.12.5.2);
- **message-tool.py** – просмотр пометок сообщений (см. раздел 6.13.2);
- **querytool** – экспорт и удаление сообщений в БД архива по сформированному запросу (см. раздел 6.13.3);
- **export-messages.py** – экспорт сообщений из архива KEO DLP (см. раздел 6.13.4);
- **import-messages.py** – импорт сообщений в архив KEO DLP (см. раздел 6.13.5);
- **qtool.py** – просмотр результатов поисковых запросов (см. раздел 6.13.8);
- **policy-tool** – генерация политики фильтра KEO DLP (см. раздел 6.16.1);
- **objs.py** – просмотр информации об объектах политики (см. раздел 6.16.2);
- **mailfilter-report** – создание отчетов по состоянию сервиса **mailfilter** (см. раздел 6.16.3);
- **idid-tool** и **idid-tool.py** – работа с модулем IDID (см. раздел 6.20);
- **difi-tool** и **difi-tool.py** – работа с модулем DIFI (см. раздел 6.21);
- **as-tool.py** – работа с сервером действий (см. раздел 6.22);
- **license-tool** – просмотр информации о лицензии и об идентификаторе инсталляции (см. раздел 6.25);

Функционирование KEO DLP требует регулярного выполнения ряда задач, большинство из которых может быть автоматизировано с помощью заданий программы **cron**.

Кроме описания вышеуказанных скриптов, в данном разделе также приведено описание использования списков слов уверенного определения кодировки (см. раздел 6.18).

6.1. Управление учётными записями и группами пользователей

Для управления учётными записями и группами пользователей с правами администратора безопасности предназначен скрипт **user-tool.py**, с помощью которого можно создавать и удалять учётные записи пользователей, изменять пароль пользователя, включать пользователя в группу и прочее.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат команды для запуска скрипта **user-tool.py**:

$ user-tool.py [ключ]

Доступны следующие ключи:

- **-m <режим работы>** – выбрать режим работы скрипта. Принимает значения **api** (работа через API веб-сервиса) и **sql** (работа напрямую с БД).
- **-U <имя пользователя>**, **--login-user <имя пользователя>** – задать имя существующего пользователя.
- **-P <пароль>**, **--login-password <пароль>** – указать пароль существующего пользователя.
- **-H <имя узла/IP>**, **--login-host <имя узла/IP>** – указать имя или IP-адрес узла, к которому подключается существующий пользователь.
- **-O <порт>**, **--login-port <порт>** – указать номер порта, к которому подключается существующий пользователь.
- **-B <имя БД>**, **--login-database <имя БД>** – указать имя БД, к которой подключается существующий пользователь. При подключении к БД политики ключ **-B** указывать не требуется.
- **-l**, **--list-users** – вывести на экран список всех доступных пользователей.
- **-L**, **--list-groups** – вывести на экран список всех доступных групп.
- **-p <имя пользователя> <пароль>** – изменить пароль пользователя. **-** (дефис) выводит подсказку по паролю.
- **-V <пароль>** – проверить надежность пароля пользователя. **-** (дефис) выводит подсказку по паролю.
- **-g <число> <длина>**, **--generate-pass <число> <длина>** – автоматически сгенерировать пароль, где **<число>** – количество паролей для генерации, **<длина>** – длина пароля.

- **-G <число> <длина>**, **--generate-pass-voc <число> <длина>** – автоматически сгенерировать пароль, более удобный для запоминания, где **<число>** – количество паролей для генерации, **<длина>** – длина пароля.

- **-a <имя пользователя>**, **--add-user <имя пользователя>** – добавить учетную запись нового пользователя с указанным именем (логином).

- **-r <имя пользователя>**, **--remove-user <имя пользователя>** – удалить учетную запись пользователя с указанным именем (логином). При этом сведения, заданные в полях **Имя** и **Логин** (Рис.6.1), будут сохранены в системе. Это позволит избежать добавления УЗ с неуникальным логином.

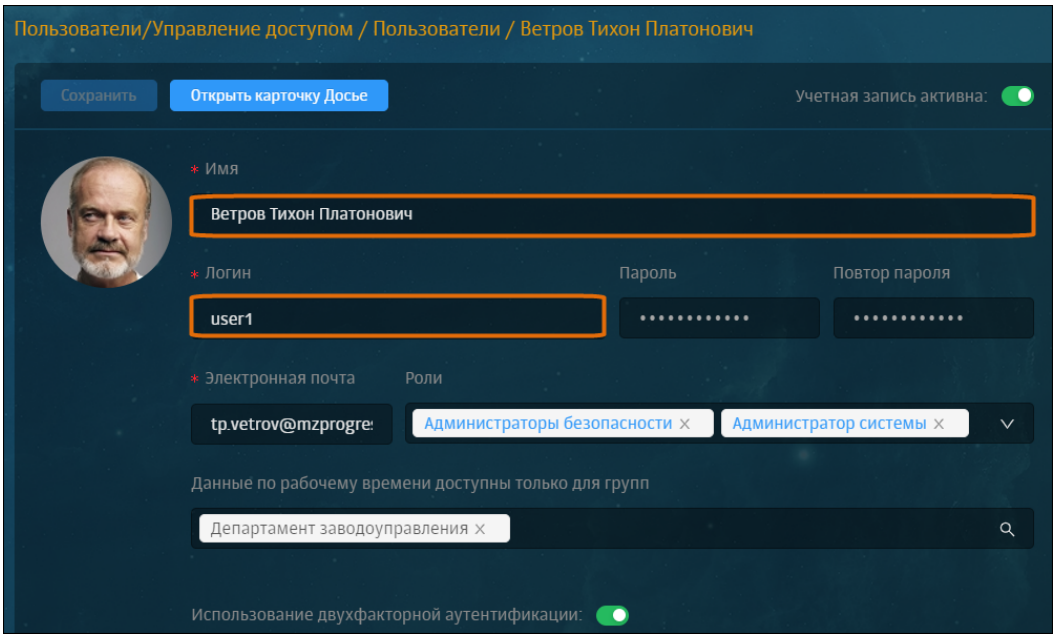


Рис. 6.1. Карточка пользователя

- **-A <имя группы>**, **--add-to-groups <имя группы>** – добавить пользователя в группу с указанным именем.

- **-R <имя группы>**, **--remove-from-groups <имя группы>** – удалить учетную запись пользователя из группы с указанным идентификатором.

- **-u <имя пользователя>**, **--unlock <имя пользователя>** – разблокировать учетную запись с указанным именем (логином). Используется совместно с параметром **-m sql** (в режиме работы с БД).

- **-e <имя пользователя>**, **--enable <имя пользователя>** – активировать учетную запись с указанным именем (логином).

- **-d <имя пользователя>**, **--disable <имя пользователя>** – заблокировать учетную запись с указанным именем (логином).

- **-f <имя пользователя>**, **--enable2fa <имя пользователя>** – включить двухфакторную аутентификацию для учетной записи с указанным именем (логином). Не применяется к учетным записям с ролью **Суперадминистратор** и используется совместно с параметром **-m sql** (в режиме работы с БД).

- **-F <имя пользователя>**, **--disable2fa <имя пользователя>** – отключить двухфакторную аутентификацию для учетной записи с указанным именем (логином). Не применяется к учетным записям с ролью **Суперадминистратор** и используется совместно с параметром**-m sql** (в режиме работы с БД).
- **-v**, **--verbose** – вывод сообщений о действиях, выполняемых скриптом.
- **-D**, **--debug** – включить отладочное журналирование.
- **-h**, **--help** – вывести на экран справочную информации об использовании скрипта.

Примеры использования скрипта:

- Показать список всех учетных записей. Формат команды для запуска скрипта:

  $ /opt/dozor/smap/bin/user-tool.py -l

  На экране отобразится информация по всем пользователям:

```
superadmin: superadmin
        Суперадминистраторы (6170705f-6772-6f75-70ff-ffff00000004)
        Администраторы безопасности (6170705f-6772-6f75-70ff-ffff00000005)
        Системные администраторы (6170705f-6772-6f75-70ff-ffff00000006)
-sysadmin: sysadmin
        Системные администраторы (6170705f-6772-6f75-70ff-ffff00000006)
-test: None
```

- Создать новую учетную запись. Формат команды для запуска скрипта:

  $ /opt/dozor/smap/bin/user-tool.py -a Test-user2

  На экране отобразится строка:

```
Пароль:
Имя: Тестовый
Группа (Enter - продолжить):
```

  Необходимо ввести с клавиатуры имя, пароль и группу, в которую входит пользователь, после на экран будет выведено сообщение:

```
Пользователь "Test-user2" добавлен
```

- Автоматически сгенерировать 2 пароля длиной 6 символов. Формат команды для запуска скрипта:

  $ /opt/dozor/smap/bin/user-tool.py -g 2 6

  Пример автоматической генерации паролей:

```
.1iBo8
`bC4$Q
```

- Разблокировать учетную запись пользователя. Формат команды для запуска скрипта:

  $ /opt/dozor/smap/bin/user-tool.py -m sql -u new-user3

В результате выполнения скрипта будет разблокирована учетная запись с логином **new-user3**.

- Удалить учетную запись пользователя. Формат команды для запуска скрипта:

  $ /opt/dozor/smap/bin/user-tool.py -r TEST2

  В результате выполнения скрипта будет удалена учетная запись с логином **TEST2**. При этом сведения, заданные в полях **Имя** и **Логин** (Рис.6.1), будут сохранены в системе. Это позволит избежать добавления УЗ с неуникальным логином.

6.2. Настройка ограничений на ввод пароля

Неверный пароль можно вводить 3 раза (число попыток изменить нельзя), после этого учетная запись пользователя будет заблокирована по умолчанию на 15 минут. Все неудачные попытки входа сбрасываются системой по умолчанию раз в час.

Чтобы изменить настройку ограничений на ввод пароля, необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройки обеспечивающих средств > Безопасность**.
2. Если требуется изменить время, необходимое для снятия блокировки пароля, отредактировать в секции **Правила аутентификации** значение параметра **Время блокировки учётной записи после исчерпания попыток входа, мин.**

   Примечание

   *Допустимое время блокировки – от 15 до 1440 минут. Принудительно снять блокировку можно, запустив скрипт **user-tool.py** с ключом **-u** или **--unlock**. Подробное описание формата команды разблокировки УЗ и примеров использования скрипта приведено в разделе 6.1.*

3. Если требуется изменить периодичность сброса неудачных попыток входа, в секции **Правила аутентификации** изменить значение параметра **Период времени, в течение которого подсчитываются неудачные попытки аутентификации, мин.**

   Примечание

   Допустимое время подсчета неудачных попыток – от 60 до 1440 минут.

4. Нажать **Сохранить** и **Применить**.

6.3. Шифрование паролей

KEO DLP позволяет запретить несанкционированный доступ к паролям пользователей. Это обеспечивается двусторонним шифрованием паролей с помощью скрипта **config-protection**. Формат двустороннего шифрования предусматривает хранение зашифрованных паролей в файле значений параметров конфигурации **/data/repos/dozor/config-base.git/values.json** и финальных конфигурационных файлах сервисов **aboook-daemon**, **agent-control-ng**, **agent-media-server**, **agent-server**, **archive-server**, **crawler-ccc**, **crawler-**

im, **crawler-pccc**, **crawler-snapshot**, **difi-server**, **filestorage-ng**, **grafana**, **incident-daemon**, **indexer-ng**, **mailfilter**, **monitor-server**, **report-server** и **webserver** с возможностью расшифровки по команде системного администратора. Применяется алгоритм AES-GCM с 256-разрядным ключом.

Внимание!

Скрипт работает только на master-узле и только от пользователя dozor или root.

Перед выполнением скрипта следует запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта **config-protection**:

 # config-protection [ключ]

Доступны следующие ключи:

- **enable basic** – зашифровать пароли с помощью применяемого алгоритма.

  В результате выполнения команды пароли отображаются в следующем формате:

  ```
  #SECURE#basic:base64(IV):base64(maskedBytes)
  ```

  где:

  - **#SECURE#** – признак того, что пароль замаскирован.
  - **basic** – алгоритм шифрования. Отображается всегда. В дальнейшем список алгоритмов будет расширяться.
  - **base64(IV)** – вектор инициализации, представляющий собой случайное число размера 12 байт. Значение уникально для каждого пароля.
  - **base64(maskedBytes)** – зашифрованный массив байтов пароля.

  Пример:

  ```
  #SECURE#basic:lCjCnqv5zT7jVQAT:A1NlaPvoKACA12OQFIhQvVOpNCBHOA==
  ```

- **disable** – расшифровать пароли.
- **status** – вывести на экран информацию о том, используется ли в текущей момент шифрование паролей или нет.

  Примеры:

  ```
  Protection enabled
  Protection disabled
  ```

6.4. Управление процессами KEO DLP

Расширенные возможности управления сервисами KEO DLP предоставляет скрипт **dsctl**. Он позволяет запускать, перезапускать, останавливать сервисы KEO DLP и получать информацию о их статусе.

Перед выполнением скрипта следует запустить интерпретатор команд **shell**, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта:

 # dsctl <action> [<services>...]

где **<action>** – действие, которое требуется совершить, а **<services>** – список сервисов KEO DLP, над которыми будет совершено это действие. Сервисы перечисляются через пробел. Скрипт необходимо запускать от имени пользователя **root**.

Доступны следующие действия:

- **boot** – запуск системы управления сервисами и всех сервисов (список сервисов определён ролями узла, см. раздел 5.3).
- **down** – остановка всех запущенных сервисов и затем самой системы управления сервисами.
- **start** – запуск заданного включённого, но ещё не запущенного сервиса. При использовании этого действия без указания имени сервиса запускаются все сервисы.
- **stop** – остановка заданного запущенного ранее сервиса. При использовании этого действия без указания имени сервиса останавливаются все сервисы.
- **restart** – перезапуск (например, после применения конфигурации) заданного сервиса. При использовании этого действия без указания имени сервиса перезапускаются все сервисы.
- **reload** – применение конфигурации без перезапуска сервиса. Данное действие доступно только для сервиса **webserver**.
- **status** – вывод текущего статуса включённых сервисов.
- **enable** – включение и запуск выключенного сервиса.
- **disable** – остановка и выключение включённого сервиса.
- **service-list** – вывод списка всех имеющихся в системе сервисов. При этом символом ***** в списке отмечаются сервисы, которые находятся в статусе **enabled**, например:

```
* abook-daemon
* action-server
* action-server-database
* agent-control-ng
* agent-media-server
  agent-server
  api-gateway
```

```
* archive-server
  archiver
  category-server
  clickhouse
  crawler-ccc
  crawler-database
  crawler-pccc
  crawler-processor
  crawler-scanner
  crawler-snapshot
* database
* detective-database
* detective-server
* ds-bus-rc
* filestorage-ng
  god-server
* grafana
  haproxy
  im-crawler
* incident-daemon
* indexer-ng
* license-server
  mailfilter
  media-processor-action-server
  media-processor-action-server-database

* monitor-agent
* monitor-httpd
* monitor-ng
* monitor-server

* opensearch
* report-server
* sender
* skvt-cassandra
  smap-activemq
* smap-difi
  smap-idid
* smap-redis
* smap-request-handler
  smap-smtp-gw
* smap-tikaserver
* software-center
* software-center-database
  stt-server
  tragent
  uba-server
* webserver
  webserver-local
```

- **-h** или **--help** – вывод справочной информации.

При распространении конфигураций скрипт **accept-settings** может принудительно запускать выключенные локально (с помощью скрипта **dsctl**) сервисы. Поэтому для включения или отключения сервисов на постоянной основе необходимо либо использовать кнопки **Активировать** и **Отключить** (раздел **Система > Администрирование > Процессы** в

GUI), либо использовать скрипт **config cluster** (см. раздел 6.10.1), который запускается на master-узле.

Скрипт **dsctl** следует запускать от имени пользователя **root** (кроме выполнения с параметрами **status** и **service-list** – в этих случаях можно запускать скрипт от имени любого пользователя).

При указании в качестве параметра скрипта **dsctl** имени процесса соответствующее действие применяется только к этому процессу. Если имя процесса не указано, действие выполняется над всеми процессами. Для действий **boot** и **down** указывать конкретный процесс не требуется, они выполняются над всеми процессами сразу.

Имена процессов (как их следует указывать в командной строке) приведены в следующей таблице:

Табл. 6.1. Имена процессов KEO DLP

Имя процесса	Описание
abook-daemon	Сервис доступа к Досье.
action-server	Сервис выполнения действий над сообщениями в архиве.
action-server-database	База данных сервера действий.
agent-control-ng	Сервис управления модулем KEO DLP Endpoint Agent при помощи GUI.
agent-media-server	Сервис хранения медиаинформации.
agent-server	Сервис обслуживания и управления агентами.
archiver	Сервис записи данных в хранилище снимков экрана, файловое хранилище, БД инцидентов и БД архива сообщений.
archive-server	Сервис доступа к сообщениям в архиве.
category-server	Сервис категоризации сообщений.
clickhouse	Сервис БД ClickHouse для хранения статистических данных.
crawler-ccc	Сервис управления ботами краулера.
crawler-database	Сервис хранения БД краулера.
crawler-pccc	Сервис управления краулером.
crawler-processor	Сервис обработки файловых данных.
crawler-scanner	Сервис поиска файловых данных.
crawler-snapshot	Сервис хранения метаданных файлов.
database	Сервис СУБД для хранения настроек политики и Досье.
detective-database	БД сервиса **Расследование**.
detective-server	Сервис **Расследование**.
ds-bus-rc	Сервис выполнения административных функций в распределённой системе.
filestorage-ng	Сервис файлового хранилища.
god-server	Сервис определения графических объектов.
grafana	Сервис построения графиков и диаграмм.
haproxy	Сервис распределения трафика по серверам фильтрации KEO DLP.
im-crawler	Сервис загрузки сообщений пользователей в корпоративных мессенджерах через официальный API.
incident-daemon	Сервис хранения и индексации инцидентов и событий информационной безопасности.
indexer-ng	Сервис индексации сообщений в архиве.

Имя процесса	Описание
license-server	Сервис, обеспечивающий доступ других сервисов к информации в лицензии.
mailfilter	Сервис обработки почтовых сообщений.
media-processor-action-server	Сервис выполнения действий по обработке медиаданных
media-processor-action-server-database	БД сервиса выполнения действий по обработке медиаданных
monitor-agent	Сервис мониторинга на узле.
monitor-httpd	Сервис HTTP-интерфейса к системе мониторинга Zabbix. Обеспечивает работу пользовательского интерфейса мониторинга.
monitor-ng	Сервис валидации параметров конфигурации.
monitor-server	Сервер мониторинга.
opensearch	Сервис поиска и индексации сообщений и инцидентов.
report-server	Сервис построения отчётов.
sender	Сервис передачи данных и уведомлений по протоколу SMTP.
skvt-cassandra	Сервис хранения индексов файлового хранилища, значений уровней доверия и кэша результатов распознавания текста изображений.
smap-activemq	Сервис очереди обрабатываемых файлов для краулера.
smap-difi	Сервис работы с цифровыми отпечатками.
smap-idid	Сервис контроля идентификаторов.
smap-redis	Сервис хранения счётчиков, очередей сообщений для обработки и очередей действий над сообщениями.
smap-request-handler	Сервис обработчика веб-запросов.
smap-smtp-gw	Сервис приёма сообщений по протоколу SMTP.
smap-tikaserver	Сервис извлечения текстовых данных из содержимого сообщений.
software-center	Сервис развёртывания агентов.
software-center-database	БД Центра приложений.
stt-server	Сервис распознавания речи.
tragent	Сервис перехвата и анализа сетевого трафика (модуль KEO DLP Traffic Analyzer).
uba-server	Сервис сбора данных о поведении пользователей.
webserver	Сервис веб-сервера для доступа к GUI.

Ниже приведены примеры запуска скрипта **dsctl**.

Для запуска системы управления процессами следует запустить скрипт ключом **boot**. Формат команды для запуска скрипта:

 # dsctl boot

В результате выполнения команды на экран будет выведена информация о запуске системы управления процессами:

```
05/25 17:27:28.9142> waiting one second for system booting
05/25 17:27:28.9146> waiting one second for system booting
05/25 17:27:29.9401> system is loaded
```

Если система управления процессами уже запущена, будет показано следующее сообщение:

```
05/25 17:31:31.1042> System already booted
```

Для остановки работы системы управления процессами следует запустить скрипт с ключом **down**. Формат команды для запуска скрипта:

 # dsctl down

В результате выполнения команды на экран выводится следующая информация:

```
05/25 16:13:38.6289> waiting for services(agent-control-ng agent-server mailfilter) down 2 second
05/25 16:13:41.1079> waiting for services(agent-control-ng agent-server mailfilter) down 2 second
05/25 16:13:43.6139> waiting for services(agent-control-ng agent-server) down 2 second
05/25 16:13:46.1079> waiting for services(agent-control-ng agent-server) down 2 second
05/25 16:13:48.6109> waiting for services(agent-control-ng agent-server) down 2 second
```

При выполнении команды down в течение 5 секунд происходит ожидание завершения запущенных процессов. При этом с интервалом в 1 секунду этим процессам посылается сигнал на завершение. Если в течение 5 секунд какие-то процессы не завершились, происходит их принудительная остановка.

Для включения и запуска процессов следует запустить скрипт **dsctl** с ключом **enable**. Формат команды для запуска скрипта:

 # dsctl enable sender

В результате выполнения команды будет включён процесс **sender**, отвечающий за передачу данных по протоколу SMTP, а на экран будет выведено следующее сообщение:

```
08/07 13:50:36.9695> => service /opt/dozor/service/sender activation
```

Примечание

*При включении процесса выполняются следующие действия: создаётся скрипт запуска процесса (**/opt/dozor/var/lib/service/sender/run**), его выполняет подсистема инициализации **systemd** из каталога **/usr/lib/systemd/system/dozor_sender.service**. С помощью supervise-процессов запускается скрипт **run** для запускаемого процесса **sender**.*

Примечание

*Команда **dsctl enable** не меняет статуса включённых, но не запущенных процессов. Для запуска включённого процесса необходимо выполнить для него команду **dsctl start**.*

*Команда **dsctl enable webserver** автоматически включает и запускает сервис **webserver**. Поэтому дополнительно не требуется выполнять команду **dsctl start webserver**.*

Для остановки и выключения процесса используется скрипт **dsctl** с ключом **disable**. Формат команды для запуска скрипта:

 # dsctl disable sender

В результате выполнения скрипта будет остановлен и выключен процесс **sender**, а на экран будет выведена следующая информация:

```
08/07 13:49:43.0254> => service /opt/dozor/service/sender deactivation
08/07 13:49:43.1033> waiting one second for service sender down
```

```
08/07 13:49:44.1090> service sender is down
08/07 13:49:44.1853> service sender is finished
```

Примечание

*При выключении процесса выполняются следующие действия: управляющие процессы останавливают процесс журналирования и сам процесс **sender**. При этом выключение процесса **sender** происходит аналогично выполнению команды **down**, то есть в течение 5 секунд ожидается завершение процесса, а если он не завершился за это время, происходит его принудительная остановка. Также удаляются рабочий каталог и каталог с журнальным файлом, созданные при включении процесса **sender**. Поэтому, если данные журналирования работы процесса нужны для дальнейшего анализа, необходимо предварительно скопировать журнальный файл.*

Для получения данных о статусе процесса следует запускать скрипт **dsctl** с ключом **status** с указанием имени сервиса.

Формат команды для запуска скрипта следующий:

 # dsctl status <service_name>

где
<service_name>
– имя сервиса, состояние которого требуется показать.

В результате выполнения скрипта на экран выводится следующая информация:

```
/usr/lib/systemd/system/dozor_smap-tikaserver.service: up (pid 31346) 12 seconds
```

Данные статуса выводятся только для включённых процессов. Если процесс не включён, то никакой информации о его статусе не выводится.

Для вывода информации о всех запущенных сервисах следует запустить скрипт **dsctl** без ключей. Формат команды для запуска скрипта:

 # dsctl status

Пример вывода в результате выполнения скрипта:

```
/usr/lib/systemd/system/dozor_abook-daemon.service:..... up (pid 27299) 1288 seconds
/usr/lib/systemd/system/dozor_action-server.service:..... up (pid 27302) 1288 seconds
/usr/lib/systemd/system/dozor_action-server-database.service:. up (pid 27300) 1288 seconds
/usr/lib/systemd/system/dozor_agent-control-ng.service:..... up (pid 27306) 1288 seconds
/usr/lib/systemd/system/dozor_agent-media-server.service:..... up (pid 27307) 1288 seconds
/usr/lib/systemd/system/dozor_agent-server.service:..... up (pid 27314) 1288 seconds
/usr/lib/systemd/system/dozor_archive-server.service:..... up (pid 27317) 1288 seconds
/usr/lib/systemd/system/dozor_clickhouse.service:..... up (pid 27321) 1288 seconds
/usr/lib/systemd/system/dozor_database.service:..... up (pid 27329) 1288 seconds
/usr/lib/systemd/system/dozor_ds-bus-rc.service:..... up (pid 27331) 1288 seconds
/usr/lib/systemd/system/dozor_grafana.service:..... up (pid 27336) 1288 seconds
/usr/lib/systemd/system/dozor_incident-daemon.service:..... up (pid 27341) 1288 seconds
/usr/lib/systemd/system/dozor_indexer-ng.service:..... up (pid 27342) 1288 seconds
/usr/lib/systemd/system/dozor_license-server.service:..... up (pid 27344) 1288 seconds
/usr/lib/systemd/system/dozor_monitor-agent.service:..... up (pid 27348) 1288 seconds
/usr/lib/systemd/system/dozor_monitor-ng.service:..... up (pid 27349) 1288 seconds
```

```
/usr/lib/systemd/system/dozor_monitor-server.service:..... up (pid 27352) 1288 seconds
/usr/lib/systemd/system/dozor_report-server.service:..... up (pid 27354) 1288 seconds
/usr/lib/systemd/system/dozor_sender.service:..... up (pid 27355) 1288 seconds
/usr/lib/systemd/system/dozor_smap-difi.service:..... up (pid 27357) 1288 seconds
/usr/lib/systemd/system/dozor_smap-idid.service:..... up (pid 27363) 1288 seconds
/usr/lib/systemd/system/dozor_smap-redis.service:..... up (pid 27365) 1288 seconds
/usr/lib/systemd/system/dozor_smap-request-handler.service:... up (pid 27367) 1288 seconds
/usr/lib/systemd/system/dozor_smap-tikaserver.service:..... up (pid 27370) 1287 seconds
/usr/lib/systemd/system/dozor_software-center.service:..... up (pid 27372) 1287 seconds
/usr/lib/systemd/system/dozor_stt-setver.service:..... up (pid 27389) 1287 seconds
/usr/lib/systemd/system/dozor_uba-server.service:..... up (pid 30622) 1178 seconds
/usr/lib/systemd/system/dozor_webserver.service:..... up (pid 27375) 1287 seconds
```

6.5. Просмотр информации о настроенных соединениях с БД

Системный администратор имеет возможность просматривать информацию о настроенных соединениях с БД в виде, удобном для использования в sh-скриптах. Для этого используется скрипт **db-conn.py**.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд **shell**, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат команды для запуска скрипта:

$ db-conn.py [ключ]

Доступны следующие ключи:

- **-c**, **--subclusters** – использовать БД всех подкластеров.
- **-a**, **--all** – вывести на экран всю информацию о всех настроенных соединениях.
- **-l**, **--list** – вывести на экран только список имён всех соединений.
- **-s**, **--list-ids** – вывести на экран только список идентификаторов соединений.
- **-A**, **--active** – вывести на экран информацию об активных соединениях с БД архива.
- **-n <name>**, **--name <name>** – вывести на экран информацию о соединении с указанным именем.
- **-i <id>**, **--id <id>** – вывести на экран информацию о соединении с указанным идентификатором.
- **-v**, **--verbose** – вывести сообщения о действиях, выполняемых скриптом.
- **-d**, **--debug** – включить отладочное журналирование.

6.6. Просмотр информации о глобальных настройках системы и локальных настройках узла

Чтобы просмотреть информацию о глобальных настройках системы и локальных настройках узла, можно воспользоваться скриптом **get-config.py**.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд **shell**, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат команды для запуска скрипта **get-config.py**:

$ get-config.py [ключ]

Доступны следующие ключи:

- **-r <выражение>**, **--regexp <выражение>** – вывести глобальные настройки системы по значению подстроки в пути к каталогу.
- **-n <ИД>**, **--node <ИД>** – отобразить локальные настройки для узла с **<ИД>**, где <**ИД**> задается в формате **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**. Пример: **151ba831-80ed-4734-ac38-0b4e0557a47c**.
- **-p**, **--hide-passwords** – вывести на экран символы «*» вместо пароля.
- **-l**, **--localized** – показать названия параметров конфигурации, переведенные на русский язык.
- **-v**, **--verbose** – вывести на экран сообщения о действиях, выполняемых скриптом.
- **-d**, **--debug** – включить отладочное журналирование.
- **-h**, **--help** – вывести на экран справочную информации об использовании скрипта.

Необходимо вывести все локальные настройки (формат команды для запуска скрипта **$ get-config.py -n <ИД узла>**). Тогда вывод команды имеет вид:

```
/agent-server/agent-server-settings/listen-addr/ip[0]: 0
/agent-server/agent-server-settings/listen-addr/ip[1]: 0
/agent-server/agent-server-settings/listen-addr/ip[2]: 0
/agent-server/agent-server-settings/listen-addr/ip[3]: 0
/agent-server/agent-server-settings/status-write-interval: 30
/agent-server/agent-server-settings/listen-port: 4444
/agent-server/agent-server-settings/spool-dir: "/data/spool/dozor/agent-server"
/agent-server/agent-server-settings/mediaserver-conns: []
/agent-server/agent-server-settings/update-interval: 30
/agent-server/agent-server-settings/mailfilter-conns/auto: []
/agent-server/agent-server-settings/keylogger/timeout: 300
/agent-server/agent-server-settings/keylogger/size-limit: 10
/agent-server/agent-server-settings/status-send-interval: 40
/agent-server/agent-server-settings/control-server/host: "localhost"
/agent-server/agent-server-settings/control-server/port: 3005
/agent-server/agent-server-settings/log-dir: "/opt/dozor/var/log/agents"
```

```
/agent-server/agent-server-settings/max-memory: 512
/agent-server/agent-server-settings/max-threads: 30
```

6.7. Ротация событий и инцидентов ИБ

При переполнении хранилища событий и инцидентов ИБ, объем которого ограничен, происходит ротация – старые события и инциденты удаляются или архивируются.

Настройка параметров ротации событий и инцидентов выполняется в секции **Сервис хранения и индексации событий и инцидентов** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > События и инциденты**). Перед настройкой параметров ротации событий и инцидентов необходимо задать базу данных для их хранения (см. документ *Руководство по установке и настройке*).

Ротация событий и инцидентов выполняется с помощью скрипта **incident-tool**. Скрипт запускается от имени пользователя **dozor** командой следующего вида:

$ /opt/dozor/bin/incident-tool {параметр} [ключ]

Перед выполнением команды необходимо запустить интерпретатор команд shell:

$ /opt/dozor/bin/shell

Доступны следующие параметры:

- **list** – запросить список секций и их текущее состояние.
- **archive** – архивировать секции;
- **restore** – восстановить секции;
- **delete** – удалить секции;
- **import** – импортировать секции.

Доступны следующие ключи:

- **-h, --help** – справка по использованию.
- **-p YYYY-WW, --partition YYYY-WW** – указать секцию.
- **-f YYYY-WW, --from YYYY-WW** – задать нижнюю границу диапазона секций (включая).
- **-u YYYY-WW, --until YYYY-WW** – задать верхнюю границу диапазона секций (не включая).
- **-a, --all** – указать все секции.
- **--host HOST** – задать имя узла с сервисом **incident-daemon**.
- **--port PORT** – задать порт, на котором сервис **incident-daemon** ожидает соединения.
- **--protocol PROTOCOL** – задать протокол **incident-deamon**.

- **-d DIR, --dir DIR** – указать каталог на файловой системе для архивирования/восстановления.
- **-s SUBCLUSTER, --subcluster SUBCLUSTER** – указать связанный с событиями и инцидентами подкластер. **00000000-0000-0000-0000-000000000000** – указывается для master-узла.

Примеры использования скрипта:

1. Запросить список секций:

   $ /opt/dozor/bin/incident-tool list

   Пример вывода команды:

```
+-----------+----------+-----------+--------+----------+-----------------+
| Partition | Writable | Indexable | Locked | Archived | ArchiveLocation |
+-----------+----------+-----------+--------+----------+-----------------+
| 2023-11   | True     | True      | False  | False    |                 |
| 2023-18   | True     | True      | False  | False    |                 |
| 2023-19   | True     | True      | False  | False    |                 |
+-----------+----------+-----------+--------+----------+-----------------+
```

2. Удалить все секции, используя заданные параметры подключения к **incident-daemon**:

   $ /opt/dozor/bin/incident-tool delete -a --host host12.company.com --port 2268 --protocol http

   Пример вывода команды:

```
Following partitions were deleted: 2023-11, 2023-18, 2023-19
```

3. Удалить секции, начиная с 2023-15:

   $ /opt/dozor/bin/incident-tool delete -f 2023-15

   Пример вывода команды:

```
Following partitions were deleted: 2023-18, 2023-19
```

4. Архивировать секцию 2023-09 в указанный каталог:

   $ /opt/dozor/bin/incident-tool archive -p 2023-09 -d /data/archive/incident-storage

   Пример вывода команды:

```
Following partitions will be archived: 2023-09
```

5. Архивировать секции в диапазоне (2023-09, 2023-12):

   $ /opt/dozor/bin/incident-tool archive -f 2023-09 -u 2023-12

   Пример вывода команды:

```
Following partitions will be archived: 2023-09, 2023-10, 2023-11, 2023-12
```

6. Восстановить все секции по 2023-09 (не включая):

   $ /opt/dozor/bin/incident-tool restore -u 2023-09

   Пример вывода команды:

   ```
   Following partitions will be restored: 2023-07, 2023-08
   ```

7. Восстановить все секции из указанного каталога:

   $ /opt/dozor/bin/incident-tool restore -a -d /data/archive/incidents

   Пример вывода команды:

   ```
   Following partitions will be restored: 2023-07, 2023-08, 2023-09, 2023-10, 2023-11, 2023-12
   ```

8. Импортировать секцию 2023-09 в БД событий и инцидентов master-узла:

   $ /opt/dozor/bin/incident-tool import -p 2023-09 -s 00000000-0000-0000-0000-000000000000

   Пример вывода команды:

   ```
   Following partitions will be imported: 2023-09
   ```

9. Импортировать секцию 2023-09 в БД событий и инцидентов подкластера с ИД **78540f12-08ee-4fca-b942-1fea61dbed78**:

   $ /opt/dozor/bin/incident-tool import -p 2023-09 -s 78540f12-08ee-4fca-b942-1fea61dbed78

   Пример вывода команды:

   ```
   Following partitions will be imported: 2023-09
   ```

6.8. Журналирование событий и инцидентов ИБ в syslog

При наличии в организации SIEM-системы, её можно использовать для получения и накопления данных о событиях и инцидентах ИБ, создаваемых при работе KEO DLP. Для этого следует настроить журналирование событий и инцидентов ИБ в системный журнал. При журналировании можно использовать простой текстовый формат и формат CEF, а также применять фильтр по критичности инцидентов.

Для настройки журналирования событий и инцидентов необходимо выполнить следующие шаги:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > События и инциденты**.

2. В секции **Сервис хранения и индексации событий и инцидентов** установить переключатель **Журналировать регистрацию событий** в положение **Включено**.

3. При необходимости отслеживания изменения статуса событий и инцидентов установить флажок **Журналировать изменение статуса событий и инцидентов**. В этом случае при любом изменении полей **status** или **state** в БД событий и инцидентов будет выполняться журналирование этих событий.

4. Установить флажок **Журналировать в формате CEF**.

5. Для параметра **Уровень критичности событий и инцидентов** выбрать необходимый уровень критичности событий и инцидентов.

6. Нажать **Сохранить**, **Применить**.

7. На узлах с ролями **Сервер управления** и **Сервер управления событиями и инцидентами подкластера** настроить отправку журнала сервиса **incident-daemon** на удаленный сервер с использованием очереди.

   Для этого создать файл **/etc/syslog-ng/conf.d/incident-events.conf** с содержимым следующего вида:

```
@define allow-config-dups 1
@define REMOTE_SERVER "c7-syslog.organisation.com"
@define REMOTE_PORT 10514
filter f_dozor_event {program("events")};
destination d_udp { syslog("`REMOTE_SERVER`" transport("udp") port(`REMOTE_PORT`)); };
destination d_dozor_event {
file("/var/log/dozor/incident-event.log"
create-dirs(yes)
dir-group("dozor")
dir-owner("dozor")
dir-perm(0755)
group("dozor")
owner("dozor")
perm(0640)
);
};
log {
source(s_src);
filter(f_dozor_event);
destination(d_udp); };
log {
source(s_src);
filter(f_dozor_event);
destination(d_dozor_event);
flags(final,flow-control); };
```

   Значения **c7-syslog.organisation.com** и 10514 следует заменить на актуальные.

8. Проверить синтаксис конфигурационного файла, выполнив команду:

   # sudo syslog-ng -s

   Если обнаружены ошибки синтаксиса – исправить их и повторить команду.

9. Перезапустить сервис **syslog-ng**, выполнив команду:

 # sudo systemctl restart syslog-ng

10. Проверить статус службы **syslog-ng**, выполнив команду:

 # sudo systemctl status syslog-ng

Об успехе будет свидетельствовать вывод следующего вида:

```
root@a173-d79:~# systemctl status syslog-ng
● syslog-ng.service - System Logger Daemon
Loaded: loaded (/lib/systemd/system/syslog-ng.service; enabled; vendor preset: enabled)
Drop-In: /etc/systemd/system/syslog-ng.service.d
└─override.conf
Active: active (running) since Sun 2023-01-22 00:00:04 MSK; 1 day 11h ago
Docs: man:syslog-ng(8)
Main PID: 26197 (syslog-ng)
Tasks: 10 (limit: 4915)
Memory: 17.9M
CGroup: /system.slice/syslog-ng.service
└─26197 /usr/sbin/syslog-ng -F --no-caps
янв 22 00:00:04 a173-d79 systemd[1]: Starting System Logger Daemon...
янв 22 00:00:04 a173-d79 systemd[1]: Started System Logger Daemon.
янв 23 00:00:02 a173-d79 systemd[1]: Reloading System Logger Daemon.
янв 23 00:00:02 a173-d79 systemd[1]: Reloaded System Logger Daemon.
```

11. Для просмотра актуальных настроек конфигурации выполнить команду:

syslog-ng-ctl config --preprocessed

12. Для возможности получать статистику от внутренних счетчиков **syslog-ng** следует создать файл **/etc/syslog-ng/conf.d/stat.conf** с содержимым:

```
options {
  stats-freq(60);
  stats-level(0);
};

filter f_syslog-ng { "${PROGRAM}" eq "syslog-ng"; };

destination d_syslog-ng { file("/var/log/syslog-ng.log"); };

log {
  source(s_src);
  filter(f_syslog-ng);
  destination(d_syslog-ng);
};
```

В данном примере настроена запись статистики каждые 60 секунд (**stats-freq**) с записью сообщений от **syslog-ng** в файл **/var/log/syslog-ng.log**.

Также статистику можно просматривать с помощью команды следующего вида:

 # syslog-ng-ctl query get dst.syslog.d_*

Для сброса статистики следует выполнить команду:

 # syslog-ng-ctl stats --reset

При журналировании событий и инцидентов используется фиксированный набор полей с фиксированным порядком. Если поле пустое, в него записывается значение **null** (никакие поля не пропускаются в любом случае).

Табл. 6.2. Описание полей журнальных записей для событий и инцидентов ИБ

№	Имя поля	Описание	Пример значения
1	id	Уникальный идентификатор события в KEO DLP	**"c80f2520-797e-11ee-b34e-2350458598f3"**
2	eventid	Идентификатор события в KEO DLP	**"EVENT-2022-27-1"**
3	messageid	ID сообщения в KEO DLP, которое породило событие	**"2410f894-fdc0-11ec-a244-fa163e364e19"**
4	regdate	Дата регистрации события	**"2022-07-07T09:43:54.629+03:00"**
5	state	Описание статуса события: открыто, ложное срабатывание, закрыто	**"open"**
6	status	Описание типа события: событие или инцидент	**"event"** **"incident"**
7	severity	Критичность в текстовом представлении (критичный, высокий, средний, низкий, информация)	**"critical"** **"intermediate"**
8	severityscore	Критичность в численном представлении от 1 до 5	**5**
9	title	Заголовок события	**"Привет, смотри внутри файл"**
10	originaldate	Дата составления сообщения	**"2022-07-07T06:43:42.000+03:00"**
11	category	Тип угрозы	**"Конфиденциальные данные"**
12	subcategory	Подтип угрозы	**"Персональные данные"**
13	origin	Имя контроллера домена, на котором было зафиксировано событие	**"dozor76"**
14	rulesetname	Набор правил, по которому произошло срабатывание	**"1. Головной набор правил"**
15	condsetname	Набор условий, по которым произошло срабатывание	**"почта"**
16	infobjects	Инфообъекты	**"СНИЛС"**
17	closedby	Кем был закрыт инцидент	**"superadmin"**
18	statechangedate	Дата изменения типа события	**"2022-06-27T13:09:50.292+03:00"**
19	statechangeby	Кем был изменен тип события	**"superadmin"**
20	statuschangedate	Дата изменения статуса события	**"2022-06-27T13:09:55.576+03:00"**
21	statuschangeby	Кем был изменен статус события	**"superadmin"**
22	sourceaddress	Почтовый адрес отправителя либо его имя пользователя и hostname, IP-адрес его машины с агентом	**"email:user@test.com"**
23	commchannel	Канал перехвата (внутренняя, входящая, исходящая почта, мессенджер, USB, печать на принтере и т. п.)	**"email-out"**
24	url	Прямая ссылка на событие или инцидент	
25	attachments	Имена прикрепленных файлов	**"inserted_object_fdf.docx"**
26	preview	Preview сообщения со срабатываниями политик. Срабатывания выделены тегами <mark></mark>	**"ООО Вектор\n\n\t\n,\t\n,\t\n,\n\tИнфосистемы Джет\n, \t\n,\n\t\n,\t\n,\t\n,\n\tТехнико-<mark>коммерческое предложение</mark>\n на Создание системы управления данными\nдля\n,\n\tОАО «Специали-**

№	Имя поля	Описание	Пример значения
			зированный депозитарий «ИНФИ-УМ»\n,\n\t\n...\n\n... информационных систем, поставляет ключевые компоненты информационной инфраструктуры, предоставляет <mark>услуги</mark> по сервисной поддержке информационных систем своих Заказчиков, а также оказывает комплекс консультационных <mark>услуг</mark> в области информационных технологий и обеспечения информационной безопасности."
27	destinationaddress	Почтовые адреса получателей (первые 15 адресов)	**"email:user@test.com"**
28	comment	Комментарий, который пишет пользователь KEO DLP при закрытии инцидента. В БД событий и инцидентов хранится в поле **comment**. Максимально возможная длина комментария 300 символов	**"comment": "Закрываю инцидент по причине ..."**
29	labels	Все пометки на сообщении - "системные", "пользовательские" и "бизнес"	

Описание синтаксиса записей в формате CEF:

1. Дата, время, имя сервера KEO DLP, имя БД событий и инцидентов.
2. Версия CEF, наименование производителя, наименование продукта, версия продукта.
3. Тип события (зарегистрировано – **create-event**, изменено – **update-event**).
4. ID события.
5. Уровень критичности события от DLP-системы для SIEM-системы (от 1 до 10).
6. Расширение (все поля по порядку из таблицы выше).

Пример записи в формате CEF:

Dec 30 14:21:59 vm1020164101 events: CEF:0|Organisation|KEO DLP|7.9.0|update-event|EVENT-2022-52-160|4|eventid="EVENT-2022-52-160" messageid="6d2f00fa-87b5-11ed-956f-fa163ebb37f6" regdate="2022-12-30T11:45:20.642+03:00" state="open" status="incident" severity="intermediate" severityscore=3 title="foreing_8" originaldate="2022-02-24T07:35:17.000+03:00" category="Подозрительная активность" subcategory="Намеренное нарушение" origin="vm1020164101" rulesetname=null condsetname=null infobjects=null closedby=null statechangedate="2022-12-30T14:21:59.526+03:00" statechangeby="superadmin" statuschangedate=null statuschangeby=null sourceaddress="login:llcorganisation;hostname:macbook-pro.local;ip:192.168.0.102" commchannel="webmail" attachments=null url="https://vm1020164101/#!securityevents/eventszone/eyJ0eXBlIjoiZXZlbnRzIiwicGFyYW1zIjp7Im9wZW5DYXJkSWQiOiI0YWY2ODYyMC04ODFlLTExZWQtYjFiYy05ZDkzYjgwNWIzMmYifSwgIm9wZW5DYXJkRnVsbCI6dHJ1ZX0" preview=null destinationaddress="email:user5@organisation.local;email:user3@organisation.local;email:user1@organisation.local;email:user15@organisation.local;email:user7@organisation.local;email:user6@organisation.local;email:user13@organisation.local;email:user16@organisation.local;email:user14@organisation.local;email:user2@organisation.local;email:user11@organisation.local;email:user12@organisation.local;email:user8@organisation.local;email:user4@organisation.local;email:user9@organisation.local..." comment="Тест комментария - не инцидент" labels="Получено;Имя узла;Канал коммуни-

кации;Приложение;Обнаружен информационный объект;Зарегистрировано событие ИБ;Помещено в архив;Зарегистрировано событие ИБ;Зарегистрировано событие ИБ;Зарегистрировано событие ИБ;Зарегистрировано событие ИБ;Зарегистрировано событие ИБ;Torrent-файлы;URL копирования файла;URL обнаружения файла;URL перемещения файла;Азартные игры;Алкоголь;Анонимайзеры;Антивирус;Архив с сохраненным паролем;Бесплатная иностранная почта;Бесплатная российская почта;Блатной жаргон;Буфер обмена;Бухгалтерия;Важное сообщение;Вложение без текста;Вложение без темы;Внешнее входящее сообщение;Внешнее исходящее сообщение;Внешнее сообщение;Внутреннее сообщение;Выполнена команда;Графический шаблон;Данные доступа;Данные кредитных карт;Долги и кредиты;Заблокировано;Заблокировано (ICAP);Заболевания;Закупка;Записано в журнал;Запрещенный адрес"

Описание синтаксиса записей в простом текстовом формате:

1. Дата, время, имя сервера KEO DLP, имя БД событий и инцидентов.

2. Все поля по порядку из таблицы выше.

Пример записи в простом текстовом формате:

Jan 12 12:52:28 vm1020164101 events: eventid="EVENT-2023-02-62" messageid="e205acf0-925d-11ed-bd95-8d2d58491741" regdate="2023-01-12T12:52:27.956+03:00" state="open" status="incident" severity="intermediate" severityscore=3 title="smb://10.201.66.113/crawler/Текстовые_документы/RCO_test_data/load/bank/3.pdf" originaldate="2022-11-30T10:43:20.000+03:00" category="Конфиденциальные данные" subcategory="Персональные данные" origin="vm1020164101" rulesetname=null condsetname=null infobjects=null closedby=null statechangedate=null statechangeby=null statuschangedate=null statuschangeby=null sourceaddress="ip:10.201.66.113;sid:s-1-5-21-1817128565-1441266754-716483134-1000" commchannel="storage" attachments="3.pdf" url="https://vm1020164101/#!securityevents/eventszone/eyJ0eXBlIjoiZXZlbnRzIiwicGFyYW1zIjp7Im9wZW5DYXJkSWQiOiJkMmNjOWY0MC05MjVlLTExZWQtOGM5Ny05ZDkzYjgwNWIzMmYifSwgIm9wZW5DYXJ0RnVsbCI6dHJ1ZX0" preview=null destinationaddress=null comment=null labels="Получено;Имя узла;Канал коммуникации;URL обнаружения файла;Превышен допустимый размер файла;Помещено в архив"

6.9. Проверка пользовательских данных в базе LDAP

В KEO DLP реализована поддержка протокола **LDAP over TLS**, то есть имеется возможность хранить данные на LDAP-сервере с их передачей по протоколу TLS. Можно объединять данные пользователей в группы, централизованно хранить информацию о почтовых адресах и аутентификационные данные. Подробнее о протоколе LDAP см. соответствующую документацию.

Проверка почтового адреса в базе данных LDAP выполняется по следующему принципу:

1. Для проверяемого почтового адреса выполняется поиск LDAP-сервера, в списке обслуживаемых доменов которого присутствует проверяемый почтовый адрес.

2. Проверяется наличие почтового адреса в домене.

3. Если не удается найти LDAP-сервер с указанным доменом, то поиск происходит на LDAP-сервере по умолчанию, для которого не указано никаких доменов.

Для получения списка имеющихся групп на LDAP-сервере используется скрипт **ldap-tool**.

Перед его использованием необходимо переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат команды для запуска скрипта (выполняется от имени пользователя **dozor**):

$ ldap-tool [<ключи> ...]

Доступны следующие ключи:

- **-l** – задать один или несколько (через пробел) URI для LDAP.
- **-b** – выбрать указанный base DN.
- **-B** – выбрать указанный bind DN.
- **-P** – задать указанный пароль для выбранного bind DN.
- **-f** – задать указанный фильтр LDAP.
- **-s** – задать указанный диапазон поиска (принимает значения **base**, **onelevel**, **subtree**).
- **-a** – отобразить только указанные атрибуты (перечисляются через пробел).
- **-e** – проверить, существует ли пользователь с указанным email-адресом в настроенных серверах LDAP.
- **-G** – проверить, состоит ли пользователь, заданный через ключ **-e**, в указанной группе в настроенных серверах LDAP.
- **-g** – отобразить список доступных групп LDAP для заданного домена.
- **-L** – отобразить список всех доступных групп LDAP со всех настроенных серверов.
- **-d** – включить отладочное журналирование.
- **-h** – отобразить справочную информацию.

6.10. Управление конфигурацией кластера KEO DLP

Для управления конфигурацией кластера KEO DLP предназначен скрипт **config**. Формат команды для запуска скрипта **config** выглядит следующим образом:

 # config <действие>

где **<действие>** – действие, которое требуется совершить

Внимание!

Данный скрипт следует запускать на master-узле KEO DLP.

Используются следующие действия:

- **cluster** – управление структурой кластера (см. раздел 6.10.1);
- **map** – вывод всех соединений между узлами кластера (см. раздел 6.10.2)
- **values** – управление конфигурацией сервисов (см. раздел 6.10.3);
- **upgrade** – обновление конфигурации (см. раздел 6.10.4);
- **init** – создание начальной конфигурации (см. раздел 6.10.5).

6.10.1. Управление структурой кластера

Для управления структурой кластера предназначен скрипт **config cluster**.

Для работы со скриптом необходимо запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта выглядит следующим образом:

 # config cluster [общий ключ] <действие> [ключ действия]

где **[общий ключ]** – ключ, используемый при выполнении любого действия, **<действие>** – действие, которое требуется совершить, а **[ключ действия]** – ключ, который используются для того или иного действия.

Используются следующие общие ключи:

- **-R <DIR>**, **--roles-dir <DIR>** – каталог, содержащий файлы с описанием ролей узлов.
- **-C <FILE>**, **--cluster-file <FILE>** – файл, содержащий описание кластера.

Используются следующие действия:

- **print** – вывод текущего состояния кластера. Работает со следующим ключом:
  - **-f <FORMAT>**, **--format <FORMAT>** – вывести состояние кластера в формате **<FORMAT>**. Принимает значения **text**, **json**, **edn**. По умолчанию используется **text**.
- **add-node** – добавление узла кластера. Работает со следующими ключами:
  - **-i <ID>**, **--id <ID>** – идентификатор узла (UUID).
  - **-n <NAME>**, **--name <NAME>** – имя узла.
  - **-h <HOSTNAME>**, **--hostname <HOSTNAME>** – значение **hostname** узла.
  - **-S <SUBCLUSTER>**, **--subcluster <SUBCLUSTER>** – идентификатор узла или имя подкластера.
- **update-node** – модификация узла кластера. Работает с ключами действия **add-node**.
- **delete-node** – удаление узла кластера. Работает с ключами действия **add-node**.

- **add-roles** – добавление ролей узла. Работает со следующими ключами:
  - **-N <NODE>**, **--node <NODE>** – идентификатор (UUID) или имя узла.
  - **-r <ROLES>**, **--roles <ROLES>** – список ролей через запятую.
- **set-roles** – установка ролей узла. Работает с ключами действия **add-roles**.
- **delete-roles** – удаление ролей узла. Работает с ключами действия **add-roles**.
- **enable-services** – включение сервисов. Работает со следующими ключами:
  - **-N <NODE>**, **--node <NODE>** – идентификатор (UUID) или имя узла.
  - **-s <SERVICES>**, **--services <SERVICES>** – список сервисов через запятую.
- **disable-services** – отключение сервисов. Работает с ключами действия **add-roles**.
- **add-subcluster** – добавление подкластера. Работает со следующими ключами:
  - **-i <ID>**, **--id <ID>** – идентификатор подкластера (UUID).
  - **-n <NAME>**, **--name <NAME>** – имя подкластера.
- **update-subcluster** – модификация подкластера. Работает с ключами действия **add-subcluster**.
- **delete-subcluster** – удаление подкластера. Работает с ключами действия **add-subcluster**.

Пример вывода команды **config cluster print**:

```
Common nodes:
  Node: main
  ID: 0f676af8-e25d-481e-a193-2aaecb2a2eed
  Hostname: t29.isim.local
  Roles: analyzer, master, action-server, fsng-storage, incident-indexer, smtp-filter, text-indexer
  Services:
    smap-difi
    smap-idid
    smap-tikaserver
    ds-bus-rc
    monitor-ng
    smap-diag
    smap-settings
    sender
    internal-connectors
    smap-redis
    database
    agent-control-ng
    software-center
    smap-agents
    smap-address-book
    incident-daemon
    archive-server
    report-server
    abook-daemon
```

```
    smap-activemq
    action-server
    agent-media-server
    license-server
    smap-request-handler
    webserver
    skvt-cassandra
    filestorage-ng

    smap-smtp-gw
    archiver
    mailfilter
    indexer-ng
  Node: t30
  ID: 78540f12-08ee-4fca-b942-1fea61dbed78
  Hostname: t30.isim.local
  Roles: smtp-filter
  Services:
    smap-smtp-gw
    smap-tikaserver
    smap-address-book
    archiver
    mailfilter
    ds-bus-rc
    monitor-ng
    smap-diag
    smap-settings
    sender
    internal-connectors
    smap-redis

    skvt-cassandra
  Node: t31
  ID: 8feca55f-8530-4f9b-b1d8-cbc4779893f3
  Hostname: t31.isim.local
  Roles: smtp-filter
  Services:
    smap-smtp-gw
    smap-tikaserver
    smap-address-book
    archiver
    mailfilter
    ds-bus-rc
    monitor-ng
    smap-diag
    smap-settings
    sender
    internal-connectors
    smap-redis

    skvt-cassandra
Subclusters:
```

В данном примере видно, что в кластер входит один master-узел **t29.isim.local** и 2 slave-узла **t30.isim.local** и **t31.isim.local**.

Пример: предполагается, что роль **Анализ поведения (UBA)** назначена на master-узел. Чтобы отключить сервис **uba-server**, следует выполнить действия:

1. Подключиться по протоколу SSH к master-узлу.
2. Запустить интерпретатор команд shell, выполнив команду:

   # /opt/dozor/bin/shell
3. Остановить сервис **uba-server** на узле, выполнив команду:

   # dsctl stop uba-server
4. Получить UUID узла кластера KEO DLP, на которой требуется отключить сервис **uba-server** (в текущем примере – master-узел). Для этого выполнить команду:

   # node_name

   В результате выполнения команды будет выведен UUID узла, например:

   ```
   0f676af8-e25d-481e-a193-2aaecb2a2eed
   ```

   Необходимо запомнить UUID, т.к. он будет использоваться далее.
5. Отключить сервис **uba-server**, выполнив команду:

   **# config cluster disable-services -s uba-server -N **
   0f676af8-e25d-481e-a193-2aaecb2a2eed
6. Перейти в git-репозиторий, выполнив команду:

   # cd /data/repos/dozor/config-base.git
7. Переключиться на пользователя dozor, выполнив команду:

   # su dozor
8. Добавить изменения в репозиторий. Для этого выполнить команду:

   $ git add .
9. Сохранить изменения, выполнив команду:

   $ git commit -m "disable uba-server"
10. Завершить сессию пользователя dozor, выполнив команду:

    $ exit
11. Применить конфигурацию, выполнив команду:

    # accept-settings

В результате выполнения действий, описанных выше, сервис **uba-server** пропадет из списка сервисов KEO DLP.

6.10.2. Вывод всех соединений между узлами кластера

Для просмотра карты соединений между узлами кластера предназначен скрипт **config map**. Можно просмотреть информацию только по номерам портов, указанных в настройках конфигурации KEO DLP.

Для работы со скриптом необходимо запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта выглядит следующим образом:

 # config map [ключ]

Используются следующие ключи:

- **-C <FILE>**, **--cluster-file <FILE>** – файл, содержащий описание кластера;
- **-T <DIR>**, **--types-dir <DIR>** – каталог, содержащий описание типов параметров конфигурации. По умолчанию файлы описания типов параметров конфигурации расположены в каталоге **/opt/dozor/config/default/types.d**.
- **-V <FILE>**, **--values-file <FILE>** – файл, содержащий описание значений;
- **-f <FORMAT>**, **--format <FORMAT>** – формат выходного файла. Принимает значения: **text**, **json**, **edn**.
- **--hide-loopback** – скрыть соединения с узлом, имеющим IP-адрес **127.0.0.1**.
- **--hide-local** – скрыть соединения с узлами аналогичного подкластера.
- **-h**, **--help** – вывести справку по работе со скриптом.

Пример вывода скрипта:

```
ds-mode@doc001 /opt/dozor # config map
Common nodes:
  Node: main
  ID: 0f676af8-e25d-481e-a193-2aaecb2a2eed
  Hostname: doc001.isim.local
  Roles: master, incident-indexer, text-indexer, uba-server
  Connections:
    localhost:5444
    doc001.isim.local:9200
    doc001.isim.local:10050
    127.0.0.1:25
    doc001.isim.local:9201
    localhost:5434
    doc001.isim.local:8123
    doc001.isim.local:16379
    doc001.isim.local:3004
    doc001.isim.local:3006
    doc001.isim.local:9001
    doc001.isim.local:3000
    doc001.isim.local:2269
    doc001.isim.local:61616
```

```
    doc001.isim.local:2272
    localhost:5440
    doc001.isim.local:443
    doc001.isim.local:3001
    doc001.isim.local:7837
    doc001.isim.local:9301
    doc001.isim.local:9000
    doc001.isim.local:3003
    doc001.isim.local:5555
    doc004.isim.local:5555
    doc003.isim.local:5555
    doc005.isim.local:5555
    doc001.isim.local:3030
    doc001.isim.local:3900
    doc001.isim.local:9401
    127.0.0.1:1025
    doc003.isim.local:3004
    doc005.isim.local:3004
Subcluster: Датацентр_Тверь
ID: ab1762e5-d0df-4d3f-99d0-933dca68877f
Nodes:
  Node: doc004
  ID: f50d66c9-4d15-4e69-941e-73593a3ea929
  Hostname: doc004.isim.local
  Roles: smtp-filter
  Connections:
    doc001.isim.local:9301
    doc004.isim.local:9998
    doc003.isim.local:9998
    doc004.isim.local:16379
    doc001.isim.local:443
    doc003.isim.local:3004
    doc001.isim.local:2269
    doc001.isim.local:10050
    127.0.0.1:25
    doc001.isim.local:2272
    doc001.isim.local:3000
    doc001.isim.local:3003
  Node: doc003
  ID: a60158b5-9007-48e0-bf32-296547802f60
  Hostname: doc003.isim.local
  Roles: smtp-filter, license-server
  Connections:
    doc001.isim.local:9301
    doc003.isim.local:9998
    doc004.isim.local:9998
    doc003.isim.local:16379
    doc001.isim.local:443
    doc003.isim.local:3004
    doc001.isim.local:2269
    doc001.isim.local:10050
    127.0.0.1:25
    doc001.isim.local:2272
    doc001.isim.local:3000
    doc001.isim.local:3003
    doc004.isim.local:16379
Subcluster: Тульский подкластер
ID: de2b4d19-2011-40a3-995a-76712f4c8273
```

```
Nodes:
  Node: doc005
  ID: 0db25b78-c4b3-42d2-b459-0d9ae617348e
  Hostname: doc005.isim.local
  Roles: smtp-filter, license-server
  Connections:
    doc001.isim.local:9301
    doc005.isim.local:9998
    doc005.isim.local:16379
    doc001.isim.local:443
    doc005.isim.local:3004
    doc001.isim.local:2269
    doc001.isim.local:10050
    127.0.0.1:25
    doc001.isim.local:2272
    doc001.isim.local:3000
    doc001.isim.local:3003
```

6.10.3. Управление конфигурацией сервисов

Для управления конфигурацией сервисов предназначен скрипт **config values**.

Для работы со скриптом необходимо запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта выглядит следующим образом:

 # config values [общий ключ] <действие> [ключ действия]

где **[общий ключ]** – ключ, используемый при выполнении любого действия, **<действие>** – действие, которое требуется совершить, а **[ключ действия]** – ключ, который используются для того или иного действия.

Используются следующие общие ключи:

- **-C <FILE>**, **--cluster-file <FILE>** – указать файл **/data/repos/dozor/config-base.git/cluster.json**, содержащий описание кластера.
- **-T <DIR>**, **--types-dir <DIR>** – указать файл **/data/repos/dozor/config-base.git/types.d**, содержащий описание типов параметров конфигурации.
- **-V <FILE>**, **--values-file <FILE>** – указать файл **/data/repos/dozor/config-base.git/values.json**, содержащий значения значения параметров конфигурации.

Используются следующие действия:

- **get** – получение значений параметров конфигурации. Работает со следующими ключами:
  - **-N <NODE>**, **--node <NODE>** – вывести на экран имя или ID узла для получения локальных настроек (конфигурации узла).
  - **-l**, **--legacy** – вывести на экран пути и значения в старом формате.

- **-s <SERVICES>**, **--services <SERVICES>** – вывести на экран список сервисов (через запятую).
- **-r**, **--regexp <REGEXP>** – задать регулярное выражение, применяемое к пути, необходимое для выборки значений.

- **set** – установка значений параметров конфигурации. Работает со следующими ключами:
  - **-N <NODE>**, **--node <NODE>** – задать имя или ID узла для получения локальных настроек (конфигурации узла).
  - **-l**, **--legacy** – считать пути и значения в старом формате.
  - **-p <PATH>**, **--path <PATH>** – задать путь для значения (указывается в том виде, в котором выводит его выводит команда **get**).
  - **-v <VALUE>, --value <VALUE>**– задать значение.
  - **-d**, **--delete-list-item** – удалить элемента списка, заданного ключом **--path**.
  - **-f <FILE>**, **--file <FILE>** – прочитать пути и значения из файла.
  - **--stdin** – прочитать пути и значения с потока ввода ОС (stdin).
- **export** – экспорт значений параметров конфигурации. Работает со следующими ключами:
  - **-f <FILE>**, **--file <FILE>** – экспортировать в файл. Если ключ не указан, информация выводится в поток **stdout**.
  - **-n <NODE>**, **--nodes <NODE>** – задать имена или идентификаторы узлов для экспорта. Не используется вместе с ключом **-g** (**--global**).
  - **-g**, **--global** – экспортировать глобальную конфигурацию.
  - **-s <SERVICES>**, **--services <SERVICES>** – задать список сервисов, конфигурация которых будет экспортирована. Может использоваться совместно с ключами **-n** (**--nodes**) или **-g** (**--global**).
- **import** – импорт значений параметров конфигурации. Работает со следующими ключами:
  - **-f <FILE>**, **--file <FILE>** – импортировать в файл. Если ключ не указан, информация выводится в поток **stdout**.
  - **-n <NODE>**, **--nodes <NODE>** – задать имена или идентификаторы узлов для импорта. Не используется вместе с ключом **-g** (**--global**).
  - **-g**, **--global** – импортировать глобальную конфигурацию.
  - **-s <SERVICES>**, **--services <SERVICES>** – задать список сервисов, конфигурация которых будет импортирована. Может использоваться совместно с ключами **-n** (**--nodes**) или **-g** (**--global**).
- **add-local** – создание локальных настроек узла. Работает со следующими ключами:

- **-N <NODE>**, **--node <NODE>** – добавить локальные настройки для узла с именем **<NODE>**.
- **-s <SERVICE>**, **--services <SERVICE>** – добавить конфигурацию для сервиса **<SERVICE>**.
- **-t <TYPE>, --type <TYPE>** – тип параметров конфигурации. Файлы описания типов параметров конфигурации расположены в каталоге **/opt/dozor/config/default/types.d**.

- **delete-local** – удаление локальных настроек узла. Работает со следующими ключами:
  - **-N <NODE>**, **--node <NODE>** – удалить конфигурацию узла с именем **<NODE>**.
  - **-s <SERVICE>**, **--service <SERVICE>** – удалить конфигурацию для сервиса **<SERVICE>**.
  - **-t <TYPE>, --type <TYPE>** – тип параметров конфигурации. Файлы описания типов параметров конфигурации расположены в каталоге **/opt/dozor/config/default/types.d**.
- **list-local** – просмотр локальных настроек узла. Работает со следующими ключами:
  - **-N <NODE>**, **--node <NODE>** – просмотреть конфигурацию узла с именем **<NODE>**.
  - **-s <SERVICE>**, **--service <SERVICE>** – просмотреть конфигурацию для сервиса **<SERVICE>**.
  - **-t <TYPE>, --type <TYPE>** – тип параметров конфигурации. Файлы описания типов параметров конфигурации расположены в каталоге **/opt/dozor/config/default/types.d**.

Примеры:

Команда
 # config values get -s sender
выводит глобальную конфигурацию сервиса **sender**. Пример вывода команды:

```
/sender/relay-config/relay-settings[0]/id: 1
/sender/relay-config/relay-settings[0]/name: "default"
/sender/relay-config/relay-settings[0]/transport/smtp/connections[0]/proto: "smtp"
/sender/relay-config/relay-settings[0]/transport/smtp/connections[0]/server: "localhost"
/sender/relay-config/relay-settings[0]/transport/smtp/connections[0]/port: 1025
/sender/relay-config/relay-settings[0]/transport/smtp/smtp-binary: false
/sender/relay-config/relay-settings[1]/id: 2
/sender/relay-config/relay-settings[1]/name: "toT011"
/sender/relay-config/relay-settings[1]/transport/smtp/connections[0]/proto: "smtp"
/sender/relay-config/relay-settings[1]/transport/smtp/connections[0]/server: "10.199.29.101"
/sender/relay-config/relay-settings[1]/transport/smtp/connections[0]/port: 1025
/sender/relay-config/relay-settings[1]/transport/smtp/smtp-binary: false
/sender/relay-config/relay-settings[2]/id: 3
/sender/relay-config/relay-settings[2]/name: "organisation.local"
/sender/relay-config/relay-settings[2]/transport/smtp/connections[0]/proto: "smtp"
/sender/relay-config/relay-settings[2]/transport/smtp/connections[0]/server: "10.199.28.17"
/sender/relay-config/relay-settings[2]/transport/smtp/connections[0]/port: 25
/sender/relay-config/relay-settings[2]/transport/smtp/smtp-binary: false
/sender/sender-config/chunk-size: 100
/sender/sender-config/hs-divisors: "3600 700 50"
/sender/sender-config/slots: "0 1 2 3"
/sender/sender-config/read-slots: "0 1 2 3"
```

```
/sender/sender-config/read-slots-high: "0 1"
/sender/sender-config/timeout: 60
/sender/sender-config/spool-dir: "${smap-settings/common/smap-home}/spool/smap-send"
/sender/sender-config/debug: false
/sender/sender-config/max-threads: 2
/sender/sender-config/write-slots: "0 1 2 3"
/sender/sender-config/write-slots-high: "0 1"
/sender/sender-config/slots-high: "0 1"
/sender/sender-spool-config/spool-dir: ""
/sender/sender-spool-config/slots: ""
/sender/sender-spool-config/read-slots: ""
/sender/sender-spool-config/write-slots: ""
/sender/sender-spool-config/slots-high: ""
/sender/sender-spool-config/read-slots-high: ""
/sender/sender-spool-config/write-slots-high: ""
/sender/sender-spool-config/hs-divisors: ""
```

Для создания локальной конфигурации сервиса **sender** на узле **filter1** и установки значения SMTP-порта равным 2025 необходимо выполнить следующую команду:

**# config values add-local -N filter1 -s sender set -N filter1 -p **
/sender/relay-config/relay-settings[0]/transport/smtp/connections[0]/port -v 2025

Экспорт всей конфигурации в файл:

 # config values export -f values-backup.json

Примечание

*Также можно скопировать файл **/data/repos/dozor/config-base.git/values.json**.*

Экспорт локальных настроек сервиса **mailfilter** и узлов **dozor-filter-1** и **dozor-filter-2**:

 # config values export -n dozor-filter-1,dozor-filter-2 -s mailfilter -f values-backup.json

Импорт всей конфигурации:

 # config values import -f values-backup.json

Импорт только глобальной конфигурации (рекомендуется использовать, если в экспортированном файле у узлов есть неактуальные локальные настройки):

 # config values import -g -f values-backup.json

Команды:

**# config values add-local -N 7e852a19-297a-4ae7-9251-0dad0409855a **
-s filestorage-ng -t filestorage-ng-volumes

**# config values delete-local -N 7e852a19-297a-4ae7-9251-0dad0409855a **
-s filestorage-ng -t filestorage-ng-volumes

 # config values set -p /webserver/passwords-params/pass-min-level -v 3

а также команды импорта конфигурации имеют вывод:

Writing new values file /data/repos/dozor/config-base.git/values.json ...

Внимание!

*Скрипт **config values** не предназначен для сохранения изменений (commit) в репозитории **git**. При последующем выполнении команды*
 # accept-settings
не получится применить конфигурацию, об этом будут свидетельствовать строки:

There are local changes in cluster.json or values.json.
Commit your changes before running accept-settings.

*Поэтому после правки конфигурации вручную или использования скрипта **config values** следует сохранить изменения (commit) в репозитории **git**, выполнив команды:*

 # /opt/dozor/bin/shell

 # cd /data/repos/dozor/config-base.git

git add values.json && git commit -m "описание изменений"

Далее необходимо применить конфигурацию, выполнив команду:

 # accept-settings

6.10.4. Обновление конфигурации

Обновление конфигурации заключается в заполнении параметров конфигурации новой версии значениями соответствующих параметров предыдущей версии. Полученные файлы конфигурации KEO DLP записываются в указанный каталог.

Для работы со скриптом необходимо запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта выглядит следующим образом:

 # config upgrade [ключ]

Скрипт необходимо запускать от имени пользователя **dozor**.

Используются ключи:

- **-R <DIR>**, **--roles-dir <DIR>** – каталог, содержащий файлы с описанием ролей узлов.
- **-C <FILE>**, **--cluster-file <FILE>** – файл, содержащий описание кластера.
- **-T <FILES>**, **--types-files <FILES>** – файл(ы), содержащий(е) описания типов параметров конфигурации.
- **-O <FILES>**, **--old-types-files <FILES>** – файл(ы), содержащий(е) описания типов параметров конфигурации (предыдущей версии).

- **-D <FILES>**, **--defcfg-files <FILES>** – файл(ы), содержащий(е) описания значений параметров конфигурации по умолчанию.
- **-V <FILE>**, **--old-values-file <FILE>** – файл(ы), содержащий(е) описания значений параметров конфигурации (предыдущей версии).
- **-B <DIR>**, **--config-base-repo <DIR>** – каталог, предназначенный для хранения файлов конфигурации/

6.10.5. Создание начальной конфигурации

Создание начальной конфигурации выполняется однократно после чистой установки KEO DLP. При этом создается описание кластера из одного узла с указанными атрибутами. Конфигурации сервисов создаются на основе значений по умолчанию. Полученные файлы конфигурации систему записываются в указанный каталог.

Для работы со скриптом необходимо запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта выглядит следующим образом:

 # config init [ключ]

Скрипт необходимо запускать от имени пользователя **dozor**.

Используются ключи:

- **-R <DIR>**, **--roles-dir <DIR>** – каталог, содержащий файлы с описанием ролей узлов.
- **-T <DIR>**, **--types-dir <DIR>** – каталог с файлами, содержащими описания типов конфигурационных параметров.
- **-D <DIR>**, **--defcfg-dir <DIR>** – каталог с файлами, содержащими значения конфигурационных параметров по умолчанию.
- **-B <DIR>**, **--config-base-repo <DIR>** – каталог для хранения файлов конфигурации.
- **-i <ID>**, **--id <ID>** – идентификатор master-узла кластера.
- **-n <NAME>**, **--name <NAME>** – имя master-узла кластера.
- **-h <HOSTNAME>**, **--hostname HOSTNAME** – значение **hostname** master-узла кластера.

6.11. Журналирование работы KEO DLP

Работа с журнальными файлами выполняется либо в разделе GUI **Система> Администрирование > Журналы** (см. раздел 5.5.2), либо с помощью CLI. Посмотреть содержимое одних журнальных файлов можно с помощью скрипта **seelog**, других – открыв их для просмотра как обычный текстовый файл.

Настройка общих параметров журналирования выполняется в секции **Общие настройки системы** (раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование системы > Общее**).

Кроме того, для некоторых сервисов существуют свои конфигурационные файлы с именами вида **<имя процесса>.debug**, в которых можно либо оставить наследование общих настроек либо назначить другие параметры журналирования с помощью задания значения **Уровень журналирования** вместо **inherit**.

Получить список конфигурационных файлов, в которых можно устанавливать настройки журналирования, можно, указав в поле для поиска в дереве объектов ключевое слово **debug** и нажав кнопку  (Рис.5.35).

Для сервисов, для которых выполняется журналирование, в соответствующих конфигурационных файлах задан определенный список модулей (facility). Для каждого из модулей могут быть установлены свои параметры журналирования, отличающиеся от установленных для самого сервиса (Рис.6.2).

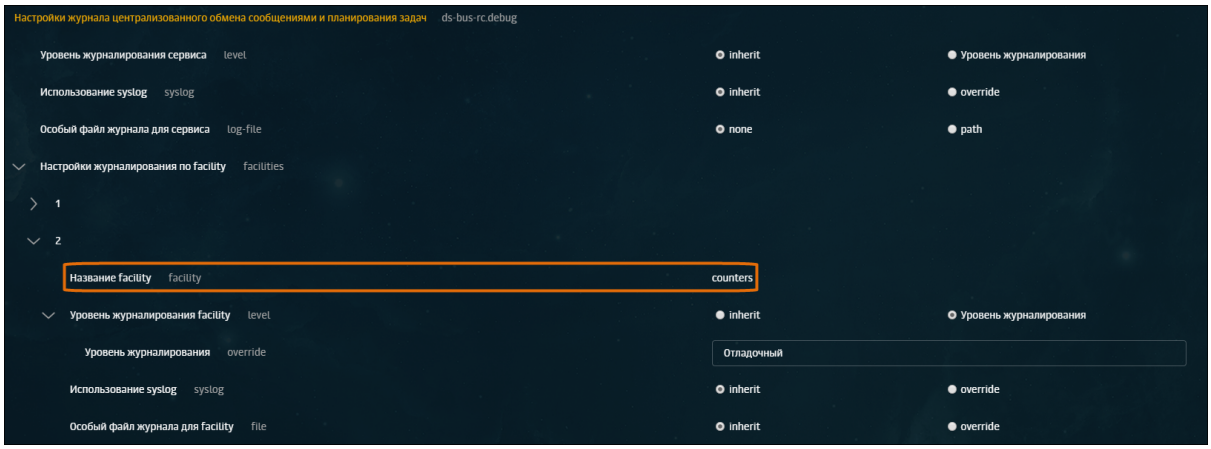


Рис. 6.2. Установка требуемых параметров журналирования для отдельных модулей

Табл. 6.3. Вывод типов записей в зависимости от уровня журналирования

Уровень журналирования	Типы выводимых записей (приоритеты)
Обычный	fatal, error
Повышенный	fatal, error, warning, notice, info
Отладочный	fatal, error, warning, notice, debug

Примечание

*Все сообщения модуля **support** журналируются всегда и не зависят от настроек.*

При достижении определенного размера журнального файла происходит автоматическая ротация файлов: создается новый файл журнала, запись данных продолжается в новый файл. При этом старые файлы сохраняются. В настройках конфигурации KEO DLP можно определить размер журнального файла, при достижении которого происходит ротация и количество сохраняемых журнальных файлов. Более подробно это описано в разделе 6.11.3.

Кроме того, можно настроить запись данных о работе процессов KEO DLP в журнальный файл операционной системы **syslog** (см. раздел 6.11.4).

6.11.1. Создание журнальных файлов

Поскольку сервисы KEO DLP запускаются в отдельной подсистеме управления сервисами ОС **systemd**, БД журналов о работе сервисов формируется с помощью системного демона журналов **journald** и располагается в каталоге **/var/log/journal**. Максимальный размер журнального файла задается параметром **Максимальный размер журнала (МБ)** (секция **Параметры сервиса журнала journald**, раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование системы > Общее**) и по умолчанию равен 4096 МБ, но рекомендуется задать значение как минимум в половину размера свободного пространства раздела **/var**. В файле **/opt/dozor/var/log/cmdline-utils.log** формируется журнал работы скриптов, список которых приведен в таблице ниже (см. Табл.6.4).

В Табл.6.4 приведены данные о том, каким способом создаются файлы журналов для каждого процесса или сервиса, в каком каталоге эти файлы хранятся и с помощью какого средства можно посмотреть содержимое журнального файла.

Примечание

*Подробное описание журналов **message-stat.log** и **deletes.log** приведено в приложении (см. Приложение В. Описание журнала обработки сообщений).*

Табл. 6.4. Журналирование процессов и сервисов KEO DLP

Процесс, сервис, скрипт	Журналируемый поток данных	Способ журналирования	БД журнала	Способ просмотра
abook-daemon	stdout	journald	/var/log/journal	seelog
action-server	stdout	journald	/var/log/journal	seelog
action-server-database	stdout	journald	/var/log/journal	seelog
agent-control-ng	stdout	journald	/var/log/journal	seelog
agent-server	stdout	journald	/var/log/journal	seelog
archiver	stdout	journald	/var/log/journal	seelog
archive-server	stdout	journald	/var/log/journal	seelog
category-server	stdout	journald	/var/log/journal	seelog
crawler-database	stdout	journald	/var/log/journal	seelog
crawler-processor	stdout	journald	/var/log/journal	seelog
crawler-scanner	stdout	journald	/var/log/journal	seelog
crawler-snapshot	stdout	journald	/var/log/journal	seelog
database	stdout	journald	/var/log/journal	seelog
detective-database	stdout	journald	/var/log/journal	seelog
detective-server	stdout	journald	/var/log/journal	seelog
ds-bus-rc	stdout	journald	/var/log/journal	seelog
filestorage-ng	stdout	journald	/var/log/journal	seelog
god-server	stdout	journald	/var/log/journal	seelog
haproxy	stdout	journald	/var/log/journal	seelog
im-crawler	stdout	journald	/var/log/journal	seelog
incident-daemon	stdout	journald	/var/log/journal	seelog

Процесс, сервис, скрипт	Журналируемый поток данных	Способ журналирования	БД журнала	Способ просмотра
indexer-ng	stdout	journald	/var/log/journal	seelog
mailfilter	stdout	journald	/var/log/journal	seelog
media-processor-action-server	stdout	journald	/var/log/journal	seelog
media-processor-action-server-database	stdout	journald	/var/log/journal	seelog
monitor-httpd	stdout	journald	/var/log/journal	seelog
monitor-ng	stdout	journald	/var/log/journal	seelog
monitor-server	stdout	journald	/var/log/journal	seelog
opensearch	stdout	journald	/var/log/journal	seelog
sender	stdout	journald	/var/log/journal	seelog
skvt-cassandra	stdout	journald	/var/log/journal	seelog
smap-counters	stdout	journald	/var/log/journal	seelog
smap-crawler	stdout	journald	/var/log/journal	seelog
smap-difi	stdout	journald	/var/log/journal	seelog
smap-idid	stdout	journald	/var/log/journal	seelog
smap-redis	stdout	journald	/var/log/journal	seelog
smap-request-handler	stdout	journald	/var/log/journal	seelog
smap-smtp-gw	stdout	journald	/var/log/journal	seelog
smap-tikaserver	stdout	journald	/var/log/journal	seelog
software-center	stdout	journald	/var/log/journal	seelog
software-center-database	stdout	journald	/var/log/journal	seelog
stt-server	stdout	journald	/var/log/journal	seelog
tragent	stdout	journald	/var/log/journal	seelog
uba-server	stdout	journald	/var/log/journal	seelog
webserver	stdout	journald	/var/log/journal	seelog
abook.log	stdout	journald	/var/log/journal	seelog
accept-policy.log	stdout	journald	/var/log/journal	seelog
accept-settings.log	stdout	journald	/var/log/journal	seelog
db-control.log	stdout	journald	/var/log/journal	seelog
dsctl.root.log	stdout	journald	/var/log/journal	seelog
infra.log	stdout	journald	/var/log/journal	seelog
message-stat.log	stdout	journald	/var/log/journal	seelog
set-role.log	stdout	journald	/var/log/journal	seelog
/opt/dozor/smap/bin/get-file-text.scm /opt/dozor/smap/bin/upgrade-policy-26-28.scm /opt/dozor/smap/bin/export-messages.scm /opt/dozor/smap/bin/scheduler-tool.scm /opt/dozor/smap/bin/ds-client.scm	cmdline-utils.log	сами сервисы	/opt/dozor/var/log/cmdline-utils.log	tail, less

Процесс, сервис, скрипт	Журналируемый поток данных	Способ журналирования	БД журнала	Способ просмотра
/opt/dozor/smap/bin/mount-dir2fs.scm /opt/dozor/smap/bin/export-message2fs.scm /opt/dozor/smap/bin/validate-fss-data.scm /opt/dozor/smap/bin/ds-tool.scm /opt/dozor/smap/bin/dozor-counters-tool.scm /opt/dozor/smap/bin/agent-tool.py /opt/dozor/smap/bin/as-tool.py /opt/dozor/smap/bin/difi-tool.py /opt/dozor/smap/bin/export-messages.py /opt/dozor/smap/bin/idid-tool.py /opt/dozor/smap/bin/import-messages.py /opt/dozor/smap/bin/message-tool.py /opt/dozor/smap/bin/qtool.py /opt/dozor/smap/bin/spool-move.py /opt/dozor/smap/bin/user-tool.py /opt/dozor/smap/bin/vendor-report.scm				

6.11.2. Просмотр журнальных файлов

Посмотреть содержимое журнальных файлов можно как с помощью GUI, так и CLI.

В GUI KEO DLP файлы журналов можно просмотреть в основном окне раздела **Система > Администрирование > Журналы**.

Примечание

*Журнальные файлы не отображаются на вкладке **Журналы** до тех пор, пока в них не будет записана какая-либо информация.*

Более подробно работа с вкладкой **Журналы** описана в разделе 5.5.2.

Информацию из этих файлов можно посмотреть либо с помощью скрипта **seelog**, либо с помощью команд **tail** и **less** (см. Табл.6.4).

Для отображения информации из большинства журнальных файлов служит скрипт **seelog**. Для запуска скрипта необходимо выполнить следующие действия:

- Переключиться на работу от имени пользователя **dozor**, выполнив команду:

  # su - dozor

- Запустить интерпретатор команд shell, выполнив команду:

  $ /opt/dozor/bin/shell

- Запустить скрипт **seelog**.

  Команда для запуска скрипта **seelog** имеет следующий формат:

  $ seelog <имя_процесса> [ключ]

  Имена процессов, журналы для которых открываются с помощью скрипта **seelog**, можно посмотреть в **Табл.6.4**.

  Доступны следующие ключи, определяющие режим работы скрипта:

  - **stream** – в этом режиме отображаются последние записи журнала, причем для запущенных процессов это происходит в режиме реального времени, то есть при появлении новой записи в журнале она сразу будет показана.
  - **content** – в этом режиме отображаются все имеющиеся на момент запуска скрипта записи журнала.
  - **num** <N> – в этом режиме отображаются N последних строк журнала.
  - **info** – в этом режиме выводится время последней модификации файла и его размер в байтах.

  Пример команды для запуска скрипта:

  $ seelog message-stat.log info

  В результате работы скрипта на экран будет выведена следующая информация:

  ```
  1401109095 109832
  ```

- Чтобы завершить работу скрипта и закрыть журнал, следует в режиме **content** нажать на клавиатуре клавишу **Q**, а в режимах **stream** и **tail** нажать **CTRL-C**.

Команды **less** и **tail** выдают в результате работы аналогичные данные.

Пример запуска команды **less**:

$ less /opt/dozor/var/log/cmdline-utils.log

В результате выполнения команды на экран выводятся следующие данные:

```
[30.10.2012 15:32:28] filter:debug (14852) Wtf (file-ng) initialized!
[30.10.2012 15:32:28] license:info (14852) Plugin difi not allowed by license.
[30.10.2012 15:32:28] license:info (14852) Plugin difi not allowed by license.
```

```
[30.10.2012 15:32:28] license:info (14852) Plugin difi not allowed by license.
[30.10.2012 15:32:28] license:info (14852) Plugin difi not allowed by license.
[30.10.2012 15:32:28] license:info (14852) Plugin difi not allowed by license.
[30.10.2012 15:32:45] counters:error (23128) (warning) Base counter smap:sender.count has less than
 2 values; using initial value of smap:sender.count.period.
[30.10.2012 15:32:45] counters:error (23128) (warning) Base counter smap:sender.err.count has less
than 2 values;
```

Чтобы завершить работу скрипта **less** и закрыть журнал, следует нажать на клавиатуре клавишу **Q**.

Команда **tail** работает аналогичным образом, но выводит на экран последние 10 строк указанного файла.

Пример запуска команды **tail**:

$ tail /opt/dozor/var/log/cmdline-utils.log

В результате выполнения команды на экран выводятся последние 10 строк журнального файла **cmdline-utils.log**:

```
[30.10.2012 15:41:12] counters:error (27831) (warning) Replacing annotation for stats
sys:monitor.snapshots
[30.10.2012 15:41:12] counters:error (27831) (warning) Replacing annotation for stats sys:monitor.hourly
[30.10.2012 15:41:12] counters:error (27831) (warning) Replacing annotation for stats sys:monitor.daily
[30.10.2012 15:41:12] counters:error (27831) (warning) Replacing annotation for stats sys:monitor.weekly
[30.10.2012 15:41:12] counters:error (27831) (warning) Replacing annotation for stats sys:monitor.monthly
[30.10.2012 15:41:15] filter:debug (27835) Wtf (file-ng) initialized!
[30.10.2012 15:41:17] modules:info (27835) Module difi is disabled
[30.10.2012 15:41:19] filter:debug (27843) Wtf (file-ng) initialized!
[30.10.2012 17:44:44] filter:debug (32686) Wtf (file-ng) initialized!
[30.10.2012 17:44:46] modules:info (32686) Module difi is disabled
```

Более подробную справку по работе с командами **less** и **tail** можно получить, выполнив следующие команды:

$ less --help

или

$ tail --help

6.11.3. Архивирование журнальных файлов KEO DLP

Постепенное увеличение объема журналов сервисов может привести к аварийной ситуации. Чтобы этого избежать, следует дополнительно задать значения параметров ротации в конфигурационном файле **/etc/systemd/journald.conf**. Для этого следует отредактировать строки, выделенные жирным.

Ниже приведен пример конфигурационного файла:

```
Journald Configuration File
# See journald.conf(5) for details. [Journal]
#Storage=auto
#Compress=yes
#Seal=yes
#SplitMode=uid
```

```
#SyncIntervalSec=5m
#RateLimitInterval=30s
#RateLimitBurst=1000
#SystemMaxUse=
#SystemKeepFree=
#SystemMaxFileSize=
#SystemMaxFiles=100
#RuntimeMaxUse=
#RuntimeKeepFree=
#RuntimeMaxFileSize=
#RuntimeMaxFiles=100
#MaxRetentionSec=
#MaxFileSec=1month
#ForwardToSyslog=yes
#ForwardToKMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg
```

Параметры **SystemMaxUse** и **RuntimeMaxUse** определяют размеры журналов в каталогах **/var/log/journal/** и **/run/log/journal** соответственно. Параметр **SystemKeepFree** определяет объем свободного места на диске после сохранения журналов. Параметр **RuntimeKeepFree** определяет объем свободного места, которое остается в каталоге **/run/** после сохранения журналов.

Пример содержимого файла **/etc/systemd/journald.conf** при ограничении размера журнала в 50 МБ и оставшегося места в 1 ГБ:

```
SystemMaxUse=50M
SystemKeepFree=1G
```

Для параметра **SystemMaxUse** рекомендуется задавать значение как минимум в половину размера свободного пространства раздела **/var**.

6.11.4. Организация записи информации о работе процессов KEO DLP в журнальный файл ОС (syslog)

В качестве демона **rsyslog** в ОС Astra Linux SE версии 1.7.5 и Debian 12.4 используется **syslog-ng**.

6.11.4.1. Настройка syslog-ng

Общие команды и настройки для управления **syslog-ng**:

1. Перезапустить **syslog-ng**:

   a. Проверить синтаксис конфигурационного файла, выполнив команду:

      # sudo syslog-ng -s

      Если обнаружены ошибки синтаксиса – исправить их и повторить команду.

b. Перезапустить сервис **syslog-ng**, выполнив команду:

 # sudo systemctl restart syslog-ng

c. Проверить статус сервиса **syslog-ng**, выполнив команду:

 # sudo systemctl status syslog-ng

Пример вывода, свидетельствующего об успешном запуске сервиса:

```
root@a173-d79:~# systemctl status syslog-ng
● syslog-ng.service - System Logger Daemon
   Loaded: loaded (/lib/systemd/system/syslog-ng.service; enabled; vendor preset: enabled)
  Drop-In: /etc/systemd/system/syslog-ng.service.d
           └─override.conf
   Active: active (running) since Sun 2023-01-22 00:00:04 MSK; 1 day 11h ago
     Docs: man:syslog-ng(8)
 Main PID: 26197 (syslog-ng)
    Tasks: 10 (limit: 4915)
   Memory: 17.9M
   CGroup: /system.slice/syslog-ng.service
           └─26197 /usr/sbin/syslog-ng -F --no-caps

янв 22 00:00:04 a173-d79 systemd[1]: Starting System Logger Daemon...
янв 22 00:00:04 a173-d79 systemd[1]: Started System Logger Daemon.
янв 23 00:00:02 a173-d79 systemd[1]: Reloading System Logger Daemon.
янв 23 00:00:02 a173-d79 systemd[1]: Reloaded System Logger Daemon.
```

2. Для просмотра актуальных настроек конфигурации выполнить команду:

syslog-ng-ctl config --preprocessed

3. Для возможности получать статистику от внутренних счетчиков **syslog-ng** следует создать файл **/etc/syslog-ng/conf.d/stat.conf** с содержимым:

```
options {
  stats-freq(60);
  stats-level(0);
};

filter f_syslog-ng { "${PROGRAM}" eq "syslog-ng"; };

destination d_syslog-ng { file("/var/log/syslog-ng.log"); };

log {
  source(s_src);
  filter(f_syslog-ng);
  destination(d_syslog-ng);
};
```

В данном примере настроена запись статистики каждые 60 секунд (**stats-freq**) с записью сообщений от **syslog-ng** в файл **/var/log/syslog-ng.log**.

Также статистику можно просматривать с помощью команды следующего вида:

 # syslog-ng-ctl query get dst.syslog.d_tls_q*

Для сброса статистики следует выполнить команду:

 # syslog-ng-ctl stats --reset

После любого изменения конфигурационных файлов, описанных в процедурах ниже, необходимо выполнять перезапуск **syslog-ng**, как описано в шаге 1.

6.11.4.2. Настройка журналирования в файл с использованием syslog-ng

Для записи сообщений сервисов KEO DLP в файлы локальной файловой системы в каталоге **/var/log/dozor** при условии, что журнал сервиса хранится в отдельном файле, который называется именем модуля **systemd**, необходимо создать файл **/etc/syslog-ng/conf.d/dozor.conf** со следующим содержимым:

```
filter f_dozor_unit {match("dozor" value (".journald._SYSTEMD_UNIT"));};

destination d_dozor {
  file("/var/log/dozor/${.journald._SYSTEMD_UNIT}.log"
    create-dirs(yes) dir-group("dozor") dir-owner("dozor") dir-perm(0755)
    group("dozor") owner("dozor") perm(0640)
    );
};

log {
  source(s_src); filter(f_dozor_unit); destination(d_dozor); flags(final);
};
```

Для записи сообщений сервисов KEO DLP в файлы локальной файловой системы в каталоге **/var/log/dozor** при условии, что журнал сервиса хранится в отдельном файле, имя которого создается на базе заголовка **APP-NAME** из строки **syslog**, необходимо создать файл **/etc/syslog-ng/conf.d/dozor.conf** со следующим содержимым:

```
@define allow-config-dups 1

filter f_dozor_unit {match("dozor" value (".journald._SYSTEMD_UNIT"));};
filter f_syslog3 { not facility(auth, authpriv, mail) and not filter(f_debug) and not filter(f_dozor_unit); };

destination d_dozor {
  file("/var/log/dozor/${PROGRAM}.log"
    create-dirs(yes) dir-group("dozor") dir-owner("dozor") dir-perm(0755)
    group("dozor") owner("dozor") perm(0640)
    );
};

log {
  source(s_src); filter(f_dozor_unit); destination(d_dozor); flags(final);
};
```

6.11.4.3. Настройка журналирования на удаленный сервер

Для отправки журналов отдельного сервиса (например, **mailfilter**) следует создать файл **/etc/syslog-ng/conf.d/by_mailfilter.conf** с содержимым следующего вида:

```
@define REMOTE_SERVER "c7-syslog.organisation.com"
@define REMOTE_PORT 10514

filter f_mailfilter { "${PROGRAM}" eq "mailfilter"};
```

```
destination d_udp {
  syslog("`REMOTE_SERVER`" transport("udp") port(`REMOTE_PORT`));
};

log {
  source(s_src); filter(f_mailfilter); destination(d_udp);
};
```

где для констант **REMOTE_SERVER** и **REMOTE_PORT** заданы значения FQDN и порта удаленного сервера.

6.11.4.4. Настройка журналирования на удаленный сервер с использованием очереди

Для отправки журналов с возможностью буферизации на локальном сервере для обеспечения временного сохранения сообщений в буфере при проблемах доступа к удаленному серверу следует создать файл **/etc/syslog-ng/conf.d/dozor.conf** с содержимым следующего вида:

```
@define allow-config-dups 1

@define REMOTE_SERVER "c7-syslog.organisation.com"
@define REMOTE_PORT 10514

filter f_dozor_unit {match("dozor" value (".journald._SYSTEMD_UNIT"));};
filter f_syslog3 { not facility(auth, authpriv, mail) and not filter(f_debug) and not filter(f_dozor_unit); };

destination d_tcp_q {
  syslog("`REMOTE_SERVER`" transport("tcp") port(`REMOTE_PORT`)
    disk-buffer(
      reliable(yes)
      dir("/var/lib/syslog-ng")
      disk-buf-size(524288000)
      mem-buf-size(134217728)
      qout-size(10000)
    )
  );
};

destination d_dozor {
  file("/var/log/dozor/${PROGRAM}.log"
    create-dirs(yes) dir-group("dozor") dir-owner("dozor") dir-perm(0755)
    group("dozor") owner("dozor") perm(0640)
    );
};

log {
  source(s_src); filter(f_dozor_unit); destination(d_dozor);
};

log {
  source(s_src);
  filter(f_dozor_unit);
  destination(d_tcp_q);
  flags(final,flow-control);
};
```

где для констант **REMOTE_SERVER** и **REMOTE_PORT** заданы значения FQDN и порта удаленного сервера.

6.11.4.5. Настройка журналирования с использованием TLS

Для настройки сообщений syslog с использованием шифрования по протоколу TLS необходимо:

1. Предварительно настроить прием сообщений с использованием TLS на стороне syslog-сервера. Подробные настройки см. в документации выбранной SIEM-системы.

   Примечание

   Для отправки данных на сервер необходимо получить следующие файлы:

   - *сертификата SIEM-системы, подписанного ЦС (например, **syslog_ca.crt**);*
   - *сертификата клиента (узла, с которого выполняется отправка), подписанного ЦС (например, **a173-d79f.crt**);*
   - *закрытого ключа клиента (например, **a173-d79f.key**).*

2. На сервере отправки журнальных данных скопировать файлы сертификатов узла и центра сертификации в каталог **/etc/ssl/certs**, файл ключа – в каталог **/etc/ssl/private**. Установить права доступа к файлу ключа, выполнив команды:

   chown root:root /etc/ssl/private/a173-d79f.key

   chmod 600 /etc/ssl/private/a173-d79f.key

3. Добавить сертификат центра сертификации в доверенные, выполнив команды:

   cp /tmp/syslog_ca.crt /usr/local/share/ca-certificates/

   update-ca-certificates

4. Создать файл настройки с общими параметрами под названием **/etc/syslog-ng/conf.d/dozor_remote.conf** с содержимым следующего вида:

```
@define allow-config-dups 1

# set variable
@define ROOT_DIR "/var/log/dozor/"
@define KEY_FILE "/etc/ssl/private/a173-d79f.key"
@define CERT_FILE "/etc/ssl/certs/a173-d79f.crt"
@define REMOTE_SERVER "c7-syslog.organisation.com"
@define REMOTE_PORT 10514

# set date format
options {
  ts-format(iso);
};

filter f_dozor_unit { match("dozor" value (".journald._SYSTEMD_UNIT")); };
# override default f_syslog3
```

```
filter f_syslog3 { not facility(auth, authpriv, mail) and not filter(f_debug) and not filter(f_dozor_unit); };


destination d_tls_q {
  syslog("`REMOTE_SERVER`" transport("tls") port(`REMOTE_PORT`)
    disk-buffer(
      reliable(yes)
      dir("/var/lib/syslog-ng")
      disk-buf-size(524288000)
      mem-buf-size(134217728)
      qout-size(10000)
    )
    tls ( key-file("`KEY_FILE`") cert-file("`CERT_FILE`") ca-dir("/etc/ssl/certs")
    )
  );
};

destination d_dozor {
  file("`ROOT_DIR`${PROGRAM}.log"
    create-dirs(yes) dir-group("dozor") dir-owner("dozor") dir-perm(0755)
    group("dozor") owner("dozor") perm(0640)
    );
};

log {
  source(s_src); filter(f_dozor_unit); destination(d_dozor);
};

log {
  source(s_src);
  filter(f_dozor_unit);
  destination(d_tls_q);
  flags(final,flow-control);
};
```

подставляя для констант соответствующие значения.

6.11.4.6. Настройка ротации журналов

Для ротации журнальных файлов используется скрипт **logrotate**. Настройки этого скрипта содержатся в файле **/etc/logrotate.conf** и файлах в директории **/etc/logrotate.d/**. Например, для ежедневной ротации файлов в директории **/var/log/dozor/**, со сжатием и хранением последних 10 копий, необходимо создать файл **/etc/logrotate.d/dozor** со следующим содержимым:

```
/var/log/dozor/*.log{
    daily
    compress
    missingok
    rotate 10
    sharedscripts
    postrotate
        # /usr/bin/pkill -HUP rsyslogd
        /usr/bin/pkill -HUP syslog-ng
        true
    endscript
}
```

Для принудительного запуска ротации указанных файлов необходимо выполнить команду:

sudo logrotate -f /etc/logrotate.d/dozor

Для ротации файлов по достижении определенного размера (например, 100 МБ) необходимо отредактировать файл настроек следующим образом:

```
/var/log/dozor/*.log{
    size 100M
    compress
    missingok
    rotate 10
    sharedscripts
    postrotate
        /usr/bin/pkill -HUP syslog-ng
        true
    endscript
}
```

По умолчанию скрипт **logrotate** запускается системой раз в сутки. Если настроена ротация по достижении определенного размера журнальных файлов, в момент запуска скрипта по расписанию этот размер может существенно превысить заданное ограничение. Для решения этой проблемы можно увеличить частоту запуска скрипта **logrotate** (например, раз в час) следующим образом:

1. Выполнить команду:

   systemctl edit logrotate.timer

2. В открывшемся редакторе добавить следующие строки:

   ```
   [Timer]
   OnCalendar=daily
   OnCalendar=hourly
   AccuracySec=10min
   ```

6.12. Сопровождение БД

В KEO DLP можно сопровождать схему БД через CLI. Для этого необходимо использовать учётную запись пользователя **dozor** и скрипты **create-database.sh** и **update-db.sh**. Первый скрипт (см. раздел 6.12.1) применяется для создания схемы базы данных, а второй (см. раздел 6.12.2) – для её обновления.

Сопровождение БД сервиса **Расследование** производится с помощью скрипта **reset-db-password.sh**,предназначенного для установки пароля пользователя этой БД в соответствии с конфигурацией. Также этот скрипт применяется для устранения ошибок в процессе обновления версий KEO DLP (см. раздел 6.12.3).

СУБД PostgreSQL предоставляет инструменты для резервного копирования (см. раздел 6.12.6) и восстановления баз данных (см. раздел 6.12.7), оптимизации таблиц в БД и создания отчётов о работе БД (см. раздел 6.12.12).

6.12.1. Создание схемы БД

Скрипт **create-database.sh** предназначен для создания схемы БД.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor**, выполнив команду:

 # su - dozor

Скрипт **create-database.sh** имеет следующие варианты запуска:

$ /opt/dozor/smap/schema/pgsql/create-database.sh <db-path> [<dbport> [<dbname> [<password> [<host>]]]] [--empty-db | --create-startup-only] [--calc-mem-params]

$ /opt/dozor/smap/schema/pgsql/create-database.sh <db-path> [-con <connection>] [--empty-db | --create-startup-only | --create-schema-only] [--calc-mem-params]

$ /opt/dozor/smap/schema/pgsql/create-database.sh <db-path> [-p <dbport>] [-d <dbname>] [-P <password>] [-H <host>] [--empty-db | --create-startup-only | --create-schema-only] [--calc-mem-params]

где:

- **<db-path>** – путь к каталогу с создаваемой БД (например, **/data/base/smaparchive/**).
- **-con** – дополнительный необязательный ключ. Имя схемы соединения с БД, указанное в конфигурации KEO DLP (**dbconn.conf**).
- **<dbport>** – номер порта, на котором новая БД будет ожидать соединения (например, 5435). Если ключ не указывать и задан параметр **-con** – будет использован порт, указанный в конфигурации KEO DLP (**dbconn.conf**). Если ключ не указан и не задан параметр **-con** – будет использовано значение по умолчанию: 5445.
- **<dbname>** – имя новой БД (например, **archive**). Если ключ не указывать и задан параметр **-con** – будет использовано имя БД, указанное в конфигурации KEO DLP (**dbconn.conf**). Если ключ не указан и не задан параметр **-con** – будет использовано имя по умолчанию: **dozor**.
- **<dbpass>** – пароль для доступа к БД. Если ключ не указывать, и задан параметр **-con** – будет использован пароль, указанный в конфигурации KEO DLP (**dbconn.conf**). Если ключ не указан и не задан параметр **–con** – будет создана БД без пароля.

  Внимание!

  Не рекомендуется создавать БД с пустым паролем из-за риска утечки информации.

- **<dbhost>** – FQDN или IP-адрес сервера, на котором предполагается размещение БД. Если ключ не указывать и задан параметр **-con** – будет использовано сетевое имя сетевое имя сервера базы данных, указанное в конфигурации KEO DLP (**dbconn.conf**) Если ключ не указан и не задан параметр **–con** – будет использован адрес текущего сервера.
- **--empty-db** – дополнительный необязательный ключ, при использовании которого будет создана пустая БД без загрузки объектов KEO DLP.
- **--create-startup-only** – дополнительный необязательный ключ, при использовании которого будет создан только скрипт автозапуска БД.

- **--create-schema-only** – дополнительный необязательный ключ, при использовании которого будет создана только схема в уже существующей БД. Рекомендуется использовать при наличии уже созданной пустой БД.
- **--calc-mem-params** – дополнительный необязательный ключ. Предназначен для вычисления и изменения размера памяти, которую БД использует в своей работе. Значение рассчитывается исходя из того, что доступная память составляет 25 процентов от общей памяти сервера, на котором расположена БД.

6.12.2. Обновление схемы БД

Обновление схемы БД выполняется с помощью скрипта **update-db.sh**, который находится в каталоге **/opt/dozor/smap/schema/liquibase/**.

Перед обновлением схемы БД рекомендуется подключить все отключённые секции.

Для обновления схемы БД необходимо выполнить следующие действия:

1. Запустить интерпретатор команд **shell**, выполнив команду:

   # /opt/dozor/bin/shell

2. Остановить все процессы KEO DLP, выполнив от имени пользователя **root** следующую команду:

   # dsctl stop

3. Переключиться на работу от имени пользователя **dozor**, выполнив следующую команду:

   # su - dozor

4. Если сервер БД не запущен, то запустить его, выполнив следующую команду:

   $ pg_ctl -D /data/base/smap start

5. Перейти в каталог **/opt/dozor/smap/schema/liquibase**, выполнив следующую команду:

   $ cd /opt/dozor/smap/schema/liquibase/

6. Запустить обновление версии, выполнив команду:

   $ ./update-db.sh -con <db-conn-name>

   Примечание

   *Можно отключить ввод пароля для пользователя **SYS**, указав при выполнении скрипта дополнительный ключ **-nosys**.*

7. Дождаться, пока обновление будет завершено. Это может занять некоторое время.

8. Запустить процессы KEO DLP, выполнив от имени пользователя **root** следующую команду:

   # /opt/dozor/bin/dsctl start

Если при обновлении БД работа процесса **liquibase** была прекращена аварийно (системой или пользователем), то может возникнуть ситуация, когда останется блокировка этого процесса в обновляемой базе. Данная блокировка предназначена для предотвращения одновременной работы нескольких процессов **liquibase** с одной и той же базой данных.

В этом случае при повторном запуске скрипта обновления БД **update-db.sh** появляется ошибка liquibase:

```
INFO 19.12.13 9:15:liquibase: Waiting for changelog lock....
SEVERE 19.12.13 9:15:liquibase: Could not acquire change log lock.
Currently locked by fe80:0:0:0:20c:29ff:fe95:cec9%2
(fe80:0:0:0:20c:29ff:fe95:cec9%2) since 18.12.13 21:10
```

Решение этой проблемы описано в разделе 7.2.2.

6.12.3. Сопровождение БД сервиса Расследование

Скрипт **reset-db-password.sh** предназначен для установки пароля пользователя БД сервиса Расследование в соответствии с конфигурацией. Также этот скрипт применяется для устранения ошибок в процессе обновления KEO DLP, возникающих в случае, когда для пользователя БД сервиса Расследование изначально не был задан пароль.

Для смены пароля пользователя БД сервиса Расследование необходимо выполнить следующие действия:

1. Запустить интерпретатор команд shell, выполнив команду:

   # /opt/dozor/bin/shell

2. Задать новый пароль, выполнив команду вида:

   # set-config global /detective-database/detective-database.conf/
   detective-database-settings/password <new_pass>

   подставляя вместо **<new_pass>** желаемое значение пароля для пользователя БД сервиса Расследование.

3. Применить настройки, выполнив команду:

   # accept-settings

4. Запустить скрипт **reset-db-password.sh**, выполнив команду:

   # /opt/dozor/detective/bin/reset-db-password.sh

5. Запустить сервисы, используемые ролью **Расследование**, выполнив команду:

   # dsctl start detective-database detective-server

6. Удалить журнальный файл PostgreSQL, выполнив команду:

   # rm /opt/dozor/var/log/reset-db-password-pgsql.log

6.12.4. Обновление СУБД PostgreSQL до версии 11

KEO DLP поддерживает работу БД архива под управлением СУБД PostgreSQL версии 11. Для обновления СУБД PostgreSQL версии 9.6 до версии 11 необходимо выполнить следующие действия:

1. Установить пакеты **postgresql** версии 11, выполнив команды:

   sudo apt-get install ./postgresql-11_11.9-0+deb10u1_amd64.deb

   sudo apt-get install ./postgresql-client-11_11.9-0+deb10u1_amd64.deb

   sudo apt-get install ./postgresql-client-common_215.pgdg90+1_all.deb

   sudo apt-get install ./postgresql-common_215.pgdg90+1_all.deb

   sudo apt-get install ./postgresql-plpython-11_11.9-0+deb10u1_amd64.deb

2. На всех slave-узлах, на которых запущен процесс **archiver**, выполнить команды:

   # /opt/dozor/bin/shell

   # dsctl stop ds-bus ds-bus-rc archiver

3. На master-узле остановить работу KEO DLP, выполнив команды:

   # /opt/dozor/bin/shell

   # dsctl down

4. Создать каталог для резервной копии БД архива прежней версии PostgreSQL, выполнив команду:

   # mkdir /var/tmp/basebackup

   Следует убедиться, что в выбранном разделе достаточно дискового пространства для хранения резервной копии БД.

5. Назначить пользователя **dozor** владельцем этого каталога, выполнив команду:

   # chown dozor:dozor /var/tmp/basebackup

6. Остановить БД архива, выполнив команду вида:

   # systemctl stop dozor-postgresql.service

   Вместо **dozor-postgresql.service** подставить актуальное имя, если оно отличается.

7. Выполнить синхронизацию каталога БД и резервной копии, выполнив команду следующего вида:

   # rsync -v -r -l -p /data/base/archive/* /var/tmp/basebackup

   где **/data/base/archive** – каталог БД архива

8. Переименовать каталог БД архива, выполнив команду следующего вида:

 # mv -v /data/base/archive/ /data/base/archive.old/

где **/data/base/archive** – каталог БД архива

9. Переключиться на работу от имени пользователя **dozor**, выполнив команду:

   # su dozor

10. Создать новую БД PostgreSQL версии 11 в каталоге БД архива с прежним названием, выполнив команду следующего вида:

    $ /usr/pgsql-11/bin/initdb -D /data/base/archive --locale=ru_RU.UTF-8

11. Загрузить командную оболочку KEO DLP, выполнив команду:

    $ /opt/dozor/bin/shell

12. Обновить СУБД PostgreSQL, выполнив команду следующего вида:

    $ /usr/pgsql-11/bin/pg_upgrade -b /usr/pgsql-9.6/bin -B /usr/pgsql-11/bin -d /data/base/archive.old -D /data/base/archive -p 5435

    После ключей подставлять следующие значения:

    - **-b** – прежний каталог с исполняемыми файлами **postgresql** версии 9.6.
    - **-B** – новый каталог с исполняемыми файлами **postgresql** версии 11.
    - **-d** – каталог с прежней БД архива.
    - **-D** – каталог с новой БД архива.
    - **-p** – порт БД архива.

    Внимание!

    *Обновление СУБД можно выполнить быстрее, с потерей читаемости данных **/data/base/archive.old**. Для этого следует выполнить следующую команду (пример для БД архива):*

    # /usr/pgsql-11/bin/pg_upgrade --link -b /usr/pgsql-9.6/bin -B /usr/pgsql-11/bin -d /data/base/archive.old -D /data/base/archive -p 5435

    Значения ключей те же, что в предыдущем примере.

13. Выйти из командной оболочки и вернуться к работе от имени пользователя **root**, выполнив команды:

    $ exit

    $ exit

14. Открыть конфигурационный файл **/data/base/archive/postgresql.conf** и внести в него следующие изменения:

- Раскомментировать параметр **listen_addresses** (список адресов, на которых БД ожидает соединения) и задать для него актуальное значение: либо использовать значение из аналогичного файла в резервной копии БД, либо установить значение по усмотрению, исходя из реалий сетевой инфраструктуры
- Раскомментировать параметр **port** и задать актуальное значение порта, на котором БД ожидает соединения.
- Раскомментировать параметр **unix_socket_directories** и задать для него значение **'/tmp'**. Строка с этим параметром должна выглядеть следующим образом:

```
unix_socket_directories = '/tmp'
```

15. Отредактировать конфигурационный файл **/data/base/archive/pg_hba.conf** таким образом, чтобы они содержал строки следующего вида:

```
host all all <dozor-host> trust
```

где **<dozor-host>** – FQDN или IP-адрес узла KEO DLP. Следует добавить записи обо всех узлах кластера.

16. Создать скрипт автозапуска **dozor-postgresql.service**, выполнив команды:

$ /opt/dozor/smap/schema/pgsql/create-database.sh /data/base/archive 5435 --empty-db --create-startup-only

$ exit

17. Скопировать файл **dozor-postgresql.service** из каталога **/opt/dozor/smap/schema/pgsql** в **/etc/systemd/system/dozor-postgresql-archive.service**, выполнив команды:

 # cd /opt/dozor/smap/schema/pgsql

 # cp dozor-postgresql.service /etc/systemd/system/dozor-postgresql-archive.service

18. Открыть для редактирования файл **/etc/systemd/system/dozor-postgresql-archive.service**, полученный на предыдущем шаге. Найти строки **ExecStart**, **ExecStop** и **ExecReload**, и заменить в них вхождения **/usr/pgsql-12/bin/pg_ctl** на **/usr/pgsql-11/bin/pg_ctl**. Сохранить и закрыть файл.

19. Выполнить команды:

 # systemctl daemon-reload

 # systemctl enable dozor-postgresql-archive.service

 # systemctl start dozor-postgresql-archive.service

20. Удалить неактуальный скрипт автоматического запуска БД архива **dozor-archive**.

21. На master-узле запустить работу KEO DLP, выполнив команды:

 # /opt/dozor/bin/shell

 # dsctl boot

22. На slave-узлах запустить сервисы KEO DLP, выполнив команды:

    # /opt/dozor/bin/shell

    # dsctl boot

23. Проверить версию БД архива на master-узле, выполнив команду следующего вида:

    # ps ax | grep 5435

    Вместо **5435** следует указать актуальный порт, на котором БД архива ожидает соединения. В выводе команды будет содержаться путь к каталогу с исполняемыми файлами PostgreSQL. Например:

    ```
    15444 ?        S      0:00 /usr/pgsql-11/bin/postmaster -p 5435 -D /data/base/archive
    ```

    Также версию БД архива можно узнать, выполнив команду следующего вида:

    # psql -U dozor -p 5435 -h localhost -d archive

    где **5435** – актуальный порт БД архива, **archive** – название БД архива. Это название можно узнать, выполнив команду:

    # db-conn -a

    Названием БД является значение параметра **DBNAME**.

24. Проверить работу БД архива, выполнив в GUI поисковый запрос с каким-либо заведомо известным результатом.

6.12.5. Секционирование БД PostgreSQL

Чтобы избежать появления сообщения об ошибке **ERROR:out of shared memory** при работе с секционированной схемой в БД PostgreSQL, следует убедится, что значение параметра **max_locks_per_transaction** увеличено по сравнению со значением, принятым по умолчанию. В таком случае рекомендуется установить значение, равное 1024.

Секционирование в БД PostgreSQL реализовано в соответствии со следующими принципами:

- Каждая секция хранит данные за определённый в конфигурации интервал времени (параметр **Период секционирования**). Интервал измеряется в неделях. Значение по умолчанию: 4 (4 недели).
- В момент создания секции ей присваивается имя вида **message_YYYYMMDD** и границы интервала. Началом считается дата окончания предыдущей секции, концом – дата, полученная сложением даты начала интервала и заданной величины интервала. Шифр вида **YYYYMMDD** соответствует дате начала секции. Например, если дата начала секции – 1 июня 2017 года, то секции будет присвоено имя **message_20170601**.
- Даты окончания предыдущей секции и начала следующей совпадают. Например, если секция имеет границы **2017-06-01 – 2017-07-01**, то следующая секция будет иметь в качестве даты начала **2017-07-01**.

- Границей между секциями является время 00:00:00 даты начала следующей секции. Например, если секция имеет границы **2017-06-01 – 2017-07-01**, то в ней будут храниться данные за период от 00:00:00 1 июня 2017 года до 23:59:59 30 июня 2017 года.

- Датой начала первой секции является дата создания БД. Дата окончания первой секции получается прибавлением величины интервала к дате начала и округлением вниз до ближайшего понедельника.

- Следующая секция создаётся заранее, за определённый параметром **Интервал опережения при создании секций** интервал до окончания предыдущей секции. Например, если секция имеет границы **2017-06-01 – 2017-07-01**, а параметр **Интервал опережения при создании секций** имеет значение **8D**, то следующая секция будет создана 23 июня 2017 года.

- Всегда существует секция, интервал который содержит дату, получаемую путём сложения текущей даты и значения параметра **Интервал опережения при создании секций**. Например, БД была создана 1 июля 2017 года со следующими параметрами:

  - **Конец диапазона первой секции** – **2017-07-10**
  - **Период секционирования** – **1**
  - **Интервал опережения при создании секций** – **31D**

  В этом случае будут созданы следующие секции:

  - **2017-07-01 – 2017-07-10**
  - **2017-07-10 – 2017-07-17**
  - **2017-07-17 – 2017-07-24**
  - **2017-07-24 – 2017-07-31**
  - **2017-07-31 – 2017-08-07**

6.12.5.1. Настройка хранения табличных пространств MAIN и MESSAGE

Если используется хранение табличных пространств MAIN и MESSAGE, то для его настройки необходимо выполнить следующие действия:

1. Создать требуемые каталоги для хранения табличных пространств и установить для них права доступа 755, пользователь – тот же, что и пользователь БД (по умолчанию – **dozor**).

2. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Хранение** и открыть секцию **Схемы соединений с БД**. Раскрыть параметры нужной схемы соединения.

3. Раскрыть группу параметров **Тип базы данных > Использование секционирования > Параметры хранения данных в БД**.

4. Задать параметры **Список каталогов для табличных пространств MAIN** и **Список каталогов для табличных пространств MESSAGE**. Если для какого-то табличного

пространства задано несколько каталогов – их следует перечислять через запятую без пробелов.

5. Нажать **Сохранить**, **Применить**.

Внимание!

В одном каталоге может храниться табличное пространство только одной схемы БД.

6.12.5.2. Автоматическое отключение, архивация и удаление секций

Отключение, архивация и удаление секций используются для увеличения производительности и упрощения обслуживания БД архива.

Автоматическое отключение позволяет не учитывать отключенные секции при поиске по архиву и таким образом повысить производительность БД архива. Данный механизм реализован в соответствии со следующими принципами:

- Наиболее старые секции отключаются от БД архива через интервал времени, заданный параметром **Время до автоматического отключения секций**.
- Время поиска секций сокращается.
- Далее системный администратор может архивировать или удалить отключенные секции вручную.

Для настройки автоматического отключения секций необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** и в секции **Схемы соединений с БД** задать значения следующих параметров:
   - **Интервал опережения при создании секций** – **8D**
   - **Автоматическое отключение секций** – **используется**
   - **Время до автоматического отключения секций** – указать интервал времени, по истечении которого секция будет автоматически отключена. Значение по умолчанию: **3M**.
   - **detach-action** – **Ручная обработка отключенных секций**
2. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Поиск** и в секции **Сервис поиска и индексации OpenSearch** нажать кнопку **Добавить** в строке параметра **Разделяемая файловая система для хранения snapshot'ов индексов**.
3. В появившейся строке **1** задать путь к каталогу для хранения резервных копий индексов почтового архива (например, **/data/backup**).
4. Сохранить и применить значения параметров конфигурации, нажав кнопки **Сохранить** и **Применить**.

5. Переключиться на работу от имени пользователя **dozor**, выполнив следующую команду:

   # su - dozor

6. Перейти в каталог **/opt/dozor/smap/schema/liquibase**, выполнив следующую команду:

   $ cd /opt/dozor/smap/schema/liquibase/

7. Запустить обновление схемы БД, выполнив команду:

   $ ./update-db.sh -con <db-connection-name>

   где **db-connection-name** – имя соединения с БД, например: **db-conn-1**.

8. Выполнить следующую команду:

   $ bash /opt/dozor/smap/schema/pgsql/shell/part-control -con <db-connection-name>

   где **db-connection-name** – имя соединения с БД, например: **db-conn-1**.

Автоматическое удаление позволяет удалять ненужные отключенные секции и, таким образом, увеличить свободное место в БД архива. Данный механизм реализован в соответствии со следующими принципами:

- Происходит отключение ранее созданных секций через интервал времени, который указывается в значении параметра **Время до автоматического отключения секций**.
- Отключенные секции удаляются из БД архива через интервал времени, указанный в значении параметра **Время до удаления отключенных секций**.

Примечание

Интервал отсчитывается от даты окончания действия секции. Под датой окончания действия секции понимается момент времени, в который была или будет прекращена запись данных в секцию.

Для настройки автоматического удаления секций необходимо перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** и выполнить следующие действия:

1. В секции **Схемы соединений с БД** задать значения следующих параметров:
   - **Интервал опережения при создании секций – 8D**
   - **Автоматическое отключение секций – используется**
   - **Время до автоматического отключения секций – 3M**
   - **detach-action – Автоудаление отключенных секций**
   - **Время до удаления отключенных секций – 4M**
2. Сохранить и применить значения параметров конфигурации, нажав кнопки **Сохранить** и **Применить**.

3. Переключиться на работу от имени пользователя **dozor**, выполнив следующую команду:

   # su - dozor

4. Перейти в каталог **/opt/dozor/smap/schema/liquibase**, выполнив следующую команду:

   $ cd /opt/dozor/smap/schema/liquibase/

5. Запустить обновление схемы БД, выполнив команду:

   $ ./update-db.sh -con <идентификатор_соединения>

   где **x** – идентификатор соединения с базой данных.

6. Выполнить следующую команду:

   $ bash /opt/dozor/smap/schema/pgsql/shell/part-control -con <идентификатор_соединения>

   где **x** – идентификатор соединения с базой данных.

Автоматическая архивация позволяет создавать резервные копии отключенных значимых секций и, таким образом, предотвратить потерю информации в БД архива и увеличить свободное место в БД архива. Данный механизм реализован в соответствии со следующими принципами:

- Наиболее старые секции отсоединяются через интервал времени, указанный в значении параметра **Время до автоматического отключения секций**.
- Через интервал времени, указанный в значении параметра **Время до архивации отключенных секций**, происходит резервное копирование отключенных секций в каталог, указанный в значении параметра **Путь к области долговременного хранения**. В качестве значения параметра **Путь к области долговременного хранения** системный администратор также может выбрать устройство, ранее смонтированное в ОС.
- В момент резервного копирования секции файлу архива присваивается имя вида **part_YYYYMMDD.dump**. Шифр вида **YYYYMMDD** соответствует дате начала секции. Например, если дата начала секции – 5 августа 2017 года, то архиву будет присвоено имя **part__20170805.dump**.
- После выполнения резервного копирования отключенные секции удаляются из БД архива.

Для настройки автоматической архивации секций необходимо перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** и выполнить следующие действия:

1. В секции **Схемы соединений с БД** задать значения следующих параметров:
   - **Интервал опережения при создании секций** – **8D**
   - **Автоматическое отключение секций** – **используется**
   - **Время до автоматического отключения секций** – **3M**

- **detach-action – Автоархивирование отключенных секций**
- **Время до архивации отключенных секций – 4M**
- **Путь к области долговременного хранения – /data/backups**

2. Сохранить и применить значения параметров конфигурации, нажав кнопки **Сохранить** и **Применить**.
3. Переключиться на работу от имени пользователя **dozor**, выполнив следующую команду:

   # su - dozor
4. Перейти в каталог **/opt/dozor/smap/schema/liquibase**, выполнив следующую команду:

   $ cd /opt/dozor/smap/schema/liquibase/
5. Запустить обновление схемы БД, выполнив команду:

   $ ./update-db.sh -con <идентификатор_соединения>

   где **x** – идентификатор соединения с базой данных.
6. Выполнить следующую команду:

   $ bash /opt/dozor/smap/schema/pgsql/shell/part-control -con <идентификатор_соединения>

   где **x** – идентификатор соединения с базой данных.

Внимание!

*Настройки параметров конфигурации недостаточно для выполнения автоматического отключения, удаления и архивации секций. Для использования возможности автоматического управления секциями следует обеспечить регулярное (ежедневное) выполнение скрипта **part-control** с помощью планировщика **cron**.*

Для добавления в **crontab** записи об автоматическом управлении секциями необходимо выполнить следующие действия:

1. Открыть расписание планировщика одним из способов:
   - Выполнить команды:

     # su - dozor

     $ crontab -e
   - Выполнить команду:

     # crontab -u dozor -e
2. Нажать клавишу **i** и добавить в расписание после комментария **### End: schedule of crontab entry ###** следующую строку (пример запуска раз в сутки в 02:10:00):

```
10 02 * * * bash /opt/dozor/smap/schema/pgsql/shell/part-control -con <conn>
```

где **<conn>** – имя схемы соединения с БД, определённое в настройках соединения (например, **db-conn-2**).

3. Нажать клавишу **Esc**, ввести **:wq!** и нажать **Enter**.

6.12.5.3. Работа с секциями с помощью CLI

Для работы с секциями БД PostgreSQL в CLI используются следующие скрипты:

- **show-status** – вывод на экран информации о состоянии секций.

  Скрипт использует следующие ключи:

  - **-con** – используется совместно с именем схемы соединения с БД.
  - **-a** – показать дополнительную информацию.
  - **-c** – показать отключённые ограничения.
  - **-d** – показать файлы секции.
  - **-i** – показать неиспользуемые индексы.
  - **-m** – показать историю (можно указать количество последних процедур, например, **show-status -m 5 -con db-conn-4**).
  - **-o** – показать сессии, открытые пользователем схемы.
  - **-p** – показать информацию о секциях.
  - **-e** – показать информацию о сегментах.
  - **-s** – показать информацию об использовании дискового пространства.
  - **-t** – показать информацию о табличном пространстве.
  - **-u** – показать информацию о состоянии обновления таблиц.
  - **-x** – отображать секции контекстного индекса.
  - **-xsize** – отображать информацию о размере контекстного индекса.
  - **-xstat** – показать статистику по контекстному индексу.
  - **-n <номер секции>** – указать номер секции.
  - **-v** – включить вывод отладочной информации.

- **add-partition** – добавление новых секций.

  Скрипт использует следующие ключи:

  - **-d** – использовать настройки секционирования, заданные в схеме соединения с БД.

- **-l** – интервал до окончания последней секции, когда создается новая. Задаётся в формате **<NW>**,

  где:

  - **N** – количество недель, заданное в виде простого числа;
  - **W** – неделя.

- **-p** – периодичность создаваемых секций в неделях. Задаётся в формате **<N>**, где **N** – количество, заданное в виде простого числа.
- **-con** – имя схемы соединения с БД.

- **attach-partition** – подключение ранее отключённых секций.

  Скрипт использует следующие ключи:

  - **-w** – подключить секции в режиме чтения и записи. Если этот ключ не указывать, секция будет подключена только для чтения.
  - **-p** – приоритет построения контекста в случае обновления секций. Принимает значения от 0 (высший приоритет) до 100 (низший приоритет).
  - **-k** – разорвать все сессии подключения к БД перед подключением секции.
  - **-i** – пропустить секции, при подключении которых возникла ошибка.
  - **-con** – имя схемы соединения с БД.

  Внимание!

  *После подключения секций необходимо перезапустить сервис индексации данных (**indexer-ng**) на всех узлах. Подробнее об управлении процессами см. раздел 5.5.1.*

- **detach-partition** – отключение секции.

  Скрипт использует следующие ключи:

  - **-k** – разорвать все сессии подключения к БД перед отключением секции.
  - **-con** – имя схемы соединения с БД.
  - **-n** – имя отключаемой секции. Этот ключ можно указать несколько раз.

- **part-control** – автоматическое отключение секции.

  Скрипт использует следующие ключи:

  - **-con** – имя схемы соединения с БД.
  - **--skip-es** – отключить попытки соединения с сервисом **opensearch**, используется совместно с ключом **-con**.

Необязательный ключ – если не указывать, при выполнении скрипта будут происходить попытки подключения к **opensearch**.

- **move-section** – перемещение отключённой секции в указанный каталог.

  Скрипт использует следующие ключи:

  - **-n** – имя перемещаемой секции. Этот ключ можно указать несколько раз.
  - **-d** – путь к каталогу на сервере БД, в который будут перемещены данные секции.
  - **-f** – путь к файлу архива с расширением **dump**, используется совместно с ключом **-con**.
  - **-r** – переименовать файлы данных секции после перемещения.
  - **-l** – вывести на экран список файлов секции.
  - **-S** – вывести на экран список перемещаемых секций.
  - **-con** – имя схемы соединения с БД.

- **drop-section** – удаление ранее отключённой секции.

  Скрипт использует следующие ключи:

  - **-k** – разорвать все сессии подключения к БД перед удалением секции.
  - **-con** – имя схемы соединения с БД.
  - **-n** – имя удаляемой секции. Этот ключ можно указать несколько раз.

6.12.6. Резервное копирование данных средствами PostgreSQL

СУБД PostgreSQL позволяет выполнять как полное, так и частичное резервирование данных. Резервное копирование выполняется с помощью скрипта **pg_dump**, которому передаются имя БД и параметры командной строки, управляющие работой скрипта.

Формат команды для проведения резервного копирования БД СУБД PostgreSQL выглядит следующим образом:

$ pg_dump [ключи] <dbname>

где **<dbname>** является обязательным параметром и определяет имя БД.

Помимо ключей общего назначения, доступны следующие ключи:

-f <out_file>, **--file <out_file>** – задание файла, в который сохраняется архив с резервной копией (если ключ не задан, данные выводятся на экран);

F <формат> – определение формата архивного файла, где **<формат>** может принимать значения:

- **t** – создание TAR-архива;
- **c** – создание архива **.tar.gz** (файл **.tar**, сжатый в формат **gzip**);

- **p** – создание архива в виде незашифрованного текстового формата. Этот формат используется по умолчанию, если не указан какой-либо другой.

-b, **--blobs** – включение в архив больших двоичных объектов (BLOB) наряду с обычными данными БД;

-C, **--create** – включение в архив команды для создания схемы БД;

-o, **--oids** – включение в архив идентификаторов объектов (OID).

Скрипт необходимо запускать от имени пользователя **dozor**.

Для создания полной копии БД KEO DLP с именем **<dbname>** используется команда следующего вида:

$ pg_dump -b -C -F <формат> -o -f <out_file> <dbname>

Аналогичным образом можно выполнять резервное копирование отдельных таблиц, имена которых указываются в командной строке в ключе **-t**.

6.12.7. Восстановление резервной копии данных средствами PostgreSQL

СУБД PostgreSQL позволяет выполнять как полное, так и частичное восстановление зарезервированных данных.

Восстановление резервной копии выполняется с помощью скрипта **pg_restore** с параметрами командной строки, аналогичными тем, которые использовались при запуске **pg_dump** (см. раздел 6.12.6).

Внимание!

*Форматы, указанные параметром **–F**, должны совпадать. Скрипт **pg_restore** используется только для форматов архива **.tar** и **.tar.gz**. Архивы в незашифрованном текстовом формате передаются СУБД в качестве входного файла.*

Формат команды для восстановления резервной копии БД СУБД PostgreSQL выглядит следующим образом:

$ pg_restore [ключи] <out_file>

где **<out_file>** является обязательным параметром и определяет имя файла с резервной копией.

Скрипт необходимо запускать от имени пользователя **dozor**.

Дополнительные ключи:

-c, **--clean** – используется для повторной инициализации существующей БД, позволяет не производить предварительное удаление и создание пустой БД с таким же именем;

-d <имя БД>, **--dbname <имя БД>** – имя БД, к которой следует подключиться перед восстановлением. Если БД с таким именем не существует, то необходимо предварительно создать пустую БД.

Для полного восстановления БД KEO DLP в БД с именем **<dbname>** используется команда следующего вида:

$ pg_restore -c -F <тип> -o -d <dbname> <out_file>

Аналогичным образом можно выполнять восстановление отдельных таблиц, имена которых указываются в командной строке в ключе **–t**. Если ключ **–t** указан без значения, восстанавливаются все таблицы БД.

6.12.8. Работа с параметрами схемы

Скрипт **config-manager** предназначен для:

- применения настроек секционирования БД;
- получения информации о параметрах схемы БД и изменения их значений.

Для выполнения скрипта **config-manager** необходимо выполнить следующие действия:

1. Переключиться на работу от имени пользователя **dozor**, выполнив команду:

   # su - dozor

2. Запустить интерпретатор команд **shell** (выполняется от имени пользователя **dozor**):

   $ /opt/dozor/bin/shell

3. Запустить следующую команду (выполняется от имени пользователя **dozor**):

   $ config-manager [ключи] -con <идентификатор_соединения>

Доступны следующие ключи:

- **a** – применяет настройки секционирования БД;
- **l** – выводит список параметров схемы;
- **g <параметр>** – выводит значение указанного параметра;
- **s <параметр> <значение>** – позволяет изменить текущее значение указанного параметра на заданное.

Внимание!

Не рекомендуется изменять параметры схемы БД, установленные по умолчанию, без соответствующей инструкции от команды разработчиков.

Ниже приводятся примеры использования скрипта.

6.12.8.1. Применение настроек секционирования БД

Для применения настроек секционирования БД необходимо выполнить следующие действия:

 # su - dozor

$ /opt/dozor/bin/shell

$ config-manager -a -con <идентификатор_соединения>

На экран выводится примерно следующая информация:

```
Database Configuration Manager

partitioning            => y
part_period              => 1
part_start              => 2
adv_time                 => 2D
use_auto_detach          => n
detach_time              =>
detach_action            =>
drop_time               =>
archive_time             =>
archive_dir             =>
sequence_pool_size       =>
partitioning            => yes
part_period              => 1
part_start              => 2
adv_time                 => 2D
use_auto_detach          => no
detach_time              => 3M
detach_action            => manual
drop_time               => 4M
archive_time             => 4M
archive_dir             => /data/backups

INFO: Configuration parameters uploaded to database.
```

6.12.8.2. Получение списка параметров схемы

Для получения списка параметров схемы необходимо выполнить следующие действия:

 # su - dozor

$ /opt/dozor/bin/shell

$ config-manager -l -con <идентификатор_соединения>

На экран выводится примерно следующая информация:

```
      Keys       |     Values     |                        Comment
-------------------+----------------+-----------------------------------------------------
adv_time          | 2D             | Добавление секций за указанное время до окончания последней
archive_dir       | /data/backups  | Каталог для хранения архивных файлов секций
archive_time      | 4M             | Время до автоматической архивации и удаления секции
detach_action     | manual         | Действия, выполняемые при отключении секции
detach_time       | 3M             | Время до автоматического отключения секции
drop_time         | 4M             | Время до автоматического удаления секции
partitioning      | yes            | Использование секционирования (y/n)
part_period       | 1              | Период секционирования
part_start        | 2              | Количество создаваемых при инсталляции секций
```

```
use_auto_detach    | no           | Вкл/выкл автоматическое отключение секций
version            | 7.6.0.448.0  | Версия схемы базы данных
```

6.12.8.3. Получение значения параметра схемы

Для получения значения параметра схемы необходимо выполнить следующие действия:

 # su - dozor

$ /opt/dozor/bin/shell

$ config-manager -g use_auto_detach -con <идентификатор_соединения>

На экран выводится примерно следующая информация:

```
Database Configuration Manager
 partitioning             => y
 part_period               => 1
 part_start               => 2
 adv_time                  => 2D
 use_auto_detach           => n
 detach_time               =>
 detach_action             =>
 drop_time                 =>
 archive_time              =>
 archive_dir               =>
use_auto_detach = "no"
```

6.12.8.4. Изменение значения параметра схемы

Для изменения значения параметра схемы необходимо выполнить следующие действия:

 # su - dozor

$ /opt/dozor/bin/shell

$ config-manager -s use_auto_detach yes -con <идентификатор_соединения>

На экран выводится примерно следующая информация:

```
Database Configuration Manager
 partitioning             => y
 part_period               => 1
 part_start               => 2
 adv_time                  => 2D
 use_auto_detach           => y
 detach_time               =>
 detach_action             =>
 drop_time                 =>
 archive_time              =>
 archive_dir               =>
```

Внимание!

После изменения параметров схемы БД необходимо применить настройки секционирования, выполнив команду ***$ config-manager -a -con <идентификатор_соединения>*** *(см. раздел 6.12.8.1).*

6.12.9. Поддержка декларативного секционирования средствами PostgreSQL

Декларативное секционирование используется для увеличения производительности и упрощения обслуживания БД архива под управлением СУБД PostgreSQL версии 11 и выше. Для конвертации БД с табличным наследованием в БД, поддерживающее декларативное секционирование, следует выполнить действия:

1. Подключиться по протоколу SSH к узлу, на котором функционирует БД архива с табличным наследованием.
2. Получить информацию о версии СУБД PostgreSQL. Для этого выполнить одну из команд:

   # cat /data/base/<archive_db>/PG_VERSION

   или

   # psql -p 5435 -h localhost -U dozor -d <archive_db>

   где **<archive_db>** – имя БД архива.
3. Переключиться на работу от имени пользователя **dozor**, выполнив команду:

   # su - dozor
4. Загрузить командную оболочку, выполнив команду:

   # /opt/dozor/bin/shell
5. Получить информацию о секциях, выполнив команду:

   $ show-status -p -con <идентификатор_соединения>

   где **db-conn-x** – имя соединения с БД архива, которое поддерживает табличное наследование.

   Пример вывода команды на экран:

```
Тек | НомерСекции    | Статус | Archived |   BegDate  | EndDate      | PartSize
---------+--------------+--------------+------+-----------------+-----------+--------
-->message_20190204 | ATTACHED | No |2019-02-04 |2019-02-18|  440 KB
| message_20190218 | ATTACHED | No | 2019-02-18 | 2019-03-04 | 440 kB
| message_20190304 | ATTACHED | No | 2019-03-04 | 2019-03-18 | 440 kB
| message_20190318 | ATTACHED | No | 2019-03-18 | 2019-04-01 | 440 kB
```

6. Обновить СУБД PostgreSQL в соответствии с разделом 6.12.4.
7. Подключиться к обновленной БД архива, выполнив следующую команду:

$ psql -p <PORT> -h localhost -d <database_name>

где:

- **<PORT>** – порт БД архива;
- **<database_name>** – имя БД архива.

В выводе команды будут следующие предупреждения:

```
psql (9.6.10, сервер 11.1) ПРЕДУПРЕЖДЕНИЕ: psql имеет базовую версию 9.6, а сервер - 11.
Часть функций psql может не работать. Введите "help", чтобы получить справку.
```

В выводе команды будут сообщения, что версия скрипта **psql** – 9.6, а версия СУБД PostgreSQL – 11.

8. Выполнить команду:

   \d+ message

9. Проверить, что в конце вывода есть описание секций в виде блока **Дочерние таблицы**. Данная запись подтверждает, что тип секционирования – наследственный.

   Пример:

   ```
   Дочерние таблицы: message_20190204,
   message_20190218,
   message_20190304,
   message_20190318
   ```

10. На всех узлах, на которых запущены процессы **archiver** и **indexer-ng**, выполнить команду:

    $ dsctl stop indexer-ng archiver

11. Остановить сервис **archive-server** на master-узле, выполнив команду:

    $ dsctl stop archive-server

12. Выполнить команду:

    $ /opt/dozor/smap/schema/pgsql/shell/convert-to-pg11-native-part -con <идентификатор_соединения>

    где **db-conn-x** – имя соединения с БД архива, которое поддерживает табличное наследование. При появлении информации:

    ```
    Are you sure you want to run schema conversion to native partititoning (y/n)
    ```

    Подтвердить продолжение установки, нажав клавишу **y**. При успешном завершении скрипта появится сообщение **Exiting successfully**.

13. Запустить сервис **archive-server** на master-узле, выполнив команду:

    $ dsctl start archive-server

14. На всех узлах, на которых были остановлены процессы **archiver** и **indexer-ng**, выполнить команду:

    $ dsctl start indexer-ng archiver

15. Для проверки состояния БД после преобразования выполнить действия, описанные на шаге **5**.

16. Подключиться к обновленной БД архива, выполнив команду:

    $ /usr/pgsql-11/bin/psql -p <PORT> -h localhost -d <database_name>

    где **<PORT>** – порт БД архива, а **<database_name>** – имя БД архива.

17. Выполнить команду:

    \d+ message

    В конце вывода команды проверить наличие блока **Секции**, например:

    ```
    Секции: message_20190121 FOR VALUES FROM ('201901210000000000') TO
    ('201902040000000000'),
     message_20190204 FOR VALUES FROM ('201902040000000000') TO ('201902180000000000')
    , message_20190218 FOR VALUES FROM ('201902180000000000') TO ('201903040000000000'),

     message_20190304 FOR VALUES FROM ('201903040000000000') TO ('201903180000000000'),
     message_20190318 FOR VALUES FROM ('201903180000000000') TO ('201904010000000000')
    ```

    В выводе появится дополнительная секция, созданная из родительской таблицы. Вместо **Дочерние таблицы** в выводе будет **Секции**. Данная запись свидетельствует о преобразовании таблиц БД в декларативное секционирование.

6.12.10. Расширенное управление БД

Расширенные возможности управления БД предоставляет скрипт **/opt/dozor/bin/dbctl**. Он позволяет запускать, перезапускать, останавливать БД разных сервисов и получать информацию об их статусе.

Формат команды для запуска скрипта:

 # /opt/dozor/bin/dbctl <action> <datadir> <port> <dbname>

где:

- **<action>** – действие, которое требуется совершить
- **<datadir>** – каталог для хранения БД. Значение по умолчанию: **/data/base/dozor/pgsql**. Если не указать, используется значение по умолчанию.
- **<port>** – порт, на котором БД ожидает соединения. Значение по умолчанию: 5434. Если не указать, используется значение по умолчанию.
- **<dbname>** – имя БД. Значение по умолчанию: **dozor**. Если не указать, используется значение по умолчанию.

Доступны следующие действия:

- **start** – запуск заданной БД.
- **stop** – остановка заданной ранее запущенной БД.
- **restart** – перезапуск заданной БД.
- **reload** – применение конфигурации без перезапуска заданной БД.
- **status** – проверка текущего состояния сервера БД PostgreSQL.
- **create** – создание пустой БД без журналирования.

Примечание

Данный ключ используется для создания БД политики фильтрации и БД модуля File Crawler.

- **create-empty** – создание пустой БД.
- **create-data** – создание архивной БД.
- **create-data+part** – создание архивной БД с секционированными таблицами.

Примечание

*При использовании вышеуказанных действий без ключей **datadir**, **port** и **dbname** действия выполняются над БД политики.*

Примеры работы скрипта:

1. Создание архивной БД с секционированными таблицами. Формат команды для запуска скрипта:

   # /opt/dozor/bin/dbctl create-data+part /var/lib/pgsql/9.6/data 5436 dozor5

   В конце вывода команды появятся параметры секционирования, например:

```
Partitioning parameters ...
============================
 PART_DATE=2016-04-01
 PART_PERIOD=1
 PART_START=2
 PART_FIRST=10000
 ADV_TIME=8D
 AUTO_DETACH=no
 DETACH_TIME=3M
 DETACH_ACTION=manual
 DROP_TIME=4M
 ARCHIVE_TIME=4M
 ARCHIVE_DIR=/data/backups

Stop database service ...
```

2. Запуск БД. Формат команды для запуска скрипта:

   # /opt/dozor/bin/dbctl start /var/lib/pgsql/9.6/data

   Появится информация о текущем каталоге БД, например:

```
Using datadir: "/var/lib/pgsql/9.6/data"
Start database service ...
< 2018-04-16 14:40:12.452 MSK > LOG:  redirecting log output to logging collector process
< 2018-04-16 14:40:12.452 MSK > HINT:  Future log output will appear in directory "pg_log"
```

3. Проверка состояния БД. Формат команды для запуска скрипта:
   # /opt/dozor/bin/dbctl status /var/lib/pgsql/9.6/data
   .

   Появится информация о том, что БД запущена, например:

```
Using datadir: "/var/lib/pgsql/9.6/data"
pg_ctl: server is running (PID: 22265)
/usr/pgsql-9.6/bin/postgres "-D" "/var/lib/pgsql/9.6/data"
```

4. Остановка БД. Формат команды для запуска скрипта:
   # /opt/dozor/bin/dbctl stop /var/lib/pgsql/9.6/data
   .

   Появится информация о текущем каталоге БД, например:

```
Using datadir: "/var/lib/pgsql/9.6/data"
Stop database service ...
```

6.12.11. Получение статистической информации о БД архива

Скрипт **show-stats** предназначен для получения статистики о сообщениях в БД архива:

- количество писем по их размерам;
- количество вложений по их размерам;
- количество вложений по их типам;
- количество писем по количеству получателей;
- количество писем по дате и времени получения;
- количество и размер писем по типу и дате и времени получения;
- размеры объектов в схеме БД.

Для использования скрипта удобно (но не обязательно) использовать интерпретатор команд, запускаемый командой:

 # /opt/dozor/bin/shell

При использовании интерпретатора команд скрипт **show-stats** имеет следующий синтаксис запуска:

 # show-stats <actions> [-con <connection name>] [-include_deleted]

Без использования интерпретатора команд скрипт **show-stats** имеет следующий синтаксис запуска:

 # /opt/dozor/smap/schema/oracle/shell/show-stats <actions> [-con <connection name>] [-include_deleted]

Скрипт использует следующие ключи:

- **-con** – имя схемы соединения с БД как оно указано в конфигурации KEO DLP (**db-conn.conf**). Если ключ не указывать – будет использовано имя по умолчанию **db-conn-1**.
- **-m** – количество писем из определенного диапазона размеров, по всем возможным диапазонам. В результате выполнения скрипта с этим ключом на экран будет выведена информация следующего вида:

```
# show-stats -m -con message-db

Show Database Schema Statistic

      Размер письма        | Количество писем
---------------------------+------------------
 From 0 kb to 1 kb         |             298
 From 1 kb to 20 kb        |           68315
 From 20 kb to 50 kb       |            2730
 From 50 kb to 100 kb      |            2596
 From 100 kb to 150 kb     |            1341
 From 150 kb to 300 kb     |            2586
 From 300 kb to 1000 kb    |            2467
 From 1000 kb to 2000 kb   |             679
 From 2000 kb to 5000 kb   |             260
 From 10000 kb to 999999 kb |               3
```

- **-a** – количество вложений из определенного диапазона размеров, по всем возможным диапазонам. В результате выполнения скрипта с этим ключом на экран будет выведена информация следующего вида:

```
# show-stats -a -con message-db

Show Database Schema Statistic

    Размер приложения      | Количество приложений
---------------------------+----------------------
 From 0 kb to 1 kb         |               79811
 From 1 kb to 20 kb        |                4304
 From 20 kb to 50 kb       |                6565
 From 50 kb to 100 kb      |                5985
 From 100 kb to 150 kb     |                3148
 From 150 kb to 300 kb     |                4798
 From 300 kb to 1000 kb    |                6476
 From 1000 kb to 2000 kb   |                1381
 From 2000 kb to 5000 kb   |                 408
 From 5000 kb to 10000 kb  |                   7
 From 10000 kb to 999999 kb |                  8
```

- **-t** – количество вложений определенного типа, по всем имеющимся типам. В результате выполнения скрипта с этим ключом на экран будет выведена информация следующего вида:

```
# show-stats -t -con message-db

Show Database Schema Statistic

                    Тип приложения                    | Количество приложений
------------------------------------------------------------------------+----------------------
 TEXT/PLAIN                                          |              81427
 MULTIPART/MIXED                                       |              13055
 IMAGE/JPEG                                          |               3751
 IMAGE/VND.DWG                                         |               3178
 APPLICATION/VND.MS-EXCEL                                        |               2722
 APPLICATION/PDF                                       |               2395
 APPLICATION/MSWORD                                            |               2281

APPLICATION/VND.OPENXMLFORMATS-OFFICEDOCUMENT.WORDPROCESSINGML.DOCUMENT
 |               1942
 APPLICATION/X-COMPRESSED-RAR                                        |               1718
 IMAGE/PNG                                           |               296
 IMAGE/TIFF                                          |               111
 MULTIPART/FORM-DATA                                           |                  8
 IMAGE/GIF                                           |                  4
 IMAGE/VND.DJVU                                        |                  2
 APPLICATION/X-COMPRESSED-ZIP                                        |                  1
```

- **-r** – количество писем из определенного диапазона количества получателей, по всем возможным диапазонам. В результате выполнения скрипта с этим ключом на экран будет выведена информация следующего вида:

```
# show-stats -r -con message-db

Show Database Schema Statistic

 Количество получателей | Количество писем
------------------------+------------------
 From 1 to 2            |           17,822
 From 3 to 4            |              462
 From 5 to 9            |               87
 From 10 to 19          |                4
```

- **-1** – количество писем по годам, месяцам, дням и часам. Статистика по годам, месяцам и дням указывается один раз в первой строке с соответствующим годом, месяцем или днём. В результате выполнения скрипта с этим ключом на экран будет выведена информация следующего вида:

```
# show-stats -1 -con message-db

Show Database Schema Statistic

   date hh24    | y_cnt | m_cnt | d_cnt | h_cnt
----------------+-------+-------+-------+-------
 2018-03-13 15 |    26 |    26 |     8 |     1
 2018-03-13 17 |       |       |       |     1
```

```
2018-03-13 18 |      |      |      |   6
2018-03-14 02 |      |      |   10 |   1
2018-03-14 09 |      |      |      |   1
2018-03-14 10 |      |      |      |   3
2018-03-14 11 |      |      |      |   1
2018-03-14 12 |      |      |      |   1
2018-03-14 13 |      |      |      |   2
2018-03-14 23 |      |      |      |   1
2018-03-24 11 |      |      |    8 |   5
2018-03-24 12 |      |      |      |   3
2019-06-23 07 | 81182 |  4410 |   66 |   8
2019-06-23 08 |      |      |      |   7
2019-06-23 09 |      |      |      |   7
```

- **-2** – количество и суммарный размер сообщений по каналам коммуникации и дате. Заголовки столбцов имеют следующие значения:
  - **dd** – дата: год, месяц, день.
  - **email** – почтовые сообщения.
  - **im** – мгновенные сообщения (мессенджеры).
  - **removable** – сообщения о действиях со съемными носителями информации.
  - **keylog** – перехваты нажатий клавиш.
  - **network** – перехват сетевого трафика.
  - **endpoint** – сообщения от агентов на АРМ сотрудников организации.
  - **file** – перехваты файлов из ресурсов с разделяемым доступом.
  - **printjob** – перехват заданий на печать.
  - **all** – общая статистика сообщений по всем каналам коммуникации за определенную дату.

  В результате выполнения скрипта с этим ключом на экран будет выведена информация следующего вида:

```
# show-stats -2 -con message-db

Show Database Schema Statistic

   dd   |   email    |     im     | removable |   keylog   |  network   |  endpoint  |    file    | printjob
   |    all
--------+------------+------------+-----------+------------+------------+------------+------------+-----------

 20180313 |     2/114 kB | 5/3926 bytes |           |           |     1/52 kB |           |           |
|    8/170 kB
 20180314 |     4/587 kB |           |     1/56 kB |           |     1/336 kB |     1/56 kB |     2/388 kB |
 1/56 kB |   10/1481 kB
 20180324 |           |           |           | 8/6728 bytes |           |           |           |           | 8/6728
 bytes
 20190623 |   66/2750 kB |           |           |           |           |           |           |           |   66/2750
```

```
kB
20190624 |   897/40 MB |          |          |          |          |          |          |  897/40
MB
20190625 |   885/33 MB |          |          |          |          |          |          |  885/33
MB
```

- **-s** – статистика объектов схемы БД архива. В результате выполнения скрипта с этим ключом на экран будет выведена информация следующего вида:

```
# show-stats -s -con message-db

Show Database Schema Statistic

     Parameter       | Value
---------------------+----------
Mailbase size        | 4251 MB
DB size              |   11 GB
Overhead             |  2.73
Percent of lobs      | 92.00 %
Percent of originals |  1.15 %
Percent of bodies    |  1.23 %
```

  Параметры таблицы имеют следующие значения:

  - **Mailbase size** – суммарный размер исходных сообщений.
  - **DB size** – полный физический размер объектов KEO DLP в БД архива.
  - **Overhead** – отношение значения параметра **DB size** к **Mailbase size** (во сколько раз общий размер объектов БД архива больше суммарного размера исходных сообщений).
  - **Percent of lobs** – отношение физического размера таблицы с исходными сообщениями к полному размеру объектов KEO DLP в БД архива.
  - **Percent of originals** – отношение размера таблицы MESSAGE (и её индексов) к полному размеру объектов KEO DLP в БД архива (доля объема БД архива, занимаемая таблицей с исходными сообщениями).
  - **Percent of bodies** – отношение размера таблицы MIME_PART (и её индексов) к полному размеру объектов KEO DLP в БД архива (доля объема БД архива, занимаемая таблицей с текстами, извлеченными из сообщений).

- **-include_deleted** – дополнительный необязательный ключ, при использовании которого в статистику будет включена информация об удаленных сообщениях. Без этого ключа статистика приводится только об актуальных сообщениях в БД архива.

6.12.12. Формирование отчетов о работе БД средствами PostgreSQL

Отчеты о работе сервера PostgreSQL формируются в процессе создания БД и продолжают создаваться автоматически в течении всей работы БД.

Для хранения отчетов используется каталог **<каталог>/log**, где **<каталог>** – каталог, в котором создается БД (значение по умолчанию **/data/base/smap**).

В этом каталоге создаётся журнальный файл **postgresql.log.<день_недели>**, в который записываются все сообщения сервера PostgreSQL в течение суток.

Для следующих суток сервер создаёт новый файл, в названии которого указывает соответствующий день недели.

По окончании недели файл с текущим днем недели в названии файла перезаписывается. Таким образом, в каталоге **log** всегда хранятся отчеты за последние 7 суток.

6.13. Сопровождение архива сообщений

Действия над сообщениями в архиве (отправка, установка пометок, удаление и т.д.) выполняются сервером действий. Сервер действий функционирует на узлах, которым назначена роль **Вспомогательный сервер действий** или **Сервер действий подкластера**.

Примечание

Подробнее о назначении ролей узлам см. в разделе 5.3.

Параметры сервиса действий настраиваются в секции **Выполнение действий над сообщениями в архиве** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**). Подробнее о работе сервиса действий см. раздел 6.13.1.

Кроме того, для сопровождения архива сообщений используются скрипты поиска, удаления, экспорта и импорта сообщений.

Скрипты, экспортирующие и удаляющие сообщения, оперируют двумя понятиями: идентификатор сообщения и выборка сообщений.

Выборка сообщений представляет собой набор сообщений, соответствующих определённому запросу к архиву.

Идентификатор сообщения может быть получен путём выполнения поискового запроса. Запросы хранятся в БД и создаются пользователем в веб-интерфейсе KEO DLP.

Например, если требуется удалить набор сообщений за определённый месяц, то сначала необходимо создать запрос, выполняющий такую выборку, а затем выполнять действия над этой выборкой.

Все скрипты сопровождения архива поддерживают следующие ключи общего назначения:

- **-h**, **--help** – вывод подсказки с описанием аргументов командной строки для данного скрипта;
- **-v**, **--verbose** – вывод сообщений о действиях, выполняемых скриптом;
- **-d**, **--debug** – вывод отладочной информации.

В случае нормального завершения своей работы скрипты возвращают код 0, при ошибках – 1.

6.13.1. Выполнение действий над сообщениями с помощью сервера действий

Сервер действий отвечает за выполнение действий над сообщениями в архиве. Выполнить действия над сообщением можно в интерфейсе KEO DLP либо с помощью скрипта **querytool** (см. раздел 6.13.3). В первом случае следует выбрать сообщения в результатах поиска и нажать соответствующую кнопку.

Примечание

Подробное описание действий над сообщениями приведено в документе Руководство пользователя.

Информация о действии передается на главный сервер действий, функционирующий на master-узле. Полный список сообщений, над которыми требуется выполнять действие, либо передается серверу действий с интерфейса (в случае выбора конкретных сообщений), либо составляется сервером действий в результате выполнения запроса OpenSearch (в случае выбора всех результатов быстрого поиска), либо загружается из сервера архива (в случае выбора всех результатов расширенного поиска). Полученный список сообщений разбивается на блоки по 1000 сообщений (задания). Все задания размещаются в очереди метаданных, которая является общей для всех узлов кластера KEO DLP. Все очереди организованы в БД сервера действий. Выполнением заданий занимаются все экземпляры сервера действий, функционирующие на узлах с ролями **Вспомогательный сервер действий** и **Сервер действий подкластера**. В каждом сервере действий несколько потоков или тредов (параметр **Количество тредов, выполняющих действия**) забирают задания из очереди и выполняют их. Информация о выполнении каждого задания (количество успешно обработанных сообщений, а также ошибки, возникшие при обработке остальных сообщений) также передается на главный сервер действий через очередь. Действие считается выполненным, когда выполнены все составляющие его задания.

В сервере действий реализован механизм, выполняющий действия с небольшим количеством объектов (далее – "быстрые" действия) в отдельной очереди. Это количество указывается в значении параметра **Ограничение на количество объектов для быстрых действий** и по умолчанию равно 25. Когда сервер действий получает новое действие, количество объектов (сообщений, событий, MIME-частей и т.д.) сравнивается с этим параметром.

Если количество объектов не превышает указанное в параметре значение, задание размещается в отдельной очереди "быстрых" действий. Ее обрабатывают отдельные потоки, количество которых задается в значении параметра **Количество тредов, выполняющих быстрые действия**. В противном случае задание обрабатывается в основной очереди.

6.13.2. Просмотр пометок сообщения

Для просмотра пометок сообщений используется скрипт **message-tool.py**. С помощью этого скрипта можно вывести список пометок, установленных на сообщение с указанным идентификатором ID. Кроме того, скрипт позволяет определить идентификатор vID сообщения по его идентификатору в базе данных и наоборот.

Примечание

Идентификатор ID – это идентификатор сообщения в БД архива. Он может измениться, например, при переносе сообщения из одной базы данных в другую. А идентификатор vID – это идентификатор сообщения, присваиваемый ему еще до этапа фильтрации и помещения в архив. Этот идентификатор остается неизменным для сообщения.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд **shell**, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат команды для запуска скрипта:

$ message-tool.py <ключ> <vID>

где:

- **ключ** – один из доступных ключей, определяющих конкретное действие, выполняемое с помощью скрипта. Список доступных ключей приведен ниже;
- **vID** – идентификатор сообщения. Можно указывать несколько идентификаторов для получения списка пометок, установленных на каждое из указанных сообщений.

Ключи, определяющие настройки доступа:

- **-H <имя узла/IP>**, **--host <имя узла/IP>** – имя или IP-адрес узла с сервисами **archive-server**/**action-server**. Значение по умолчанию: **127.0.0.1**.
- **-P <порт>**, **--port <порт>** – порт узла с сервисом **archive-server**. Значение по умолчанию: 3000.
- **-p <порт>**, **--as-port <порт>** – порт узла с сервисом **action-server**. Значение по умолчанию: 3001.
- **-w <имя узла/IP>**, **--web-host <имя узла/IP>** – имя или IP-адрес сервера веб-интерфейса. Значение по умолчанию: **127.0.0.1**.
- **-z <порт>**, **--web-port <порт>** – порт сервера веб-интерфейса. Значение по умолчанию: 8443.
- **-U <имя пользователя>**, **--login-user <имя пользователя>** – имя учетной записи пользователя. Значение по умолчанию: **superadmin**.
- **-L password**, **--login-password password** – пароль пользователя. Значение по умолчанию: **ask**.
- **-M, --no-multiarchive** – не использовать API для работы с подкластерами.

Обязательные ключи:

- **-G**, **--get-labels** – вывести список пометок для указанного сообщения.

- **-s <тип пометки>**, **--set-label <тип пометки>**– установить на сообщение пометку указанного типа, используется совместно с ключом **-D**.
- **-r <тип пометки>**, **--remove-label <тип пометки>** – удалить из сообщения пометку указанного типа, используется совместно с ключом **-D**.
- **-S <профиль отправки>**, **--send <профиль отправки>** – отправить сообщение используя идентификатор профиля отправки.
- **-v**, **--get-vid** – определить и вывести на экран идентификатор vID для сообщения с указанным идентификатором ID.
- **-i**, **--get-id** – определить и вывести на экран идентификатор ID для сообщения с указанным идентификатором vID.
- **-b**, **--get-body** – загрузить тело сообщения (имя файла с его содержимым) на жесткий диск, используется совместно с ключом **-o**.
- **-u**, **--get-struct** – загрузить структуру сообщения на жесткий диск.
- **-a**, **--get-attachments** – загрузить вложения сообщения на жесткий диск, используется совместно с ключом **-o**.
- **-n <описание>**, **--send-notification <описание>** – отправить уведомление в формате **<ИД шаблона уведомления>:<ИД профиля отправки>:<адреса эл. почты>**.
- **-R <описание>**, **--refilter <описание>** – выполнить перефильтрацию сообщений, описание указывается в формате **<имя головного набора правил>:<действие>**. Возможны два варианта действий:
  - **archive** – выполнить повторное архивирование;
  - **send** – выполнить повторную отправку.

Необязательные ключи:

- **-D <описание>** – добавить описание к пометке, используется совместно с ключами **-s** и **-r**.
- **-f <имя файла>** – считать список идентификаторов из указанного файла.
- **-q <ID>**, **--query <ID>** – получить список vID для сообщения/сообщений из запроса с указанным идентификатором. Чтобы получить запросы, необходимо запустить скрипт querytool с ключами **-l** и **-u** (см. раздел 6.13.3).
- **-F <json-запрос>**, **--find <json-запрос>** – получить список vID для сообщения/сообщений из запроса к **webserver**.
- **-o dir**, **--out-dir dir** – путь к каталогу, в котором хранятся тела/вложения сообщений, используется совместно с ключами **-a** и **-b**.
- **-c**, **--create-subdir** – создавать подкаталоги в каталоге с вложениями сообщений, используется совместно с ключом **-a**.
- **-t email**, **--to email** – адрес получателя сообщения. Можно указывать несколько раз.

- **-h**, **--help** – вывести на экран справочную информации об использовании скрипта.

Примеры использования скрипта:

1. Загрузка тел сообщений из поискового запроса в каталог **<dir>** (формат команды для запуска скрипта – **message-tool.py -M -q 269dcdcc-cc9d-49a6-adce-8b7b25f2c68b -b -o /tmp/ms-tool-test/**):

```
Fetching ids from query 269dcdcc-cc9d-49a6-adce-8b7b25f2c68b (4)
Downloading 18c27da0-7a07-11e8-a7c7-005056880378 to
/tmp/ms-tool-test/18c27da0-7a07-11e8-a7c7-005056880378.eml
Downloading ac161f74-7a09-11e8-8a81-005056880378 to
/tmp/ms-tool-test/ac161f74-7a09-11e8-8a81-005056880378.eml
Downloading 6f9b153c-7a08-11e8-b9e9-005056880378 to
/tmp/ms-tool-test/6f9b153c-7a08-11e8-b9e9-005056880378.eml
```

2. Загрузка вложений сообщений из поискового запроса в каталог **<dir>** (формат команды для запуска скрипта – **$ message-tool.py -M -q 269dcdcc-cc9d-49a6-adce-8b7b25f2c68b -a -o /tmp/ms-tool-attach/**):

```
Fetching ids from query 269dcdcc-cc9d-49a6-adce-8b7b25f2c68b (5)
18c27da0-7a07-11e8-a7c7-005056880378:
Downloading part 15 to /tmp/ms-tool-attach/Выписка_реестр.xlsx (124.8 Kb)
fdd0e04c-7a09-11e8-9859-005056880378:
Downloading part 15 to /tmp/ms-tool-attach/YAzueki_programmirovaniya.pdf (1.4 Mb)
ac161f74-7a09-11e8-8a81-005056880378:
Downloading part 15 to /tmp/ms-tool-attach/buhbalans.docx (29.1 Kb)
6f9b153c-7a08-11e8-b9e9-005056880378:
Downloading part 15 to /tmp/ms-tool-attach/ПроектДоговора-ТехнЗадание.doc (146 Kb)
```

6.13.3. Удаление и экспорт сообщений из БД архива

Для удаления и экспорта сообщений из БД архива по заранее сформированным поисковым запросам используется скрипт **querytool**.

Внимание!

Запуск скрипта возможен только на master-узле.

Формат команды для запуска скрипта **querytool**:

 # /opt/dozor/bin/querytool [options]

Доступны следующие ключи:

- **-u, --user <username>** – имя учётной записи пользователя KEO DLP, которому принадлежит поисковый запрос.
- **-l, --list-queries** – вывести на экран список поисковых запросов указанного пользователя. Работает в территориально-распределённом режиме вместе с ключом **-u, --user <username>**.

- **-d, --delete <uuid>** – удалить все сообщения, удовлетворяющие поисковому запросу с указанным UUID.
- **-e, --export <uuid>** – экспортировать все сообщения, удовлетворяющие поисковому запросу с указанным UUID. Работает вместе с ключами **-m, ----exported-messages-format <value>** и **-u, --user <username>**. Сообщения экспортируются в каталог **/data/spool/dozor/actions**.
- **-f, --download-files** – выгружать экспортированные сообщения в виде файлов в текущий каталог. Работает вместе с ключом **-e, --export <uuid>**.
- **-M, --not-multi** – не использовать API для работы с подкластерами.
- **-m, --exported-messages-format <format_value>** – формат экспортированных сообщений. Поддерживаются значения **mbox** и **eml**. Работает вместе с ключом **-e, --export <uuid>**.
- **--help** – вывести на экран справочную информации об использовании скрипта.

Примеры использования скрипта:

1. Вывод на экран поисковых запросов указанного пользователя (формат команды для запуска скрипта – **/opt/dozor/bin/querytool -l -u <username>**):

```
Name                          | ID
Военный билет                 | 030d9a34-952a-448e-8280-2503ac5da57d
Акт о приемке                 | 0c53cec3-1458-4085-8cf1-ee749e177c8c
Кредитный отчет               | 0d6999b9-55b3-44e2-bb62-c49bee38cb78
Производственный регламент    | 123011d9-cfed-4905-97ab-8da2519a7ddf
Штатное расписание            | 233671d2-5a7d-47d1-b8f3-9b66ab53a307
Протокол совещаний            | 2bc10d58-20f7-405c-9a18-df902765878c
Форма НДФЛ                    | 2d96e63e-3d9f-4565-9778-b3911ce65902
```

2. Чтобы экспортировать все сообщения, удовлетворяющие поисковому запросу с указанным UUID, необходимо выполнить следующие действия:

   a. Запустить скрипт с ключами **-e**, **-m**, **-u**. Формат команды для запуска скрипта – **/opt/dozor/bin/querytool -e <UUID> -m <format_value> -u <username>**.

   В случае успешного завершения экспорта на экран будут выведены следующие данные:

```
15:37:04.860 [main] INFO  ru.solarsecurity.QueryTool - Finished export:
   Action: 856be6a8-3528-4714-b6b0-26cde72020e4
   Job: 37e67b0e-15e4-4f28-8515-79d2754fd910
   Status: done
   Result: {"port":3001,"filename":
"dozor_export_dozor_37e67b0e-15e4-4f28-8515-79d2754fd910.zip",
"hostname":"tt09.isim.local","messages":
[{"id":"12b91e0c-2e83-11e8-a25f-0050568844c4","status":"done"},
{"id":"0da47af0-2e84-11e8-a29f-0050568844c4","status":"done"},
{"id":"13093082-2e96-11e8-8df1-0050568844c4","status":"done"},
{"id":"6f3027c6-2e8c-11e8-ba45-0050568844c4","status":"done"},
{"id":"5019e900-2e85-11e8-9cc4-0050568844c4","status":"done"},
{"id":"743e85d8-2e8b-11e8-8d64-0050568844c4","status":"done"},
{"id":"da6b6256-2e93-11e8-ada3-0050568844c4","status":"done"},
```

{"id":"5a5e6434-2e96-11e8-8b33-0050568844c4","status":"done"}]}
Errors:
Params:

b. Выполнить проверку экспорта сообщений с помощью команды CLI **ls -lah /data/spool/dozor/actions**. В результате выполнения команды информация о сообщениях будет выведена на экран:

```
-rw-r--r-- 1 dozor dozor 698K Mar 23 15:37
dozor_export_dozor_37e67b0e-15e4-4f28-8515-79d2754fd910.zip
```

3. Чтобы удалить все сообщения из архива, удовлетворяющие поисковому запросу с указанным UUID, необходимо запустить скрипт **querytool** с ключом **-d** или **--delete**. Пример вывода команды:

10 : 19 : 26.215 [main] INFO query-tool - Finished deletion: Action: ec 13e1 c 1 -db 3 d -43 c 6 -9 c 6e-3 bbd 79 eb 449 d
Job: 6 d 8 bf 7 b 4 -8 c 87 -4317 -a 55 b-fcb 5 cf 199 f 6 f Status: done
Result: { "messages" :[{ "status" : "done" , "id" : "5db63d30-8c34-11e9-b8fb-005056aa7fac" },
{ "status" : "done" , "id" : "edd85edc-8c31-11e9-bec5-005056aa7fac" },
{ "status" : "done" , "id" : "69231e02-8c40-11e9-aa85-005056aa7fac" },
{ "status" : "done" , "id" : "a4c93d1a-8c31-11e9-9b97-005056aa7fac" }], "events" :[]} Errors:
Params:

Удаление сообщений из архива также может выполняться автоматически сервером архива. Автоматическое удаление сообщений выполняется в случае превышения определенного их количества в БД архива или в случае превышения суммарного объема сообщений. Допустимые пределы и интервал их проверки настраиваются в секции **Схемы соединений с БД** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**), а возможная реакция системы на превышение пределов определяется в секции **Сервер мониторинга** (раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование системы > Мониторинг**).

Параметры конфигурации, отвечающие за автоматическое удаление сообщений, определяются в группе параметров **Ротация данных** и редактируются в секции **Схемы соединений с БД** раздела GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** (Рис.6.3).

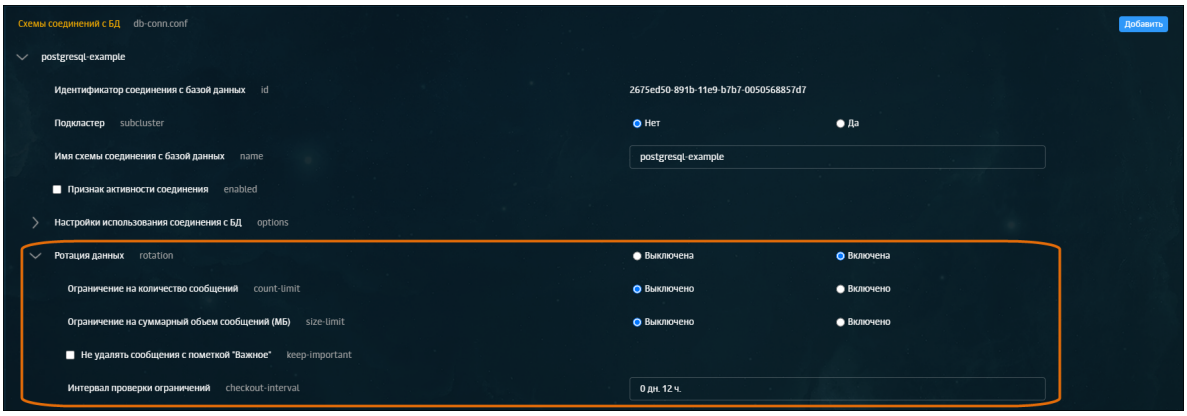


Рис. 6.3. Настройки автоматического удаления сообщений из архива

При значении параметра **Ротация данных** равным **Включена** используются следующие параметры:

1. **Ограничение на количество сообщений** – определяет ограничение на количество сообщений. При превышении этого количества старые записи удаляются. Принимает значения **Включено** и **Выключено**. При значении **Выключено** ограничение отсутствует. При значении **Включено** можно задать ограничение.

2. **Ограничение на суммарный объем сообщений (МБ)** – при превышении этого размера наиболее старые сообщения будут удалены. Принимает значения **Включено** и **Выключено**. При значении **Выключено** ограничение отсутствует. При значении **Включено** можно задать ограничение.

3. **Не удалять сообщения с пометкой "Важное"** – при включенном параметре сообщения в архиве, помеченные как важные, не удаляются при очистке БД архива. При выключенном параметре в процессе удаления сообщений из архива (при превышении их количества или объема) сообщения с пометкой **Важное сообщение** также удаляются. По умолчанию параметр выключен.

4. **Интервал проверки ограничений** – интервал проверки ограничений на количество и суммарный объем сообщений. Значение по умолчанию: **0 дн. 12 ч.**.

В системе определены два уровня критичности для случаев превышения объема сообщений и/или их количества в базе данных. Это уровни **warning** и **critical**. В случае превышения ограничений для каждого из уровней в разделе GUI **Система > Мониторинг > Состояние системы** будут отображаться проблемы соответствующего уровня критичности (см. раздел 5.4.2), но при этом работа архиватора не прекращается. При следующем запуске монитора ресурсов, если объем и/или количество сообщений в базе данных уменьшилось до допустимых значений, проблемы перестанут отображаться в GUI KEO DLP. Ограничения на количество сообщений и объем базы данных определяются параметром конфигурации **Использование базы данных** для каждого уровня критичности.

Информация об удаленных сообщениях записывается в журнал сервиса **archive-server** (см. Табл.6.4).

6.13.4. Экспорт сообщений из архива KEO DLP

Для экспорта сообщений из исходной базы данных используется скрипт **/opt/dozor/smap/bin/export-messages.py**.

Примечание

Могут возникать ситуации, когда секции БД с необходимыми сообщениями уже отключены или удалены, а тело сообщения все еще присутствует в ФХ. Таким образом, экспорт сообщений в формат EML будет выполнен напрямую из ФХ независимо от наличия в БД требуемых секций.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат команды для запуска скрипта:

$ export-messages.py <ключ> <vID>

где:

- **ключ** – один из доступных ключей, определяющих конкретное действие, выполняемое с помощью скрипта. Список доступных ключей приведен ниже;
- **vID** – идентификатор сообщения. Можно указывать несколько идентификаторов для получения списка пометок, установленных на каждое из указанных сообщений. Необязательный аргумент.

Доступны следующие ключи:

- **-H <имя узла/IP>**, **--host <имя узла/IP>** – имя или IP-адрес узла с сервисами **archive-server**. Значение по умолчанию: **127.0.0.1**.
- **-P <порт>**, **--port <порт>** – порт узла с сервисом **archive-server**. Значение по умолчанию: 3000.
- **-p <порт>**, **--as-port <порт>** – порт узла с сервисом **action-server**. Значение по умолчанию: 3001.
- **-w <имя узла/IP>**, **--web-host <имя узла/IP>** – имя или IP-адрес сервера веб-интерфейса. Значение по умолчанию: **127.0.0.1**.
- **-z <порт>**, **--web-port <порт>** – порт сервера веб-интерфейса. Значение по умолчанию: 8443.
- **-U <имя пользователя>**, **--login-user <имя пользователя>** – имя учетной записи пользователя. Значение по умолчанию: **superadmin**.
- **-L <password>**, **--login-password <password>** – пароль пользователя. Значение по умолчанию: **ask**.
- **-M, --no-multiarchive** – не использовать API для работы с подкластерами.
- **-f < имя файла>**, **--file < имя файла>** – считать список идентификаторов из указанного файла.
- **-q <ИД поискового запроса>**, **--query <ИД поискового запроса>** – получить список идентификаторов ID сообщений из поискового запроса.
- **-F <дата>**, **--storage-filter <дата>** – указать начальную и конечную даты, за которые необходимо выполнить экспорт, в формате **[YYYY-MM-DD]:[YYYY-MM-DD]**.
- **-s <ИД>**, **--storage <ИД>** – получить список сообщений из хранилища **<ИД>**.
- **-n <число потоков>**, **--number-of-threads <число потоков>** – количество потоков экспорта. Значение по умолчанию: 1.
- **-t <каталог>**, **--to-directory <каталог>** – экспортировать сообщения в указанный каталог. Значение по умолчанию: текущий каталог.
- **-o <имя файла>**, **--output-file <имя файла>** – выходной файл с расширением **mbox**.

- **-m <формат>, --format <формат>** – экспортировать сообщения в специальном формате. Принимает значения **smap**, **mbox** и **eml**. Значение по умолчанию: **smap**.
- **--stop-on-error** – завершить экспорт при ошибках.
- **-r**, **--remove** – удалить сообщения из БД архива после экспорта.
- **-v**, **--verbose** – вывод сообщений о действиях, выполняемых скриптом.
- **-d**, **--debug** – включить отладочное журналирование.
- **-h**, **--help** – вывести на экран справочную информации об использовании скрипта.

Пример экспорта контейнеров с идентификаторами ID сообщений за определенные даты (формат команды для запуска скрипта
$ export-messages.py -M -U superadmin -L Zaq1@wsX -F 2018-06-20:2018-06-21 -t /tmp/export-test/
):

```
100% [4/4] (left: 0 sec)
```

Для проверки результата экспорта следует последовательно выполнить следующие команды:

$ cd /tmp/export-test/

$ ls -lah

В результате выполнения команд на экран будут выведены следующие данные:

```
total 1.8M
drwxr-xr-x   2 root root 4.0K Jun 28 10:58 .
drwxrwxrwt. 20 root root 4.0K Jun 28 11:03 ..
-rw-r--r--   1 root root 453K Jun 28 10:58 6aa74552-7aa1-11e8-b63f-005056880378.arc-body
-rw-r--r--   1 root root  13K Jun 28 10:58 6aa74552-7aa1-11e8-b63f-005056880378.arc-message
-rw-r--r--   1 root root   88 Jun 28 10:58 6aa74552-7aa1-11e8-b63f-005056880378.arc-text.8
-rw-r--r--   1 root root 109K Jun 28 10:58 6aa74552-7aa1-11e8-b63f-005056880378.arc-text.9
-rw-r--r--   1 root root 453K Jun 28 10:58 93fdb1e8-7aa1-11e8-b9b1-005056880378.arc-body
-rw-r--r--   1 root root  13K Jun 28 10:58 93fdb1e8-7aa1-11e8-b9b1-005056880378.arc-message
-rw-r--r--   1 root root   88 Jun 28 10:58 93fdb1e8-7aa1-11e8-b9b1-005056880378.arc-text.8
-rw-r--r--   1 root root 109K Jun 28 10:58 93fdb1e8-7aa1-11e8-b9b1-005056880378.arc-text.9
-rw-r--r--   1 root root 453K Jun 28 10:58 98625542-7aa4-11e8-a26d-005056880378.arc-body
-rw-r--r--   1 root root  13K Jun 28 10:58 98625542-7aa4-11e8-a26d-005056880378.arc-message
-rw-r--r--   1 root root   88 Jun 28 10:58 98625542-7aa4-11e8-a26d-005056880378.arc-text.8
-rw-r--r--   1 root root 109K Jun 28 10:58 98625542-7aa4-11e8-a26d-005056880378.arc-text.9
-rw-r--r--   1 root root  644 Jul  2 10:52 c96892f6-753f-11e8-9e01-005056880378.arc-body
-rw-r--r--   1 root root 3.2K Jul  2 10:52 c96892f6-753f-11e8-9e01-005056880378.arc-message
-rw-r--r--   1 root root   14 Jul  2 10:52 c96892f6-753f-11e8-9e01-005056880378.arc-text.3
-rw-r--r--   1 root root 2.3K Jul  2 10:52 a5e06002-7558-11e8-815a-005056880378.arc-body
-rw-r--r--   1 root root 4.2K Jul  2 10:52 a5e06002-7558-11e8-815a-005056880378.arc-message
-rw-r--r--   1 root root   76 Jul  2 10:52 a5e06002-7558-11e8-815a-005056880378.arc-text.6
-rw-r--r--   1 root root 3.0K Jul  2 10:52 a796d862-7540-11e8-a159-005056880378.arc-body
-rw-r--r--   1 root root 4.5K Jul  2 10:52 a796d862-7540-11e8-a159-005056880378.arc-message
-rw-r--r--   1 root root   42 Jul  2 10:52 a796d862-7540-11e8-a159-005056880378.arc-text.14
-rw-r--r--   1 root root   20 Jul  2 10:52 a796d862-7540-11e8-a159-005056880378.arc-text.8
-rw-r--r--   1 root root 2.5K Jul  2 10:52 b52d403e-7558-11e8-b8c3-005056880378.arc-body
-rw-r--r--   1 root root 4.8K Jul  2 10:52 b52d403e-7558-11e8-b8c3-005056880378.arc-message
```

```
-rw-r--r--  1 root root   71 Jul  2 10:52 b52d403e-7558-11e8-b8c3-005056880378.arc-text.6
-rw-r--r--  1 root root  174 Jun 28 10:58 processed
```

6.13.5. Импорт сообщений в архив KEO DLP

Для импорта сообщений в БД, для которых установлен флажок **Использовать БД для поиска по архиву** (раздел GUI **Система > Конфигурация** > **Основные настройки** > **Доступ к данным**), используется скрипт **import-messages.py**.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат команды для запуска скрипта **import-messages.py**:

$ import-messages.py <ключ>

Доступны следующие ключи:

- **-H <имя узла/IP>**, **--host <имя узла/IP>** – указать имя или IP-адрес сервера архива сообщений. Значение по умолчанию: **127.0.0.1**.
- **-P <порт>**, **--port <порт>** – указать порт, на котором сервер архива сообщений ожидает соединения. Значение по умолчанию: 3000.
- **-F <имя узла/IP>**, **--fs-host <имя узла/IP>** – указать имя или IP-адрес узла сервера файлового хранилища. Значение по умолчанию: **127.0.0.1**.
- **-p <порт>**, **--fs-port <порт>** – указать порт, на котором сервер архива сообщений ожидает соединения. Значение по умолчанию: 2264.
- **-M, --no-multiarchive** – не использовать API для работы с подкластерами.
- **-n <число>**, **--number-of-threads <число>** – указать количество потоков, предназначенных для импорта сообщений. Значение по умолчанию: -1 (количество потоков равно количеству процессоров на узле).
- **-f <каталог>**, **--from-directory <каталог>** – импортировать сообщения из определенного каталога.
- **-a <e-mail>**, **--address <e-mail>** – импортировать сообщения с определенным адресом электронной почты.

  Примечание

  На этапе импорта невозможно определить количество сообщений, которые содержат указанный адрес электронной почты. После выполнения операции импорта на экран будут выведены соответствующие результаты.

- **-s <фильтр>**, **--start-date <фильтр>** – импортировать сообщения, полученные после определенной даты в формате **YYYY/MM/DD/hh/mm**.

- **-e <фильтр>**, **--end-date <фильтр>** – импортировать сообщения, полученные до определенной даты в формате **YYYY/MM/DD/hh/mm**.
- **--stop-on-error** – завершить импорт при ошибках.
- **-r**, **--replace** – заменить сообщения, уже существующие в БД архива.
- **-S <ИД>**, **--storage-id <ИД>** – загружать сообщения в хранилище с идентификатором <ИД>.
- **-N**, **--no-body** – не загружать тело письма на сервер архива сообщений.
- **-t <vg>**, **--to-fs <vg>** – загружать сообщения в группу томов с идентификатором **<vg>**.
- **-T**, **--no-fs-https** – отключить использование протокола HTTPS для доступа в файловое хранилище.
- **-v**, **--verbose** – вывод сообщений о действиях, выполняемых скриптом.
- **-d**, **--debug** – включить отладочное журналирование.
- **-h**, **--help** – вывести на экран справочную информации об использовании скрипта.

Пример импорта сообщений из каталога **/tmp/export-test/**, полученных 28 июня 2018 в каталог (формат команды для запуска скрипта
$ /opt/dozor/smap/bin/import-messages.py -s 2018/06/28/00/00 -e 2018/06/28/13/00 -f /tmp/export-test/
):

```
100% [8/8] (left: 0 sec) Skiped: 8
```

6.13.6. Перенос сообщений между базами данных в формате файлового хранилища

Может возникнуть необходимость перенести в файловое хранилище сообщения, имеющие формат, отличный от используемого в ФХ. В таком случае необходимо экспортировать сообщения из исходной базы данных в формате ФХ, а затем импортировать их в базу данных ФХ.

Чтобы перенести сообщения между базами данных в формате файлового хранилища, необходимо выполнить следующие шаги:

1. Подключить исходную базу данных с сообщениями к узлу, на котором размещено ФХ, в которое предполагается импортировать сообщения (более подробно описано в документе *Руководство по установке и настройке*).
2. В интерфейсе командной строки выполнить команды:

   # su - dozor

   $ /opt/dozor/bin/shell

   $ qtool.py -l -U superadmin

   В появившемся диалоговом окне аутентификации ввести пароль пользователя **superadmin**:

```
Пароль для superadmin:
```

В результате на экран будут выведены идентификаторы всех поисковых запросов.

Более подробную информацию о скрипте **qtool.py** см. в разделе 6.13.8.

3. Записать в файл идентификаторы контейнеров сообщений поискового запроса с необходимым идентификатором, выбранным на шаге 2. Для этого в интерфейсе командной строки выполнить команду:

   $ qtool.py -S <query_ID> -U superadmin -p Zaq1@wsX > /tmp/list

   где **<query_ID>** – идентификатор поискового запроса.

   В результате этого действия в файл **/tmp/list** будут записаны идентификаторы контейнеров из исходного поискового запроса.

4. Выполнить команду:

   $ export-messages.py -U superadmin -L Zaq1@wsX -t /tmp/export/ -f /tmp/list

   В результате этого действия контейнеры с идентификаторами из файла **/tmp/list** будут экспортированы в каталог **/tmp/export/**.

   Более подробную информацию о скрипте **export-messages.py** см. в разделе 6.13.4.

5. Выполнить команду:

   $ import-messages.py -p -F fs -f /tmp/export/ -t <N>

   где <N> – порядковый номер базы данных файлового хранилища в конфигурационном файле **<db-conn.conf>**. В результате этого действия контейнеры из каталога **/tmp/export/** будут импортированы в файловое хранилище.

   Более подробную информацию о скрипте **import-messages.py** см. в разделе 6.13.5.

6.13.7. Создание и добавление подготовленных запросов (шаблонов поиска)

Одним из способов поиска информации в системе является использование шаблонов поиска (раздел интерфейса **Поиск > Шаблоны поиска**). Шаблоны поиска – это заранее подготовленные запросы на поиск сообщений в архиве.

Система поставляется с набором определенных шаблонов поиска. Описание этих шаблонов приведено в документе *Руководство пользователя* (раздел **Шаблоны поиска: применение готовых поисковых запросов**).

При необходимости администратор может добавлять в систему собственные запросы. Для этого следует выполнить действия:

1. Сохранить подготовленный запрос, разработанный в соответствии с определенной структурой (см. раздел 6.13.7.1), в файл формата **edn**. Примеры запросов приведены в разделе 6.13.7.3.

2. Скопировать edn-файл в каталог, где хранятся подготовленные запросы (определяется в параметре **Директория с подготовленными запросами**, по умолчанию **/opt/dozor/etc/archive-server/queries/**).

3. Перезапустить сервис **webserver**, выполнив команду:

```
# dsctl restart webserver
```

После этого можно в интерфейсе KEO DLP перейти в раздел **Поиск > Шаблоны поиска** и проверить наличие и выполнение запроса.

6.13.7.1. Сведения о структуре подготовленного запроса

Подготовленные запросы представляют собой параметризуемые SQL-запросы на поиск сообщений. Структура такого запроса включает поля:

- **id** – числовой идентификатор запроса. Присваивается при написании нового запроса.

  Примечание

  *Чтобы посмотреть, какие идентификаторы (**id**) уже существуют, нужно собрать данные из всех .edn файлов (например, с помощью скрипта **grep**).*

- **name** – наименование запроса (строка). Отображается в интерфейсе пользователя при выборе запроса.
- **category** – категория запроса (строка). Используется для группировки запросов в интерфейсе пользователя.

  Внимание!

  При установке KEO DLP создаются системные категории, в которых содержатся запросы, поставляемые с системой.

  Для собственных подготовленных запросов настоятельно рекомендуется создавать собственные категории (то есть использовать системные категории нежелательно).

- **subcategory** – подкатегория запроса (строка, не обязательное поле). Используется для группировки запросов в интерфейсе пользователя, если требуется двухуровневая иерархия запросов.
- **query** – текст SQL-запроса. Может быть задан как строкой, когда запрос общий для всех СУБД, так и структурой, в которой для каждой СУБД задан свой текст запроса. Например,

  ```
  {:oracle "SELECT id FROM message WHERE rownum <= :limit"
   :pgsql  "SELECT id FROM message LIMIT :limit"}
  ```

- **binds** – описание параметров запроса (массив).

  Параметры запроса имеют формат **:param**, где **param** – идентификатор параметра. Параметры **idbegin** и **idend**, представляющие собой границы отчетного периода, определены всегда и не должны указываться в **binds**.

В свою очередь, описание параметров запроса (**binds**) представляет собой структуру с полями:

- **id** – идентификатор (строка), которым параметр представлен в тексте SQL-запроса;
- **name** – название параметра, отображаемое в интерфейсе пользователя;
- **type** – тип значения параметра (**integer**, **string**, **timestamp**);
- **default** – значение, предлагаемое пользователю по умолчанию (не используется, если задан набор вариантов (dict) со своим значением по умолчанию);
- **dict** – набор вариантов значений параметра. Содержит следующие поля:
  - **data** – способ получения набора вариантов:
    - **fixed** – в виде массива объектов с полями **name** и **value** (значение **name** отображается в интерфейсе, **value** передается в качестве значения параметра). Пример:

      ```
      ...
      :data {:fixed [{:name "последние 3 дня" :value 3}
      {:name "последнюю неделю" :value 7}
      {:name "последние 30 суток" :value 30}]}
      ...
      ```

    - **query** – в виде набора вариантов из БД политики, полученных с помощью соответствующего SQL-запроса. SQL-запрос должен возвращать значения полей **name** и **value** (значение **name** отображается в интерфейсе, **value** передается в качестве значения параметра). Пример:

      ```
      ...
      :data {:query  "SELECT id AS value, value AS name FROM label_type ORDER BY name" }
      ...
      ```

      После того, как пользователь выбрал подготовленный запрос в интерфейсе, ему предлагается полученный набор вариантов.

    - **ui** – в виде набора, полученного с помощью выбора значений в заданном пользовательском интерфейсе:
      - *persons* – интерфейс выбора персон с возможностью поиска по ФИО, адресам и т.п.
      - *person-group* – интерфейс выбора групп персон с возможностью просмотра иерархии, поиска по названию и т.п.
  - **multiple** – возможность множественного выбора значений (**true**/**false**). Значение **true** допускается только для параметров типа **string**. Значение параметра формируется в виде строки, в которой выбранные значения (каждое в одинарных кавычках) объединены через запятую.
  - **default** – значение (или набор значений (массив) в случае **multiple** = **true**), которое будет выбрано при первоначальном отображении формы.

6.13.7.2. Сведения о таблицах БД для хранения сообщений

В этом разделе приведены необходимые для написания подготовленных запросов сведения о полях и связях таблиц БД, которые используются для хранения сообщений (**Рис.6.4**).

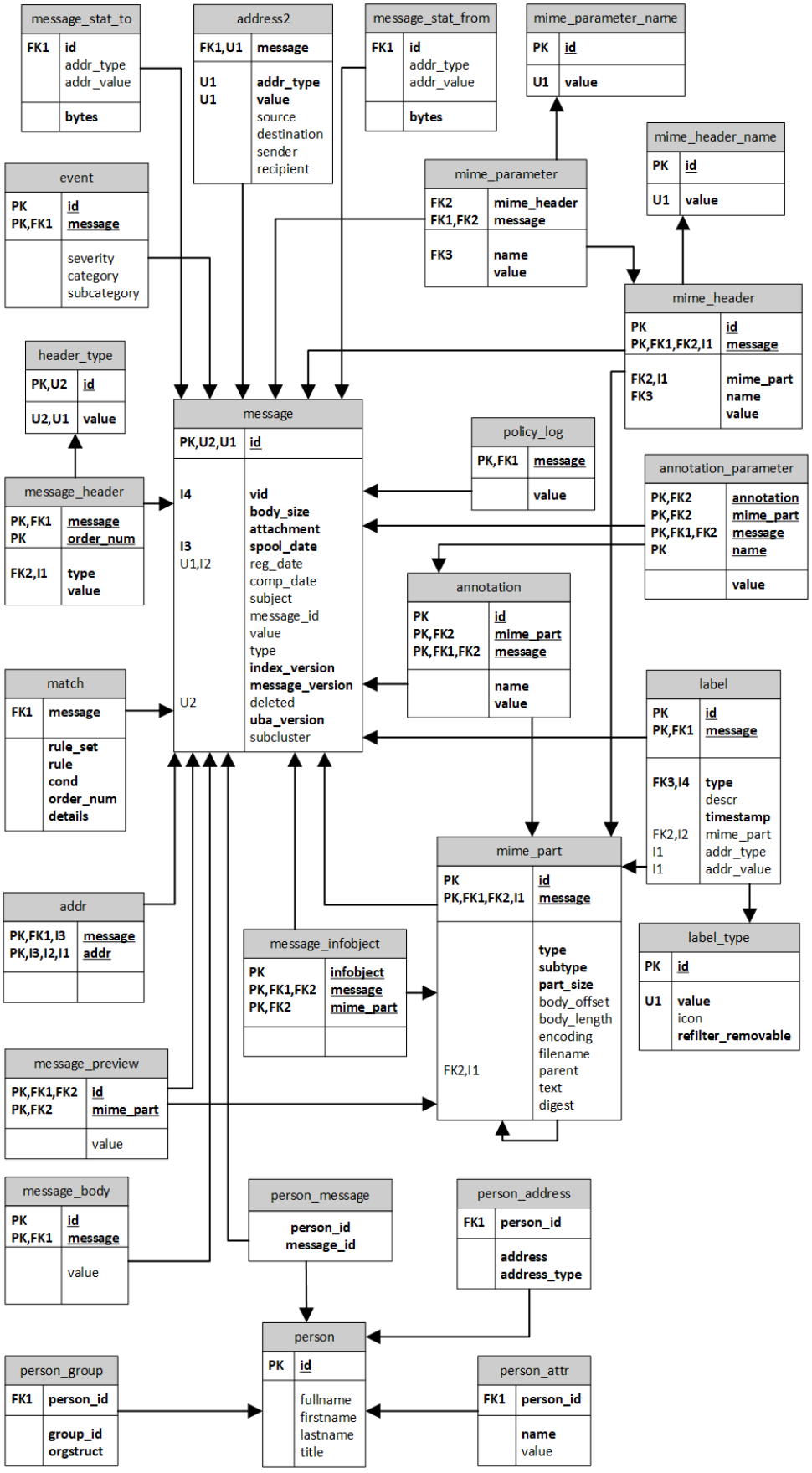


Рис. 6.4. Схема БД (в части таблиц для хранения сообщений и данных персон)

Табл. 6.5. Таблица message: данные о сообщениях

Имя столбца	Тип данных	Описание
ID	BIGINT	Идентификатор сообщения в архиве
VID	TEXT	Идентификатор сообщения на этапе фильтрации, не совпадает с ID
BODY_SIZE	BIGINT	Размер тела сообщения в байтах
ATTACHMENT	INTEGER	Число вложенных в сообщение файлов
SPOOL_DATE	TIMESTAMP	Дата и время попадания сообщения в очередь сообщений
REG_DATE	TIMESTAMP	Дата и время регистрации сообщения в архиве
COMP_DATE	TIMESTAMP	Дата составления сообщения (значение заголовка Date)
SUBJECT	TEXT	Тема сообщения
MESSAGE_ID	TEXT	Значение заголовка message-id в сообщении
VALUE	OID	Тело сообщения. Устаревшее поле, не используется. См. Табл.6.13
TYPE	TEXT	Тип сообщения
INDEX_VERSION	INTEGER	Версия представления сообщения, проиндексированного для быстрого поиска
MESSAGE_VERSION	INTEGER	Версия представления сообщения в БД
DELETED	CHAR (1)	Признак удаления сообщения
UBA_VERSION	BIGINT	Версия представления сообщения, проиндексированного в модуле UBA
SUBCLUSTER	UUID	Идентификатор подкластера, в котором сообщение было обработано

Табл. 6.6. Таблица addr: используется для разграничения доступа к сообщениям; хранит адреса, домены и поддомены адресов

Имя столбца	Тип данных	Описание
MESSAGE	BIGINT	Ссылка на сообщение в таблице MESSAGE
ADDR	TEXT	Адрес, домен, поддомен

Табл. 6.7. Таблица address2: адресная информация сообщений

Имя столбца	Тип данных	Описание
MESSAGE	BIGINT	Ссылка на сообщение в таблице MESSAGE
ADDR_TYPE	TEXT	Тип адреса
VALUE	TEXT	Значение адреса
SOURCE	CHAR (1)	Признак источника (y/n)
DESTINATION	CHAR (1)	Признак назначения (y/n)
SENDER	CHAR (1)	Признак отправителя (y/n)
RECIPIENT	CHAR (1)	Признак получателя (y/n)

Табл. 6.8. Таблица annotation: описания частей сообщений

Имя столбца	Тип данных	Описание
ID	INTEGER	Идентификатор описания
MIME_PART	INTEGER	MIME-часть сообщения
MESSAGE	BIGINT	Ссылка на сообщение в таблице MESSAGE
NAME	TEXT	Наименование описания
VALUE	TEXT	Содержание

Табл. 6.9. Таблица annotation_parameter: параметры описаний частей сообщений

Имя столбца	Тип данных	Описание
ANNOTATION	INTEGER	Идентификатор описания
MIME_PART	INTEGER	MIME-часть сообщения
MESSAGE	BIGINT	Ссылка на сообщение в таблице MESSAGE
NAME	TEXT	Наименование параметра
VALUE	TEXT	Значения параметра

Табл. 6.10. Таблица event: события ИБ, созданные в результате обработки сообщений в соответствии с правилами политики ИБ

Имя столбца	Тип данных	Описание
ID	UUID	Идентификатор события
MESSAGE	BIGINT	Ссылка на сообщение в таблице MESSAGE
SEVERITY	TEXT	Критичность, уровень серьезности события
CATEGORY	UUID	Идентификатор категории события (условная ссылка на категорию событий)
SUBCATEGORY	UUID	Идентификатор подкатегории события (условная ссылка на подкатегорию событий)

Табл. 6.11. Таблица label: пометки сообщений (могут относиться не просто к сообщению, а к определенному свойству сообщения)

Имя столбца	Тип данных	Описание
ID	INTEGER	Идентификатор пометки
TYPE	INTEGER	Тип пометки (ссылка на соответствующий тип в таблице типов пометок label_type)
DESCR	TEXT	Описание пометки
TIMESTAMP	TIMESTAMP	Дата и время создания пометки
MIME_PART	INTEGER	Часть сообщения, для которой определена пометка
MESSAGE	BIGINT	Ссылка на сообщение в таблице MESSAGE
ADDR_TYPE	TEXT	Тип адреса (ссылка на соответствующее поле в таблице address2)

Имя столбца	Тип данных	Описание
ADDR_VALUE	TEXT	Значение адреса (ссылка на соответствующее поле в таблице address2)

Табл. 6.12. Таблица message_header: заголовки сообщений

Имя столбца	Тип данных	Описание
MESSAGE	BIGINT	Идентификатор сообщения в таблице MESSAGE
TYPE	INTEGER	Тип заголовка (ссылка на запись в таблице *header_type* в справочнике типов заголовков сообщений).
ORDER_NUM	INTEGER	Порядковый номер заголовка в сообщении
VALUE	TEXT	Значение заголовка

Табл. 6.13. Таблица message_body: тела сообщений

Имя столбца	Тип данных	Описание
MESSAGE	BIGINT	Идентификатор сообщения в таблице MESSAGE
ID	BIGINT	ID фрагмента тела сообщения
VALUE	BYTEA	Тело сообщения

Табл. 6.14. Таблица message_infobject: информационные объекты, обнаруженные в сообщениях

Имя столбца	Тип данных	Описание
INFOBJECT	UUID	Идентификатор информационного объекта
MESSAGE	BIGINT	Идентификатор сообщения в таблице MESSAGE
MIME_PART	INTEGER	MIME-часть сообщения

Табл. 6.15. Таблица message_stat_from: статистическая информация об отправленных сообщениях

Имя столбца	Тип данных	Описание
ID	BIGINT	Идентификатор сообщения в таблице MESSAGE
BYTES	INTEGER	Размер сообщения в байтах
ADDR_TYPE	TEXT	Тип адреса
ADDR_VALUE	TEXT	Значение адреса

Табл. 6.16. Таблица message_stat_to: статистическая информация о полученных сообщениях

Имя столбца	Тип данных	Описание
ID	BIGINT	Идентификатор сообщения в таблице MESSAGE
BYTES	INTEGER	Размер сообщения в байтах
ADDR_TYPE	TEXT	Тип адреса
ADDR_VALUE	TEXT	Значение адреса

Табл. 6.17. Таблица mime_header: MIME-заголовки частей сообщения

Имя столбца	Тип данных	Описание
ID	INTEGER	Идентификатор MIME-заголовка
MIME_PART	INTEGER	Ссылка на часть сообщения, к которой относится MIME-заголовок
NAME	INTEGER	Имя MIME-заголовка (ссылка на запись в таблице *mime_header_name* в справочнике MIME-заголовков)
VALUE	TEXT	Значение параметра MIME-заголовка (например, *koi8-r* для параметра *charset*)
MESSAGE	BIGINT	Ссылка на сообщение в таблице MESSAGE

Табл. 6.18. Таблица mime_part: структура MIME-частей сообщения (к MIME-части относятся также файлы, пересылаемые в архивах, файлы, внедренные в документы MS Office и т.д.).

Имя столбца	Тип данных	Описание
ID	INTEGER	Идентификатор части сообщения
TYPE	TEXT	MIME-тип части тела сообщения (примеры значений: *text, image, video, audio* и т.д.)
SUBTYPE	TEXT	Подтип MIME-части тела сообщения, например, *plain* (*text/plain*), *gif* (*image/gif*)
PART_SIZE	BIGINT	Размер декодированной части сообщения
BODY_OFFSET	INTEGER	Смещение MIME-части относительно начала тела сообщения
BODY_LENGTH	INTEGER	Размер MIME-части тела сообщения. Используется совместно с полем BODY_OFFSET для определения точного положения части сообщения
ENCODING	TEXT	Кодировка, в которой передается часть сообщения (значение MIME-поля *Content-Transfer-Encoding*. Примеры значений: 7bit, binary, base64 и т.д.).
FILENAME	TEXT	Имя файла, вложенного в сообщение
MESSAGE	BIGINT	Ссылка на сообщение в таблице MESSAGE
PARENT	INTEGER	Идентификатор родительской части сообщения, используется для вложенных сообщений
TEXT	TEXT	Текстовое представление части сообщения. Поле TEXT используется для построения полнотекстового индекса в OpenSearch
DIGEST	TEXT	Контрольная сумма MIME-части

Табл. 6.19. Таблица header_type: типы заголовков сообщения

Имя столбца	Тип данных	Описание
ID	INTEGER	Идентификатор типа заголовка сообщения
VALUE	TEXT	Имя типа заголовка сообщения

Табл. 6.20. Таблица label_type: типы пометок

Имя столбца	Тип данных	Описание
ID	INTEGER	Идентификатор типа пометки
VALUE	TEXT	Имя типа пометки
ICON	TEXT	Путь к файлу иконки для отображения пометок данного типа
REFILTER_REMOVABLE	INTEGER	Признак удаления данного типа пометок при рефильтрации сообщения

Табл. 6.21. Таблица mime_header_name: имена MIME-заголовков сообщений и их частей. Примеры: content-type, content-encoding, language и т.п.

Имя столбца	Тип данных	Описание
ID	INTEGER	Идентификатор имени MIME-заголовка
VALUE	TEXT	Имя MIME-заголовка

Табл. 6.22. Таблица mime_parameter_name: имена параметров MIME-заголовков сообщений. Пример: charset

Имя столбца	Тип данных	Описание
ID	INTEGER	Идентификатор имени параметра MIME-заголовка
VALUE	TEXT	Имя параметра MIME-заголовка

Табл. 6.23. Таблица message_preview: представления MIME-частей сообщения, предназначенные для быстрого просмотра в интерфейсе в виде HTML-страниц

Имя столбца	Тип данных	Описание
ID	BIGINT	Ссылка на сообщение в таблице MESSAGE
MIME_PART	INTEGER	MIME-часть сообщения
VALUE	TEXT	HTML-представление части сообщения

Табл. 6.24. Таблица match: срабатывания политики

Имя столбца	Тип данных	Описание
ID	BIGINT	Ссылка на сообщение в таблице MESSAGE
RULE_SET	UUID	Идентификатор набора правил, в котором произошло срабатывание
RULE	UUID	Идентификатор правила, в котором произошло срабатывание
COND	UUID	Идентификатор сработавшего условия

Имя столбца	Тип данных	Описание
ORDER_NUM	BIGINT	Порядковый номер срабатывания
DETAILS	JSONB	Подробная информация о срабатывании

Табл. 6.25. Таблица mime_parameter: параметры MIME-заголовков

Имя столбца	Тип данных	Описание
MIME_HEADER	INTEGER	Ссылка на MIME-заголовок
NAME	INTEGER	Имя параметра MIME-заголовка
VALUE	TEXT	Значение параметра MIME-заголовка
MESSAGE	BEGINT	Ссылка на сообщение в таблице MESSAGE

Табл. 6.26. Таблица person: основная информация о персонах

Имя столбца	Тип данных	Описание
ID	UUID	Идентификатор персоны
FULLNAME	TEXT	Полное имя (ФИО) персоны
FIRSTNAME	TEXT	Имя персоны
LASTNAME	TEXT	Фамилия персоны
TITLE	TEXT	Должность персоны

Табл. 6.27. Таблица person_address: адресная информация персон

Имя столбца	Тип данных	Описание
PERSON_ID	UUID	Идентификатор персоны из таблицы PERSON
ADDRESS	TEXT	Значение адреса персоны
ADDRESS_TYPE	TEXT	Тип адреса персоны

Табл. 6.28. Таблица person_attr: атрибуты персон (ФИО, должность, руководитель и т.д.)

Имя столбца	Тип данных	Описание
PERSON_ID	UUID	Идентификатор персоны из таблицы PERSON
NAME	TEXT	Название атрибута
VALUE	TEXT	Значение атрибута в текстовом представлении

Табл. 6.29. Таблица person_group: информация о вхождении персоны в группу

Имя столбца	Тип данных	Описание
PERSON_ID	UUID	Идентификатор персоны из таблицы PERSON
GROUP_ID	UUID	Идентификатор группы
ORGSTRUCT	CHAR (1)	Признак принадлежности группы организационно-штатной структуре

Табл. 6.30. Таблица person_message: связь сообщений с персонами

Имя столбца	Тип данных	Описание
PERSON_ID	UUID	Идентификатор персоны из таблицы PERSON
MESSAGE_ID	BIGINT	Идентификатор сообщения

Табл. 6.31. Таблица policy_log: журнал обработки сообщений политикой

Имя столбца	Тип данных	Описание
MESSAGE	BIGINT	Ссылка на сообщение в таблице MESSAGE
VALUE	TEXT	События обработки сообщения в формате JSON

6.13.7.3. Примеры подготовленных запросов

В этом разделе приведены примеры подготовленных запросов:

1. Запрос для поиска сообщений, текст которых содержит слово из списка:

```
{:name "Текст содержит слово из списка",
 :category "Мои запросы",
 :id 104,
 :query
 {:pgsql "
WITH
  z_input as (SELECT lower(trim(:listword::varchar)) list_word),
  z_word as ( SELECT distinct a_value FROM ( SELECT trim( unnest( string_to_array(list_word, ',')
 ) ) a_value FROM z_input ) z1 WHERE a_value<>'' )
SELECT m.message FROM mime_part m WHERE m.message BETWEEN :idbegin::bigint AND
:idend::bigint AND lower(m.text) ~ any (SELECT a_value FROM z_word)",
:oracle "
SELECT * FROM (
  WITH z_input as ( SELECT trim( :listword ) list_word FROM dual ),
  z_word as ( SELECT distinct trim(s) as a_value FROM ( SELECT regexp_substr(list_word, '[^,]+',
1, level) s FROM z_input connect by instr(list_word, ',', 1, level - 1) > 0 )
WHERE trim(s) IS NOT NULL )
SELECT distinct t.message FROM mime_part t WHERE t.message BETWEEN :idbegin AND :idend
 AND lower(t.text) ~ any (SELECT a_value FROM z_word)"},
 :binds
 [
  {:id "listword", :name "Список слов (слово_1,слово_2,..)"}
 ]}
```

2. Запрос для поиска сообщений, в тексте которых содержатся все слова из списка:

```
{:name "Текст содержит все слова из списка",
 :category "Мои запросы",
 :id 105,
 :query
 {:pgsql "
WITH
  z_input as (SELECT lower(trim(:listword::varchar)) list_word),
  z_word as ( SELECT distinct a_value FROM ( SELECT trim( unnest( string_to_array(list_word, ',')
 ) ) a_value FROM z_input ) z1 WHERE a_value<>'' )
SELECT m.message FROM mime_part m WHERE m.message BETWEEN :idbegin::bigint AND
```

```
:idend::bigint AND lower(m.text) ~ all (SELECT a_value FROM z_word)",
:oracle "
SELECT * FROM (
  WITH z_input as ( SELECT trim( :listword ) list_word FROM dual ),
  z_word as ( SELECT distinct trim(s) as a_value FROM ( SELECT regexp_substr(list_word, '[^,]+',
1, level) s FROM z_input connect by instr(list_word, ',', 1, level - 1) > 0 ) WHERE trim(s) IS NOT
NULL )
SELECT distinct t.message FROM mime_part t WHERE t.message BETWEEN :idbegin AND :idend
 AND lower(t.text) ~ all (SELECT a_value FROM z_word)"},
 :binds
 [
  {:id "listword", :name "Список слов (слово_1,слово_2,..)"}
 ]}
```

После добавления этих запросов в систему в интерфейсе в разделе **Поиск > Шаблоны поиска** в списке шаблонов поиска должны присутствовать элементы:

- **Мои запросы**
  - **Текст содержит слово из списка**
  - **Текст содержит все слова из списка**

При выборе какого-либо из указанных запросов должно отобразиться поле **Список слов (слово_1,слово_2,..)**, предназначенное для ввода искомых слов в соответствующем формате, например: *глагол,прилагательное,наречие*.

6.13.8. Просмотр результатов поисковых запросов

Для просмотра результатов поисковых запросов используется скрипт **qtool.py**.

Формат команды для запуска скрипта **qtool.py**:

$ qtool.py [options]

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Доступны следующие ключи:

- **-H <имя узла/IP>**, **--host <имя узла/IP>** – указать имя или IP-адрес узла с сервисами **archive-server**. Значение по умолчанию: **127.0.0.1**.
- **-P <порт>**, **--port <порт>** – указать порт узла с сервисом **archive-server**. Значение по умолчанию: 3000.
- **-U <имя пользователя>**, **--login-user <имя пользователя>** – указать имя учетной записи пользователя. Значение по умолчанию: **superadmin**.
- **-p <пароль>**, **--login-password <пароль>** – пароль пользователя. Значение по умолчанию: **ask**.

- **-l, --list-querys** – вывести на экран список поисковых запросов указанного пользователя.
- **-s <ИД>**, **--show-query <ИД>** – вывести на экран информацию по поисковому запросу с идентификатором <ИД>.
- **-i <ИД>**, **--list-query <ИД>** – вывести на экран идентификаторы vID сообщений из поискового запроса с идентификатором <ИД>.
- **-r <ИД> <номер строки> <число строк>, --results <ИД> <номер строки> <число строк>** – показать <число строк> из поискового запроса с идентификатором <ИД>, начиная со строки <номер строки>.
- **-e <ИД>, --execute-query <ИД>** – выполнить поисковый запрос с идентификатором <ИД>.
- **-v**, **--verbose** – вывод сообщений о действиях, выполняемых скриптом.
- **-d**, **--debug** – включить отладочное журналирование.
- **-h**, **--help** – вывести на экран справочную информации об использовании скрипта.

Примечание

*При работе с ключами **-r** и **-i** по объектам запроса, кроме сообщений (событиям и инцидентам, участникам переписки, файлам, беседам, нажатиям клавиш) результат просмотреть невозможно.*

Примеры использования скрипта:

1. Вывод на экран всех поисковых запросов (формат команды для запуска скрипта: **$ qtool.py -l -U superadmin -p Zaq1@wsX**):

```
Сообщения | 24 часа: 3174 (messages, quick, e2702239-0f80-418d-a330-ddb9e1f3a7b3)
События и инциденты | 24 часа: 718 (events, quick, 4aae7463-bf6c-45c2-a7ef-e77215432a6a)
События и инциденты | 24 часа: 719 (events, quick, 3b295feb-cd51-40b4-8ff5-150440751c16)
Количество::Больше::2 | Все время: 25 (messages, extended,
10a1578b-cadb-4653-beff-fdc46f4ff828)
```

2. Вывод на экран информации по поисковому запросу с идентификатором (формат команды для запуска скрипта: **$ qtool.py -s 10a1578b-cadb-4653-beff-fdc46f4ff828 -U superadmin -p Zaq1@wsX**):

```
status: completed
count: 25
temporary: True
name: Количество::Больше::2 | Все время
created: 2018-06-25T15:31:39.697+03:00
completed: 2018-06-25T15:32:39.897+03:00
lastRunIp: 10.199.199.51
id: 10a1578b-cadb-4653-beff-fdc46f4ff828
duration: 60200
queryObject: messages
```

```
type: query
queryType: extended
```

3. Вывод на экран идентификаторов vID сообщений для поискового запроса с идентификатором (формат команды для запуска скрипта:
$ qtool.py -i 10a1578b-cadb-4653-beff-fdc46f4ff828 -U superadmin -p Zaq1@wsX
):

```
15d476ec-632e-11e8-8007-005056880378
163c91dc-632e-11e8-a64f-005056880378
15a67eea-632e-11e8-96b8-005056880378
15957bcc-632e-11e8-96b8-005056880378
12ddb426-632e-11e8-bda0-005056880378
13327b78-632e-11e8-bd67-005056880378
125f7dea-632e-11e8-bda0-005056880378
```

6.13.9. Извлечение текста сообщений

Для извлечения текста сообщений, содержащихся в архиве, используется скрипт **get-message**. Для поиска документов в сообщении или файле используются скрипты **get-message-text** и **get-file-text** соответственно.

Формат команды для запуска скрипта **get-message**:

$ get-message <id> [> filename]

где:

- **<id>** – идентификатор сообщения в архиве;
- **[> filename]** – оператор перенаправления вывода в файл с указанным именем.

Пример команды запуска скрипта:

$ get-message 780 > message.id780

В результате выполнения этой команды будет извлечен текст сообщения с идентификатором 780 и записан в файл с именем **message.id780**.

Формат команды для запуска скрипта **get-message-text**:

get-message-text [ключи] <id>

где **<id>** – идентификатор сообщения в архиве.

Доступны следующие ключи:

- **-s** – разделять части сообщения в соответствии со структурой;
- **-e** – экспортировать сообщения в файл;
- **-a** – при экспорте сообщения в файл экспортировать части сообщений как есть, без преобразования их в текстовый формат;
- **-d** – включить режим отладки и журналирования;

- **-h** – получить справку по работе со скриптом.

Два символа тире (--) в качестве ключа означают, что следующие ключи, указанные в командной строке, не будут обработаны.

Данный скрипт может выводить текст сообщения либо сплошным текстом, либо с разделением на части в соответствии со структурой сообщения с указанием имен файлов где это возможно.

Формат команды для запуска скрипта **get-file-text**:

get-file-text [ключи] <filename>

где **<filename>** – имя файла, в котором необходимо выполнить поиск документов.

Текстовые или графические представления документов сохраняются в специально создаваемый временный каталог. Для каждого извлеченного документа на стандартный вывод направляется строка вида:

тип:md5:документ

где

- **тип** – тип документа ('image' или 'text');
- **md5** – md5-хэш оригинального документа (от которого было получено его текстовое или графическое представление);
- **документ** – полный путь к файлу с текстовым или графическим представлением документа.

Доступны следующие ключи:

- **-d** – включить режим отладки и журналирования;
- **-h** – получить справку по работе со скриптом.

6.13.10. Диагностика проблем функционирования OpenSearch

OpenSearch – это поисковая машина в составе модуля поиска по внешнему индексу, предназначенная для индексирования сообщений и выполнения полнотекстового поиска сообщений в архиве. Параметры поиска задаются в секции **Сервис поиска и индексации OpenSearch** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**). Описание работы сервисов **indexer-ng** и **opensearch** приведено в документе *Руководство по установке и настройке*.

При распределенной конфигурации KEO DLP узлы с сервисом **opensearch** связываются друг с другом, образуя кластер OpenSearch. Чтобы получить информацию о его состоянии, необходимо на любом узле с таким сервисом выполнить команду в CLI:

curl -s --cacert /opt/dozor/etc/ssl/ca.crt --key /opt/dozor/etc/ssl/bus.key --cert /opt/dozor/etc/ssl/bus.pem -X GET https://<OS_host>:<OS_port>/_cluster/health?pretty

где:

- **<OS_host>** – IP-адрес или имя узла с сервисом **opensearch**.
- **<OS_port>** – порт сервиса **opensearch**. Значение по умолчанию: 9200.

В результате выполнения команды на экран будут выведены следующие сведения:


```
{
  "cluster_name" : "isimpc",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 1,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 6,
  "active_shards" : 6,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```


Такая запись указывает на то, что кластер OpenSearch работает корректно, т.к. состояние кластера (индексов всех узлов) принимает значение **"green"**. За более подробной информацией о кластере и индексах OpenSearch следует обратиться к соответствующей документации.

Существуют следующие состояния кластера OpenSearch:

- **green** – нормальное функционирование кластера и готовность к работе, доступность копий индексов;
- **yellow** – недоступность одной или нескольких копий индексов OpenSearch, снижение надежности и производительности работы кластера.
- **red** – неработоспособность кластера (запросы и индексация сообщений в БД архива не работают).

  Кластер OpenSearch переходит в состояние **red** в следующих случаях:

  1. Узел с данными недоступен или произошло аварийное завершение работы сервиса **opensearch**.
  2. Если один из узлов с сервисом **opensearch** был недавно перезапущен, то в момент его запуска индексы недоступны в течении 1 минуты.
  3. Данные индекса повреждены или удалены.

Также для более детальной диагностики проблем поиска текста с помощью **opensearch** используется скрипт **indextool**, имеющий следующие параметры:

- **-d, --delete** – удалить временные индексы, созданные более 4 часов назад.

- **-do, --drop-old <arg>** – удалить индексы сообщений, созданные более заданного количества недель назад.
- **-host, --host <arg>** – задать сетевой адрес и порт узла, где OpenSearch принимает соединения, в следующем виде: <адрес:порт> (если используется порт, заданный по умолчанию, то можно указывать только адрес).
- **-h, --help** – выводит справочную информацию.
- **-i, --info** – выводит базовую информацию о кластере.

  Пример вывода команды:

```
ds-mode@keodlp6 /opt/dozor # indextool -i
Host: https://localhost:9200
Timeout: 60 seconds
Executing...
Cluster status: yellow (70.31% active shards)
Number of nodes: 1

Host                    | Size       | Heap                  | Rack   | Roles
------------------------------------------------------------------------------------------------------
Organisation6.isim.local    | 4.1 Mb    | 387.4 Mb / 4.0 Gb    |        | incident,media,text
------------------------------------------------------------------------------------------------------
Total: 4.1 Mb
```

- **-l, --list-indexes** – выводит список всех индексов.

  Пример вывода команды:

```
ds-mode@keodlp6 /opt/dozor # indextool -l
Host: http://localhost:9200
Timeout: 60 seconds
Executing...
Fast-search library version 15.32
Index name                              |Status  |Primaries  |Total      |Entries  |Version  |Roles
-------------------------------------------------------------------------------------------------------
chats                                   |green   |1248       |1248       |0        |15.31    |text
events-2025-04 (20.01.2025-27.01.2025)      |green   |261.9 Kb   |261.9 Kb   |47       |15.31    |incident
events-2025-05 (27.01.2025-03.02.2025)      |green   |130.9 Kb   |130.9 Kb   |15       |15.31    |incident
msg-2024-52 (23.12.2024-30.12.2024)         |green   |73.8 Kb    |73.8 Kb    |27       |15.31    |text
msg-2025-03 (13.01.2025-20.01.2025)         |green   |125.5 Kb   |125.5 Kb   |15       |15.31    |text
msg-2025-04 (20.01.2025-27.01.2025)         |green   |381.3 Kb   |381.3 Kb   |269      |15.31    |text
msg-2025-05 (27.01.2025-03.02.2025)         |green   |230.9 Kb   |230.9 Kb   |45       |15.31    |text
```

  Такая запись указывает на то, что индексы OpenSearch функционируют корректно (состояния индексов в кластере описаны выше).

- **-m, --message-counts** – выводит список соответствия индексов с количеством MIME-частей и сообщений.

  Пример вывода команды:

```
ds-mode@keodlp6 /opt/dozor # indextool -m
Host: https://localhost:9200
Timeout: 60 seconds
```

```
Executing...
Index name                                          |Messages   |Parts
-------------------------------------------------------------------------------
msg-2024-52 (23.12.2024-30.12.2024)                 |9          |18
msg-2025-03 (13.01.2025-20.01.2025)                 |5          |10
msg-2025-04 (20.01.2025-27.01.2025)                 |93         |176
msg-2025-05 (27.01.2025-03.02.2025)                 |15         |30
-------------------------------------------------------------------------------
Total messages: 122, parts: 234
```

- **-r**, **--reset-ro** – выводит сервис **opensearch** из состояния **read-only** (только чтение).
- **-rr**, **--reroute** – в случае ошибки перераспределяет копии индексов на свободные и доступные узлы кластера opensearch.
- **-t, --timeout <секунд>** – задает ограничение времени на исполнение программы (в секундах).

6.14. Работа с БД ClickHouse

Для работы сервиса **clickhouse**, запускаемого ролями **Контроль рабочего времени** и/или **Анализ поведения (UBA)**, используется СУБД ClickHouse. Для хранения данных, относящихся к функционированию одной и другой роли, создаются отдельные БД.

Для работы с БД ClickHouse необходимо подключиться к СУБД, выполнив в CLI команду следующего вида:

 # clickhouse-client --port 9001 -h <hostname>

где **<hostname>** – IP-адрес или FQDN узла, на котором находится БД. Если БД находится на том же узле, на котором выполняется команда – ключ **-h** необязателен. Если имя БД известно заранее, можно подключиться к ней, выполнив команду вида:

 # clickhouse-client --port 9001 -h <hostname> -d <db_name>

где **<db_name>** – имя БД.

После подключения к СУБД становятся доступны следующие действия:

- Показать имена имеющихся БД:

  SHOW DATABASES

- Выбрать БД:

  USE <db_name>

  где **<db_name>** – имя БД.

- Показать имена таблиц выбранной БД:

  SHOW TABLES

- Показать описание полей заданной таблицы:

DESC <table_name>

где **<table_name>** – имя таблицы.

Также доступны SQL-запросы. Для отключения от СУБД следует выполнить команду **exit** или **quit**.

6.15. Работа с ФХ

Для работы с ФХ используются следующие скрипты:

- **fsng** – скрипт для работы с ФХ. Позволяет получать файлы из хранилища, размещать их в нём и удалять из него, а также экспортировать контейнеры в хранилище (см. раздел 6.15.1).
- **import-messages.py** и **export-messages.py** – скрипты, используемые для переноса контейнеров из произвольной базы данных архива в БД ФХ. Подробнее см. разделы 6.13.4, 6.13.5, 6.13.6.
- **fs-backup.sh** – скрипт резервного копирования файлового хранилища (см. раздел 6.15.2).

6.15.1. Работа с ФХ с помощью скрипта fsng

Скрипт **fsng** предназначен для работы с ФХ с помощью CLI. Формат команды для запуска скрипта:

$ fsng [<ключ> ...] [<параметр>] ...

Скрипт необходимо запускать от имени пользователя **dozor**.

Скрипт имеет следующие команды:

- **get** – получить файл из хранилища.
- **put** – разместить файл или каталог в хранилище. Каталог перед размещением упаковывается архиватором.
- **delete** – удалить контейнер из хранилища.
- **export** – экспортировать контейнер в хранилище.

Доступны следующие ключи:

- **-u** – имя пользователя.
- **-r** – команда. Ставится перед командами **get**, **put**, **delete** и **export**.
- **-s** – путь для сохранения файла на локальной машины.
- **-f** – имя файла.

Ниже показаны примеры использования скрипта **fsng**.

1. Извлечение файла из контейнера в ФХ и сохранение его на локальной машине.

Чтобы извлечь файл из контейнера из ФХ и сохранить его на локальной машине, следует запустить скрипт **fsng get** с ключом **-s**, выполнив от имени пользователя **dozor** следующую команду:

**$ fsng -u dozor -r get **
https://<fs-server>:2266/vg-000000/c1b6ab8c-bbdb-11e3-8634-0050569225a4/data/body
-s /tmp/body.gz

где **c1b6ab8c-bbdb-11e3-8634-0050569225a4** – идентификатор vID контейнера, **<fs-server>** – FQDN узла, на котором организовано ФХ.

В результате выполнения команды на экран будет выведена информация следующего вида:

```
200 OK
transfer-encoding: chunked
last-modified: Fri, 04 Apr 2014 09:30:32 GMT
content-type: application/octet-stream
server: Funky(9.0.z-SNAPSHOT)
'Received: from 127.0.0.1\n\tby 127.0.0.1 with smtp (....'
```

2. Удаление контейнера с данными из ФХ.

Чтобы удалить из ФХ контейнер с данными, следует запустить скрипт **fsng delete**, выполнив от имени пользователя **dozor** следующую команду:

**$ fsng -u dozor -r delete -f body.gz **
https://<fs-server>:2266/vg-000000/c1b6ab8c-bbdb-11e3-8634-0050569225a4/

где **c1b6ab8c-bbdb-11e3-8634-0050569225a4** – идентификатор vID контейнера, **<fs-server>** – FQDN узла, на котором организовано ФХ.

В результате выполнения команды контейнер с данными будет удален из хранилища, а на экран будет выведена информация следующего вида:

```
200 OK
content-length: 0
server: Funky(9.0.z-SNAPSHOT)
```

3. Размещение файла в контейнере ФХ.

Чтобы разместить файл в контейнере ФХ, следует запустить скрипт **fsng put**, выполнив от имени пользователя **dozor** следующую команду:

**$ fsng -u dozor -r put -f tmp/body.gz **
https://<fs-server>:2266/vg-000000/c1b6ab8c-bbdb-11e3-8634-0050569225a4/

где **c1b6ab8c-bbdb-11e3-8634-0050569225a4** – идентификатор vID контейнера, **<fs-server>** – FQDN узла, на котором организовано ФХ.

4. Экспорт контейнера в ФХ.

Чтобы экспортировать контейнер в ФХ, следует запустить скрипт **fsng export**, выполнив от имени пользователя **dozor** следующую команду:

$ fsng -u dozor -r export -f /tmp/body.gz https://<fs-server>:2266/vg-000000/

6.15.2. Резервное копирование файлового хранилища

Скрипт **fs-backup.sh** предназначен для резервного копирования контейнеров файлового хранилища (в том числе с учетом ротированных данных). Формат команды для запуска скрипта:

$ /opt/dozor/smap/bin/fs-backup.sh [-s|-p|-d|-h|-last] [-volume volume_name] [-r] -dir BACKUP_DIR

Скрипт запускается от имени пользователя **dozor**. Пользователь **dozor** должен иметь права на запись в каталог, указываемый после ключа **-dir**.

Доступны следующие ключи:

- **-s** – резервирование контейнеров за период действия указанной секции. При использовании скрипта с этим ключом необходимо указать номер секции в используемой базе данных, идентификатор тома и путь к каталогу, в котором будут сохранены контейнеры ФХ. Пример:

  $ fs-backup.sh -s message_20190218 db-conn-3 -volume fs-1 -dir /backup/

- **-p** – резервирование контейнеров за определенный интервал времени. При использовании скрипта с этим ключом необходимо указать начальную и конечную даты желаемого интервала, идентификатор тома и путь к каталогу, в котором будут сохранены контейнеры ФХ. Пример:

  $ fs-backup.sh -p 2014/06/14 2014/06/16 -volume fs-1 -dir /backup/

- **-d** – резервирование контейнеров за определенное количество дней, предшествующих текущему моменту. При использовании скрипта с этим ключом необходимо указать количество дней, идентификатор тома и путь к каталогу, в котором будут сохранены контейнеры ФХ. Пример:

  $ fs-backup.sh -d 2 -volume fs-1 -dir /backup/

- **-h** – вывод справочной информации о команде.

- **-last** – резервирование заданного количества последних отключенных секций. При использовании скрипта с этим ключом необходимо указать количество секций и путь к каталогу, в котором будут сохранены контейнеры ФХ. Пример:

  $ fs-backup.sh -last 3 db-conn-3 -volume fs-1 -dir /backup/

- **-r** – удаление ротированных данных после резервирования.

- **-volume** – идентификатор тома файлового хранилища, подлежащий резервированию.

- **-dir** – путь к каталогу, в котором будут сохранены контейнеры.

6.15.3. Диагностика работы ФХ

Работа файлового хранилища обеспечивается сервисами **filestorage-ng** и **skvt-cassandra**. Чтобы проверить, запущены ли эти сервисы, следует запустить от имени пользователя

root скрипт **dsctl** с ключом **status** с указанием имени сервиса. Формат команды для запуска скрипта следующий:

 # dsctl status <service_name>

где **<service_name>** – имя сервиса, состояние которого требуется показать. Для вывода списка всех сервисов следует запустить скрипт **dsctl** без ключей.

Пример команды запуска скрипта **dsctl** для получения статуса сервиса **filestorage-ng**:

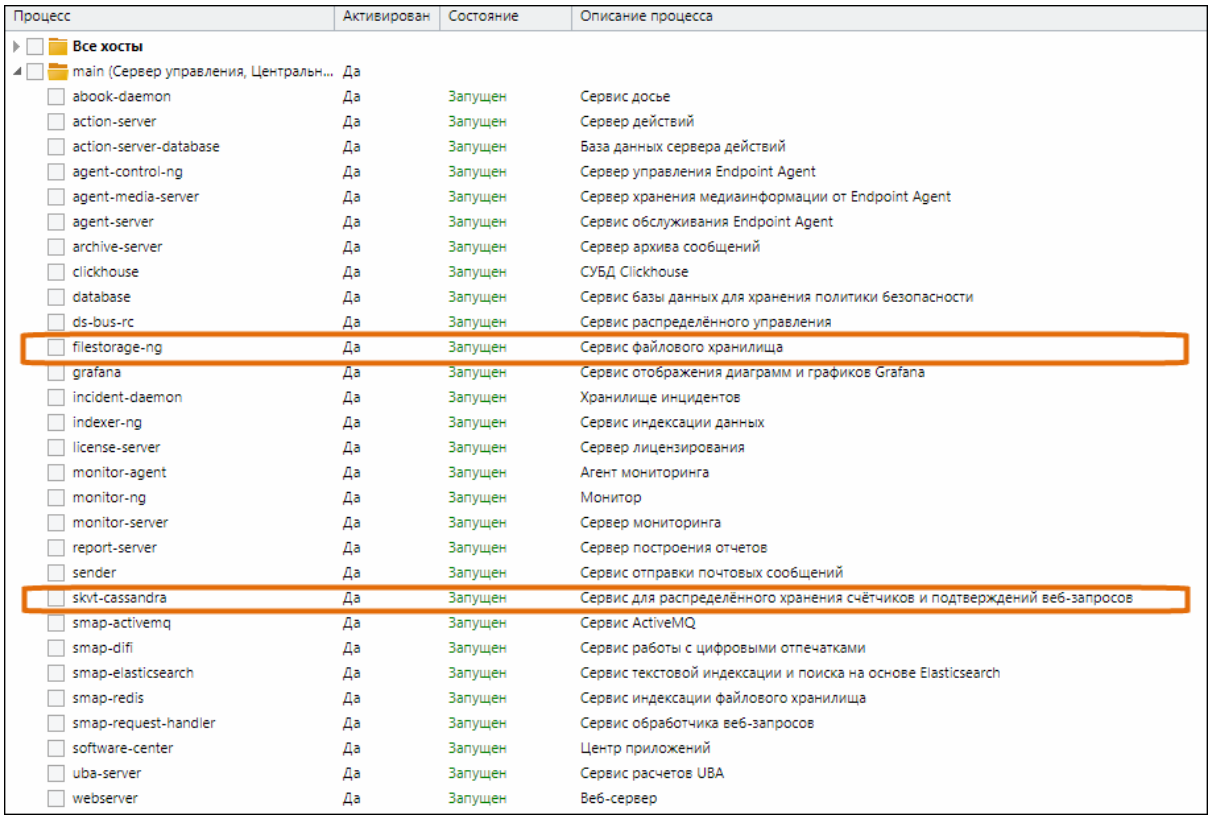
 # dsctl status filestorage-ng

В результате выполнения команды на экран будут выведены следующие сведения:

```
/opt/dozor/service/filestorage-ng: up (pid 13991) 72292 seconds
```

Такая запись указывает на то, что сервис **filestorage-ng** запущен (состояние **up**), указан идентификатор процесса **pid** и время непрерывной работы процесса в секундах.

Также состояние сервисов файлового хранилища можно посмотреть в разделе GUI **Система > Администрирование > Процессы**. В этом разделе показан список и состояние всех процессов KEO DLP. Процессы, имеющие отношение к файловому хранилищу, обведены оранжевой рамкой (см. Рис.6.5):



Процесс	Активирован	Состояние	Описание процесса
Все хосты			
main (Сервер управления, Центральн...	Да		
abook-daemon	Да	Запущен	Сервис досье
action-server	Да	Запущен	Сервер действий
action-server-database	Да	Запущен	База данных сервера действий
agent-control-ng	Да	Запущен	Сервер управления Endpoint Agent
agent-media-server	Да	Запущен	Сервер хранения медиаинформации от Endpoint Agent
agent-server	Да	Запущен	Сервис обслуживания Endpoint Agent
archive-server	Да	Запущен	Сервер архива сообщений
clickhouse	Да	Запущен	СУБД Clickhouse
database	Да	Запущен	Сервис базы данных для хранения политики безопасности
ds-bus-rc	Да	Запущен	Сервис распределённого управления
filestorage-ng	Да	Запущен	Сервис файлового хранилища
grafana	Да	Запущен	Сервис отображения диаграмм и графиков Grafana
incident-daemon	Да	Запущен	Хранилище инцидентов
indexer-ng	Да	Запущен	Сервис индексации данных
license-server	Да	Запущен	Сервер лицензирования
monitor-agent	Да	Запущен	Агент мониторинга
monitor-ng	Да	Запущен	Монитор
monitor-server	Да	Запущен	Сервер мониторинга
report-server	Да	Запущен	Сервер построения отчетов
sender	Да	Запущен	Сервис отправки почтовых сообщений
skvt-cassandra	Да	Запущен	Сервис для распределённого хранения счётчиков и подтверждений веб-запросов
smap-activemq	Да	Запущен	Сервис ActiveMQ
smap-difi	Да	Запущен	Сервис работы с цифровыми отпечатками
smap-elasticsearch	Да	Запущен	Сервис текстовой индексации и поиска на основе Elasticsearch
smap-redis	Да	Запущен	Сервис индексации файлового хранилища
smap-request-handler	Да	Запущен	Сервис обработчика веб-запросов
software-center	Да	Запущен	Центр приложений
uba-server	Да	Запущен	Сервис расчетов UBA
webserver	Да	Запущен	Веб-сервер

Рис. 6.5. Процессы файлового хранилища

Если нужный процесс не запущен, то следует установить флажок рядом с названием процесса и выбрать пункт меню **Запустить**.

В разделе **Система > Мониторинг > Подробные данные** можно просмотреть информацию о состоянии ресурсов системы, в том числе и процессов файлового хранилища. Для этого в списке показателей следует выбрать **Состояние сервиса – filestorage-ng** и **Состояние сервиса – skvt-cassandra** (см. Рис.6.6).

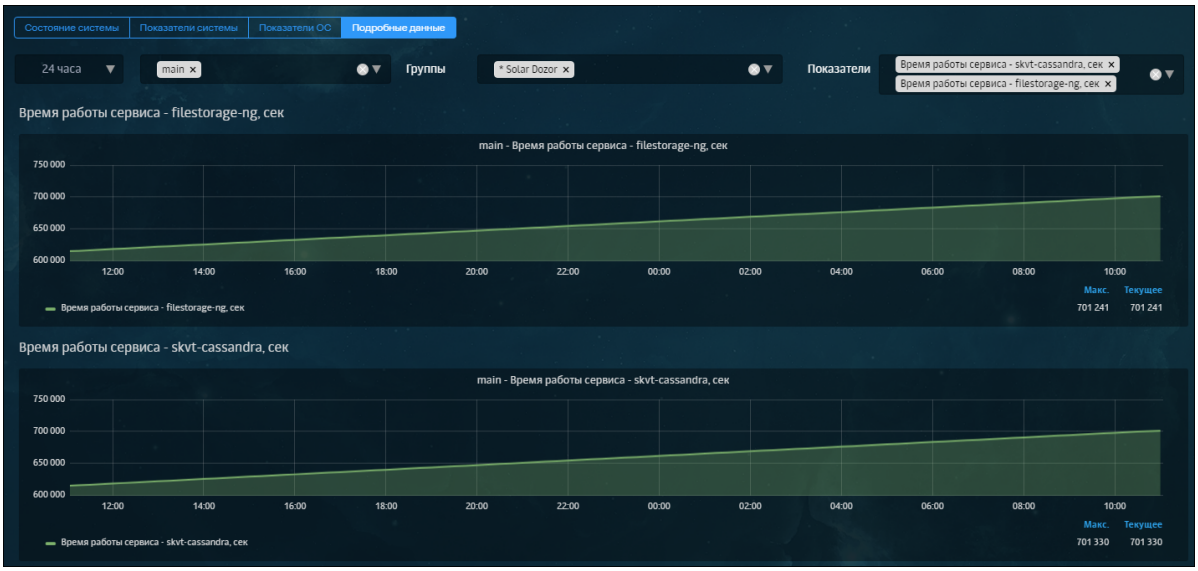


Рис. 6.6. Состояние процессов файлового хранилища

Подробнее о работе с журналами см. раздел 5.5.2.

6.16. Сопровождение фильтра KEO DLP

6.16.1. Генерация политики фильтра

Для генерации политики фильтра предназначен скрипт CLI **policy-tool**.

Для выполнения скрипта **policy-tool** необходимо выполнить следующие действия:

1. Запустить командную оболочку KEO DLP, выполнив следующую команду:

   # /opt/dozor/bin/shell

2. Выполнить команду, имеющую следующий формат:

   # policy-tool [<ключ>...] [<действие>...]

Доступны следующие ключи:

- **-h <HOST>**, **--host <HOST>** – указать IP-адрес или имя узла с БД политики (значение по умолчанию: **localhost**);
- **-p <PORT>**, **--port <PORT>** – указать порт, на котором БД политики ожидает соединения (значение по умолчанию: 5434);
- **-d <DB>**, **--database <DB>** – указать название БД политики (значение по умолчанию: **dozor**);

- **-u <имя пользователя>**, **--user <имя пользователя>** – выполнить скрипт от имени указанного в СУБД PostgreSQL пользователя (по умолчанию от имени пользователя **dozor**);
- **-w <пароль пользователя>**, **--password <пароль пользователя>** – указать пароль пользователя из СУБД PostgreSQL (по умолчанию пароль пользователя **dozor**);
- **--database-config <путь к конфигурации БД политики>** – указать путь к конфигурации БД политики;
- **-H <HOST>**, **--abook-host <HOST>** – указать IP-адрес или имя узла сервисом **abook-daemon** (если не указано, используется IP-адрес или имя узла с БД политики);
- **-P <PORT>**, **--abook-port <PORT>** – указать порт, на котором сервис **abook-daemon** ожидает соединения (значение по умолчанию: 2269);
- **--difi-host <HOST>** – указать IP-адрес или имя узла сервисом цифровых отпечатков (если не указано, используется IP-адрес или имя узла с БД политики);
- **--difi-port <PORT>** – указать порт, на котором сервис цифровых отпечатков ожидает соединения (значение по умолчанию: 9301);
- **--agent-control-host <HOST>** – указать IP-адрес или имя узла сервисом **agent-control** (если не указано, используется IP-адрес или имя узла с БД политики);
- **--agent-control-port <PORT>** – указать порт, на котором сервис **agent-control** ожидает соединения (значение по умолчанию: 3006);
- **-r <ID>**, **--root <ID>** – указать головной набор правил политики;
- **-l, --lang <LANGUAGE>** – выбрать язык, используемый для перевода (значение по умолчанию: **ru**, принимает значения **en** или **ru**).
- **--lang-resource-path <PATH>** – указать путь к каталогу с языковыми ресурсами (значение по молучанию: **/opt/dozor/lib/intl**).
- **-o <filename>**, **--output-file <filename>** – вывод результатов работы скрипта в указанный файл **<filename>**;
- **-i <filename>**, **--input-file <filename>** – указать файл **<filename>**, из которого импортируется политика в KEO DLP;
- **-f <format>**, **--input-format <format>** – указать формат файла, из которого выполняется импорт политики;
- **-m**, **--migration** – объединить системные списки слов, используется совместно с действием **import** и ключом **-i** (**--input-format**);
- **-F <format>**, **--output-format <format>** – указать формат файла, предназначенного для экспорта политики;
- **-a**, **--pairs** – указать необходимые для экспорта наборы правил, можно указать набор с определенным идентификатором в формате **rule-set:<ID>**;
- **-t, --transliteration-dir <PATH>** – указать путь к каталогу с таблицами транслитерации;

- **--debug** – включить ведение журнала отладки;
- **--force** – сбросить правила политики, используемые в параметрах групп рабочих станций;
- **--help** – вывести справку по работе со скриптом.

Доступны следующие действия:

- **graph** – напечатать граф политики в формате GraphML;
- **tgf** – напечатать граф политики в формате TGF;
- **generate** – сгенерировать политику и связанные с ней объекты;
- **list** – показать список доступных объектов политики;
- **print** – вывести подробную информацию по объектам политики;
- **stat** –вывести на экран статистику по политике;
- **check** – проверить наличие объектов политики, указанных в файле с названием **<filename1>** и вывести результаты в файл с именем **<filename2>**;
- **clear** – очистить политику в KEO DLP;
- **import** – импортировать политику в KEO DLP из файла;
- **export** – экспортировать политику KEO DLP в файл;
- **validate** – проверить политику на соответствие XSD.

Примеры использования скрипта:

1. Чтобы вывести на экран статистику по политике, следует запустить скрипт **policy-tool** с действием **stat**. Формат команды для запуска скрипта:

   # policy-tool stat

   В результате выполнения команды на экран будет выведена статистика по политике, например:

   ```
   cond 3
   rule-set 1
   storage-profile 4
   filter-file 5
   ```

2. Чтобы показать список доступных объектов политики, следует запустить скрипт **policy-tool** с действием **list**. Формат команды для запуска скрипта:

   # policy-tool list

   В результате выполнения команды на экран будут выведены объекты политики, например:

```
cond
  b3a9a348-6bc1-4635-ac76-99f6c3475a0b Проверка наличия текста
  636f6e64-ffff-ffff-ffff-ffff00000001 Имя файла pdf
  c5566f17-7587-44f5-bd26-ac3599933647 Мусор
rule-set
  72756c65-5f73-6574-ffff-ffff00000002 Все в архив
storage-profile
  73746f72-6167-655f-7072-6f6600000001 Зарегистрировать факт прохождения
  73746f72-6167-655f-7072-6f6600000002 Зарегистрировать
  73746f72-6167-655f-7072-6f6600000003 Поместить в архив
  73746f72-6167-655f-7072-6f6600000004 Поместить в архив без исходного текста
filter-file
  66696c74-6572-5f66-696c-65ff00000004 ms-office-mime-types
  66696c74-6572-5f66-696c-65ff00000005 crypt-mime-types
  a188ddf8-c9a2-472d-86e6-169adb9c9138 Мессенджеры
  f1598b6f-8c81-40a7-a70c-ee723a96fe08 Внутренний периметр
  c4cf095f-ffb7-4baf-b766-dbc7506c5bbd Облачные хранилища
```

3. Чтобы вывести подробную информацию по объектам политики, следует запустить скрипт **policy-tool** с действием **print**. Формат команды для запуска скрипта:

   # policy-tool print

   В результате выполнения команды на экран будут выведена детальная информация по объектам политики, например:

```
;; cond 636f6e64-ffff-ffff-ffff-ffff00000001 Все сообщения

{:type :cond,
 :id #uuid "636f6e64-ffff-ffff-ffff-ffff00000001",
 :name "Все сообщения",
 :value [:compound {:bool-op :and}]}

;; cond c5566f17-7587-44f5-bd26-ac3599933647 Мусор

{:type :cond,
 :id #uuid "c5566f17-7587-44f5-bd26-ac3599933647",
 :name "Mycop",
 :value
 [:compound
  {:bool-op :and,
   :args [[:atomic {:comp-op "eq", :type "m.size", :arg "-1"}]]}]}

;; rule-set 72756c65-5f73-6574-ffff-ffff00000002 Все в архив

{:id #uuid "72756c65-5f73-6574-ffff-ffff00000002",
 :name "Все в архив",
 :type :rule-set,
 :value
 ({:id #uuid "72756c65-ffff-ffff-ffff-ffff00000002",
   :cond #uuid "636f6e64-ffff-ffff-ffff-ffff00000001",
   :name "Все сообщения",
   :continue false,
   :enabled true,
   :actions
   ({:type :archive,
     :undo false,
```

```
    :storage-profile #uuid "73746f72-6167-655f-7072-6f6600000003"})}),
:refs
([:cond #uuid "636f6e64-ffff-ffff-ffff-ffff00000001"]
 [:storage-profile #uuid "73746f72-6167-655f-7072-6f6600000003"])}
```

4. Чтобы импортировать политику из файла, следует запустить скрипт **policy-tool** с действием **import** и ключом **-i**. Формат команды для запуска скрипта:

   # policy-tool -i <file> import

   В результате вывод команды имеет вид:

   ```
   Политика импортирована успешно
   ```

6.16.2. Просмотр информации об объектах политики

Для вывода информации о существующих в БД политики объектах (шаблонах уведомлений, правилах, условиях и т.д.) используется скрипт **objs.py**. Для выполнения скрипта необходимо выполнить следующие действия:

1. Запустить командную оболочку KEO DLP, выполнив следующую команду:

   # /opt/dozor/bin/shell

2. Запустить следующую команду:

   # objs <ключ>

Используются следующие ключи:

- **-E <имя пользователя>**, **--login-user <имя пользователя>** – задать имя существующего пользователя.
- **-S <пароль>**, **--login-password <пароль>** – указать пароль существующего пользователя.
- **-H <имя узла/IP>**, **--login-host <имя узла/IP>** – указать имя или IP-адрес узла, к которому подключается существующий пользователь.
- **-L <порт>**, **--login-port <порт>** – указать номер порта, к которому подключается существующий пользователь.
- **-D <имя БД>**, **--login-database <имя БД>** – указать имя БД, к которой подключается существующий пользователь.
- **-l**, **--label-types** – вывести на экран список всех пометок, присутствующих в сообщениях;
- **-C <описание пометки>**, **--create-label <описание пометки>** – создать новую пометку;
- **-c**, **--commands-templates** – вывести на экран список шаблонов внешних команд;
- **-n**, **--notifications-templates** – вывести на экран список шаблонов уведомлений;

- **-N <идентификатор шаблона уведомлений>**, **--notification-template <идентификатор шаблона уведомлений>** – вывести на экран информацию по указанному шаблону уведомлений;
- **-j**, **--journal-templates** – вывести на экран список шаблонов журнальных записей;
- **-o**, **--conditions** – вывести на экран список возможных условий;
- **-r**, **--rule-set** – вывести на экран список возможных наборов правил;
- **-w**, **--word-lists** – вывести на экран списки слов;
- **-W <идентификатор набора>**, **--word-list <идентификатор набора>** – вывести на экран информацию по указанному набору списка слов;
- **-U <идентификатор набора>**, **--upload-words <идентификатор набора>** – загрузить слова в набор списка слов (старые слова будут удалены);
- **-p**, **--list-relay-profiles** – вывести на экран информацию по профилям отправки;
- **-P <идентификатор профиля>**, **--show-relay-profile <идентификатор профиля>** – вывести на экран информацию по указанному профилю отправки;
- **-v** – вывести подробную информацию по работе со скриптом;
- **-d** – включить ведение журнала отладки;
- **-h** – вывести справку по работе со скриптом.

Примеры использования скрипта:

1. Чтобы вывести на экран список всех пометок, присутствующих в сообщениях, следует запустить скрипт **objs** с ключом **-l**. Формат команды для запуска скрипта:

   # objs -l

   В результате выполнения команды на экран будет выведен список пометок, например:

   ```
   92c56e09-eb97-41ca-a860-901d1d25e491 Ожидается подтверждение отправки
   bf97dfa1-e30c-4636-bf1b-a794468fc8ac СПАМ
   6c616265-6c5f-7479-7065-ffff0000002c Заблокировано
   ```

2. Чтобы вывести на экран список всех условий, следует запустить скрипт **objs** с ключом **-o**. Формат команды для запуска скрипта:

   # objs -o

   В результате выполнения команды на экран будет выведен список условий с идентификаторами, например:

   ```
   1277e683-b1b7-469c-b059-e146bb7e2c15 Проверка наличия текста
   72bf7e8f-7eb7-4ece-9e19-9119190c9c91 Имя файла pdf
   7229e11e-d822-4209-bc67-76c44cfaf15c Информационный объект
   ```

3. Чтобы вывести на экран список возможных правил, которые могут использоваться для генерации фильтра, следует запустить скрипт **objs** с ключом **-r**. Формат команды для запуска скрипта:

   # objs -r

   В результате выполнения команды на экран будет выведен список наборов правил с идентификаторами, например:

   ```
   7dc45677-ef0e-415a-9479-7a1413871a9c: Обработка ошибок [#policy.rule-set.handle-error]
   371152b7-43d6-411e-a0aa-5b954af69bc3: #["group.rule.set", "", "#abook.group.group002"]
   93f87d05-e3b3-404c-93b7-2189dc27ca8e: IN — Внутренние коммуникации
   676f72ac-acd4-4be4-b816-0db473960549: OU — Внешние коммуникации
   43995195-1483-4500-a0c8-57f0c5f3fbf4: #["group.rule.set", "Тульский филиал, ",
   "#abook.group.group002"]
   eeb2a828-0714-4cdd-a2d4-9abcc044c76d: Распознавание банковских карт
   7782594e-82f7-4235-a9f9-70cd7a94674e: Контроль целостности агента
   [#policy.rule-set.agent-integrity-control]
   ```

4. Чтобы вывести на экран список шаблонов внешних команд, следует запустить скрипт **objs** с ключом **-c**. Формат команды для запуска скрипта:

   # objs -c

   В результате выполнения команды на экран будет выведен список шаблонов внешних команд с идентификаторами, например:

   ```
   6cd665e1-1c9f-40f0-a5bf-2ab27b65e4ae: Новый шаблон внешних команд
   56567671-143f-1045-dfhd-234j23h35h33: Основной шаблон внешних команд
   ```

5. Чтобы вывести на экран список шаблонов журнальных записей, следует запустить скрипт **objs** с ключом **-j**. Формат команды для запуска скрипта:

   # objs -j

   В результате выполнения команды на экран будет выведен список шаблонов журнальных записей с идентификаторами, например:

   ```
   5c040ae4-c3ca-4cde-8605-0004602617ea: Новый шаблон журнальной записи
   ```

6.16.3. Создание отчетов по состоянию фильтра

Для создания отчетов по состоянию сервиса **mailfilter** предназначен скрипт **mailfilter-report**. Отчеты включают в себя следующую информацию:

- версию, сборку и состояние переменных среды KEO DLP
- последние 3000 записей журнала сервиса **mailfilter**
- сгенерированную политику фильтрации
- конфигурации сервиса **mailfilter**
- файлы ошибок из **error-spool**

- статистику спулов фильтрации
- информацию по диску

Для работы со скриптом необходимо запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта **mailfilter-report**:

 # mailfilter-report

В результате выполнения команды на экран выводится следующая информация:

```
Creating mailfilter report:
Report dir: /opt/dozor/smap/tmp/mailfilter-report.1531221267
- last 3000 lines of log
- generated policy dir
- mailfilter configuration (all nodes)
/data/repos/dozor/config-final.git/0c3416cd-d8e3-408d-b604-eff2d104c253/mailfilter/mailfilter.edn
/data/repos/dozor/config-final.git/a0a0a91d-897b-42ad-8b21-9f3580d4727a/mailfilter/mailfilter.edn
- errors from error spool
- spool stat
- disk info
Mailfilter report archive created: /opt/dozor/smap/tmp/mailfilter-report.1531221267.tar.bz2
```

6.16.4. Анализ журналов фильтра

Для анализа журналов фильтра, собранных в режиме отладки, предназначен скрипт **mfprof**. По завершении работы скрипта формируется отчет, который содержит данные о временных затратах на проверку наиболее часто встречающихся типов файлов и сообщений, каналов коммуникаций и шаблонов документов.

Примечание

*Собирать такую же статистику работы сервиса mailfilter также можно в разделе GUI **Система > Узлы и Роли** с помощью скрипта **mailfilter-profiling**.*

Для работы со скриптом необходимо запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат команд для запуска скрипта **mfprof**:

 # mfprof [ключ] <file1> <file2> ... <fileN>

 # cat <file1> <file2> ... <fileN> | mfprof [ключ]

 # seelog mailfilter <количество последних строк журнала> | mfprof [ключ]

где:

- **<file1> <file2> ... <fileN>** – журнальные файлы сервиса **mailfilter**.

- **ключ** – один из доступных ключей.

Доступны следующие ключи:

- **-o <file1> <file2> ... <fileN>**, **--output <file1> <file2> ... <fileN>** – вывести результаты работы скрипта в файл.
- **-h**, **--help** – вывести справку по работе со скриптом.

Пример фрагмента вывода скрипта:

```
==== Messages stat ====
Total messages processed: 345
Archived: 86 Blocked: 0 Sent 0 Events 0
Total proc time: 0:00:32 Timing [12 | 18 |> 26 <| 42 | 2386] ms
Total sizes: 260.8 Kb Sizing [701 | 737 |> 770 <| 811 | 896] bytes
```

Записи выше свидетельствуют о том, что проверено 345 сообщений общим объемом в 260.8 Кб за 32 секунды. Минимальное и максимальное значения извлекаются из нижней и верхней границы журнала, в этом примере 701 и 896 байт, обработанные за 12 и 2386 мс соответственно. 25% сообщений объемом меньшим или равным 737 байт обработано за 18 мс, а 75% – большим или равным 811 б обработано за 42 мс. Сообщения объемом 770 байт обработаны за 26 мс. Значения 770 и 26 являются средними по отношению к своему ряду и заключены между символами |> и <|.

6.16.5. Настройка приема сообщений по протоколу ICAP

Протокол ICAP (RFC 3507) позволяет сервису **mailfilter** обмениваться данными с внешними клиентами (обычно – с прокси-серверами). С помощью этого протокола **mailfilter** получает от прокси данные для анализа и отправляет в ответ результат применения политики.

Для настройки приема сообщений по протоколу ICAP следует перейти в секцию **Сервис фильтрации сообщений** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений**), включить использование ICAP-интерфейса в настройках сервиса фильтрации и указать проверяемые типы сообщений, задав для параметров следующие значения:

- **Включить ICAP-интерфейс** – установить флажок.
- **Порт ICAP-интерфейса** – 2344.

  Примечание

  По умолчанию используется значение 2344. Его можно изменить на 1344 согласно RFC.

- **Обрабатывать только указанные MIME-типы** – установить флажок.
- **MIME-типы** – задать список MIME-типов сообщений, проверяемых ICAP-интерфейсом.
- **Не обрабатывать сообщения без тела** – установить флажок.
- **Выдавать ответ с кодом 200/204 при ошибках обработки** – установить флажок.

После этого необходимо выполнить настройку клиента, чтобы он мог обмениваться данными с фильтром. Для этого следует указать URL-адрес, по которому будет передаваться трафик.

Сообщения проходят полную (выполняется контроль информационных объектов и групп особого контроля) или ограниченную (без учета контроля информационных объектов и групп особого контроля) проверки в соответствии с заданными в KEO DLP правилами политик, начиная с головного набора правил.

Некоторым прокси-серверам не требуется результат обработки сообщения по политике. В этом случае отправленное в **mailfilter** сообщение будет перемещено в спул, а ICAP-клиент получит от прокси-сервера ответ, не дожидаясь обработки файла.

Исходя из типов проверки, можно указать следующие значения:

- **icap://<icap-mailfilter>:2344/icap/full** – полная проверка сообщений;
- **icap://<icap-mailfilter>:2344/icap/fast** – ограниченная проверка сообщений;
- **icap://<icap-mailfilter>:2344/icap/filter** – полная проверка сообщений с получением ответа с результатами проверки в JSON-формате;
- **icap://<icap-mailfilter>:2344/icap/filter/fast** – ограниченная проверка сообщений с получением ответа с результатами проверки в JSON-формате;
- **icap://<icap-mailfilter>:2344/icap/spool** – перемещение сообщений в спул **mailfilter**,

где **<icap-mailfilter>** – IP-адрес узла с сервисом **mailfilter**.

Подробное описание запросов к API сервиса фильтрации приведена в документе *Спецификация интеграции внешних систем с KEO DLP для приема сообщений на обработку по протоколу ICAP*.

6.16.6. Настройка идентификации трафика от внешних источников

Сервис **mailfilter** принимает сообщения из спула, а также от внешних источников по протоколам HTTP/ICAP. Изначально при мониторинге показателей KEO DLP невозможно определить, от какой сторонней системы поступает трафик на сервер фильтрации, есть ли проблемы с обработкой трафика и т.д. Чтобы KEO DLP смог идентифицировать внешние источники в ICAP-трафике, необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений > Сервис фильтрации сообщений**.
2. Настроить прием сообщений по протоколу ICAP в соответствии с разделом 6.16.5.
3. В строке **ICAP-источники** нажать кнопку **Добавить** и задать значения следующих параметров:
   - **Метка источника** – ввести название, отражающее реалии ICAP-источника.
   - **Имя заголовка** – ввести имя заголовка, определяющего источник.

- **Значение заголовка (точное совпадение или регулярное выражение)** – ввести значение заголовка, определяющего источник.

4. Нажать **Сохранить**.

5. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование системы > Мониторинг > Сервер мониторинга**.

6. Раскрыть строку **ICAP-интерфейс** и в раскрывшемся списке задать значения следующих параметров:

   - **Период проверки отсутствия принятых фильтром сообщений** – оставить значение по умолчанию, равное 10 минутам.

   - **Период проверки отсутствия обработанных фильтром сообщений** – оставить значение по умолчанию, равное 10 минутам.

   - **Пороговое значение количества ошибок в ответах фильтра** – оставить значение по умолчанию, равное 10.

7. Раскрыть строку **Рабочее время, в течение которого следует проверять отсутствие сообщений** и заполнить обязательные поля значениями по усмотрению или согласно реалиям организации.

8. Нажать **Сохранить** и **Применить**.

Внимание!

В связи с особенностями настройки обнаружения ICAP-источников в системе мониторинга Zabbix время между применением конфигурации и попаданием информации о них в KEO DLP может составлять:

- *при добавлении или изменении источников – от нескольких минут до 1 часа.*

- *при удалении источников – от 12 до 24 часов.*

Примечание

*Параметр **Рабочее время, в течении которого следует проверять отсутствие сообщений** не учитывает выходные и праздничные дни.*

6.17. Управление структурой спулов для хранения сообщений

Спул (spool) представляет собой некоторую структуру каталогов файловой системы, предназначенную для временного хранения исходных данных определенного сервиса. В KEO DLP имеется возможность создавать и управлять структурой спулов хранения сообщений для сервисов фильтрации (**mailfilter**), архивирования (**archiver**) и отправки сообщений (**sender**).

Каждый спул состоит из слотов, которые представляют собой каталоги нижнего уровня в корневом каталоге спула. При этом слоты могут быть как одного типа и применяться

для распределения нагрузки при чтении и записи данных, так и использоваться для хранения данных разных типов, например, для простых сообщений или для сообщений с высоким приоритетом. Подробнее о разных типах слотов см. 6.17.1.

Слоты могут использоваться как точки монтирования файловых систем для распределения нагрузки между дисками при записи и чтении данных. При этом в каждый момент времени для записи и чтения могут использоваться любые наборы имеющихся слотов. Запись данных выполняется равномерно во все доступные для записи слоты, то есть по одному сообщению последовательно в каждый слот. Так же и чтение сообщений выполняется из всех доступных для чтения слотов, при этом очередность чтения соответствует очередности записи.

6.17.1. Управление конфигурацией слотов

Параметры конфигурации слотов для сервисов фильтрации, архивирования и отправки сообщений определяются в группе параметров **Спул сообщений** и редактируются в секции **Сервис фильтрации сообщений** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений**). Можно указать количество слотов разного типа, набор слотов, доступных для записи и чтения (Рис.6.7):

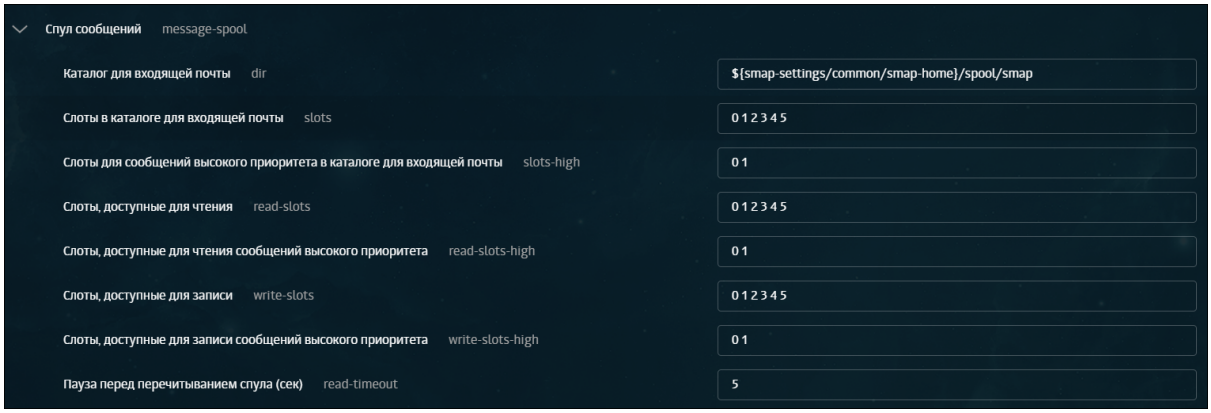


Рис. 6.7. Настройки спула сообщений

Для конфигурирования слотов для сервиса фильтрации используются следующие параметры:

1. **Каталог для входящей почты**.

   Этот параметр определяет каталог (спул), в котором хранятся исходные данные. Для сервиса фильтрации это каталог **${smap-settings/common/smap-home}/spool/smap** (далее имена каталогов будут указаны относительно каталога **${smap-settings/common/smap-home}**, то есть в данном случае каталог для хранения данных сервиса фильтрации – **spool/smap**).

2. **Слоты в каталоге для входящей почты**.

   Этот параметр определяет количество слотов для сообщений с нормальным приоритетом в каталоге для входящей почты. Значение параметра **0 1 2 3 4 5** означает, что в спуле имеется шесть слотов с именами **spool/smap/norm0**, **spool/smap/norm1**, **spool/smap/norm2**, **spool/smap/norm3**, **spool/smap/norm4** и **spool/smap/norm5**.

3. **Слоты для сообщений высокого приоритета в каталоге для входящей почты**.

   Этот параметр определяет слоты для сообщений с высоким приоритетом. Значение параметра **0** означает, что в каталоге для входящей почты имеется один слот для сообщений с высоким приоритетом с именем **spool/smap/high0**. Значение параметра **0 1** означает, что имеется два слота с именами **spool/smap/high0** и **spool/smap/high1**. И так далее.

4. **Слоты, доступные для чтения**.

   Этот параметр определяет слоты, доступные для чтения. Например, значение параметра **0 1 2 3 4 5** означает, что чтение сообщений с нормальным приоритетом выполняется последовательно из каталогов **spool/smap/norm0**, **spool/smap/norm1**, **spool/smap/norm2**, **spool/smap/norm3**, **spool/smap/norm4** и **spool/smap/norm5**.

5. **Слоты, доступные для чтения сообщений высокого приоритета**.

   Этот параметр определяет слоты, доступные для чтения сообщений с высоким приоритетом. Например, значение параметра **0 1** означает, что чтение сообщений с высоким приоритетом выполняется последовательно из каталогов **spool/smap/high0**, **spool/smap/high1**.

6. **Слоты, доступные для записи**.

   Этот параметр определяет слоты, доступные для записи. Например, значение параметра **0 1 2 3 4 5** означает, что запись входящих сообщений с нормальным приоритетом будет выполняется равномерно в каталоги **spool/smap/norm0**, **spool/smap/norm1**, **spool/smap/norm2**, **spool/smap/norm3**, **spool/smap/norm4** и **spool/smap/norm5**.

7. **Слоты, доступные для записи сообщений высокого приоритета**.

   Этот параметр определяет слоты, доступные для записи сообщений с высоким приоритетом. Например, значение параметра **0 1** означает, что запись входящих сообщений с высоким приоритетом будет выполняется равномерно в каталоги **spool/smap/high0**, **spool/smap/high1**.

8. **Пауза перед перечитыванием спула**.

   Этот параметр определяет периодичность обработки спула сообщений сервисом **mailfilter** в секундах. Значение по умолчанию: 5.

Примечание

*Для сообщений, обработка которых завершилась с ошибкой, существует один слот, всегда доступный для записи, размещаемый в каталоге **spool/smap/err0**. Слот такого типа создается автоматически, поэтому соответствующего параметра настройки на вкладке **Конфигурация** нет.*

Конфигурация слотов для сервисов архивирования и отправки сообщений аналогична, за исключением того, что для сервиса архивирования нет понятия сообщений высокого приоритета.

Далее необходимо применить конфигурацию, запустив от имени пользователя **root** скрипт **accept-settings**:

 # /opt/dozor/bin/accept-settings

Примечание

*Изменение наборов слотов, доступных для чтения и записи, не требует применения конфигурации, если оно не касается настройки процесса **smap-smtp-gw** (в этом случае следует нажать в меню вкладки кнопку **Сохранить**, затем **Применить**, см. Рис.6.7).*

6.17.2. Иерархическая структура спулов

Спул сообщений каждого сервиса состоит из слотов разного назначения, которые используются для хранения данных разных типов, например, для сообщений с высоким приоритетом. Слот в свою очередь представляет собой иерархию каталогов с фиксированной глубиной вложенности. Иерархия представляет собой список целых чисел, так называемых делителей. При записи каждого сообщения в слот, каталог, в который оно будет помещено, определяется как результат целочисленного деления текущего числа секунд (которое определяется по показаниям системных часов операционной системы) на соответствующий делитель. Пустой список делителей является частным случаем и соответствует стандартному «плоскому» спулу.

Следующий пример показывает, как создается иерархия каталогов в слоте сообщений.

В KEO DLP задана следующая иерархия в каталоге для входящей почты: 3600 700 50 и текущее время (то есть количество секунд) по показаниям системных часов: 1244444878. Тогда для записи сообщения в корневом каталоге соответствующего слота будет создан каталог с именем, равным числу, которое получено делением текущего времени на первый делитель: 1244444878 поделить на 3600, получится 345679. То есть для сообщения будет создан каталог (если такого еще нет) с именем 345679, в который будут записываться также сообщения, пришедшие в течение следующего часа (3600 секунд равняются одному часу).

В этом каталоге будет создан вложенный каталог, имя которого определяется делением на второй делитель: 1244444878 поделить на 700, получится 1777778. В этот каталог будут также записываться сообщения, пришедшие в течение следующих 11 минут (700 секунд).

В каталоге с именем 2074074 будет создан каталог следующего уровня вложенности, имя которого определяется делением на третий делитель: 1244444878 поделить на 50, получится 24888898. Каталог с этим именем будет использоваться для записи приходящих сообщений в течение следующих 50 секунд.

Таким образом, сообщение будет записано в каталог с именем **spool/smap/norm0/345679/1777778/24888898**.

Удалением неиспользуемых каталогов занимается сервис, который читает данные из спула. При этом каталог считается неиспользуемым, если он не содержит сообщений и вложенных каталогов, и если согласно текущей настройке конфигурации он не должен использоваться в данный момент.

Чтение сообщений из иерархической структуры каталогов происходит в соответствии с очередностью – каталоги сортируются по возрастанию их числовых имен, а сообщения в каталогах по дате изменения файлов.

6.17.3. Просмотр состояния спулов

Чтобы получить информацию о состоянии спулов (количество сообщений в них и объем дискового пространства), можно воспользоваться скриптом **spool-stat.py**.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат команды для запуска скрипта **spool-stat.py**:

$ spool-stat.py <ключ> <spool-id> <spool-id> ... <spool-id>

где **spool-id** – идентификатор спула, который может принимать одно из следующих значений:

- **sender** – все спулы сервиса отправки;
- **sender-norm** – слоты спула сервиса отправки, используемые для размещения простых сообщений;
- **sender-high** – слоты спула сервиса отправки, используемые для размещения сообщений высокого приоритета;
- **sender-err** – слоты спула сервиса отправки, используемые для размещения сообщений, при обработке которых произошла ошибка.
- **mailfilter-norm** – слоты спула сервиса фильтрации, используемые для размещения простых сообщений;
- **mailfilter-high** – слоты спула сервиса фильтрации, используемые для размещения сообщений высокого приоритета;
- **mailfilter-err** – слоты спула сервиса фильтрации, используемые для размещения сообщений, при обработке которых произошла ошибка.
- **archiver-err** – слоты спула сервиса архивации, используемые для размещения сообщений, при обработке которых произошла ошибка.
- **archiver-norm** – слоты спула сервиса архивации, используемые для размещения простых сообщений;

Используются следующие ключи:

- **-i**, **--internal** – использовать встроеное чтение очередей.
- **-j**, **--json** – вывести информацию в формате **json**.
- **-d**, **--debug** – вывести отладочную информацию по ходу выполнения скрипта.

- **-v**, **--verbose** – вывести подробную информацию по ходу выполнения скрипта.
- **-h**, **--help** – вывести справочную информацию о скрипте.

Пример вывода информации по всем спулам сервиса отправки:

```
sender-norm:
/opt/dozor/smap/spool/smap-send/norm0 rw 1 messages 2 files 1 kbytes
/opt/dozor/smap/spool/smap-send/norm1 rw 2 messages 4 files 1 kbytes
total  3 messages 6 files 2 kbytes
sender-high:
/opt/dozor/smap/spool/smap-send/high0 rw 34 messages 68 files 19 kbytes
total  34 messages 68 files 19 kbytes
sender-err:
/opt/dozor/smap/spool/smap-send/err0 rw 18 messages 36 files 10 kbytes
total  18 messages 36 files 10 kbytes
```

Пример вывода информации по слотам **archiver-norm**:

```
archiver-norm:
/opt/dozor/smap/spool/smap-db/norm0 rw 5 messages 0 fs-messages 0 events
0 screenshots 1 levels 10 files 6 kbytes
/opt/dozor/smap/spool/smap-db/norm1 rw 0 messages 0 fs-messages 0 events
0 screenshots 0 levels 0 files 0 kbytes
/opt/dozor/smap/spool/smap-db/norm2 rw 0 messages 0 fs-messages 0 events
0 screenshots 0 levels 0 files 0 kbytes
/opt/dozor/smap/spool/smap-db/norm3 rw 0 messages 0 fs-messages 0 events
0 screenshots 0 levels 0 files 0 kbytes
/opt/dozor/smap/spool/smap-db/norm4 rw 0 messages 0 fs-messages 0 events
0 screenshots 0 levels 0 files 0 kbytes
/opt/dozor/smap/spool/smap-db/norm5 rw 0 messages 0 fs-messages 0 events
0 screenshots 0 levels 0 files 0 kbytes
total  5 messages 0 fs-messages 0 events 0 screenshots 1 levels 10 files 6 kbytes
```

Пример вывода информации по слотам **archiver-err**:

```
archiver-err:
/opt/dozor/smap/spool/smap-db/err0 rw 5 messages 0 fs-messages 0 events
0 screenshots 1 levels 10 files 6 kbytes
total  5 messages 0 fs-messages 0 events 0 screenshots 1 levels 10 files 6 kbytes
```

Пример вывода информации по слотам **mailfilter-err**:

```
mailfilter-err:
/opt/dozor/smap/spool/smap/err0 rw 309 messages 927 files 1878053 kbytes
total  309 messages 927 files 1878053 kbytes
```

Посмотреть состояние спулов можно также на вкладке **Очереди** раздела GUI **Система > Администрирование** (см. Рис.6.8):

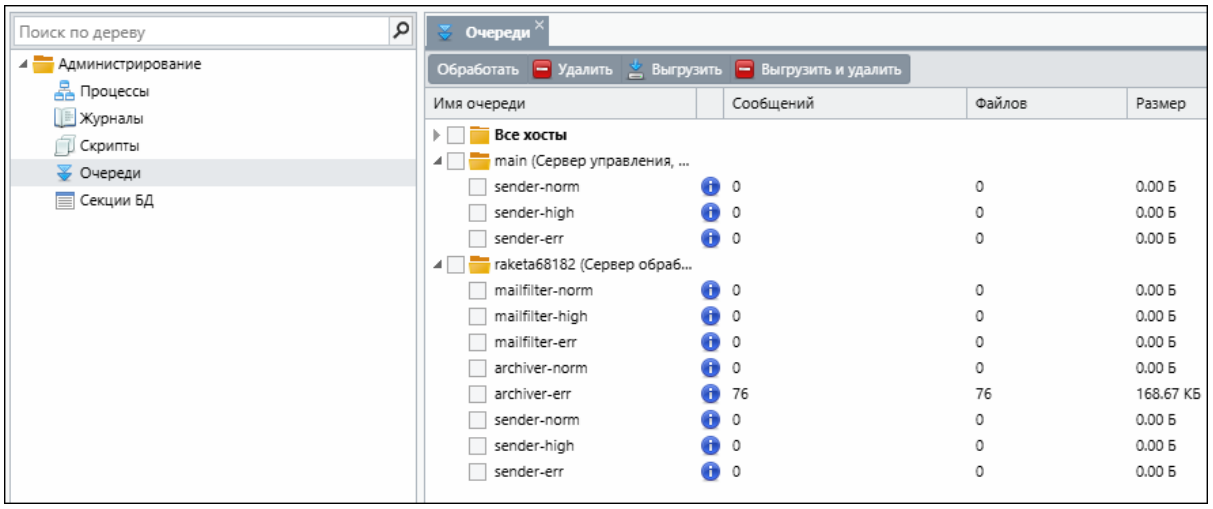


Рис. 6.8. Просмотр состояния очереди сообщений

6.17.4. Перенос сообщений между спулами

С помощью скрипта **spool-move.py** можно переносить сообщения между спулами. Перенос возможен только между спулами одного сервиса. При этом нельзя переносить сообщения из слотов, с которыми в данный момент работает читающий или записывающий сервис. Но наоборот, помещать сообщения в такие слоты можно.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат команды для запуска скрипта **spool-move.py** выглядит следующим образом:

$ spool-move.py [ключ] <spool-id> [ключ] <spool-id>

где **spool-id** – идентификатор спула, возможные значения которого приведены в 6.17.3.

Скрипт необходимо запускать от имени пользователя **dozor**.

Используются ключи:

- **-f** – указывает на спул, из которого следует перенести сообщения;
- **-t** – указывает на спул, в который следует перенести сообщения.

Например, команда:

$ spool-move.py -f archiver-err -t archiver-norm

переместит сообщения из слота **spool/smap/err0** (независимо от его структуры) в спул **spool/smap/norm0** и разложит их в слоты, доступные для записи, в соответствующую иерархическую структуру.

Кроме того, доступны некоторые другие ключи. Примеры использования скрипта **spool-move.py** с этими ключами рассмотрены ниже:

- Изменение иерархии целевого спула (ключ **-c**):

  $ spool-move.py -f archiver-err -t archiver-norm -c '3600' '300' '1'

  Эта команда переносит сообщения из слота **spool/smap/err0** (независимо от его структуры) в слоты спула сервиса архивирования, доступные для записи, в иерархическую структуру с конфигурацией **3600 300 1** (см. раздел 6.17.2).

- Перенос сообщения из произвольного каталога (ключ **-s**) или в произвольный каталог (ключ **-d**):

  $ spool-move.py -f sender-norm -d /var/tmp/d1

  Эта команда переносит сообщения из слотов, доступных на чтение, спула для сообщений, ожидающих отправки, в каталог **/var/tmp/d1** в структуру **3600 700 50**.

  В результате выполнения команды на экран выводится следующая информация:

```
Сервис: sender
Перемещаем сообщения из каталогов:
/opt/dozor/smap/spool/smap-send/norm0
/opt/dozor/smap/spool/smap-send/norm1
в каталоги:
/var/tmp/d1
с настройкой иерархии: 3600 700 50
Регулярное выражение для головного файла: ^(norm|high)[-0-9a-f]*$
Ограничение на количество: -
norm-3e6413f8-c99c-4b4c-ab4d-50cd5a249300
norm-03a762f4-63bc-444c-aa9b-c675ec06d118
norm-f0aa2b12-8f8a-4e3a-9bfc-d29622246c2b
Перемещено сообщений: 3
Ошибок: 0
```

  Аналогично следующая команда перенесет сообщения из произвольного каталога в слоты, доступные для записи, предназначенные для хранения сообщений высокого приоритета, ожидающих отправки:

  $ spool-move.py -s /var/tmp/d1 -t sender-high

- Перенос сообщения из произвольного каталога в произвольный каталог:

  $ spool-move.py -f archiver-norm -s /var/tmp/a1 -d /mnt/disk0

  При переносе сообщений из произвольных каталогов в произвольные должен быть указан **spool-id** (аргументом **-t** или **-f**), даже если все параметры конфигурации переопределены аргументами командной строки. Это требуется для идентификации сервиса, к которому относятся переносимые сообщения. Так, указанная команда перенесет сообщения в формате сервиса архивирования из каталога **/var/tmp/a1** в каталог **/mnt/disk0**.

- Ограничение количества переносимых сообщений (ключ **-n**):

  $ spool-move.py -f archiver-err -t archiver-norm -n 1000

  Эта команда перенесет 1000 сообщений из слота **spool/smap/err0** в слоты спула сервиса архивирования, доступные для записи.

- Остановка выполнения программы для контроля правильности указанных параметров (ключ **--arg-check**):

  $ spool-move.py -f archiver-err -t archiver-norm -n 1000 --arg-check

  Перед выполнением переноса сообщений программа **spool-move.py** выводит все данные разбора конфигурации, а также данные, определенные указанными ключами. На экран выводятся каталоги, откуда и куда будет выполнен перенос, параметры иерархии, ограничение на количество переносимых файлов и т.д. Ключ **--arg-check** останавливает выполнение программы после вывода этих данных для контроля правильности аргументов, переданных командой.

- Получение списка возможных ключей (ключ **-h**):

  $ spool-move.py -h

  Эта команда выводит на экран список возможных ключей программы **spool-move.py**.

- Удаление сообщений из спула (ключ **-r**, **--remove-from-spool**):

  $ spool-move.py -r <spool-id>

  $ spool-move.py --remove-from-spool <spool-id>

  где **spool-id** – идентификатор спула, возможные значения которого приведены в 6.17.3.

  В результате выполнения команды на экран выводится следующая информация:

```
Очищаем /opt/dozor/smap/spool/smap-send/norm0
Очищаем /opt/dozor/smap/spool/smap-send/norm1
```

6.18. Использование списков слов уверенного определения кодировки

Статистический алгоритм для определения языков и кодировок сообщений использует принцип максимального правдоподобия. Этот принцип сравнивает частоты встречаемости частей исследуемого текста с частотами эталона, выбранного для каждого естественного языка. Таким эталоном служит набор текстов на каждом языке, сконвертированных в интересующее множество кодировок. Наиболее близкий результат признается за распознанную кодировку (язык) с соответствующим числом похожести, посчитанным для всех эталонных карт.

Для большинства длинных текстов, содержащих распространенные слова, этот метод позволяет достаточно точно определить кодировку. Но на менее распространенных, нетипичных (чаще всего, заимствованных) словах метод дает ошибочные результаты.

Для устранения нечитаемых из-за неверно определенной кодировки частей сообщений была реализована поддержка списков слов, наиболее актуальных для конкретного пользователя. Эти списки называются списками слов уверенного определения. Они хранятся в файлах **/opt/dozor/mapsbase/<язык>.<диалект>.dic**

где:

- **язык** – значение из списка {ru, en, uk, ja, vi, de, fr};

- **диалект** – означает либо диалект, либо тематику эталонных текстов, рекомендуемое значение: common (общеиспользуемые слова).

Например, в файле **ru.common.dic** хранится список общеиспользуемых слов русского языка.

Данные в файлах списков хранятся в текстовом формате, в кодировке utf-8. При этом каждое слово отделено символом новой строки.

Принцип работы метода определения кодировки с использованием указанных списков слов: если исследуемый текст короткий, то в тексте производится поиск каждого слова из списка в каждой используемой для данного языка кодировке. В случае успеха определенной кодировкой признается та, в которой нашлось слово из списка. Данный метод применяется в тех случаях, когда полученное KEO DLP сообщение, содержащее текстовые части небольшой длины, нечитаемо из-за неверно определившейся кодировки текста части сообщения.

Для создания нового списка слов необходимо средствами ОС в каталоге **/opt/dozor/mapsbase/** создать файл списка.

Для добавления слова в определенный список необходимо выполнить команду:

 # echo <слово> >> /opt/dozor/mapsbase/<словарь>

Например, для добавления слова «телефон» в список **ru.common.dic** необходимо выполнить команду

 # echo телефон >> /opt/dozor/mapsbase/ru.common.dic

Внимание!

*После создания или изменения словарей необходимо перезапустить процесс **mailfilter**.*

6.19. Работа с досье

Досье располагается в отдельной БД PostgreSQL на master-узле (по умолчанию это БД, в которой размещена политика фильтрации). LDAP(S)-серверы организации могут являться источниками информации для досье, которых может быть несколько. Для каждого источника в конфигурации настраиваются: параметры подключения к LDAP(S); отображение полей в досье; приоритеты источников данных для каждого атрибута персоны.

Досье синхронизируется с существующей структурой каталогов организации (Active Directory, ALD Pro, 389 Directory Server) по запросу от сервиса **abook-daemon**. Информация в досье может пополняться и редактироваться как вручную с помощью интерфейса, так и с помощью внешних источников, подключаемых через API extinfo. Программа синхронизации загружает из каталога начальную информацию о персонах: ФИО, фото, email-адреса, принадлежность к группам.

Примечание

При синхронизации с источником, в котором есть персона, у которой есть ссылка на группу (primary group), но этой группы нет в источнике, данная персона будет пропущена.

Примечание

Если в карточке персоны, полученной из LDAP, в параметрах ФИО, должность, дата рождения и отдел нет значений, то при задании им значений они успешно сохраняются. При этом сохраняются только перечисленные реквизиты, остальные реквизиты карточки персоны редактировать нельзя. Если у этих параметров есть значения, то они не редактируются.

Если синхронизация с одним или несколькими серверами LDAP, указанными в настройках системы в качестве источников, невозможна, система генерирует и отправляет администратору уведомление на адрес, указанный в параметре **Имя почтового ящика** секции **Общие настройки системы** (раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование системы > Общее**). Более подробно описано в разделе **Приложение А, *Параметры конфигурации KEO DLP***. Допустимо указание в конфигурации нескольких адресатов. Для этого в строке параметра **Имя почтового ящика** необходимо нажать кнопку **Добавить** или щелкнуть мышью на значок  .

Уведомление имеет следующий вид:

Тема: Check ldap connection

Сообщение:

LDAP read Root DSE from source 2 finished with errors. See details below.

ldap_sasl_bind(SIMPLE): Can't contact LDAP server (-1)

Система отправляет одно сообщение администратору на каждую неудачную операцию обновления целиком, независимо от количества опрашиваемых серверов.

Одна и та же персона может входить в несколько групп одновременно, и эти группы могут быть указаны при выборе персон. Группы персон могут быть получены из внешней системы (Active Directory, ALD Pro, 389 Directory Server), а также определены администратором в интерфейсе KEO DLP. При этом "группы извне" отличаются только тем, что они не могут быть изменены в редакторе досье.

6.19.1. Настройка приоритетов источников данных для каждого атрибута персоны

Данные персон (ФИО, должность, номер телефона и т.д.) в Досье могут быть загружены из нескольких источников данных. При этом может быть ситуация, когда данные персоны, хранящиеся в одном источнике, не совпадают с данными этой же персоны в другом. Чтобы в Досье (в карточке персоны) отображалась достоверная информация о персоне, необходимо определять источники, содержащие более актуальные/достоверные данные. Это делается с помощью расстановки приоритетов источников для каждого свойства персоны (атрибута). Например: известно, что первый источник содержит более актуальные

данные о персоне, чем второй. В этом случае первый источник является более приоритетным.

Схема источника данных содержит атрибуты с уникальными и множественными значениями (уникальные и множественные атрибуты). К уникальным атрибутам относятся:

- ФИО
- День рождения
- Должность
- Фотография
- Уменьшенная фотография
- Кому подчиняется
- Чем руководит

К множественным атрибутам относятся прочие атрибуты источника данных. Приоритеты для множественных атрибутов можно не указывать, т.к. при слиянии итоговая персона будет содержать значения атрибутов, которые были получены из всех источников.

Примечание

*Сопоставление по атрибуту **Подразделения** более не задается, т.к. значение этого атрибута получается всегда из наиболее приоритетного источника.*

Возникают ситуации, когда в Досье встречаются дублирующиеся персоны с одинаковыми (ФИО, логин, день рождения и т.д.) и различающимися (например: адрес электронной почты, номер телефона и т.д.) атрибутами. Чтобы в Досье отсутствовали дубли, необходимо задать атрибуты, по которым данные персон будут объединены, в секции **Сопоставление загружаемых данных из разных источников** раздела GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Досье** (см. раздел A.2.5).

В качестве наиболее приоритетного для конкретного атрибута можно задать только один источник.

Пример: имеются персоны **Сидорова А.П.** и **Васечкина Н. В.** в первом источнике и **Семенова А.П.** и **Михайлова Н. В.** во втором. У персон **Сидорова А.П.** – **Семенова А.П.** и **Васечкина Н. В.** – **Михайлова Н. В.** одинаковые логины.

В секции **Сопоставление загружаемых данных из разных источников** задан атрибут **Логин**. Первый источник хранит актуальное ФИО персоны – **Васечкина Н. В.**, а второй – **Семенова А.П.**.

Таким образом, если для первого источника в списке соответствий атрибутов указать **ФИО** и задать приоритет, равный 1, в результате слияния появятся персоны **Сидорова А.П.** и **Васечкина Н. В.** В противном случае в результате слияния появятся персоны **Семенова А.П.** и **Михайлова Н. В.**

Если в секции указано несколько параметров сопоставления (например, адрес электронной почты и логин), то персоны из разных источников при слиянии будут считаться одинаковыми при совпадении всех указанных параметров сопоставления. Если множественный атрибут указан в параметрах сопоставления, он является совпадающим для персон из разных источников при совпадении хотя бы одного из его значений.

Пример: имеются персоны **Сидорова А.П.** и **Васечкина Н. В.** в первом источнике и **Семенова А.П.** и **Михайлова Н. В.** во втором. У персон **Сидорова А.П.** и **Семенова А.П.** одинаковые логины и адреса электронной почты, у персон **Васечкина Н. В.** и **Михайлова Н. В.** одинаковые логины.

В секции **Сопоставление загружаемых данных из разных источников** заданы атрибуты **Логин** и **Адрес электронной почты**.

Таким образом, произойдет слияние персон **Сидорова А.П.** и **Семенова А.П.**. При этом слияния персон **Михайлова Н. В.** и **Васечкина Н. В.** не произойдет, т.к. они имеют одинаковые логины, а адреса электронной почты не совпадают. После слияния персон в результатах поиска будет показана переписка (сообщения, события и инциденты, беседы и т.д.) новой персоны.

Приоритеты источников задаются для узла, Досье которого функционирует в режиме **Главный**. Для настройки приоритетов необходимо выполнить следующие действия:

1. Добавить несколько источников, указав значения следующих параметров:

   - **Параметры доступа к источнику данных** – **ldap**.
   - **Название источника** – указать произвольное название источника данных. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
   - **DN пользователя** – имя учётной записи с правами чтения каталога. Имя указывается вместе с доменом (например – **admin@isim.local**).
   - **Пароль пользователя** – пароль учётной записи, указанной в предыдущем параметре.
   - **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например – **ldap://ldap.isim.local:389**).
   - **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов AD организации.
   - **Число записей на странице** – размер страницы запроса. Измеряется в записях.
   - **Фильтр подразделений** – строковое представление фильтра, применяемого при поиске подразделений.
   - **Фильтр групп** – строковое представление фильтра, применяемого при поиске групп.
   - **Фильтр персон** – строковое представление фильтра, применяемого при поиске персон.

2. Раскрыть группу параметров **Список соответствий атрибутов** и при необходимости задать соответствия между атрибутами внешней системы (Active Directory, ALD Pro, 389 Directory Server) и атрибутами Досье, задать приоритеты источников для каждого атрибута. Нажать **Сохранить**.

3. В том же разделе GUI перейти в секцию **Сопоставление загружаемых данных из разных источников** и при необходимости задать параметры, по которым происходит сопоставление, загружаемых из разных источников. Нажать **Сохранить**.

4. При необходимости перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Досье > Сервис доступа к Досье**, раскрыть группу **Настройка работы в режиме главного сервера Досье** установить флажок Автоматическая синхронизация Досье и задать в соответствии с рекомендациями значения параметров **Периодичность запуска синхронизации (ч)**, **Периодичность запуска синхронизации (м)**,**Метод синхронизации** и **Количество соединений с БД**.

   Примечание

   Периодичность запуска синхронизации происходит вне зависимости от наступления новой даты.

   Не рекомендуется устанавливать значение периодичности синхронизации меньше 20 минут, т.к. при объемном LDAP-каталоге и большом количестве пользователей для успешного завершения обновления данного времени может быть недостаточно.

   При значении 0 часов 0 минут синхронизация работать не будет.

5. Нажать **Сохранить** и **Применить**.

6. При необходимости вручную синхронизировать БД Досье с источником, выбрав один из способов:

   - Нажать кнопку **Синхронизировать** (Рис.6.9).

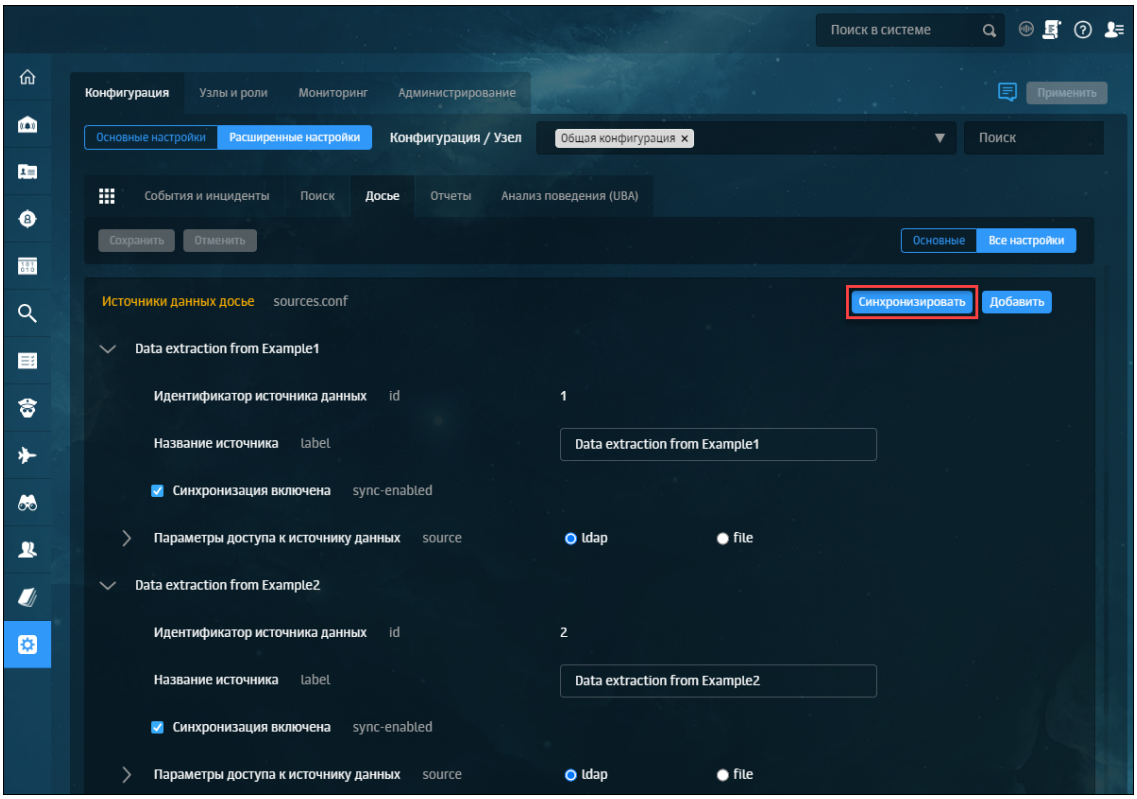


Рис. 6.9. Кнопка принудительной синхронизации Досье

- Перейти в CLI и выполнить команду:

  # /opt/dozor/abook-daemon/bin/abook-sync

После применения параметров конфигурации Досье будет обновлено в течение суток при следующей синхронизации, интервал которой задается в параметре **Периодичность запуска синхронизации (ч)**. Слияние произойдет после синхронизации с несколькими источниками или после применения измененных атрибутов сопоставления. Изменения в карточках персон будут отображаться в соответствии с заданными системным администратором приоритетами. Об успешном слиянии персон будет свидетельствовать вывод журнала сервиса **abook-daemon**. В примере ниже произошло слияние 2 персон из первого и второго источников:

```
INFO  service.DossierMergeServiceImpl - Persons merge has been successfully finished
INFO  service.DossierMergeServiceImpl – Merged 2 persons from source [1], 2 persons from source [2]
INFO  service.DossierMergeServiceImpl - Successfully refreshed merged persons' info
```

6.19.2. Проверка корректности настроек источника досье

Для проверки корректности настроек источника досье используется скрипт **abook-check-ldap**. Перед запуском скрипта необходимо выполнить следующие действия:

1. Переключиться на работу от имени пользователя **dozor**, выполнив команду:

   # su - dozor

2. Запустить интерпретатор команд **shell** (выполняется от имени пользователя **dozor**):

$ /opt/dozor/bin/shell

Формат для запуска скрипта следующий:

$ abook-check-ldap [source_id [-guid hex_value|-dn "distinguished name"|-sid "sid"]]

где **ключ** – один из доступных ключей, определяющих конкретное действие, выполняемое с помощью скрипта.

Список доступных ключей:

- **-source_id** – проверка подключения к источнику с указанным id.

  Пример запуска скрипта **abook-check-ldap** с ключом **-source_id**, где id=2:

```
/opt/dozor/abook-daemon/bin/abook-check-ldap 2
-----------------------------------------------------
Connection and search parameters for source #2 .....
Bind DN                    : root@nihil.local
Password                   : q1
Ldap url                   : ldap://10.31.5.222:389
Base DN                    : dc=nihil,dc=local
Page size                  : 1000
Filter OrgUnits            : (objectCategory=organizationalUnit)
Filter Groups              : (objectCategory=group)
Filter Persons             : (objectCategory=person)
-----------------------------------------------------
DS Service Name          : CN=NTDS Settings,CN=VM222,CN=Servers,CN=Default-First-Site-Name,
 ...
DNS Host Name              : vm222.nihil.local
Current Time               : 20131030070248.0Z
Default Naming Context     : DC=nihil,DC=local
Configuration Naming Context  : CN=Configuration,DC=nihil,DC=local
Highest Committed USN      : 127716
Invocation ID              : [d9e444eefb1f9e4183ba1e52bdd4bc7a]
-----------------------------------------------------
```

- **-guid hex_value** – вывод всех параметров и их значений по id указанной персоны из досье.
- **-dn "distinguished name"** – вывод всех параметров и их значений по dn указанной персоны из досье.
- **-sid "sid"** – вывод всех параметров и их значений по sid указанной персоны из досье.

Запуск команды без указания ключа выводит список настроенных параметров конфигурации для источников досье. Пример вывода скрипта **abook-check-ldap** без указания ключей:

```
/opt/dozor/abook-daemon/bin/abook-check-ldap
/ab-sources//1//label                    => "Data extraction from Example2"
/ab-sources//1//source/ldap//bind-dn     => "root@nihil.local"
/ab-sources//1//source/ldap//password    => "q1"
/ab-sources//1//source/ldap//ldap-url    => "ldap://10.31.5.222:389"
/ab-sources//1//source/ldap//base-dn     => "dc=nihil,dc=local"
/ab-sources//1//source/ldap//page-size   => "1000"
```

```
/ab-sources//1//source/ldap//filter-orgunit   => "(objectCategory=organizationalUnit)"
/ab-sources//1//source/ldap//filter-group     => "(objectCategory=group)"
/ab-sources//1//source/ldap//filter-person    => "(objectCategory=person)"

Select one of existing LDAP source ids.
```

6.19.3. Редактор досье в интерфейсе командной строки

Для управления досье через командную строку используется скрипт **ab-tool.py**. С его помощью можно управлять персонами и их группами.

Перед запуском скрипта **ab-tool.py** необходимо выполнить следующие действия:

1. Переключиться на работу от имени пользователя **dozor**, выполнив команду:

   # su - dozor

2. Запустить интерпретатор команд **shell** (выполняется от имени пользователя **dozor**):

   $ /opt/dozor/bin/shell

Формат команды для запуска скрипта **ab-tool.py**:

$ ab-tool.py [<ключ>] ...

где **<ключ>** – один из ключей, определяющих действие скрипта.

Список доступных ключей:

- **-s**, **--list-sections** – вывести на экран список разделов;
- **-c <section-id>**, **--list-section <section-id>** – показать список групп из раздела;
- **-g <идентификатор группы>**, **--editable-groups <идентификатор группы>** – вывести на экран группы, доступные для редактирования;
- **-u <идентификатор группы>**, **--list-users <идентификатор группы>** – вывести на экран список пользователей из группы с соответствующим идентификатором;
- **-i <идентификатор пользователя>**, **--user-info <идентификатор пользователя>** – вывести на экран полную информацию о пользователе;
- **-f**, **--find-user** – найти пользователей по указанному адресу. На экран выводится только полное имя и все адресные атрибуты;
- **-F**, **--find-by-name** – найти пользователей по указанному имени. Значение имени можно задавать частично. На экран выводится идентификатор персоны, полное имя, ФИО руководителя и системные атрибуты **deletable** и **deleted**;
- **-S <название раздела>**, **--add-section <название раздела>** – добавить новый раздел;
- **-n <идентификатор раздела>:<новое название раздела**, **--rename-section <идентификатор раздела>:<новое название раздела** – переименовать раздел;
- **-E <идентификатор раздела>**, **--remove-section <идентификатор раздела>** – удалить раздел;

- **-a <идентификатор группы>:<название группы>**, **--add group <идентификатор группы>:<название группы>** – добавить группу;
- **-e <идентификатор группы>:<идентификатор раздела>:<название группы>**, **--edit-group <идентификатор группы>:<идентификатор раздела>:<название группы>** – переименовать группу;
- **-r <идентификатор группы>**, **--remove-group <идентификатор группы>** – удалить группу;
- **-A <имя пользователя>:<e-mail>:<идентификатор группы>**, **--add-user <имя пользователя>:<e-mail>:<идентификатор группы>** – добавить пользователя;
- **-R <идентификатор пользователя>**, **--remove-user <идентификатор пользователя>** – удалить пользователя;
- **-G <имя пользователя>:<список идентификаторов групп>** – добавить пользователя в группу/группы;
- **-D <имя пользователя>:<список идентификаторов групп>** – удалить пользователя из группы/групп;
- **-t <идентификатор пользователя>:<список атрибутов>**, **add-attrs <идентификатор пользователя>:<список атрибутов>** – добавить атрибуты для пользователя;
- **-T <идентификатор пользователя>:<список атрибутов>**, **remove-attrs <идентификатор пользователя>:<список атрибутов>** – удалить атрибуты пользователя;
- **-m <идентификатор пользователя>:<идентификатор менеджера>**, **--set-manager <идентификатор пользователя>:<идентификатор менеджера>** – добавить менеджера для пользователя;

  Примечание

  *При работе с ключом **-m** идентификатор менеджера указывать не обязательно.*

- **-x <файл визитной карточки>**, **--get-vcard <файл визитной карточки>** – получить электронную визитную карточку для пользователя;
- **-X <файл визитной карточки>**, **--set-vcard <файл визитной карточки>** – установить электронную визитную карточку для пользователя;
- **-H**, **--host** – IP-адрес или имя узла с сервисом **abook-daemon** (указывается случае нестандартной конфигурации **abook-daemon**);
- **-P**, **--port** – порт, на котором сервис **abook-daemon** ожидает соединения (указывается случае нестандартной конфигурации **abook-daemon**);
- **-C <cert>**, **--cert <cert>** – использовать сертификат из заданного файла;
- **-K <key>**, **--key <key>** – использовать секретный ключ из заданного файла;
- **-d**, **--debug** – включить журнал отладки;

- **-v**, **--verbose** – вывод сообщений о действиях, выполняемых скриптом;
- **-h**, **--help** – вывести справку по работе со скриптом.

Внимание!

При работе с ключами, содержащими указание файла, необходимо прописывать полный путь к файлу.

Примеры работы скрипта:

- Вывести на экран список всех доступных групп. В результате в этот список попадут только созданные пользователем группы, например:

```
ds-mode@doc001 ~ $ ab-tool.py -s
Юридический отдел [67726f75-705f-7365-6374-696f00000002]
Энергетический комплекс [67726f75-705f-6374-696f00000002]
Служба безопасности [67726f75-705f-6374-696f00000002]
```

- Вывести на экран список всех доступных групп из раздела, например:

```
ds-mode@doc001 ~ $ ab-tool.py -c 67726f75-705f-7365-6374-696f00000001
Локальные:
   To be fired (61625f67-726f-7570-ffff-ffff00000001)
   Probation period (61625f67-726f-7570-ffff-ffff00000002)
   Под подозрением (61625f67-726f-7570-ffff-ffff00000004)
 > Тверской филиал (add1701a-b28f-4b29-a1d7-053b28c9a995)
 > Тульский филиал (89e23fdc-5665-4736-b7b1-7ef985a6a3b6)
 > Центральный офис (3cf841ac-dab0-43a0-9e6a-02b9e5172a61)
```

- Вывести на экран пользователей по части имени, например:

```
ds-mode@doc007 /opt/dozor # ab-tool.py -F 'Булат'
0: personId: 00000000-0000-0001-0030-000000000001
  deleted: False
  fullname: Булатов Андрей Леонидович
  deletable: False
  title: Президент АО "Машиностроительный завод "Прогресс"
1: personId: 00000000-0000-0001-0030-000000000077
  deleted: False
  fullname: Булатов Аркадий Львович
  deletable: False
  title: Юрист
```

- Добавить группу. В результате появится сообщение об успешном добавлении группы, например:

```
ds-mode@doc001 ~ $ ab-tool.py -a 67726f75-705f-7365-6374-696f00000002:Example_Group
Группа добавлена, id: 34f7d1cd-70c9-4e17-8862-c10e38a26b06
```

- Удалить группу. В результате появится сообщение об успешном удалении группы, например:

```
ds-mode@doc001 ~ $ ab-tool.py -r cba54a26-2b81-11e8-876b-0050568830d0
Группа удалена
```

- Переименовать группу. Переименовывать можно только созданные пользователем группы.

  Пример:

```
ds-mode@doc001 ~ $ ab-tool.py -e
3cd0420e-2b83-11e8-8fe8-0050568830d0:67726f75-705f-7365-6374-696f00000002:Economics_Department_Main
Группа переименована
```

- Создать новый раздел досье. В результате появится сообщение об успешном создании нового раздела, например:

```
ds-mode@doc001 ~ $ ab-tool.py -S Мировой_суд
Раздел добавлен, id: 34f7d1cd-70c9-4e17-8862-c10e38a26b06
```

- Удалить раздел досье. В результате появится сообщение об успешном удалении раздела, например:

```
ds-mode@doc001 ~ $ ab-tool.py -E 0145c4bc-2b87-11e8-9942-0050568830d0
Раздел удалён
```

- Показать список пользователей, входящих в группу с указанным идентификатором.

  Пример:

```
ds-mode@doc001 ~ $ ab-tool.py -u 6bbb8f94-8a7a-4a93-b13d-1b889af68742
Ветров Тихон Платонович, Начальник управления хозобеспечения
(00000000-0000-0001-0030-000000000040)
Могутов Богдан Леонидович, Главный технолог (00000000-0000-0001-0030-000000000015)
Пугачева Елена Филипповна, Ст. бухгалтер (00000000-0000-0001-0030-000000000098)
Сильвестров Дмитрий Иосифович, Ст.инженер-механик
(00000000-0000-0001-0030-000000000058)
Фишбах Галина Павловна, Начальник финансового отдела
(00000000-0000-0001-0030-000000000137)
```

- Вывести полную информацию по пользователю с указанным идентификатором.

  Пример:

```
ds-mode@doc001 ~ $ ab-tool.py -i 00000000-0000-0001-0030-000000000015
trustLevel: status: normal
            deviationFactor: 0
            min: -1000
            max: 1000
            dtld: 0
            current: 0
addresses: 0: type: hostname
             value: pc-blmogutov.mzprogress.ru
           1: type: skype
             value: bl.mogutov
           2: type: email
```

```
          value: bl.mogutov@mzprogress.ru
        3: type: ip
          value: 192.105.172.146
        4: type: login
          value: bl.mogutov
        5: type: sid
          value: s-1-5-21-793904598-208165932-2932072800-1146
title: Главный технолог
personId: 00000000-0000-0001-0030-000000000015
deleted: False
manager: personId: 00000000-0000-0001-0030-000000000086
       fullname: Давыдов Мирослав Ерофеевич
       deletable: False
       title: Вице-Президент, Производственный директор
deletable: False
groups: 0: orgStruct: True
         id: 00000000-0000-0000-0030-000000000001
         name: АО "Машиностроительный завод "Прогресс"
       1: orgStruct: False
         locId: #abook.group.group002
         id: 6bbb8f94-8a7a-4a93-b13d-1b889af68742
         parent: add1701a-b28f-4b29-a1d7-053b28c9a995
         name: Probation period
       2: orgStruct: True
         id: 00000000-0000-0000-0030-000000000017
         parent: 00000000-0000-0000-0030-000000000001
         name: Производственный департамент
       3: orgStruct: True
         id: 00000000-0000-0000-0030-000000000172
         parent: 00000000-0000-0000-0030-000000000017
         name: Управление главного технолога
       4: orgStruct: False
         id: add1701a-b28f-4b29-a1d7-053b28c9a995
         name: Тверской филиал
department: path: 0: id: 00000000-0000-0000-0030-000000000001
                  name: АО "Машиностроительный завод "Прогресс"
                1: id: 00000000-0000-0000-0030-000000000017
                  name: Производственный департамент
         id: 00000000-0000-0000-0030-000000000172
         name: Управление главного технолога
fullname: Могутов Богдан Леонидович
attributes:
  1795: department: Управление главного технолога
  1796: hostname: pc-blmogutov.mzprogress.ru
  1797: birth_day: 1986-09-29
  1799: skype: bl.mogutov
  1800: email: bl.mogutov@mzprogress.ru
  1801: ip: 192.105.172.146
  1802: title: Главный технолог
  1804: priveleges: Внешняя почта - доступ
  1805: telephone_number: 2476
  1806: login: bl.mogutov
  1807: submit_to: 86
  1808: fullname: Могутов Богдан Леонидович
  1809: sid: S-1-5-21-793904598-208165932-2932072800-1146
```

- Найти пользователей по заданным атрибутам.

Пример поиска по части фамилии:

```
ds-mode@doc001 ~ $ ab-tool.py -F Могут
0: personId: 00000000-0000-0001-0030-000000000015
  deleted: False
  fullname: Могутов Богдан Леонидович
  deletable: False
  title: Главный технолог
```

При работе с ключами могут возникнуть следующие ошибки:

- незаэкранированные от shell «спецсимволы» (например, пробел);
- указанной группы не существует (неправильно задан **id** группы);
- указанная группа запрещена для редактирования;
- указанного пользователя не существует (неправильно задан id пользователя);
- неправильный формат указания файла;
- указанного файла не существует.

6.19.4. Предварительная проверка взаимодействия с AD

Для предварительной проверки взаимодействия с AD используется скрипт **check_ad**. Скрипт необходимо запускать от имени пользователя **dozor**. Скрипт может быть использован без предварительной установки пакетов KEO DLP на платформу.

Формат для запуска скрипта следующий:

 # /opt/dozor/abook-daemon/bin/check_ad ldap[s]://[<адрес> ...]:[<порт> ...] [<ключ> ...]

где:

- **адрес** – URL LDAP-сервера;
- **порт** – порт, на котором LDAP-сервер ожидает соединения;
- **ключ** – один из доступных ключей, определяющих конкретное действие, выполняемое с помощью скрипта.

Список доступных ключей:

- **-help** – вывести справку по работе со скриптом. Результатом запуска скрипта с этим ключом будет являться сообщение системы, со списком возможных ключей:

  ```
  Usage: check_ad ldap[s]://host[:port] [-binddn user -passwd pass [-basedn dn]]
  ```

- **-binddn** – проверяет корректность bind-параметров на сервере (AD). Если **bind** проходит без ошибок, **sid** домена получен, **invocation id** получен, то скрипт выгружает в текущий каталог все подразделения, группы и персоны в формате ldif:

```
rw-rr- 1 root root 41798 Aug 15 11:34 bvm197.exch.local.person.ldf
rw-rr- 1 root root 2801 Aug 15 11:34 bvm197.exch.local.orgunit.ldf
rw-rr- 1 root root 49818 Aug 15 11:34 bvm197.exch.local.group.ldf
```

В примере префикс в именах файлов **DNS Host Name** из данных **Root DSN**.

После этого пишет количество выгруженных объектов на экран и ищет все первичные группы выгруженных персон в AD:

```
./check_ad ldaps://bvm197 -binddn administrator -passwd q1
INFO: Use Default Naming Context as the starting point for the search (basedn).
-------------------------------------------------------
DS Service Name : CN=NTDS Settings,CN=BVM197,CN=Servers,CN=Default-First-Site-Name ...
DNS Host Name : bvm197.exch.local
Current Time : 20130815073446.0Z
Default Naming Context : DC=exch,DC=local
Configuration Naming Context : CN=Configuration,DC=exch,DC=local
Highest Committed USN : 68136
Domain SID : S-1-5-21-2205848573-4034669592-3688812088
Invocation ID : [39ecea116bf3064db4e674d3a9fc6015]
-------------------------------------------------------
Bind DN : administrator
Password : q1
Ldap url : ldaps://bvm197
Base DN : DC=exch,DC=local
Page size : 1000
Filter OrgUnits : (objectCategory=organizationalUnit)
Filter Groups : (objectCategory=group)
Filter Persons : (&(objectCategory=person)(objectClass=user))
-------------------------------------------------------
Loading Active Directory objects ...
>>> Number of orgunits : 5
>>> Number of groups : 44
>>> Number of persons : 29
Check primary groups for persons ...
>>> Check primary group 513 ...
>>> Check primary group 514 ...
>>> Check primary group 1126 ...
```

- **-basedn** – выгружает объекты только для указанного **basedn**. Используется совместно с ключом **-binddn**.

Обязательным параметром является только **ldap-url**.

С единственным параметром **ldap-url** этот скрипт фактически играет ту же роль, что и **ping** применительно к AD. В этом случае он читает Root DSE атрибуты, доступ к которым не требует **bind** под пользователем. Пример использования скрипта с указанием параметра **ldap-url**:

```
[root@freshbox parts]# ./check_ad ldaps://bvm197
-------------------------------------------------------
DS Service Name : CN=NTDS Settings,CN=BVM197,CN=Servers,CN=Default-First-Site-Name ...
DNS Host Name : bvm197.exch.local
Current Time : 20130815073442.0Z
Default Naming Context : DC=exch,DC=local
Configuration Naming Context : CN=Configuration,DC=exch,DC=local
```

```
Highest Committed USN : 68136
----------------------------------------------------
```

Если указанные значения ключей проходят предварительную проверку, то можно создавать новый источник в конфигурации досье и переносить в него проверенные выше параметры соединения с AD. Выгруженные из AD объекты в формате **ldif** могут быть использованы разработчиком для детального анализа проблем.

6.19.5. Сброс состояния досье

Для очистки/сброса состояния досье используется скрипт **abook-reset**. Скрипт необходимо запускать от имени пользователя **dozor**. Формат для запуска скрипта следующий:

 # /opt/dozor/abook-daemon/bin/abook-reset [<ключ> ...]

где **ключ** – один из доступных ключей, определяющих конкретное действие, выполняемое с помощью скрипта.

Внимание!

*Перед запуском скрипта **abook-reset** с ключом **-hard** необходимо остановить сервис **abook-daemon**, а после – запустить обратно.*

Список доступных ключей:

- **-help** – вывести справку по работе со скриптом. Результатом запуска скрипта с этим ключом будет являться сообщение системы, со списком возможных ключей:

  ```
  Usage: abook-reset [-src source_id] [-hard]
  ```

- **-src N** – сбрасывает параметры синхронизации досье для источника N.
- **-hard** – выполняет полную очистку всех таблиц досье до исходного состояния.
- **-src N -hard** – очищает таблицы досье от данных источника N.

Запуск команды без указания ключа сбрасывает параметры синхронизации досье для всех источников.

Примечание

*Ключ **-hard** выполняет удаление данных из таблиц, поэтому работает значительно медленнее. При этом, из досье удаляются все созданные ранее объекты указанного источника или всех источников данных.*

*Сброс параметров синхронизации (ключ **-src N**) означает, что последующий вызов скрипта **abook-sync** будет выполнять полную синхронизацию вместо обновления. При этом, из досье не удаляются никакие данные.*

6.19.6. Диагностика проблем импорта данных ОШС из файлов

В системе реализована проверка следующих данных:

- наличие доступа к каталогу, в котором размещаются файлы с данными о структуре ОШС (значение параметра **Каталог с данными ОШС** из раздела **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Досье > Источники данных досье**);
- кодировка и размеры файлов **groups.csv** и **persons.csv**;
- формат данных в вышеуказанных файлах.

Файлы со списками групп и персон должны быть в формате CSV в кодировке **Unicode UTF-8**, а максимальный размер каждого из файлов не может превышать 100 Мб.

Файл **groups.csv** должен содержать поля **id**,**pid**, **group** и хотя бы одну запись, например так:

```
id;pid;group
001;;ПАО "МКБ ТВХ"
290;001;Совет Директоров
303;001;Маркетинг
543;001;Отдел экономики и статистики
```

где:

- **id** – идентификатор группы (является обязательным);
- **pid** – идентификатор родительской группы;
- **group** – наименование группы (является обязательным).

Первая строка не должна содержать пробелов. В строке, выделенной жирным, отсутствует описание поля **pid**. Это означает, что группа сотрудников является родительской по отношению ко всем. Запись считается корректной, у нее заполнены поля **id** и **group**.

Файл **persons.csv** должен содержать поля **id**, **group-id**, **fullname** и хотя бы одну запись, например так:

```
id;group-id;fullname;title;submit_to;email;login
154;303;Сидорова ИРИНА Александровна;Директор по маркетингу;;sidorova-ia@abc.ab;sidorova-ia
119;543;Иванова Наталья Алексеевна;Специалист;154390;ivanova-na@abc.ab;ivanova-na
156;290;Петрова Ольга Николаевна;Руководитель группы;119798;;petrova.on
```

где:

- **id** – идентификатор сотрудника (является обязательным);
- **group-id** – идентификатор группы (является обязательным);
- **fullname** – ФИО сотрудника (является обязательным);
- **title** – должность сотрудника;
- **submit_to** – идентификатор руководителя сотрудника;
- **email** – адрес электронной почты сотрудника;
- **login** – логин персоны (если заполнено, должен быть уникальным);

- **image_preview** – строка закодированного в **Base64** файла изображения в PNG-формате.

Первая строка не должна содержать пробелов. Запись считается корректной, у нее заполнены поля **id**, **group_id** и **fullname** и каждая персона имеет свой уникальный идентификатор.

Ошибки проверки данных сохраняются в журнальный файл с именем **errors.log**. Расположение журнала настраивается в значении атрибута **file** в конфигурационном файле **/opt/dozor/abook-daemon/conf/logback.xml**.

При достижении определенного размера журнального файла происходит автоматическая ротация файлов: создается новый файл журнала, запись данных продолжается в новый файл. При этом старые файлы сохраняются в формате **errors%d{гггг-ММ-дд}.log**. В файле **/opt/dozor/abook-daemon/conf/logback.xml** можно определить размер журнального файла, при достижении которого происходит ротация (параметр **maxFileSize**) и промежуток времени в днях, через который создается новый файл (параметр **maxHistory**).

Примечание

В текущей версии KEO DLP возможен однократный импорт ОШС по данным из файлов.

6.20. Работа с модулем IDID в интерфейсе командной строки

Для работы с модулем IDID в интерфейсе командной строки используются скрипты **idid-tool** и **idid-tool.py**. Для работы со скриптами необходимо запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Формат запуска скрипта **idid-tool** следующий:

 # idid-tool [<ключ> ...]

Доступны следующие ключи:

- **-l**, **--list-rules** – вывести на экран список имеющихся в системе правил IDID.
- **-L**, **--list-cats** – вывести на экран список имеющихся в системе категорий IDID.
- **-c <str>**, **--check-file <str>** – вывести на экран результат IDID-проверки указанного после ключа файла.
- **-g <str>**, **--get-key-phrases <str>** – вывести на экран 20 ключевых (наиболее часто встречающихся) фраз, содержащихся в указанном после ключа файле.
- **-a <str>**, **--annotate-file <str>** – вывести на экран аннотацию результата IDID-проверки указанного после ключа файла. Формат выводимой аннотации совпадает с форматом аннотаций писем в архиве.
- **-C <str>**, **--categories <str>** – использовать при IDID-проверке только заданные категории IDID. Если категорий больше одной, они перечисляются внутри двойных прямых кавычек через пробел.

- **-R <str>**, **--rules <str>** – использовать при IDID-проверке только заданные правила IDID. Если правил больше одного, они перечисляются внутри двойных прямых кавычек через пробел.
- **-d**, **--debug** – вывести отладочную информацию по ходу выполнения скрипта.
- **-h**, **--help** – вывести справочную информацию о скрипте.

Формат запуска скрипта **idid-tool.py** следующий:

 # idid-tool.py [<ключ> ...]

Доступны следующие ключи:

- **-a**, **--annotate** – вывести детализацию совпадений при проверке файла.
- **-C <имя категории>**, **--category <имя категории>** – использовать при IDID-проверке только заданные категории IDID.
- **-R <имя правила>**, **--rule <имя правила>** – использовать при IDID-проверке только заданные правила IDID.
- **-H <имя узла/IP>**, **--host <имя узла/IP>** – указать имя или IP-адрес узла с сервисом **smap-idid**. Значение по умолчанию: **127.0.0.1**.
- **-P <порт>**, **--port <порт>** – указать порт узла с сервисом **smap-idid**. Значение по умолчанию: 9302.
- **-l**, **--list-rules** – вывести на экран список имеющихся в системе правил IDID.
- **-L**, **--list-cats** – вывести на экран список имеющихся в системе категорий IDID.
- **-c <str>**, **--check-file <str>** – вывести на экран результат IDID-проверки указанного после ключа файла или строки.
- **-g <str>**, **--get-key-phrases <str>** – вывести на экран ключевые (наиболее часто встречающиеся) фразы, содержащиеся в указанном после ключа файле или строке.
- **-v**, **--verbose** – вывод сообщений о действиях, выполняемых скриптом.
- **-d**, **--debug** – вывести отладочную информацию по ходу выполнения скрипта.
- **-h**, **--help** – вывести справочную информацию о скрипте.

Примеры использования скрипта:

1. Вывод на экран список имеющихся на узле **test1.isim.local** правил IDID (формат команды для запуска скрипта
   idid-tool.py -l -H test1.isim.local
   ):

```
ru-drugs: Русская лексика о злоупотреблении наркотиками (Специальная лексика)
ru-finance-INN: ИНН (10 или 12 цифр) (ИНН)
URL: URL (Сетевые адреса)
data-uri: Data-URI в соответствии с RFC-2397 (Сетевые адреса)
ru-okpo: Номер ОКПО (Реквизиты)
```

```
ru-pass-number: Номер российского внутреннего паспорта (Номера удостоверений личности)
any-phone-number: Любой телефонный номер (Телефонные номера)
samba-share: Сетевой ресурс Windows (Samba) (Сетевые адреса)
kz-inn: ИНН/БНН Казахстана (ИНН)
ru-finance-bik: Российский код BIC (Реквизиты)
ru-gangs: Русская бандитская лексика (Специальная лексика)
IPv4: Адрес IPv4 (Сетевые адреса)
ru-pornography: Русская порнографическая лексика (Специальная лексика)
email: Адрес электронной почты (Сетевые адреса)
ua-inn: ИНН Украины (ИНН)
ru-obscene: Русская ненормативная лексика (Специальная лексика)
IPv6: Адрес IPv6 (Сетевые адреса)
ru-financial-lexic: Русская финансовая лексика (Специальная лексика)
ru-documents: Договоры, ТКП, Счета (Специальная лексика)
kz-rnn: Казахстанский регистрационный номер налогоплательщика (Реквизиты)
ru-foreign-pass-number: Номер заграничного паспорта РФ (Номера удостоверений личности)
ru-phone-number: Российский телефонный номер (Телефонные номера)
ru-names: Русское имя (Имена собственные)
ru-mobile-phone-number: Российские мобильные телефонные номера (Телефонные номера)
```

2. Вывод на экран список имеющихся на узле **test1.isim.local** категорий IDID (формат команды для запуска скрипта
idid-tool.py -L -H test1.isim.local
):

```
insurance-numbers: Номера страховых свидетельств
special-vocabulary: Специальная лексика
inn: ИНН
person-identity-numbers: Номера удостоверений личности
transport: Транспорт
proper-names: Имена собственные
network-address: Сетевые адреса
phone-numbers: Телефонные номера
properties: Реквизиты
bank-cards-and-accounts: Банковские карты и счета
```

3. Вывод на экран результата IDID-проверки указанной после ключа **-c** строки (формат команды для запуска скрипта
idid-tool.py -c лексика -H test1.isim.local
):

```
категории
правила
```

Слово **лексика** встречается в категориях и правилах.

6.21. Работа с модулем DIFI в интерфейсе командной строки

Для работы с модулем DIFI в интерфейсе командной строки используются скрипты **difi-tool.py** и **difi-tool**, где второй скрипт является ярлыком для запуска первого. Для работы со скриптами необходимо запустить интерпретатор команд shell, выполнив команду:

 # /opt/dozor/bin/shell

Перед выполнением скриптов следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат запуска скрипта **difi-tool.py** следующий:

$ difi-tool.py [<ключ> ...]

Доступны следующие ключи:

- **-h**, **--help** – вывести справочную информацию о скрипте.
- **-m {text,binary,image,table}**, **--mode {text,binary,image,table}** – режим проверки файла на тип данных. Принимает следующие значения: **text**, **binary**, **image**, **table**. Значение по умолчанию: **text**.
- **-H <имя узла/IP>**, **--host <имя узла/IP>** – указать имя или IP-адрес узла с сервисом **smap-difi**. Значение по умолчанию: **127.0.0.1**.
- **-P <порт>**, **--port <порт>** – указать порт узла с сервисом **smap-difi**. Значение по умолчанию: 9301.
- **-s**, **--stats** – вывести на экран статус и статистику DIFI.
- **-c <имя файла>**, **--check <имя файла>** – выполнить проверку файла на совпадения.
- **-v**, **--verbose** – вывести сообщения о действиях, выполняемых скриптом.
- **-d**, **--debug** – вывести отладочную информацию по ходу выполнения скрипта.

Примеры использования скрипта:

1. Вывод на экран статуса и статистики по всем цифровым отпечаткам (формат команды для запуска скрипта
   $ difi-tool.py -s -H test1.isim.local
   ):

```
Статус: OK
Статистика базы знаний:
 Местоположение: /data/base/difi-kb
 Группы (4):
 Группа Бухгалтерия:
  IMAGE_1.jpg-textpart (BINARY, PLAIN_TEXT)
  IMAGE_2.jpg-textpart (BINARY, PLAIN_TEXT)
  годовой отчет2.xlsx (BINARY)
  годовой отчет2.xlsx-textpart (BINARY, PLAIN_TEXT)
  нет масштабирования вложений.pdf (BINARY)
  нет масштабирования вложений.pdf-extract-IMAGE_1.jpg.png (BINARY, IMAGE)
  нет масштабирования вложений.pdf-extract-IMAGE_2.jpg.png (BINARY, IMAGE)
  нет масштабирования вложений.pdf-textpart (BINARY, PLAIN_TEXT)
 Группа Юристы:
  act (5).pdf (BINARY)
  act (5).pdf-textpart (BINARY, PLAIN_TEXT)
 Группа Директор:
```

```
  wl2.txt (BINARY, PLAIN_TEXT)
Группа Легкая промышленность:
  chrome.pdf (BINARY)
  chrome.pdf-textpart (BINARY, PLAIN_TEXT)
  Desktop.rar (BINARY)
  Desktop.rar-extract-office365.txt (BINARY, PLAIN_TEXT)
  Desktop.rar-extract-wl3.txt (BINARY, PLAIN_TEXT)
  Desktop.rar-extract-годовой отчет2.xlsx (BINARY)
  Desktop.rar-textpart (BINARY, PLAIN_TEXT)
  firefox.pdf (BINARY)
  firefox.pdf-textpart (BINARY, PLAIN_TEXT)
  scan.pdf (BINARY)
  scan.pdf-textpart (BINARY, PLAIN_TEXT)
  годовой отчет2.xlsx-textpart (BINARY, PLAIN_TEXT)
```

2. Вывод на экран результатов проверки файла на совпадения с эталоном (формат команды для запуска скрипта
$ difi-tool.py -m text -c /var/tmp/difi/ContractForPDServices.pdf
):

```
Нет совпадений
```

В данном случае совпадения с эталоном отсутствуют.

Если файл совпадает с эталоном, результат проверки будет иметь вид:

```
Документ: wl2.txt
  процент: 100(base: 70)
  тип хеша: PLAIN_TEXT
  группа: Бухгалтерия
  регионы в файле:
    27 - 158
  регионы в базе:
    27 - 158
```

где:

- **процент: 100** – процент **self.match**, т.е. отношение совпавших хешей в общему размеру анализируемого документа.
- **base: 70** – процент **base.match**, т.е. отношение совпавших хешей к общему размеру эталона.

6.21.1. Поиск конфликтов в политике в части DIFI

Для поиска конфликтов в политике KEO DLP в части DIFI в интерфейсе командной строки используется скрипт **difi-conflict-tool.jar**.

Формат запуска скрипта **difi-conflict-tool.jar** следующий:

 # $JAVA_HOME/bin/java -jar /opt/dozor/difi/difi-conflict-tool.jar [<ключ> ...]

Доступны следующие ключи:

- **-p <порт>, --port <порт>** – порт для взаимодействия сервисов **webserver-local** и **webserver**. Значение по умолчанию: 8445.

- **-h <имя/IP-адрес>, --host <имя/IP-адрес>** – имя или IP-адрес master-узла. Значение по умолчанию: localhost.
- **-l <язык>, --lang <язык>** – выбор языка для подсказок в выводе скрипта. Поддерживаемые значения: **en**, **ru** (значение по умолчанию).
- **-m <режим работы>, --mode <режим работы>** – выбор режима работы скрипта. Принимает значения:
  - **silent** – запускает поиск конфликтов, и в случае нахождения хотя бы одного конфликта завершает скрипт с соответствующим уведомлением.
  - **show** – запускает поиск конфликтов, и в случае их нахождения выводит список конфликтов в интерфейс командной строки вместе с подсказками по их возможному разрешению.

  Значение по умолчанию: **show**.
- **--help** – вывести справочную информацию о скрипте.

Внимание!

*Для разрешения конфликтов необходимо перейти в GUI KEO DLP, исправить настройки политики в части DIFI в соответствии с рекомендациями из подсказок, выводимых в результате работы скрипта, далее подтвердить изменения, нажав кнопки **Сохранить** и **Применить политику**.*

Примеры использования скрипта (вывод в интерфейсе командной строки):

1. Скрипт запущен в режиме silent при наличии конфликтов в политике DIFI:

```
Найдены конфликты, для детализации запустите скрипт в режиме "show"
```

2. Скрипт запущен в режиме show при наличии конфликтов в политике DIFI (вывод в примере приведен в сокращенном виде):

```
Цифровой отпечаток "ЦО, где диапазон выше 100" используется в условиях:
* "Результат проверки больше чем ЦО, где диапазон выше 100" с оператором "Больше чем".
Условие используется в правилах:
Тестовое правило: Активное 1 (вкл); Тестовое правило: Неактивное 1 (выкл)
* "Результат проверки в диапазоне ЦО, где диапазон выше 100" с оператором "В диапазоне".
Условие используется в правилах:
Тестовое правило: Активное 5 (вкл); Тестовое правило: Неактивное 5 (выкл)
...
* "Результат проверки части меньше чем ЦО, где диапазон выше 100" с оператором
"Меньше чем". Условие используется в правилах:
Тестовое правило: Активное 21 (вкл); Тестовое правило: Неактивное 21 (выкл)

Для устранения конфликта рекомендуется удалить ненужные правила, использовать одинаковый
 оператор или создать копию ЦО для использования с разными операторами. При обновлении
 Дозора будет использован случайный оператор из данных условий (приоритет для
использованных во включённых правилах).

...
```

В группе "Группа, где диапазон от 122 до 200" цифрового отпечатка "ЦО, где диапазон выше 100" указано значение совпадения "(122 200)", но используется в условиях:
* "Результат проверки больше чем ЦО, где диапазон выше 100" с оператором "Больше чем".
Условие используется в правилах:
Тестовое правило: Активное 1 (вкл); Тестовое правило: Неактивное 1 (выкл)
* "Результат проверки меньше чем ЦО, где диапазон выше 100" с оператором "Меньше чем".
Условие используется в правилах:
Тестовое правило: Активное 9 (вкл); Тестовое правило: Неактивное 9 (выкл)
...

Для устранения конфликтов рекомендуется использовать оператор "в диапазоне" с указанием значения в диапазоне, а для операторов "больше чем" и "меньше чем" с указанием числа, либо удалить ненужные условия. При обновлении Дозора будет использовано:
1) максимальное значение в диапазоне, используемого с оператором "больше"
2) минимальное значение в диапазоне, используемого с оператором "меньше"
3) диапазон с одинаковым максимальным и минимальным значением (т.е. пустой диапазон) с оператором "в диапазоне"

В группе "Группа, где диапазон от 122 до 200" цифрового отпечатка "ЦО, где диапазон выше 100" указано значение совпадения "(122 200)" (более 100%)
Цифровой отпечаток "ЦО, где диапазон выше 100" используется в условиях:
* "Результат проверки больше чем ЦО, где диапазон выше 100" с оператором "Больше чем".
Условие используется в правилах:
Тестовое правило: Активное 1 (вкл); Тестовое правило: Неактивное 1 (выкл)
* "Результат проверки в диапазоне ЦО, где диапазон выше 100" с оператором "В диапазоне".
Условие используется в правилах:
Тестовое правило: Активное 5 (вкл); Тестовое правило: Неактивное 5 (выкл)
...

Рекомендуется установить значение не превышающее 100%. При обновлении Дозора значения более 100% будут приравнены к 100%.

6.22. Работа с сервером действий в интерфейсе командной строки

Для работы с сервером действий в интерфейсе командной строки используется скрипт **as-tool.py**.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить командную оболочку, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат запуска скрипта **as-tool** следующий:

$ as-tool.py [<ключ> ...]

Доступны следующие ключи:

- **-H <имя узла/IP>**, **--host <имя узла/IP>** – указать имя или IP-адрес узла с сервисом **action-server**. Значение по умолчанию: **127.0.0.1**.

- **-P <порт>**, **--port <порт>** – указать порт узла с сервисом **action-server**. Значение по умолчанию: 3001.
- **-c**, **--count** – вывести на экран количество сообщений для каждого действия.
- **-m <vID>**, **--id <vID>** – указать один или несколько идентификаторов сообщения для отложенного действия.
- **-f <vID>**, **--from <vID>** – указать один или несколько файлов с идентификаторами сообщений для отложенного действия.
- **-p <имя> <значение>**, **--param <имя> <значение>** – указать имя и значение параметра для отложенного действия.
- **-F**, **--force** – включить принудительное создание действий в случае, если параметры некорректны.
- **-l**, **--list-actions** – вывести на экран список доступных действий.
- **-i <ИД>**, **--info <ИД>** – вывести на экран информацию о действии с идентификатором <ИД>.
- **-r <ИД>**, **--remove <ИД>** – удалить действие с идентификатором <ИД>.
- **-a** – вывести на экран список всех действий.
- **-A <название действия>** – вывести на экран информацию по указанному действию;
- **-s <имя файла>** – создать отложенное действие из имени файла;
- **-d**, **--debug** – вывести отладочную информацию по ходу выполнения скрипта.
- **-h**, **--help** – вывести справочную информацию о скрипте.

Примеры использования скрипта:

1. Вывод на экран списка доступных действий. Формат команды для запуска скрипта – **as-tool.py -l**:

```
02a13621-1337-41ec-bc6f-a980c271990a export (format: eml)
42862876-84c6-43c3-85a0-530641ac3c73 add-label (type: #dict.label-type.blocked; description: )
15d19b5a-6ae8-4dd3-804a-fd83128813a9 send (relay-profile:
b6feb470-9e66-46a6-9bfe-226a8bc237e1)
7e860580-2009-4e5a-964f-d58ceda60efb send (relay-profile:
d2e06166-adf8-4ba4-b991-648b36ad1125)
6b764c53-8f99-48f8-b5f8-3c9287a8bd9a send (relay-profile: b6feb470-9e66-46a6-9bfe-226a8bc237e1)
f2505773-3e78-4f0b-a8d8-b5d572fb07e2 send (relay-profile: b6feb470-9e66-46a6-9bfe-226a8bc237e1)
a3f05f1d-866a-4365-ba9b-fc760041115b send (relay-profile: b6feb470-9e66-46a6-9bfe-226a8bc237e1)
92647c63-8c28-4994-ad07-61f0c71dc66d send (relay-profile:
b6feb470-9e66-46a6-9bfe-226a8bc237e1)
efa964f1-6116-4e23-a36f-b9757a483cec add-label (type: Аномальное поведение; description: )
78a0f9e4-2d39-49c0-90ee-3f6315163865 add-label (type: Бухгалтерия; description: баланс)
 officer; type: incident; severity: info)
f2b16a01-d110-4759-bdec-2531cefcf177 add-label (type: #dict.label-type.antivirus; description: )
17edd240-6a39-453f-93c8-e3d3382eebc1 add-label (type: Бухгалтерия; description: )
81ed6e88-d073-453b-8646-6401099622d8 delete-label (type: Бухгалтерия; description: )
533f15b3-f662-4afd-a989-7695e256b396 delete-label (type: Бухгалтерия; description: None)
```

2. Вывод на экран информации о действии с идентификатором <ИД>. Формат команды для запуска скрипта – **as-tool.py -i 02a13621-1337-41ec-bc6f-a980c271990a**:

```
Действие 02a13621-1337-41ec-bc6f-a980c271990a
Параметры:
 host:
  10.199.199.168
 user:
  superadmin
Аргументы:
 format:
  eml
Задания:
 fd86facf-fa3e-4fc0-b7f3-ab32ae3ede12 done 17
```

3. Вывод на экран информации об удалении действия с идентификатором <ИД>. Формат команды для запуска скрипта – **as-tool.py -r 868040b6-dcc8-488b-99a4-b20cdc9c496c**:

```
Действие 868040b6-dcc8-488b-99a4-b20cdc9c496c удалено
```

4. Вывести на экран информацию о всех действиях (формат команды для запуска скрипта – **$ as-tool.py -a**:

```
export: экспорт
delete-label: удаление пометки
create-event: создание события/инцидента
notification: отправка уведомления
add-label: установка пометки
send-to: отправка на указанные адреса
send-pending: отправка тем получателям, которым не было отправлено ранее
send: отправка всем получателям
delete: удаление
```

6.23. Отправка сообщений по протоколу SMTP

Для отправки сообщений по протоколу SMTP предназначен скрипт **smtp-send**.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат запуска скрипта **smtp-send** следующий:

$ smtp-send [from] [to] [host] [port] [file] <ключи>

где:

- **from** – адрес отправителя. При значении "–" адреса извлекаются из заголовков сообщения, при **random** создается случайный адрес.

- **to** – адреса получателей. При значении "–" адреса извлекаются из заголовков сообщения, при **random** создается случайный адрес. Список адресов необходимо указывать в кавычках, например:**"aaa@domain bbb@domain"**.
- **host** – адрес SMTP–сервера. Можно также указать в формате: **smtps://адрес** или **tls://адрес**.
- **port** – порт SMTP–сервера.
- **file** – имя файла с сообщением в формате **eml**.

Доступны следующие ключи:

- **-b**, **--binary** – использовать расширения BINARYMIME/CHUNKING при отправке сообщения.
- **-p sec**, **--pause sec** – задать задержку после отправки сообщения в секундах. По умолчанию: 0 секунд.
- **-m num**, **--messages num** – задать количество сообщений, необходимое для отправки в одной сессии, по умолчанию 10.
- **-d str**, **--domain str** – задать домен, используемый в команде **HELO**/**EHLO**. Если домен не задан, используется **localhost**.
- **-v**, **--verbose** – вывести подробную информацию.
- **-d**, **--debug** – вывести отладочную информацию по ходу выполнения скрипта.
- **-h**, **--help** – вывести справочную информацию о скрипте.

Пример вывода команды **smtp-send - - 10.201.20.146 1025 /var/tmp/test.eml**:

```
От: -
К: -
Протокол: smtp
Хост:10.201.20.146
Порт: 1025
Всего файлов: 1
```

Пример вывода команды **smtp-send - - tls://10.201.20.146 1025 /var/tmp/test.eml**:

```
От: -
К: -
Протокол: tls
Хост:10.201.20.146
Порт: 1025
Всего файлов: 1
```

При выполнении команды с ключом **-v** вывод будет содержать дополнительные строки, например:

```
Отправляем /var/tmp/test.eml
От: <i.vorobeyeva@isim.ru>
К: <z.krylova@isim.ru>
```

6.24. Управление агентами

Для управления агентами предназначен скрипт **agent-tool.py**.

Перед выполнением скрипта следует переключиться на работу от имени пользователя **dozor** и запустить интерпретатор команд shell, выполнив команды:

 # su - dozor

$ /opt/dozor/bin/shell

Формат запуска скрипта **agent-tool** следующий:

$ agent-tool.py [<ключ> ...]

Доступны следующие ключи:

- **-H <имя узла/IP>**, **--login-host <имя узла/IP>** – указать имя или IP-адрес сервера управления Агентами. Значение по умолчанию: **127.0.0.1**.
- **-O <порт>**, **--login-port <порт>** – указать порт сервера управления Агентами.
- **--cert cert** – использовать сертификат из заданного файла. Следует использовать параметр, если планируется подключение к серверу агентов на другом узле.
- **--key key** – использовать секретный ключ из заданного файла. Следует использовать параметр, если планируется подключение к серверу агентов на другом узле.
- **-A <имя узла/IP>**, **--httpd-host <имя узла/IP>** – указать имя или IP-адрес сервера веб-интерфейса.
- **-o <порт>**, **--httpd-port <порт>** – указать порт сервера веб-интерфейса.
- **-u <имя пользователя>**, **--httpd-user <имя пользователя>** – задать имя существующего пользователя веб-интерфейса.
- **-p <пароль>**, **--httpd-password <пароль>** – указать пароль существующего пользователя веб-интерфейса.
- **-l**, **--list-agents** – показать список доступных Агентов. В скобках выводятся идентификаторы групп, в которых состоят станции с Агентами (при отсутствии группы – **Неизвестно**).
- **-D <кол-во дней>**, **--list-idle-agents <кол-во дней>** – вывести на экран список Агентов, которые не выходили на связь более указанного количества дней.
- **-R**, **--tree** – вывести дерево агентов.
- **-L**, **--list-groups** – вывести список всех доступных групп.
- **-s**, **--list-settings** – вывести список доступных настроек.
- **-c**, **--list-configurations** – показать список доступных конфигураций.
- **-P**, **--list-policies** – вывести список доступных политик.

- **-t**, **--list-dist-set** – показать список доступных наборов дистрибутивов.
- **-T <ИД дистрибутива>**, **--list-dist <ИД дистрибутива>** – показать состав дистрибутива с идентификатором ИД.
- **-i <агент>**, **--agent-info <агент>** – показать информацию об агенте.
- **-I <ИД>**, **--group-info <ИД>** – вывести информацию о группе с указанным идентификатором.
- **-S <ИД настроек агента>**, **--settings-info <ИД настроек агента>** – показать информацию о настройках с указанным идентификатором.
- **-C <ИД конфигурации>**, **--configuration-info <ИД конфигурации>** – вывести информацию о конфигурации с указанным идентификатором.
- **-n <ИД набора дистрибутивов>**, **--dist-set-info <ИД набора дистрибутивов>** – вывести информацию о наборе дистрибутивов с указанным идентификатором.
- **-N <ИД набора дистрибутивов> <ИД дистрибутива>**, **--dist-info dist-set-id <ИД набора дистрибутивов> <ИД дистрибутива>** – вывести информацию о дистрибутиве.
- **-a**, **--auth-info** – вывести информацию об авторизации.
- **-e <название группы> <ОС> <ИД настроек агента> <ИД конфигурации> <ИД политики><ИД набора дистрибутивов>**, **--create-group <название группы> <ОС> <ИД настроек агента> <ИД конфигурации> <ИД политики><ИД набора дистрибутивов>** – создать новую группу.
- **-r <ИД группы>**, **--delete-group <ИД группы>** – удалить группу с указанным идентификатором.
- **-G <ИД группы> <агент1> ... <агентN>**, **--add-agents <ИД группы> <агент1> ... <агентN>** – добавить агента/агентов в группу с указанным идентификатором.
- **-V <агент1> ... <агентN>**, **--remove-agents <агент1> ... <агентN>** – удалить агента/агентов.
- **-U <агент1> ... <агентN>**, **--update-agents <агент1> ... <агентN>** – обновить агента/агентов в группе с указанным идентификатором.
- **-E <агент1> ... <агентN>**, **--recover-agents <агент1> ... <агентN>** – восстановить агента/агентов из группы с указанным идентификатором.
- **-x <агент1> ... <агентN>**, **--uninstall-agents <агент1> ... <агентN>** – деинсталлировать агента/агентов.
- **-m <ИД группы> <агент1> ... <агентN>**, **--relocate-agents <ИД группы> <агент1> ... <агентN>** – выполнить перемещение агента/агентов в группу с указанным идентификатором.
- **-d**, **--debug** – вывести отладочную информацию по ходу выполнения скрипта.
- **-h**, **--help** – вывести справочную информацию о скрипте.

Примеры использования скрипта:

1. Вывод на экран списка доступных агентов (формат команды для запуска скрипта – **agent-tool.py -l**):

```
vt.platonov.akbprogress.ru: 54c5b734-b3f2-43fd-b467-da2a512af99c (Неизвестно)
vv.dubinkin.akbprogress.ru: 2081cb2f-48a9-4c2d-8a6f-3c4073c6b2df (Неизвестно)
vv.jablokov.akbprogress.ru: c0a31298-0d84-49b9-ae7c-60a80e6ccd0a (Неизвестно)
yd.rataeva.akbprogress.ru: 69b6073f-a1fd-45c5-88ce-b477c2976e80
(097a436f-6a6c-424b-b955-82bdb307b9a8)
yn.ababkov.akbprogress.ru: ac740a67-426e-49af-afe3-5df7b690685a
(1f7c565d-88cc-4334-93f2-6008ce2db71e)
ys.klueva.akbprogress.ru: c5d5a883-a5bd-413b-afee-cfebadfd44bf
(1f7c565d-88cc-4334-93f2-6008ce2db71e)
```

   В скобках выводятся идентификаторы групп, в которых состоят станции с Агентами (при отсутствии группы – **Неизвестно**).

2. Вывод на экран информации о состоянии агента (формат команды для запуска скрипта – **agent-tool.py -i righttop.agent.local**):

```
status:
  name: run
  value: Работает
 domain: agent.local
 group:
  osType: Windows
  id: 151ba831-80ed-4734-ac38-0b4e0557a47c
  name: 3.3.0.088
users:
  login: DWM-1
  title: None
  fullname: None
  id: None
  sid: S-1-5-90-1

  login: DWM-2
  title: None
  fullname: None
  id: None
  sid: S-1-5-90-2

  login: administrator
  title: None
  fullname: None
  id: None
  sid: S-1-5-21-3290733501-3725838525-2805556546-500

versions:
  name: Стандартные настройки
  installed: 2019-05-24T12:19:47.174+03:00
  state: None
  accepted: 2019-05-24T09:20:39Z
  type: setting
  id: f5ddd0d2-710d-4fa7-93e3-5da885d8a567

  name: default-agent-settings
  installed: 2019-05-24T09:20:31.618Z
  state: None
  accepted: 2019-05-24T09:20:39Z
```

```
 type: configuration
 id: default-agent-settings

timestamp: 2019-05-24T10:17:53Z
hostname: righttop.agent.local
shortLived: False
state:  <пусто>
mode: full
ipAddresses: 10.199.28.235, 10.199.28.235
online: True
osType: Windows
stateHistory:
 category:
   name: ok
   value: Успешное действие
 status:
   name: run
   value: Работает
 users:
   login: DWM-1
   title: None
   fullname: None
   id: None
   sid: S-1-5-90-1

   login: DWM-2
   title: None
   fullname: None
   id: None
   sid: S-1-5-90-2

   login: administrator
   title: None
   fullname: None
   id: None
   sid: S-1-5-21-3290733501-3725838525-2805556546-500

 timestamp: 2019-05-24T10:50:43+03:00
 subStatus:
   name: policy-accepted
   value: Политика применена
 message: None

 category:
   name: ok
   value: Успешное действие
 status:
   name: run
   value: Работает
 users:
   login: DWM-1
   title: None
   fullname: None
   id: None
   sid: S-1-5-90-1

 timestamp: 2019-05-23T13:12:50+03:00
 subStatus:
```

```
  name: config-accepted
  value: Конфигурация применена
message: None
```

3. Вывод на экран информации о группах станций (формат команды для запуска скрипта – **agent-tool.py -L**):

```
С полнофункциональными агентами: ea60c6e5-bca3-4608-bf81-6c0048cf082f
Без перехвата: fe312774-83de-46f1-8923-fb35c4e53d99
Citrix: 4b4b3b09-e3e4-4ec5-83dd-046ea428f90d
```

4. Вывод на экран информации о группе с идентификатором <ИД>, например **ea60c6e5-bca3-4608-bf81-6c0048cf082f** (формат команды для запуска скрипта – **agent-tool.py -l ea60c6e5-bca3-4608-bf81-6c0048cf082f**):

```
name: С полнофункциональными агентами
schedule: None
forcedRestart: False
configurationId: default-agent-settings
reboot:
  comment:
  timeout: 0
settingId: ab095e75-65cd-4444-b534-33cf8849dde5
distributionSetId: a87442a3-be5c-4186-be8d-f7095052efce
policyId: 57fb7d17-a488-4ae8-bace-f56bd1d9709c
osType: Windows
accounts:  <пусто>
id: ea60c6e5-bca3-4608-bf81-6c0048cf082f
groupHint: None
```

5. Удаление группы с идентификатором <ИД>, например **e67ae0e7-8a1f-4f00-976e-2932b8fa366a** (формат команды для запуска скрипта – **agent-tool.py -r e67ae0e7-8a1f-4f00-976e-2932b8fa366a**). Вывод команды имеет вид:

```
Группа успешно удалена
```

6.25. Просмотр информации о лицензии

Для просмотр информации о лицензии, об идентификаторе инсталляции и активных адресах электронной почты предназначен скрипт **license-tool**.

Перед выполнением скрипта следует запустить интерпретатор команд **shell**, выполнив команду:

 # /opt/dozor/bin/shell

Формат запуска скрипта **license-tool** следующий:

 # license-tool [ключ]

Доступны следующие ключи:

- **-i**, **--installation-id** – вывести информацию об идентификаторе инсталляции.

- **-l dozor**, **--license dozor** – вывести информацию о состоянии лицензии.
- **-a**, **--active-addresses** – вывести информацию об активных адресах электронной почты.
- **-c**, **--active-addresses-count** – вывести информацию о количестве активных адресов электронной почты.
- **-h**, **--help** – вывести справочную информацию о скрипте.

Примечание

*Информацию об активных адресах электронной почты можно также получить, выполнив в GUI скрипт **license-user-list** (5.3).*

6.26. Распаковка tnef-файлов с помощью скрипта командной строки

Чтобы открыть файлы формата TNEF (**winmail.dat**), которые были созданы в Microsoft Outlook, сервис **mailfilter** использует специальный скрипт **tnefparse.py**. С помощью скрипта можно просматривать содержимое этого файла, извлекать вложения, преобразовывать тело сообщения в необходимые форматы и прочее.

Перед выполнением скрипта следует запустить интерпретатор команд **shell**, выполнив команду:

 # /opt/dozor/bin/shell

Формат команды для запуска скрипта **tnefparse.py**:

 # tnefparse.py [ключ] <файл или список файлов, указываемых через пробел>

Доступны следующие ключи:

- **-o, --overview** – вывести на экран содержимое файла **winmail.dat**.
- **-a, --attachments** – извлечь содержимое в текущий каталог.
- **-z, --zip** – создать в текущем каталоге zip-архив с содержимым tnef-файла.
- **-p <путь к каталогу>**, **--path <путь к каталогу>** – указать путь к каталогу, в который будет распаковано содержимое файла **winmail.dat**.
- **-b, --body** – извлечь тело сообщения в файл **message.txt**.
- **-hb, --htmlbody** – извлечь HTML-тело в файл **message.html**.
- **-rb, --rtfbody** – извлечь RTF-тело в файл **message.rtf**.
- **-ab, --allbody** – извлечь все существующие тела сообщения.
- **-t, --list** – вывести на экран список вложений.
- **-c, --checksum** – рассчитать контрольную суммы вложений.

- **-d, --dump** – извлечь дамп в формате **json** из содержимого файла **winmail.dat**.
- **-h**, **--help** – вывести на экран справочную информации об использовании скрипта.

6.27. Контроль изменений политики и настроек конфигурации

В KEO DLP применяется механизм контроля изменений политики и настроек. Все изменения в политике и настройках отслеживаются и сохраняются. Все значения настроек расположены на master-узле в файле **/data/repos/dozor/config-base.git/values.json**.

Описание политики и необходимые для её работы ресурсы расположены в отдельной базе данных PostgreSQL в каталоге **/data/base/dozor/pgsql** на master-узле. Эта БД создаётся автоматически при назначении узлу роли **master**.

Для соединения с базой данных политики и настроек досье по умолчанию используется схема, которая указанная в секции **Сервис доступа к Досье** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Досье**). При значении **БД по умолчанию** сервис подключается к БД политики, настройки которой указаны в секции **БД настроек политики и досье** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**). При значении **Специальная БД** сервис подключается к БД политики, параметры которой может задать системный администратор.

Политика на slave-узлах применяется автоматически. Как только на master-узле генерируется новая политика, все slave-узлы синхронизируют свою локальную политику с master-узлом.

При необходимости, администратор системы может произвести аудит изменений политики и настроек, а также восстановить состояние настроек до определённого состояния и сохранить их.

Полезные сценарии для работы с данным механизмом описаны ниже в подразделах:

- Просмотр последнего изменения политики (раздел 6.27.1).
- Возврат к сохранённым изменениям политики (раздел 6.27.2).
- Аудит изменений настроек системы (раздел 6.27.3).
- Сохранение изменений настроек (раздел 6.27.4).

6.27.1. Просмотр последнего изменения политики

Для просмотра изменений политики необходимо выполнить от имени пользователя **root** следующие команды:

 # /opt/dozor/bin/shell

 # cd /data/repos/dozor/config-base.git

 # git log

6.27.2. Возврат к сохранённым изменениям политики

Для возврата к последнему состоянию конфигурации для восстановления настроек политики необходимо выполнить на master-узле от имени пользователя **root** следующие команды:

 # /opt/dozor/bin/shell

 # cd /data/repos/dozor/policy-final.git

 # git reset master~1

После этого необходимо выполнить на всех slave-узлах от имени пользователя **root** следующие команды:

 # /opt/dozor/bin/shell

 # rm -rf /data/repos/dozor/policy-final.git

 # accept-policy

6.27.3. Аудит изменений настроек системы

Если есть необходимость оставить в истории неработоспособные изменения, то необходимо выполнить от имени пользователя **root** следующие команды:

 # git checkout -f master~1

 # accept-settings

Если полученный результат не удовлетворителен, можно повторить ввод следующим образом:

 # git checkout -f master~2

 # accept-settings

При использовании команды **git checkout** правильным будет восстанавливать изменения не от последних установок на master-узле (которые меняются при каждом вызове скрипта **accept-settings**), а от конкретного последнего сохранения (commit) настроек, которые можно уточнить с помощью команды **git log**, например:

```
commit 3bf5fe815c4411f559f4a9e6db99ba915ef112b6
Author: KEO DLP <keodlp@isim.local>
Date:   Mon Dec 14 18:19:22 2015 +0400
```

где **3bf5fe815c4411f559f4a9e6db99ba915ef112b6** – последнее сохранение, **59e162f54459bb83de3db0d4e76d1e34e191fca2** – предыдущее сохранение.

Для применения предыдущего сохранения следует выполнить следующую команду (для приведенного случая):

 # git checkout -f 3bf5fe815c4411f559f4a9e6db99ba915ef112b6~1

Также можно вернуть конфигурацию на файловой системе на конкретное сохранение следующей командой (для приведенного случая):

 # git checkout -f 59e162f54459bb83de3db0d4e76d1e34e191fca2

Кроме того, можно сделать возврат сразу на несколько предыдущих сохранений, например на 2, с помощью следующей команды (для приведенного случая):

 # git checkout -f 3bf5fe815c4411f559f4a9e6db99ba915ef112b6~2

6.27.4. Сохранение изменений настроек

После восстановления настроек при попытке сохранить изменения может возникнуть следующая ошибка:

```
cannot open output file: /data/repos/dozor/config-base.git/values.json
```

В этом случае перед попыткой сохранения изменений следует выполнить следующую команду:

chown -R dozor:dozor /data/repos/dozor/config-base.git/values.json

6.28. Контроль целостности

Контроль целостности файлов KEO DLP выполняется с помощью скрипта **/opt/dozor/bin/check_dozor**. Скрипт использует стандартный механизм проверки целостности установленных файлов относительно содержащихся в исходных deb-пакетах. При проверке скрипт с помощью алгоритма MD5 подсчитывает контрольные суммы всех исполняемых файлов и библиотек серверной части, входящих в состав установочных пакетов KEO DLP, после чего сравнивает найденные контрольные суммы с эталонами, находящимися в хранилище сертификатов. Результаты проверки записываются в журнал безопасности.

Контроль целостности выполняется в следующих видах проверок:

- Диагностический контроль – при запуске KEO DLP (команда **dsctl boot**). При обнаружении несоответствий запуск KEO DLP прерывается с ошибкой нарушения целостности, а скрипт **check_dozor** выводит на экран информацию о местах нарушений. В этом случае необходимо устранить все нарушения целостности, выполнить скрипт **check_dozor** вручную и запустить KEO DLP вновь. Также можно запустить KEO DLP без устранения нарушений, под ответственность офицера безопасности – для этого необходимо создать файл **/opt/dozor/SKIP_CHECK_MODE** и запустить KEO DLP. Пока этот файл существует – никакие проверки целостности не будут выполняться ни в автоматическом режиме, ни в ручном.
- Оперативный контроль – при запуске скрипта планировщиком **cron**. По умолчанию в планировщике задан запуск скрипта раз в 24 часа. При обнаружении хотя бы одного несоответствия скрипт отправляет почтовое сообщение с результатами проверки по адресам, заданным в конфигурации. Сообщение с результатами проверки содержит следующую информацию:
  - Сетевое имя узла, на котором было обнаружено несоответствие контрольных сумм.
  - Данные об ОС.
  - Дата и время выполнения проверки.

- Сводная таблица с результатами пересчёта контрольных сумм по всем установочным пакетам KEO DLP.

- Регламентный контроль – при ручном запуске скрипта в CLI. При обнаружении несоответствий скрипт выполняет те же действия, что и при оперативном контроле.

Настройка регулярного контроля целостности описана в документе *Руководство по установке и настройке* (раздел *Настройка контроля целостности*).

Проверку можно вызвать в любой момент, выполнив команду:

 # /opt/dozor/bin/check_dozor

Чтобы узнать, какие именно установленные файлы были модифицированы, необходимо выполнить в CLI от имени пользователя **root** следующую команду:

~$ debsums -c "dlp-*"

Механизм контроля целостности по умолчанию включен. Для отключения механизма контроля целостности необходимо создать файл **/opt/dozor/SKIP_CHECK_MODE**. Пока этот файл существует – никакие проверки целостности не будут выполняться ни в автоматическом режиме, ни в ручном.

7. Аварийные ситуации

7.1. Реагирование KEO DLP на аварийные ситуации

7.1.1. Поведение архиватора в случае возникновения ошибок

Если в процессе архивирования сообщений возникли ошибки, возможны два варианта поведения архиватора:

- повторная обработка сообщения;
- прерывание процесса обработки сообщения.

7.1.1.1. Повторная обработка сообщения

Повторная обработка сообщения производится в следующих случаях:

- если разные процессы архиватора при обработке различных сообщений пытаются поместить в БД архива одинаковые данные. Например, почтовый адрес или термин словаря;
- если произошел **deadlock** (взаимная блокировка) БД архива.

При этом сообщение остается в очереди **/opt/dozor/smap/spool/smap-db** и ожидает повторной обработки.

7.1.1.2. Прерывание процесса обработки сообщения

Процесс обработки сообщения прерывается, если возникла ошибка обработки содержимого сообщения. При этом сообщение помещается в каталог **/opt/dozor/smap/spool/smap-db-err**.

7.1.2. Поведение KEO DLP в случае возникновения ошибок при распаковке содержимого сообщения

Возможно возникновение следующих ошибок при распаковке содержимого сообщения:

1. KEO DLP не удается распаковать архив, защищенный паролем. Если сообщение содержит архив, защищенный паролем, KEO DLP не сможет распаковать содержимое этого архива. В этом случае будет выдана ошибка вида:

   ```
   error: archive file is encrypted. Unable to unpack.
   ```

   Примечание

   Конкретный вид этого сообщения может различаться в зависимости от типа архива.

2. Сервис **mailfilter** не может корректно обработать объект содержимого сообщения вследствие нарушения его структуры. При разборе сообщения и выделении входящих в него объектов, например, документа pdf, может встретиться поврежденный объект. Сервис **mailfilter** не может корректно обработать такой объект, и будет выдано сообщение об ошибке:

```
error: Garbage in input buffer.
```

3. Анализатор XML не может разобрать XML-файл. Если в сообщение вложен XML-файл, неправильный с точки зрения синтаксиса, и анализатор не может разобрать этот файл, то будет выдано сообщение об ошибке следующего вида:

```
error: xml:Parse: Error: not well-formed (invalid token) at line 1 column 0.
```

4. Анализатор HTML не может разобрать HTML-файл. Если в сообщение вложен HTML-файл, содержащий синтаксическую ошибку в написании тэгов и их параметров (например, присутствует открывающий символ «<» и отсутствует закрывающий «>»), это может привести к невозможности обработать HTML-файл. В этом случае текст из файла не будет извлечен, и будет выдано сообщение об ошибке с указанием места (позиции символа) в документе, где произошла ошибка обработки:

```
HTML: invalid attribute name (position 18530)
```

Все ошибки, связанные с разбором содержимого сообщения, сохраняются, и их впоследствии можно посмотреть в журнальном файле **/opt/dozor/var/lib/service/mailfilter/log**.

Примечание

*Пароли, которые указываются для распаковки архивов, настраиваются в параметре **Пароли для распаковки архивов** (раздел GUI **Система > Конфигурация >Расширенные настройки >Настройка средств фильтрации перехваченных данных и детектирования критичной информации >Обработка сообщений**, секция **Сервис фильтрации сообщений**).*

7.1.3. Поведение KEO DLP при отсутствии лицензии Модуля долговременного хранения архива коммуникаций

Если в кластере KEO DLP есть хотя бы одна секционированная БД, сервер архива проверяет лицензию **Модуля долговременного хранения архива коммуникаций** путем отправки запроса в сервер лицензирования. Если этот модуль отсутствует в лицензии или истек его срок действия, при архивировании и поиске информации в секционированной БД появляется сообщение об ошибке вида:

```
License violation: partitioning not allowed
```

Если в кластере KEO DLP отсутствуют секционированные БД, процесс архивирования будет завершен с ошибкой вида (HTTP-код 404):

```
No storages available for archiving by default
```

7.1.4. Поведение KEO DLP при отсутствии лицензии Модуля контроля коммуникаций через корпоративные почтовые системы

Фильтр почтового потока проверяет лицензию **Модуля контроля коммуникаций через корпоративные почтовые системы** путем отправки запроса в сервер лицензирования. Если этот модуль отсутствует в лицензии или истек его срок действия, сообщения остаются в спуле. В журналах фильтра появится сообщение:

```
Module mail-server-connector is not active. Leaving message c4984e14-6d1d-11eb-a8ac-005056aa6a8e
 of type email in spool
```

Если сервис **mailfilter** не может установить соединение с сервером лицензирования, информация о лицензии загружается из кэша фильтра, в котором хранится последний ответ **license-server**. Если в течение трех дней сервер лицензирования будет недоступен, об этом будет свидетельствовать следующая запись в журнале **mailfilter**:

```
License check failed: No valid data in cache
```

В этом случае сообщения также останутся в спуле.

7.1.5. Поведение KEO DLP в случае появления ошибок при отправке сообщения

В случае возникновения ошибок при отправке сообщения предусмотрены три варианта поведения KEO DLP:

1. Остановка сервиса отправки – этот вариант применим, если возникла критическая ошибка, связанная, например, с неправильными настройками, которая не может быть устранена со временем и требует вмешательства системного администратора. Кроме того, вариант применим при ошибке, не связанной с конкретным сообщением.

2. Перемещение сообщения в каталог **smap-send-err**, чтобы сервис отправки больше не пытался его обрабатывать. Решение о дальнейших действиях с данным сообщением принимает системный администратор. Этот вариант должен применяться при ошибках, связанных с конкретным сообщением, которые не могут устраниться со временем.

3. Хранение сообщения в каталоге **spool** с целью реализации попытки отправить его позже. Этот вариант применим при временных ошибках системы, например при нехватке памяти, места на диске, недоступности тех или иных сетевых ресурсов, т.е. в тех случаях, когда предполагается, что сообщение может быть нормально отправлено через какое-то время при следующей попытке отправки.

Решение по выбору варианта принимается на основании кода ошибки. Код ошибки – это код возврата локального MTA, если он не равен 0, или код ответа SMTP-сервера, если он больше 399.

В Табл.7.1 и Табл.7.2 приведены коды возврата для Sendmail и коды ошибок SMTP.

Табл. 7.1. Коды возврата для Sendmail

Код ошибки	Описание	Пояснение
(define EX_OK 0)	successful termination	Успешное завершение.
(define EX_USAGE 64)	command line usage error	Ошибка работы с командной строкой.
(define EX_DATAERR 65)	data format error	Неверный формат данных.
(define EX_NOINPUT 66)	cannot open input	Не удается прочитать входные данные.
(define EX_NOUSER 67)	address unknown	Неизвестный адрес.
(define EX_NOHOST 68)	host name unknown	Неизвестное имя сервера.
(define EX_UNAVAILABLE 69)	service unavailable	Служба недоступна.
(define EX_SOFTWARE 70)	internal software error	Внутренняя ошибка приложения.
(define EX_OSERR 71)	system error (e.g., can't fork)	Ошибка системы.

Код ошибки	Описание	Пояснение
(define EX_OSFILE 72)	critical OS file missing	Отсутствует необходимый системный файл.
(define EX_CANTCREAT 73)	can't create (user) output file	Не удается создать выходной файл.
(define EX_IOERR 74)	input/output error	Ошибка ввода/вывода.
(define EX_TEMPFAIL 75)	temp failure; user is invited to retry	Временная ошибка. Предлагается сделать повторную попытку.
(define EX_PROTOCOL 76)	remote error in protocol	Ошибка в работе протокола.
(define EX_NOPERM 77)	permission denied	Доступ запрещен.
(define EX_CONFIG 78)	configuration error	Ошибка конфигурации.
(define EX_NOTFOUND 79)	entry not found	Запись не найдена.

Табл. 7.2. Коды ошибок SMTP

Код ошибки	Описание	Пояснение
421	<domain> Service not available, closing transmission channel	Сервис отсутствует. Канал передачи данных закрыт.
450	Requested mail action not taken: mailbox unavailable	Нет возможности записать данные в почтовый ящик.
451	Requested action aborted: local error in processing	Ошибка при обработке запроса.
452	Requested action not taken: insufficient system storage	Запрос не выполнен, недостаточно памяти.
500	Syntax error, command unrecognised	Синтаксическая ошибка: нет такой команды.
501	Syntax error in parameters or arguments	Синтаксическая ошибка в аргументах команды.
502	Command not implemented	Данная команда не может быть выполнена.
503	Bad sequence of commands	Неправильная последовательность команд.
504	Command parameter not implemented	Параметр команды не может быть использован в данном контексте.
521	<domain> does not accept mail (see rfc1846)	Домен недопустим.
530	Access denied	Доступ запрещен.
550	Requested action not taken: ailbox unavailable	Не найден соответствующий почтовый ящик.
551	User not local; please try <forward-path>	Пользователь не найден, попытайтесь отправить почту по другому адресу.
552	Requested mail action aborted: exceeded storage allocation	Превышены квоты на использование ресурсов памяти.
553	Requested action not taken: mailbox name not allowed	Имя почтового ящика неправильное.
554	Transaction failed	Обмен завершился аварийно.

Все ошибки, связанные с отправкой сообщения, сохраняются, и их впоследствии можно посмотреть в журнальном файле **/opt/dozor/var/log/sender/current**.

7.1.6. Особенности потребления памяти сервером лицензирования

Объем памяти, используемой под размещение объектов сервиса **license-server** (учитывается **heap**), ограничивается параметром **-Xmx**, указанным в файле **/opt/dozor/var/lib/service/license-server/run**. Поскольку сервер лицензирования использует помимо **heap** другие области памяти, он проигнорирует это ограничение и будет занимать больше памяти, чем указано.

7.1.7. Принципы работы фильтрации в графических шаблонах

В рамках обработки одного сообщения **mailfilter** формирует на каждое вложение отдельный запрос. Чтобы избежать нагрузки на систему, каждый запрос направляется на случайный узел с ролью **Распознавание графических объектов**, входящий в состав кластера KEO DLP. Если этот узел недоступен, запрос на распознавание графического объекта обработан не будет, и в журнале сервиса **mailfilter** появится сообщение вида:

```
Compare error: GOD-server failure: В соединении отказано
```

Поскольку запросы на распознавание графических объектов не перенаправляются на другие узлы, это сообщение будет появляться до тех пор, пока не будет обеспечена доступность узла с ролью **Распознавание графических объектов**, входящего в кластер KEO DLP.

Примечание

*Аналогичное поведение наблюдается при взаимодействии сервера фильтрации с сервисами **smap-difi** и **smap-idid**.*

7.2. Реагирование системного администратора KEO DLP на аварийные ситуации

7.2.1. Действия в случае переполнения БД архива

В случае возникновения аварийной ситуации, связанной с недостатком свободного места в БД архива, сервис архивирования прекращает обрабатывать сообщения и завершает все свои процессы.

После решения проблемы, связанной с нехваткой свободного места в БД архива, сервис архивирования необходимо запустить вручную.

Примечание

Если архиватор был остановлен намеренно, то после произведенных действий его также необходимо запустить вручную.

В случае возникновения аварийной ситуации, связанной с превышением объема какого-либо журнального файла подсистемы фильтрации, возможно прекращение работы сервиса фильтрации. Для предотвращения подобной ситуации максимальный объем журнального файла не должен превышать 2048 МБ. Для решения проблемы необходимо производить архивирование журнальных файлов KEO DLP (см. раздел 6.11.3).

7.2.2. Снятие блокировки после аварийного прекращения процесса liquibase

Для решения данной проблемы необходимо сделать следующее:

1. Убедиться, что процесс **liquibase** в данный момент не запущен на другом сервере.
2. Присоединиться к БД с помощью команды: **psql**.

3. Проверить наличие блокировки, выполнив команду:

   select * from databasechangeloglock;

   В результате будет выведена таблица, в которой необходимо проверить значение столбца **locked**.

   Если в столбце присутствует значение **true**, то блокировка установлена.

4. Снять блокировку, выполнив команду:

   update databasechangeloglock set locked=false, lockgranted=null,lockedby=null;

5. Перезапустить операцию обновления базы ещё раз.

7.2.3. Действия в случае нехватки семафоров

При нехватке семафоров сервисы не будут корректно принимать и обрабатывать входящие соединения. В этом случае будет выдана ошибка вида:

```
[emerg] (28)No space left on device: Couldn't create accept lock
```

Для решения данной проблемы необходимо выполнить следующие действия:

1. Проверить наличие свободного места на диске, выполнив команду;

   #df -h

2. Если свободного места в файловой системе меньше 1 ГБ, необходимо открыть для редактирования файл **/etc/sysctl.conf**. Если в выводе будут отсутствовать следующие строки, то их нужно добавить в конец файла:

   ```
   kernel.shmall = 4294967296
   kernel.sem = 250 1024000 250 4096
   kernel.msgmni = <x>
   ```

   где **<x>** – объем оперативной памяти узла в гигабайтах, умноженный на 1024. Объём оперативной памяти узла в гигабайтах можно узнать, выполнив команду:

   free -g

3. После редактирования конфигурации выполнить команду
   # sysctl -p
   и перезапустить сервер KEO DLP.

7.2.4. Управление кластером Cassandra

Узлы, на которых хотя бы одна из ролей использует сервис **skvt-cassandra**, образуют кластер Cassandra. Сервис **skvt-cassandra** используют следующие роли:

- Сервис распределённого хранения (cassandra);
- Центральное файловое хранилище (fsng-storage);
- Локальное файловое хранилище (fsng-client);

Ниже описаны процедуры добавления и удаления узлов кластера Cassandra.

7.2.4.1. Добавление узла в кластер Cassandra

Добавление узла в кластер Cassandra происходит в следующих случаях:

- Добавление узла в кластер KEO DLP и назначение ему роли, использующей сервис **skvt-cassandra**.
- Назначение узлу кластера KEO DLP роли, использующей сервис **skvt-cassandra**, при условии, что этот узел ранее не использовал этот сервис.

Если кластер Cassandra уже находился в использовании, то после добавления в него нового узла необходимо по очереди на каждом узле кластера Cassandra выполнить следующие команды:

 # cd /opt/dozor/cassandra/bin

 # ./nodetool --ssl repair

7.2.4.2. Удаление узла из кластера Cassandra

Удаление узла из кластера Cassandra необходимо в следующих основных сценариях:

- Необходимость перераспределения ролей между узлами кластера KEO DLP, в результате которого на одном из узлов перестаёт использоваться сервис **skvt-cassandra** (штатное удаление).
- Аварийное прекращение работы узла, использовавшего сервис **skvt-cassandra**, связанное с невозможностью его восстановления (аварийное удаление).

7.2.4.2.1. Штатное удаление

Для штатного удаления узла из кластера Cassandra необходимо выполнить следующие действия:

1. С помощью CLI выполнить на любом узле, который планируется оставить в кластере Cassandra, следующую команду:

   # /opt/dozor/cassandra/bin/nodetool --ssl status

   На экран будет выведена информация следующего вида:

   ```
   Note: Ownership information does not include topology; for complete information, specify a keyspace
   Datacenter: datacenter1
   ======================
   Status=Up/Down
   |/ State=Normal/Leaving/Joining/Moving
   --  Address       Load       Tokens  Owns   Host ID                               Rack
   UN  10.199.28.121  4,69 MB    256     36,1%  d5e87fb3-7faa-4b90-8c7c-02c4feda90c6  rack1
   UN  10.199.28.120  4,73 MB    256     63,8%  ab14fc7e-1dae-4bd1-b6af-a8b85166d08c  rack1
   ```

   Если каждая строка начинается со значения **UN** (**Up**/**Normal**), то все узлы функционируют нормально, и можно производить штатное удаление.

2. Перенести с помощью скрипта **nodetool** данные Cassandra на другие узлы:

   # /opt/dozor/cassandra/bin/nodetool --ssl --host <node> decommission

где **node** – имя или адрес удаляемого узла

3. Убедиться, что удаляемый узел покинул кластер Cassandra, выполнив следующую команду:

   # /opt/dozor/cassandra/bin/nodetool --ssl status

   Вывод команды не должен содержать запись об удаляемом узле. В противном случае следует подождать и повторить проверку.

4. Снять с удаляемого узла роли, использующие сервис **skvt-cassandra**.

5. Очистить все подкаталоги, находящиеся в каталоге **/data/spool/cassandra/** (сами подкаталоги при этом не удалять).

7.2.4.2.2. Аварийное удаление

В случае недоступности узла кластера Cassandra необходимо его удалить, выполнив следующие действия:

1. С помощью CLI выполнить на любом работающем узле кластера Cassandra следующую команду:

   # /opt/dozor/cassandra/bin/nodetool --ssl status

   На экран будет выведена информация следующего вида:

```
Note: Ownership information does not include topology; for complete information, specify a keyspace
Datacenter: datacenter1
=======================
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
--  Address       Load       Tokens  Owns   Host ID                               Rack
UN  10.199.28.121  4,69 MB    256     36,1%  d5e87fb3-7faa-4b90-8c7c-02c4feda90c6  rack1
DN  10.199.28.120  4,73 MB    256     63,8%  ab14fc7e-1dae-4bd1-b6af-a8b85166d08c  rack1
```

   Статус **D** свидетельствует о том, что узел выключен или не отвечает на запросы.

2. Удалить нерабочий узел из кластера Cassandra, выполнив следующую команду:

   # /opt/dozor/cassandra/bin/nodetool --ssl removenode <ID>

   где **<ID>** – значение в столбце **Host ID** для нерабочего узла.

3. Убедиться, что удаляемый узел покинул кластер Cassandra, выполнив следующую команду:

   # /opt/dozor/cassandra/bin/nodetool --ssl status

   Вывод команды не должен содержать запись об удаляемом узле. В противном случае следует подождать и повторить проверку.

4. На всех оставшихся узлах кластера Cassandra по очереди выполнить следующую команду:

   # /opt/dozor/cassandra/bin/nodetool --ssl repair

7.2.5. Действия при исчерпании памяти сервиса indexer-ng

Если в БД сервиса индексации данных содержится достаточно большое количество рассылок, то процесс **indexer-ng** попытается выделить себе слишком большой объем оперативной памяти. При исчерпании оперативной памяти работа процесса будет аварийно завершена. Об этой ситуации свидетельствуют сообщения следующего вида в журнале сервиса **indexer-ng**:

```
2021-07-15T11:32:00+0300 pur0.isim.local run[22384]: java.lang.OutOfMemoryError: Java heap space
2021-07-15T11:32:00+0300 pur0.isim.local run[22384]: Dumping heap to /data/temp/java_pid22384.hprof
 ...
2021-07-15T11:33:17+0300 pur0.isim.local run[22384]: Heap dump file created [3023076928 bytes in
77.622 secs]
```

Для устранения этой неисправности необходимо выполнить следующие действия:

1. Открыть для редактирования файл **/opt/dozor/indexer-ng/config/application.conf** и и найти в нём следующую строку:

   ```
   dbChunks = 500
   ```

2. Заменить значение 500 на 50. Строка должна выглядеть следующим образом:

   ```
   dbChunks = 50
   ```

3. Сохранить и закрыть файл.

4. Перезапустить сервис **indexer-ng**, выполнив команду:

   # dsctl restart indexer-ng

Внимание!

*Изменение параметра **dbChunks** может негативно сказаться на производительности сервиса **indexer-ng**.*

7.2.6. Действия при ошибках сервиса opensearch

7.2.6.1. Действия при переполнении оперативной памяти

Если в сервисе текстовой индексации и поиска на основе OpenSearch содержится достаточно большое количество данных, то процесс **opensearch** попытается выделить себе слишком большой объем оперативной памяти. При переполнении оперативной памяти работа процесса будет аварийно завершена с ошибкой **Out of memory: Kill process**.

Необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация** > **Расширенные настройки** > **Настройка средств мониторинга и анализа нарушений** > **Поиск**.

2. В секции **Производительность сервиса поиска и индексации сообщений и инцидентов** уменьшить значение параметра **Размер памяти (ГБ)**.

Данное решение может привести уменьшению вероятности возникновения данной ошибки и к повышению надежности функционирования сервиса **opensearch**.

7.2.6.2. Действия при исчерпании свободного места на диске

При исчерпании свободного места на диске сервис **opensearch** для предотвращения аварийной остановки системы переходит в режим **read-only** (только чтение), но при освобождении свободного места не выходит из этого режима. Об этой ситуации свидетельствуют сообщения следующего вида в журнале сервиса **indexer-ng**:

```
2018-09-24 11:00:33.219541500 WARN  indexer.services.ElasticServiceImpl - Operation failed bulk
indexing failed:
failure in bulk execution:
2018-09-24 11:00:33.219545500 [0]: index [msg-2018-37], type [doc], id
[b324fc9c-b675-11e8-a68a-005056885c29-1],
message [ClusterBlockException[blocked by: [FORBIDDEN/12/index read-only / allow delete (api)];]]
```

Для устранения этой неисправности необходимо выполнить следующие действия:

1. Освободить место на диске сервера, на котором наблюдается неисправность.
2. Запустить командную оболочку KEO DLP, выполнив следующую команду:

   # /opt/dozor/bin/shell
3. Выполнить команду:

   # indextool -r

7.2.6.3. Действия при повреждении индексов

При повреждении индексов OpenSearch выполнить поиск сообщений, событий и/или бесед в KEO DLP будет невозможно. В журналах сервиса **opensearch** будет сделана запись об ошибке вида:

```
2017-10-20 14:00:48.941107500 [WARN ][indices.cluster          ] [main]
[[msg-2017-43][3]] marking and sending shard failed due to [failed recovery]
2017-10-20 14:00:48.941108500 [msg-2017-44][[msg-2017-44][3]]
IndexShardRecoveryException[failed to recovery from gateway];
nested: EngineCreationFailureException[failed to create engine]; nested: EOFException;
```

Для устранения этой ошибки необходимо выполнить следующие действия:

1. Подключиться к узлу с сервисом **opensearch** по протоколу SSH.
2. Выполнить команду:

   # /opt/dozor/bin/shell
3. Остановить сервис **indexer-ng**, выполнив команду:

   # dsctl stop indexer-ng

   В случае повреждения индексов событий остановить сервис **incident-daemon**:

   # dsctl stop incident-daemon

4. Выполнить удаление индексов при помощи скрипта **curl**. Формат команды для запуска скрипта:

   **curl -s --cacert /opt/dozor/etc/ssl/ca.crt --key /opt/dozor/etc/ssl/bus.key **
   --cert /opt/dozor/etc/ssl/bus.pem -XDELETE https://`hostname -f`:9200/<имя индекса>

5. Запустить сервис **indexer-ng**, выполнив команду:

   # dsctl start indexer-ng

   Если на предыдущем шаге были удалены события, запустить сервис **incident-daemon**:

   #dsctl start incident-daemon

7.2.6.4. Проблемы совместимости сервиса opensearch и Kaspersky Security для виртуальных сред Легкий агент 4.0 для Linux

При функционировании ПО **Kaspersky Security для виртуальных сред Легкий агент 4.0 для Linux** в кластере KEO DLP попытки перестроения индексов OpenSearch завершатся неудачно. В журналах сервиса **opensearch** появится ошибка вида:

```
2018-10-09 16:53:16.491118500 java.nio.file.AccessDeniedException
```

Для решения этой проблемы следует выполнить действия:

1. На узлах с антивирусным ПО остановить службы **klnagent** и **lightagent**.

   Примечание

   *За более подробной информацией о службах **klnagent** и **lightagent** следует обратиться к соответствующей документации по продуктам **Лаборатории Касперского**.*

2. Подключиться к узлу с сервисом **opensearch** по протоколу SSH.

3. Запустить интерпретатор команд shell, выполнив команду:

   # /opt/dozor/bin/shell

4. Перезапустить сервис **opensearch**, выполнив команду:

   # dsctl restart opensearch

7.2.7. Очистка системы от неактуальных slave-узлов

Скрипт **unreg-slave** используется для очистки системы от неактуальных slave-узлов. В качестве параметра указывается **uuid** slave-узла, который необходимо удалить из системы.

Формат команды для запуска скрипта **unreg-slave**:

 # unreg-slave [uuid]

Внимание!

Перед запуском команды необходимо, остановить все сервисы KEO DLP на выбранном узле, выполнив команду:

 # dsctl stop

В противном случае статистика по этому узлу будет отображаться в разделах GUI ***Система > Мониторинг > Состояние системы****,* ***Система > Мониторинг > Показатели системы*** *и* ***Система > Мониторинг > Показатели ОС****.*

Если при удалении узла процессы системы были отключены, то при выполнении команды **dsctl boot** узел будет зарегистрирован сервером мониторинга. Чтобы этого избежать, следует подключиться к серверу мониторинга по протоколу SSH и выполнить в CLI следующую команду:

http_proxy="" $PREFIX/lib/monitor-server/zabbix_host_remove.py --host $HOSTNAME

После выполнения этой команды узел будет исключен из мониторинга.

7.2.8. Пересоздание SSL-сертификатов

Ключи и сертификаты SSL создаются при первичной установке KEO DLP и хранятся на master-узле в каталоге **/opt/dozor/etc/ssl/**. Если они становятся недействительными (например, в результате изменения hostname), их необходимо пересоздать, выполнив в CLI следующие действия:

1. Выполнить команду:

   # /opt/dozor/bin/shell

2. Остановить все сервисы KEO DLP, выполнив команду:

   # dsctl stop

3. Удалить с master-узла недействительные ключи и сертификаты, а затем сгенерировать ключ и сертификат SSL, выполнив команды:

   # rm /opt/dozor/etc/ssl/*

   # cert /opt/dozor/etc/ssl/bus.key /opt/dozor/etc/ssl/bus.pem

   где:

   - **bus.key** – файл закрытого ключа;
   - **bus.pem** – файл SSL-сертификата.

   Об успешном создании SSL-сертификата свидетельствует строка вида:

   ```
   Certificate was added to keystore
   ```

4. Запустить все остальные сервисы KEO DLP:

 # dsctl start

5. Заново зарегистрировать все slave-узлы в системе, выполнив на каждом из них команду следующего вида:

   # /opt/dozor/bin/reg-slave <master-узел> <имя узла> <роли>

   где **роли** – список ролей, перечисляемых через пробел

7.2.9. Действия при ошибках отправки сообщений на SMTP-сервер

Если на master-узле отсутствуют SSL-сертификаты SMTP-сервера, на который настроена отправка сообщений, то защищенное соединение с данным сервером master-узлу установить не удастся. Попытка отправки сообщения завершится со следующей ошибкой:

```
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
```

На master-узле необходимо включить проверку сертификатов при отправке сообщений, выполнив в CLI следующие действия:

1. Скопировать сертификат с SMTP-сервера на master-узел.

   Примечание

   *Параметры подключения к SMTP-серверу задаются в секции **Наборы параметров отправки сообщений** раздела GUI **Система > Конфигурация > Основные настройки > Работа системы**. Настройки SMTP-сервера доступны в случае выбора варианта **smtp** в качестве значения параметра **Метод доставки**. Описание наборов параметров отправки сообщений приведено в разделах A.1.1, A.2.5.*

2. Подключиться к master-узлу по протоколу SSH.

3. Импортировать сертификат в хранилище. Для этого выполнить команду:

   **# /usr/lib/jvm/jre-1.8.0/bin/keytool -import -file <cert_dir> -alias somecert **
   -keystore /usr/lib/jvm/jre-1.8.0/lib/security/cacerts

   где **<cert_dir>** – путь для сохранения сертификата на master-узле.

   В процессе выполнения данной команды будет запрошен пароль. Следует указать значение **changeit**.

4. Перезапустить сервис **monitor-ng**, выполнив команду:

   # dsctl restart monitor-ng

При временной недоступности SMTP-сервера попытка отправки сообщения завершится неудачно. Попытки отправки будут продолжаться до тех пор, пока не будет установлено подключение с SMTP-сервером.

В журналах сервиса **sender** появится сообщение вида:

```
ConnectException: Connection refused (Connection refused)
```

В случае появления данной ошибки следует обратиться к сетевому или системному администратору эксплуатирующей организации.

7.2.10. Изменение имени и IP-адреса узла кластера KEO DLP

В некоторых ситуациях потребуется изменить доменное имя и/или IP-адреса узла кластера KEO DLP, например:

- выполнение миграции KEO DLP с одного узла на другой;
- отсутствие подключения к другим узлам с KEO DLP, находящимся в одной сети, а также к другим узлам из внешней сети.

Для изменения имени узла кластера KEO DLP необходимо выполнить следующие действия:

1. Зарезервировать глобальную и локальную конфигурации KEO DLP на master-узле, выполнив команды:

   # /opt/dozor/bin/shell

   # get-config global > /var/tmp/global-conf

   **# for i in `cat /data/repos/dozor/config-base.git/cluster.json | jq -M '.nodes[].name' **
   **| tr -s '\"' ' ' `; do /opt/dozor/bin/config values **
   get -N $i > /var/tmp/local-config-$i.conf; done

2. Зарезервировать политику фильтрации KEO DLP на master-узле, выполнив команды:

   # su dozor

   $ xml-policy -f "" > /tmp/policy.xml

   $ exit

   # exit

   # mv /tmp/policy.xml /var/tmp/

3. Остановить процессы KEO DLP на slave-узлах с ролью **Фильтр почтового потока**, выполнив команды:

   # /opt/dozor/bin/shell

   # dsctl down

   # exit

4. Перейти на master-узел и выполнить следующие действия:

   a. Уточнить идентификаторы (ID) удаляемых slave-узлов с помощью команды:

      # config cluster print

Примечание

Самый первый идентификатор в списке относится к master-узлу.

Управление структурой кластера описано в разделе 6.10.1.

b. Удалить требуемые узлы, выполнив команду:

 # unreg-slave <идентификатор узла>

Пример:

 # /opt/dozor/bin/shell

 # unreg-slave c34a294b-cc07-4088-8c52-c69fc181345c

где **c34a294b-cc07-4088-8c52-c69fc181345c** — идентификатор (UUID) удаляемого узла.

c. Убедиться, что в файле конфигурации отсутствуют удаляемые узлы, выполнив команду:

 # config cluster print

5. Открыть конфигурационный файл **/etc/hostname** для редактирования и изменить содержимое файла, изменить значение параметра **HOSTNAME** в формате FQDN и перезагрузить узел.

6. Проверить имя узла в CLI с помощью команды:

 # hostname -f

Убедиться, что имя узла изменено.

7. Остановить процессы KEO DLP и проверить, что система остановлена, выполнив команды:

 # /opt/dozor/bin/shell

 # dsctl down

 # status

 # exit

8. Выполнить пересоздание ключей и сертификатов SSL (см. раздел 7.2.8).

9. Переключиться на пользователя **dozor**, выполнив команду:

 # su dozor

10. Вывести текущее состояние кластера на экран, выполнив команду:

$ config cluster print

Запомнить или записать идентификатор необходимого узла (UUID).

11. Изменить имя узла в конфигурации кластера, выполнив команду:

    $ config cluster update-node --id <id> --hostname `hostname -f`

    где **<id>** – идентификатор необходимого узла (UUID).

12. Выполнить команду:

    $ config cluster print

    Убедиться, что имя хоста (**hostname**) master-узла было изменено.

13. Перейти в git-репозиторий, выполнив команду:

    $ cd /data/repos/dozor/config-base.git

14. Добавить изменения в репозиторий. Для этого выполнить команду:

    $ git add .

15. Сохранить изменения, выполнив команду:

    $ git commit -m "change hostname"

16. Завершить сессию пользователя **dozor**, выполнив команду:

    $ exit

17. Применить конфигурацию, выполнив команду:

    # /opt/dozor/bin/accept-settings

18. Запустить систему управления процессами KEO DLP, выполнив команду:

    # /opt/dozor/bin/dsctl boot

19. Перейти в каталог БД архива сообщений, БД событий и инцидентов ИБ, БД хранения медиаинформации под управлением СУБД PostgreSQL – путь к каталогу можно узнать, выполнив команду:

    # ps ax | grep <port>

    где **<port>** – порт, на котором выбранная БД ожидает соединения. В результате выполнения команды на экран будет выведена информация следующего вида:

    ```
    # ps ax | grep 5435
    10440 ?        S      3:25 /usr/pgsql/15/bin/postgres -p 5435 -D /data/base/dozor-archive
    31078 pts/0    S+     0:00 grep 5435
    ```

    Путь **/data/base/dozor-archive** в данном примере является путем к каталогу БД.

20. Открыть файл **pg_hba.conf** для редактирования и найти строку ниже комментария **# IPv4 local connections**.

Если для подключения к БД используется **hostname**, заменить значение на новое, сохранить и закрыть файл. В случае IP-адреса не вносить изменения и закрыть файл.

21. Перезапустить БД, если в файл **pg_hba.conf** были внесены изменения. Для этого выполнить команду следующего вида:

    # systemctl restart <db-script-name>.service

    где **<db-script-name>** – имя скрипта автозапуска БД, который был создан при создании схемы этой БД, например **media**.

22. Обновить БД политики, если в кластере нет отдельной БД хранения медиаинформации. Для этого выполнить следующие действия:

    a. Подключиться к БД политики:

       psql -U dozor -h localhost -p 5434

    b. Проверить адрес узла, введя следующий запрос:

       select url from screenshot;

       где **url** – ссылка на снимок экрана.

    c. Если значение доменного имени из файла **/etc/hosts** не совпадает со значением, указанном в адресе узла KEO DLP, ввести следующий запрос:

       update screenshot set url=replace(url, <old hostname>, <new hostname>);

       где <**old hostname**> – старое имя узла кластера KEO DLP;

       <**new hostname**> – новое имя узла кластера KEO DLP.

       Примечание

       Агент перехватывает и сохраняет копии изображений с экрана пользователя (снимки экрана) для приложений, заданных в условиях политики. По умолчанию снимки экрана хранятся в БД политики, если в кластере нет отдельной БД хранения медиаинформации.

23. При наличии в кластере KEO DLP БД хранения медиаинформации, выполнить следующие действия на узле, на котором размещена эта БД:

    a. Вывести на экран список всех активных служб БД:

       systemctl list-units --type=service | grep "base"

       Пример вывода команды:

```
keodlp-postgresql.service                loaded active running KEO DLP Archive database server
keodlp_action-server-database.service    loaded active running KEO DLP action-server-database
keodlp_database.service                  loaded active running KEO DLP database
keodlp_media.service                     loaded active running KEO DLP Archive database server
keodlp_software-center-database.service  loaded active running KEO DLP software-center-database
```

Имя искомой службы выделено жирным шрифтом.

b. Вывести на экран информацию по сервису:

systemctl status keodlp_media.service

Запомнить значение порта.

c. Подключиться к БД хранения медиаинформации:

psql -U dozor -h <mediahost> -p <port> -d <mediadb>

где:

- <**dozor**> – имя пользователя БД;
- <**mediahost**> – FQDN или IP-адрес узла, на котором размещена БД;
- <**port**> – порт, на котором БД для хранения медиаинформации будет ожидать соединения;
- <**mediadb**> – имя БД.

d. Проверить адрес узла, введя следующий запрос:

select url from screenshot;

где **url** – ссылка на снимок экрана.

e. Если значение доменного имени из файла **/etc/hosts** не совпадает со значением, указанном в адресе узла KEO DLP, ввести следующий запрос:

update screenshot set url=replace(url, <old hostname>, <new hostname>);

где <**old hostname**> – старое имя узла кластера KEO DLP;

<**new hostname**> – новое имя узла кластера KEO DLP.

24. Проверить доступность файлового хранилища, последовательно выполнив в CLI следующие команды:

 # /opt/dozor/bin/shell

 # get-config global | grep enable-filestorage

На экране появится сообщение о том, что файловое хранилище включено:

```
/mailfilter/mailfilter.edn/enable-filestorage: #t
```

25. Выполнить проверку наличия медиаинформации в файловом хранилище:

 # ls -lah /data/storage/agent-media/<year>

 # ls -lah /data/storage/audio/<year>

 # ls -lah /data/storage/screen-video/<year>

где <**year**> – год, за который необходимо просмотреть информацию.

26. Проверить настройки ротации ФХ (раздел GUI **Система > Конфигурация** > **Расширенные настройки** > **Настройка обеспечивающих средств** > **Хранение**, секция **Тома файлового хранилища**) и хранения медиаинформации (раздел GUI **Система > Конфигурация** > **Расширенные настройки** > **Настройка обеспечивающих средств** > **Хранение**, секция **Хранение медиаинформации**).

27. Удалить файлы с расширением **.rescan**, выполнив команду:

    # find /data/storage/ -type f -name ".rescan*" -print -delete

28. Создать файл (в случае его отсутствия) **/root/.cassandra/cqlshrc** и записать в него следующее содержимое:

```
[connection]
factory = cqlshlib.ssl.ssl_transport_factory
[ssl]
certfile = /opt/dozor/etc/ssl/ca.crt
userkey = /opt/dozor/etc/ssl/bus.key
usercert = /opt/dozor/etc/ssl/bus.pem
```

29. Подключиться к базе данных индексов, выполнив команду:

    /opt/dozor/cassandra/bin/cqlsh -k filestorage <hostname> --ssl --cqlsh /root/.cassandra/cqlshrc

    где <**hostname**> – имя узла, на котором размещено файловое хранилище.

30. Для проверки имени узла ввести следующий запрос:

    select url from vids where vid='vg-000000/<vID>';

    где <**vID**> – идентификатор контейнера.

    Если отображаемое доменное имя неверно, необходимо последовательно выполнить в CLI следующие команды:

    # /opt/dozor/cassandra/bin/nodetool --ssl status

    # /opt/dozor/cassandra/bin/nodetool --ssl repair

31. Если не требуется менять **hostname** на slave-узлах, зарегистрировать их в кластере, выполнив следующие команды:

    # /opt/dozor/bin/shell

    # reg-slave <master-host> [name]

    # dsctl boot

    где <**master-host**> – FQDN master-узла (например, **dozormaster.isim.local**), а <**name**> – имя регистрируемого узла, которое будет отображаться в GUI KEO DLP

32. При необходимости изменения **hostname** на slave-узлах выполнить следующие действия:

a. На узлах с ролью **Фильтр почтового потока** проверить наличие файла **/opt/dozor/etc/mailfilter.edn**.

   Если он присутствует, открыть файл для редактирования, заменить имя узла на новое, сохранить и закрыть файл.

b. Проверить владельца файла, выполнив команду следующего вида:

   # ls -lah /opt/dozor/etc/mailfilter.edn

   Файлом должны владеть пользователь **dozor** и группа **dozor**. Если это не так, то сменить владельца файла **/opt/dozor/etc/mailfilter.edn**, выполнив команду следующего вида:

   # chown dozor:dozor /opt/dozor/etc/mailfilter.edn

c. Применить конфигурацию и перезапустить KEO DLP, выполнив команды:

   # /opt/dozor/bin/shell

   # accept-settings

   # dsctl restart

d. На остальных узлах проверить, что система остановлена:

   # /opt/dozor/bin/shell

   # dsctl down

   # dsctl status

   # exit

e. Выполнить команды:

   # nano /etc/hosts

   # hostnamectl set-hostname newhostname.domain.domain

   где **newhostname.domain.domain** – новое имя узла и домен.

f. Перезагрузить узлы, выполнив команду:

   # init 6

g. Проверить имена узлов с помощью команды:

   # hostname -f

   Убедиться, что оно изменено.

h. Остановить систему после перезагрузки узлов:

   # /opt/dozor/bin/shell

   # dsctl down

 # dsctl status

 # exit

i. Заменить сертификат, выполнив команды:

 # /opt/dozor/bin/shell

 # rm -rvf /opt/dozor/etc/ssl/*

 # cert /opt/dozor/etc/ssl/bus.key /opt/dozor/etc/ssl/bus.pem

j. Зарегистрировать узлы в кластере, выполнив следующие команды:

 # /opt/dozor/bin/shell

 # reg-slave <master-host> [name]

 # dsctl boot

где <**master-host**> – FQDN master-узла (например, **dozormaster.isim.local**), а <**name**> – имя регистрируемого узла, которое будет отображаться в GUI KEO DLP

33. На master-узле вывести текущее состояние кластера на экран:

 # su - dozor

$ /opt/dozor/bin/shell

$ config cluster print

Убедиться, что все узлы зарегистрированы.

Для изменения IP-адреса узла кластера KEO DLP необходимо выполнить следующие действия:

1. Остановить работу системы управления процессами KEO DLP, выполнив команду:

 # /opt/dozor/bin/dsctl down

2. Открыть файл конфигурации сетевого интерфейса **/etc/network/interfaces** для редактирования. Пример содержимого файла при статическом IP-адресе:

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 192.168.248.5
netmask 255.255.255.0
gateway 192.168.248.1
```

Примечание

*В случае подключения по протоколу DHCP редактировать файл **/etc/network/interfaces** не потребуется. Содержимое файла будет иметь вид:*

```
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
```

3. Изменить значение параметров **address** и **netmask**, указав корректные IP-адрес и маску подсети узла, нажать сочетание клавиш **Ctrl + X**, а затем нажать **Enter**.

4. Перезапустить службу сети, выполнив команду:

   # /etc/init.d/networking restart

5. Открыть файл **/etc/resolv.conf** для редактирования и указать адреса DNS серверов.

   Примечание

   *В случае подключения по протоколу DHCP редактировать файл **/etc/resolv.conf** не потребуется.*

6. Открыть конфигурационный файл **/etc/hosts** для редактирования и добавить в него строку, содержащую корректный IP-адрес и имя узла.

7. Проверить имя узла в CLI с помощью команд **hostname -s** и **hostname -f**.

8. Проверить доступность узла в сети с помощью команды **ping**.

9. Изменить IP-адреса всех соединений с БД, кроме **db-conn-1**. Для этого перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** и указать значения параметра **Сетевое имя сервера базы данных**.

10. Если значение параметра **База данных (PostgreSQL)** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**, секция **Хранение медиаинформации**) отличается от **db-conn-1**, отредактировать в каталогах БД архива и БД событий и инцидентов ИБ конфигурационные файлы **pg_hba.conf** и **postgresql.conf**. Указать в файлах IP-адреса, заданные на предыдущем шаге.

11. Применить конфигурацию, выполнив на master-узле команду:

    # /opt/dozor/bin/accept-settings rebuild

12. Выполнить пересоздание ключей и сертификатов SSL (см. раздел 7.2.8) и перерегистрировать slave-узлы в кластере KEO DLP помощью скрипта **reg-slave**.

13. Запустить систему управления процессами KEO DLP, выполнив команду:

    # /opt/dozor/bin/dsctl boot

14. Проверить работу сервисов, последовательно выполнив следующую команду через небольшие промежутки времени:

 # /opt/dozor/bin/dsctl status

В результате выполнения команды информация о всех запущенных сервисах и времени их работы будет выведена на экран.

Пример:

```
/lib/systemd/system/dozor_abook-daemon.service:..... up (pid 14881) 2560 seconds
/lib/systemd/system/dozor_action-server.service:..... up (pid 22523) 2714 seconds
/lib/systemd/system/dozor_action-server-database.service:... up (pid 22521) 2714 seconds
/lib/systemd/system/dozor_agent-control-ng.service:..... up (pid 26111) 2713 seconds
/lib/systemd/system/dozor_agent-media-server.service:..... up (pid 15105) 2588 seconds
/lib/systemd/system/dozor_archive-server.service:..... up (pid 25828) 2553 seconds
/lib/systemd/system/dozor_database.service:..... up (pid 22216) 2714 seconds
/lib/systemd/system/dozor_detective-database.service:..... activating (start)
/lib/systemd/system/dozor_detective-server.service:..... down, normally up
/lib/systemd/system/dozor_ds-bus-rc.service:..... up (pid 22230) 2714 seconds
/lib/systemd/system/dozor_filestorage-ng.service:..... up (pid 12695) 2588 seconds
/lib/systemd/system/dozor_grafana.service:..... up (pid 23321) 2714 seconds
/lib/systemd/system/dozor_incident-daemon.service:..... up (pid 22494) 2714 seconds
/lib/systemd/system/dozor_indexer-ng.service:..... up (pid 22375) 2714 seconds
/lib/systemd/system/dozor_license-server.service:..... up (pid 22221) 2714 seconds
/lib/systemd/system/dozor_monitor-agent.service:..... up (pid 22192) 2714 seconds
/lib/systemd/system/dozor_monitor-httpd.service:..... up (pid 24022) 2714 seconds
/lib/systemd/system/dozor_monitor-ng.service:..... up (pid 24082) 2714 seconds
/lib/systemd/system/dozor_monitor-server.service:..... up (pid 24136) 2713 seconds
/lib/systemd/system/dozor_opensearch.service:..... up (pid 23307) 2714 seconds
/lib/systemd/system/dozor_report-server.service:..... up (pid 27361) 2713 seconds
/lib/systemd/system/dozor_sender.service:..... up (pid 22236) 2714 seconds
/lib/systemd/system/dozor_skvt-cassandra.service:..... up (pid 12454) 2588 seconds
/lib/systemd/system/dozor_smap-difi.service:..... up (pid 25951) 2553 seconds
/lib/systemd/system/dozor_smap-redis.service:..... up (pid 22225) 2714 seconds
/lib/systemd/system/dozor_smap-request-handler.service:..... up (pid 22234) 2714 seconds
/lib/systemd/system/dozor_smap-tikaserver.service:..... up (pid 25341) 2553 seconds
/lib/systemd/system/dozor_software-center.service:..... up (pid 25558) 2713 seconds
/lib/systemd/system/dozor_software-center-database.service:. up (pid 23388) 2714 seconds
/lib/systemd/system/dozor_webserver.service:..... up (pid 25118) 2713 seconds
```

15. При изменении IP-адреса узла с ролью **Сервер агентов** выполнить действия по инструкции из раздела **Действия при смене сервера агентов** документа *Программный комплекс «KEO DLP» Модуль «Endpoint Agent». Руководство по установке, обновлению и удалению*.

7.2.11. Сбор отладочной информации при аварийном завершении работы сервисов

KEO DLP может предоставлять отладочную информацию о работе процессов **abook-daemon**, **abook-slave**, **action-server**, **activemq**, **agent-control-ng**, **agent-media-server**, **agent-server**, **archive-server**, **detective-server**, **difi**, **incident-daemon**, **indexer-ng**, **license-server**, **mailfilter**, **media-processor-action-server**, **report-server**, **sender**, **smap-tikaserver**, **uba-server**, **webserver** и **webserver-local**, которая необходима, например, инженерам поддержки KEO DLP в случае сбоев в работе системы. По умолчанию сбор отладки отключен. Для его включения используется флажок, показанный на **Рис.7.1**.

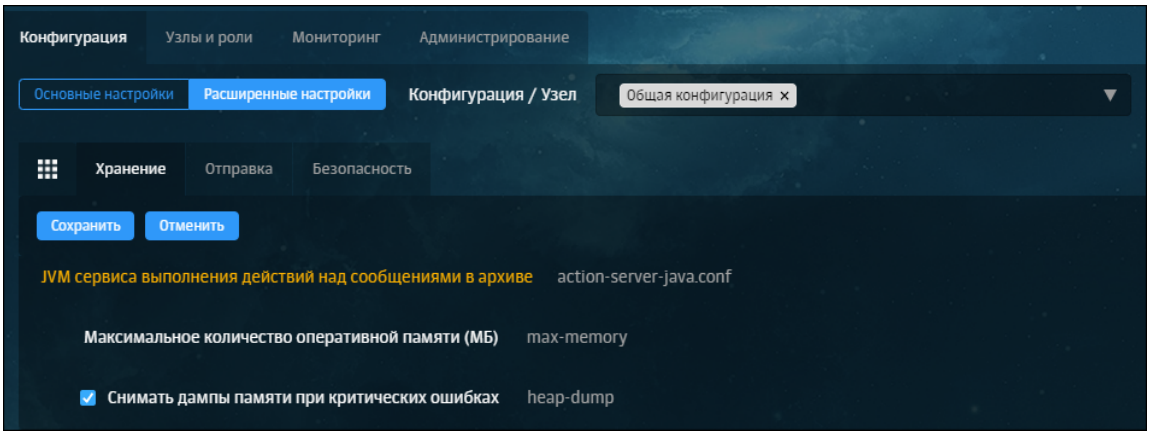


Рис. 7.1. Пример установки флажка сохранения дампа памяти для процесса action-server

После установки флажка следует нажать кнопки **Сохранить** и **Применить** для сохранения настроек и применения конфигурации.

Внимание!

*Для сохранения дампов памяти процессов **webserver** и **webserver-local** в журнальный файл необходимо после нажатия кнопок **Сохранить** и **Применить** выполнить следующие команды в CLI:*

 # /opt/dozor/bin/shell

 # dsctl restart webserver

 # dsctl restart webserver-local

Табл. 7.3. Расположение параметра в зависимости от имени процесса

Процесс	Раздел конфигурации	Секция конфигурации
abook-daemon	Досье	JVM сервиса доступа к Досье
abook-slave	Досье	Сервис репликации Досье на подчиненных узлах
action-server	Хранение	JVM сервиса выполнения действий над сообщениями в архиве
activemq	Вспомогательные сервисы	Отладка сервиса очередей
agent-control-ng	Агенты	JVM сервера управления агентами
agent-media-server	Хранение	Отладка хранения медиаинформации
agent-server	Агенты	Отладка сервера агентами
archive-server	Хранение	Отладка доступа к сообщениям в архиве
detective-server	Расследование	JVM сервиса Расследование
difi	Политика	Отладка сервиса цифровых отпечатков
incident-daemon	События и инциденты	JVM сервиса хранения и индексации событий и инцидентов
indexer-ng	Поиск	JVM сервиса индексации сообщений в архиве
license-server	Вспомогательные сервисы	Отладка сервиса лицензирования
mailfilter	Обработка сообщений	JVM сервиса фильтрации сообщений

Процесс	Раздел конфигурации	Секция конфигурации
media-processor-action-server	Вспомогательные сервисы	JVM сервера выполнения действий по обработке медиаданных
report-server	Отчеты	Отладка сервиса построения отчетов
sender	Отправка	JVM сервиса отправки сообщений
smap-tikaserver	Обработка сообщений	Отладка сервиса извлечения текстовых данных
uba-server	Анализ поведения (UBA)	JVM сервиса анализа поведения
webserver	Интерфейс	JVM веб-сервера
webserver-local	Интерфейс	JVM локального веб-сервера

7.2.12. Действия при ошибках обработки сообщений

При появлении в журналах сервиса **archive-server** ошибки вида **ОШИБКА: неверная последовательность байт для кодировки** необходимо перейти в каталог БД архива, открыть конфигурационный файл **postgresql.conf** и найти строку с параметром **lc_messages**. Строка должна выглядеть следующим образом:

```
lc_messages = 'C'
```

Если параметр имеет любое другое значение, следует заменить его на **'C'** (заглавная латинская буква C, заключённая в прямые апострофы). Сохранить и закрыть файл.

7.2.13. Получение технической поддержки

Для получения консультации по техническим вопросам необходимо связаться с поставщиком ПО.

Приложение А. Параметры конфигурации KEO DLP

В этом приложении приведено описание параметров конфигурации KEO DLP. Параметры конфигурации в разделе **Система > Конфигурация** определяют работу KEO DLP. В случае распределенной установки настройка параметров конфигурации для всех узлов выполняется из единой точки на master-узле. Подробное описание интерфейса при работе с разделом **Система > Конфигурация** приведено в разделе 5.2. В данном приложении приводится описание каждого параметра конфигурации и его назначения.

Внимание!

Параметры конфигурации KEO DLP Traffic Analyzer присутствуют в интерфейсе KEO DLP, если в кластере установлен пакет модуля KEO DLP Traffic Analyzer.

Параметры конфигурации сгруппированы в конфигурационные файлы, а конфигурационные файлы – в секции.

При установке KEO DLP некоторым параметрам конфигурации присваиваются значения по умолчанию. Изменять эти значения без необходимости не рекомендуется.

Реализована функция проверки валидности указанных значений параметров. Если установить неподходящее значение параметра, например, ввести строку символов в качестве значения числового параметра, то система не позволит сохранить такие изменения. В этом случае кнопки **Сохранить** и **Применить** будут заблокированы, а рядом с ними будут показаны ссылки на параметры с некорректными значениями.

Примечание

Числовые параметры допускают ввод только цифр от 0 до 9 и символа «.» (точка) для задания десятичных дробей. Наличие каких-либо других символов в значении числового параметра не допускается.

Также система не позволит сохранить конфигурацию, если не установлены обязательные параметры. В этом случае кнопки **Сохранить** и **Применить** будут заблокированы, а рядом также приведен список параметров с некорректными значениями.

Если какой-то параметр имеет смысл только при включенном/отключенном другом параметре, то такой параметр называется зависимым. В этом случае происходит автоматическое включение/отключение зависимого параметра при включении/отключении связанного параметра.

А.1. Основные настройки

А.1.1. Работа системы

Балансировка трафика:

Чтобы добавить конфигурацию балансировки трафика, необходимо нажать на кнопку **Добавить**. Чтобы дублировать конфигурацию, следует щелкнуть мышью на значок

и ввести ее характеристики. Для удаления конфигурации следует нажать на значок рядом с идентификатором конфигурации.

Конфигурация балансировки трафика определяется следующими параметрами:

- **Название конфигурации балансировки** – название набора конфигурации балансировки трафика.
- **Порт для внешних соединений** – порт, на котором сервис балансировки трафика ожидает соединения. Значение по умолчанию 1010.
- **Время ожидания запроса от клиента (с)** – время ожидания запроса от клиента, выраженное в секундах. Значение по умолчанию 10.

  Примечание

  В качестве клиента выступают внешние системы, например SMTP/HTTP/ICAP-серверы.

- **Время ожидания ответа от сервера (с)** – время ожидания запроса от серверов фильтрации, которые задаются в параметре **Узлы для балансировки**. Выражено в секундах. Значение по умолчанию по умолчанию 10.
- **Максимальное количество соединений** – максимальное количество соединений, которое принимает балансировщик от клиента (по умолчанию 1000).
- **Метод балансировки** – алгоритм балансировки трафика. Принимает значения: **roundrobin**, **leastconn** и **source**.

  При значении **roundrobin** нагрузка будет распределена равномерно в соответствии с весом каждого сервера фильтрации KEO DLP, если такой указан ниже. При значении **leastconn** запросы будут передаваться серверу с наименьшим количеством подключений. При значении **source** сервер для соединения назначается на основании хэша IP-адреса отправителя запроса и весов серверов.

  Значение по умолчанию **roundrobin**.

- **Узлы для балансировки** – узлы, по которым распределяется трафик. Принимает значения:
  - **Автоматическое определение доступных mailfilter (HTTP)** – автоматически определяются узлы с сервисом **mailfilter**, ожидающие трафик по HTTP-интерфейсу.
  - **Автоматическое определение доступных mailfilter (ICAP)** – автоматически определяются серверы фильтрации, ожидающие ICAP-трафик.
  - **Автоматическое определение доступных smtp-gw** – автоматически определяются узлы с сервисом **smtp-gw**.
  - **Указать вручную** – узлы для балансировки задаются вручную. При выборе **Указать вручную** следует задать следующие параметры:
    - **Тип балансировки** – протокол, по которому распределяется нагрузка между узлами.

- **Узлы** – добавить одну или несколько записей резервных узлов, предназначенных для балансировки. Запросы от внешних систем будут перенаправляться на эти узлы при недоступности серверов фильтрации KEO DLP. Для добавления новой записи необходимо нажать на кнопку **Добавить**. Чтобы дублировать запись, следует щелкнуть мышью на значок  и ввести характеристики. Для удаления записи следует нажать на значок  рядом с идентификатором записи.

  Запись резервного узла имеет следующие параметры:

  - **Сетевой адрес** – FQDN или IP-адрес резервного узла.
  - **Номер порта** – номер порта, на котором резервный узел будет ожидать соединения.
  - **Вес балансировки** – коэффициент, помогающий балансировщику распределять нагрузку между серверами фильтрации. Узел с большим весом будет получать большее число запросов.

    Пример: сервер с весовым коэффициентом 2 будет получать в 2 раза больше запросов, чем сервер с весом, равным 1.

    Пример 2: имеется 3 сервера фильтрации A, B и C. Сервера A и B имеют вес, равный 1, а третий сервер имеет весовой коэффициент 2. При недоступности сервера C нагрузка распределится равномерно между серверами A и B. При восстановлении своей работоспособности сервер C будет получать в 2 раза больше запросов, чем сервера A и B.

Общие настройки системы:

- **URL для формирования ссылок на систему** – URL для формирования ссылок, использующихся в работе модулей проведения внутренних расследований инцидентов ИБ (**Расследование**) и распознавания речи. По умолчанию указано **https://dozor**.

  Значение задается в соответствии со следующими принципами:

  1. Для активации ссылок в стенограмме с результатами распознавания речи – IP-адрес узла KEO DLP, которому назначены роли **Сервер управления** либо **Локальный веб-сервер**.
  2. Для активации ссылок в схемах и отчетах по делу, которые относятся к модулю **Расследование** – IP-адрес сервера управления KEO DLP.

- **Уровень журналирования** – степень детализации журналирования. В качестве значения выберите один из следующих параметров в раскрывающемся списке:
  - Журналирование отключено;
  - Обычный;
  - Повышенный;
  - Отладочный.
- **Использование syslog** – включает ведение журналов с помощью протокола syslog, а также определяет способ использования данного протокола. Значение по умолчанию

отключено (использование **syslog** отключено). Выберите значения **facility** в раскрывающемся списке. Параметр **facility** определяет тип программы, которая выполняет запись сообщений в журнальный файл ОС. При выборе значения **facility** открываются следующие два поля под общим заголовком **facility**:

- **Служба syslog** – предоставляет выбор значения в следующем списке:
  - LOG_AUTHPRIV – сообщения о безопасности/авторизации;
  - LOG_CRON – планировщик;
  - LOG_DAEMON – другие системные демоны, кроме планировщика;
  - LOG_LOCAL0 – значение зарезервировано;
  - LOG_LOCAL1 – значение зарезервировано;
  - LOG_LOCAL2 – значение зарезервировано;
  - LOG_LOCAL3 – значение зарезервировано;
  - LOG_LOCAL4 – значение зарезервировано;
  - LOG_LOCAL5 – значение зарезервировано;
  - LOG_LOCAL6 – значение зарезервировано;
  - LOG_LOCAL7 – значение зарезервировано;
  - LOG_MAIL – почтовая подсистема;
  - LOG_USER – общие сообщения на уровне пользователя.
- **Префикс программы для вывода syslog** – задание префиксов для различных программных средств дает возможность различать записи этих программных средств в общем файле журналирования. Рекомендуется задавать префикс схожий с именем программного средства.

- **Адрес отправителя в системных сообщениях** – адрес отправителя в системных сообщениях. Например, dozor@dozor.
  - **Имя владельца почтового ящика** – имя персоны, которой принадлежит почтовый ящик.
  - **Имя почтового ящика** – уникальная комбинация букв, цифр и служебных символов, расположенная перед доменом. Значение по умолчанию: **dozor**.
  - **Имя почтового домена** – часть почтового ящика после символа **@**. Значение по умолчанию: **dozor**.
- **Адрес получателя в системных сообщениях** – адреса получателей в системных сообщениях. Можно задать список адресов. Для добавления адреса нажмите кнопку **Добавить** рядом с параметром **Адрес получателя в системных сообщениях**. Для удаления адреса нажмите кнопку  рядом с параметром **Адрес получателя в си-**

стемных сообщениях. Для дублирования существующего адреса нажмите кнопку рядом с параметром **Адрес получателя в системных сообщениях**.

Для каждого адреса задаются следующие параметры:

- **Имя владельца почтового ящика** – имя персоны, которой принадлежит почтовый ящик.
- **Имя почтового ящика** – уникальная комбинация букв, цифр и служебных символов, расположенная перед доменом. Значение по умолчанию: **dozor**.
- **Имя почтового домена** – часть почтового ящика после символа **@**. Значение по умолчанию: **dozor.local**.

Правила аутентификации:

- **Минимальная длина пароля** – минимальная длина пароля. Значение по умолчанию: 6.
- **Минимальная допустимая сложность пароля (2-10)** – минимальная допустимая сложность пароля. Сложность пароля выражается числом от 2 до 10. Значение по умолчанию: 6.
- **Время блокировки учётной записи после исчерпания попыток входа, мин.** – время в минутах, на которое блокируется учётная запись после неудачного/неверного ввода данных для авторизации. Значение по умолчанию: 15. Допустимое значение – от 15 до 1440.
- **Период времени, в течение которого подсчитываются неудачные попытки аутентификации, мин.** – период времени в минутах, в течение которого подсчитываются неудачные попытки входа пользователя. Значение по умолчанию: 60. Допустимое значение – от 60 до 1440.
- **Доменная аутентификация через Kerberos** – включает или выключает аутентификацию в KEO DLP под доменной учетной записью без ввода логина и пароля. Используется механизм аутентификации Kerberos. Принимает значения **true** и **false**.

  При значении **true** станет доступна кнопка **Войти через домен**. Таким образом, вход в KEO DLP можно выполнить локальной и доменной учетными записями. Чтобы войти в KEO DLP под учетной записью AD, следует нажать кнопку **Войти через домен**. В этом случае вводить логин и пароль не требуется, т.к. для аутентификации в KEO DLP используются данные учетной записи, уже выполнившей вход в ОС.

  Если системный администратор организации заблокировал учетную запись пользователя в AD, активный сеанс работы такого пользователя в системе будет завершен. После этого откроется окно авторизации KEO DLP.

  Если доменная учетная запись AD не активна, удалена или заблокирована, доступ в KEO DLP под доменной учетной записью запрещен. В этом случае будет сообщение об ошибке вида **Доступ запрещен для доменного пользователя**.

  При значении **false** аутентификация в KEO DLP выполняется только под локальной учетной записью.

  Значение по умолчанию: **false**.

- **Идентификатор службы Kerberos (SPN)** – имя участника службы для Kerberos-соединений. Задается в формате **HTTP/<dozor.fqdn>@<DOMAIN>**, где **<dozor.fqdn>** – FQDN master-узла KEO DLP, **<DOMAIN>** – имя домена. Используется совместно с параметром **Доменная аутентификация через Kerberos**.

Веб-сервер:

- **Не показывать ошибки в интерфейсе** – включает или выключает отображение ошибок в интерфейсе KEO DLP. По умолчанию флажок установлен.

Загрузка сообщений из корпоративных мессенджеров:

- **Настройки прокси-сервера** – принимает значения **Настройка прокси-сервера** и **Прокси-сервер не используется**. Значение по умолчанию: **Прокси-сервер не используется**.

  Если для доступа к адресу **https://webexapis.com/** требуется соединение через прокси-сервер, следует выбрать значение **Настройка прокси-сервера**. При выборе этого значения доступны параметры:

  - **Адрес прокси-сервера** – адрес (IP или FQDN) прокси-сервера, через который предполагается соединяться с узлом **webexapis.com**.
  - **Порт прокси-сервера** – номер порта, на котором этот прокси-сервер ожидает соединения.
  - **Логин для Basic-аутентификации на прокси-сервере** – имя учётной записи пользователя для авторизации на прокси-сервере.
  - **Пароль для Basic-аутентификации на прокси-сервере** – пароль этой учётной записи.

- **Файл с токеном доступа** – путь к файлу **token.json**, необходимому для идентификации опрашивающего сервера KEO DLP на стороне серверов Webex. Значение по умолчанию: **/opt/dozor/share/im-crawler/token.json**.

  Внимание!

  *Файл **token.json** необходим для идентификации опрашивающего сервера KEO DLP на стороне серверов Webex. При отсутствии обращений серверов KEO DLP к серверам Webex с помощью этого файла в течение более 90 суток, файл становится недействительным. Для создания нового такого файла необходимо обратиться к инструкции, описанной в документе Руководство по установке и настройке.*

- **Client ID** – значение поля **CLIENT_ID**. По умолчанию не заполнено.
- **Client Secret** – значение поля **CLIENT_SECRET**. По умолчанию не заполнено.

Примечание

*Для получения **CLIENT_ID**, **CLIENT_SECRET** и файла **token.json** необходимо выполнить настройку перехвата сообщений из корпоративного мессенджера Cisco Webex Teams согласно документу Руководство по установке и настройке.*

Сервис фильтрации сообщений:

- **Включить ICAP-интерфейс** – включение ICAP-интерфейса. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Распознавать QR-коды** – при установленном флажке включает распознавание QR-кодов изображений. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Определять тип сообщений Exchange** – включает распознавание сообщений **Exchange**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**. При значении **false** сообщения **Exchange** определяются как сообщения типа **Email**.
- **Значения RCPT TO для журнальных сообщений Exchange 2003** – данный параметр определяет значения заголовков **rcpt to** для журнальных сообщений, которые будут обрабатываться парсером **exchange 2003** (только для Exchange 2003). В качестве значения параметра укажите соответствующий почтовый адрес или адреса, разделенные пробелом.

  При получении сообщения на один из указанных адресов, сервис **mailfilter** выполняет над сообщением следующие действия:

  1. Устанавливает значение типа сообщения равным **Exchange**.
  2. Удаляет из заголовков сообщения адреса отправителя и получателя, указанные в значении параметра **Значения RCPT TO для журнальных сообщений Exchange 2003**. Атрибуты **Источник** и **Назначение**, которые не содержат адресов SMTP-сервера, остаются.
  3. Устанавливает для сообщения пометку **Преобразовано из журнала Exchange**.

Наборы параметров отправки сообщений:

- **Параметры отправки** – определяют настройки наборов параметров отправки сообщений. Для соединения с сервисом отправки сообщений по умолчанию используется первый набор в списке.

  Можно добавить несколько значений, нажав кнопку **Добавить**. Для удаления набора параметров следует нажать кнопку  . Для дублирования набора параметров следует нажать кнопку  .

  - **ID** – идентификатор набора параметров отправки.
  - **Название набора параметров** – имя набора параметров отправки. Значение по умолчанию: **default**.

- **Метод доставки** – метод доставки: **Sendmail**, **SMTP** или **Скрипт**. В случае **Sendmail** сообщение передается на локальный MTA, а в случае **SMTP** KEO DLP отправляет сообщение на указанный SMTP-сервер. Значение по умолчанию: SMTP. В случае **Скрипт** сообщение обрабатывается с помощью команд, описанных в файле скрипта.

  Если выбран метод **Sendmail**, то доступны следующие параметры:

  - **Файл конфигурации sendmail** – конфигурационный файл Sendmail. Необязательный параметр.
  - **Путь к программе sendmail** – путь к программе Sendmail.
  - **Использовать sendmail с опцией -bs** – использование Sendmail с ключом **–bs**. Можно использовать Sendmail либо с ключом **–bs**, либо без него.

  Если выбран метод **smtp**, можно задать несколько SMTP-соединений, нажав кнопку **Добавить**. Для удаления значения следует нажать кнопку  . Для дублирования SMTP-соединения следует нажать кнопку  . Доступны следующие параметры в группе **Соединения SMTP**:

  - **Протокол SMTP-сервера** – протокол SMTP-сервера. Параметр определяет протокол работы SMTP-сервера. Возможные варианты выбираются в раскрывающемся списке: **SMTP**, **SMTPS**, **STARTTLS**. Значение по умолчанию: **SMTP**.
  - **SMTP-сервер** – значение SMTP-сервера. Значение по умолчанию: **localhost**.
  - **SMTP-порт** – номер SMTP-порта. Значение по умолчанию:1025.
  - **Использовать режим BINARY MIME** – включает передачу 8-битных данных на SMTP-сервер. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.

  Если выбран метод **Скрипт**, то доступен параметр **Скрипт** – определяет расположение скрипта.

Прием сообщений:

- **Порт** – номер порта, на котором будет принимать почту SMTP-прокси. Значение по умолчанию: 1025.
- **Вывод отладочной информации** – вывод отладочной информации. По умолчанию выключено.

A.1.2. Доступ к данным

Схемы соединений с БД:

- **Идентификатор соединения с базой данных** – идентификатор соединения с базой данных. Проставляется автоматически.
- **Подкластер** – подкластер, ресурсы которого использует выбранная БД. Выбирается из раскрывающегося списка. По умолчанию ничего не выбрано.

Примечание

Подкластеры могут настраиваться при наличии работающего модуля централизованного управления системой.

- **Имя схемы соединения с базой данных** – имя схемы соединения с базой данных. Параметр обязателен для заполнения.
- **Признак активности соединения** – необходимо включить параметр, чтобы активировать соединение. По умолчанию выключен.
- **Настройки использования соединения с БД** – настройки использования данного соединения:
  - **Использовать БД для поиска по архиву** – включает использование хранилища для поиска по архиву. Необходимо включить параметр, чтобы использовать хранилище для поиска по архиву. По умолчанию выключено.
  - **Использовать БД для архивирования сообщений** – включает использование хранилища для архивирования сообщений. Необходимо включить параметр, чтобы использовать хранилище для архивирования сообщений. По умолчанию выключено.
  - **Использовать БД для архивирования по умолчанию** – включает использование хранилища для архивирования сообщений, если в профиле архивирования не указано имя схемы соединения с БД. Может быть включено в нескольких схемах соединения (в этом случае БД для архивирования сообщения определяется случайным образом). По умолчанию включено.
- **Ротация данных** – включает выполнение действий по удалению старых сообщений, в т. ч. помеченных как важные, из БД архива, в которой не используется секционирование. Принимает значения: **Выключена** и **Включена**. По умолчанию параметр выключен. При значении **Включена** доступны следующие параметры:
  - **Ограничение на количество сообщений** – определяет ограничение на количество сообщений. При превышении этого количества старые записи удаляются. Принимает значения **Включено** и **Выключено**. При значении **Выключено** ограничение отсутствует. При значении **Включено** можно задать ограничение.
  - **Ограничение на суммарный объем сообщений (МБ)** – при превышении этого размера наиболее старые сообщения будут удалены. Принимает значения **Включено** и **Выключено**. При значении **Выключено** ограничение отсутствует. При значении **Включено** можно задать ограничение.
  - **Не удалять сообщения с пометкой "Важное"** – при включенном параметре сообщения в архиве, помеченные как важные, не удаляются при очистке БД архива. При выключенном параметре в процессе удаления сообщений из архива (при превышении их количества или объема) сообщения с пометкой **Важное сообщение** также удаляются. По умолчанию параметр выключен.
  - **Интервал проверки ограничений** – интервал проверки ограничений на количество и суммарный объем сообщений. Значение по умолчанию: **0 дн. 12 ч.**

- **Тип базы данных** – тип используемой СУБД: Oracle или PostgreSQL, выбирается из списка. В зависимости от выбора типа СУБД отображаются разные настройки соединения с базой данных. Ниже описаны отдельно параметры для настройки базы данных PostgreSQL и Oracle.
  - **Настройки соединения с базой** – настройки соединения с базой данных (для PostgreSQL):
    - **Сетевое имя сервера базы данных** – имя сервера с установленной БД PostgreSQL, обязательно для заполнения. Параметр обязателен для заполнения.
    - **Сетевой порт сервера базы данных** – сетевой порт сервера БД PostgreSQL. Параметр обязателен для заполнения.
    - **Имя базы данных** – имя базы данных PostgreSQL. Параметр обязателен для заполнения.
    - **Пользователь базы данных** – указывается имя пользователя базы данных, заданное при установке. Параметр обязателен для заполнения.
    - **Пароль пользователя базы данных** – пароль пользователя для доступа к базе данных. В данном поле указывается пароль пользователя, заданный при установке.
  - **Настройки соединения с базой** – настройки соединения с базой данных (для Oracle):
    - **TNS имя** – имя службы TNS. Параметр обязателен для заполнения.
    - **Пользователь базы данных** – имя учетной записи пользователя базы данных. Параметр обязателен для заполнения.
    - **Пароль пользователя базы данных** – пароль пользователя базы данных. Параметр обязателен для заполнения.
  - **Настройки пользователя для мониторинга базы данных** – настройки пользователя для мониторинга базы данных (для Oracle).
    - **Пользователь базы данных** – монитор: имя учетной записи пользователя базы данных. Параметр обязателен для заполнения.
    - **Пароль пользователя базы данных** – монитор: пароль пользователя базы данных. Параметр обязателен для заполнения.
  - **Обслуживание базы данных** – признак обслуживания базы данных (для Oracle). Необходимо выбрать из двух вариантов: **Настройки обслуживания базы данных** – БД обслуживается, **База данных не обслуживается** – БД не обслуживается. В случае выбора варианта **Настройки обслуживания базы данных** отображаются следующие параметры для заполнения:
    - **Использование секционирования** – включает использование секционированной БД. Необходимо выбрать из двух вариантов: **используется** или **не используется**. Значение по умолчанию: **не используется**. в случае выбора варианта **используется** для заполнения отображаются следующие параметры (входящие с группу **использование секционирования**):

- **Период секционирования** – период секционирования, то есть интервал времени, данные за который хранятся в одной секции. Значение состоит из длительности и размерности интервала, где размерность может быть одним из следующего: **D** – день, **W** – неделя (строго равна 7 дням), **M** – месяц. Например: **1M** – один месяц; **2W** – две недели; **10D** – десять дней. Значение по умолчанию: **1M**.

- **Количество изначально создаваемых секций** – количество изначально создаваемых в БД архива секций. Значение по умолчанию: 2.

- **Номер первой секции. Нумерация начинается с этого числа** – номер первой созданной секции. Значение по умолчанию: 1000.

- **Конец диапазона первой секции** – конец диапазона первой секции (созданной при создании БД).

- **Использование внешнего обработчика операций с секциями** – использование внешнего обработчика операций с секциями. Необходимо включить параметр, чтобы обеспечить использование обработчика. По умолчанию выключен.

- **Скрипт обработчика, вызывается при выполнении операций с секциями** – скрипт обработчика, который вызывается при выполнении операций с секциями. Значение по умолчанию: **/opt/oracle/bin/parthook.sh**.

- **Добавлять секции автоматически** – позволяет добавлять секции автоматически. Необходимо включить параметр, чтобы секции автоматически добавлялись. По умолчанию включен.

- **Добавление секций за указанное время до окончания последней** – добавление секций за указанное время до окончания последней. Значение состоит из длительности и размерности интервала, где размерность может быть одним из следующего: **D** – день, **W** – неделя (строго равна 7 дням), **M** – месяц . Например: **1M** – один месяц; **2W** – две недели; **10D** – десять дней. Значение по умолчанию: **1D**.

- **Автоматическое отключение секций** – предоставляет возможность автоматически отключать секции. Принимает значения **используется** и **не используется**. Значение по умолчанию: **не используется**. При выборе значения **используется** отображаются параметры автоматического отключения:

  - **Максимальное количество online-секций** – максимальное количество online-секций. Значение по умолчанию: 999.

  - **Час автоматического отключения секций** – час автоматического отключения секций. Значение по умолчанию: 3.

  - **detach-action** – действие при отключении секций. Принимает следующие значения: **Ручная обработка отключенных секций**, **Автоудаление отключенных секций**, **Автоархивирование отключенных секций**.

  - **Полный путь к файлу скрипта на сервере Oracle, который запускается после автоматического отключения секции (detach-part-script)** – распо-

ложение файла скрипта на сервере Oracle. Скрипт запускается после автоматического отключения секции. По умолчанию: **/opt/oracle/parthook.sh**.

- **Использование TTS** – включает использование переносимых табличных пространств (Transportable Tablespaces) в СУБД Oracle. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Каталог для файлов TTS** – каталог, в который выгружаются файлы Transportable Tablespaces. Значение по умолчанию: **/tmp**.

- **Инсталляция в конфигурации RAC** – включает установку Oracle Real Application Cluster. Используется в случае установки СУБД Oracle на нескольких узлах.
- **Параметры хранения данных в базе** – параметры хранения данных в базе:
  - **Параметры создания новых файлов данных** – параметры создания новых файлов данных.
    - **Каталог для файлов данных табличного пространства MAIN** – каталог для файлов данных табличного пространства MAIN. Параметр обязателен для заполнения. Возможно указание нескольких каталогов через запятую или запятую и пробел.
    - **Каталог для файлов данных табличного пространства MESSAGES** – каталог для файлов данных табличного пространства MESSAGES. Параметр обязателен для заполнения. Возможно указание нескольких каталогов через запятую или запятую и пробел.
    - **Каталог для файлов данных табличного пространства INDEXES** – каталог для файлов данных табличного пространства INDEXES. Параметр обязателен для заполнения. Возможно указание нескольких каталогов через запятую или запятую и пробел.
    - **Каталог для файлов данных табличного пространства DICT** – каталог для файлов данных табличного пространства DICT. Параметр обязателен для заполнения. Возможно указание нескольких каталогов через запятую или запятую и пробел.
    - **Начальные размеры для файлов данных табличного пространства MAIN** – начальные размеры для файлов данных табличного пространства MAIN. Параметр обязателен для заполнения.
    - **Начальные размеры для файлов данных табличного пространства MESSAGES** – начальные размеры для файлов данных табличного пространства MESSAGES. Параметр обязателен для заполнения.
    - **Начальные размеры для файлов данных табличного пространства INDEXES** – начальные размеры для файлов данных табличного пространства INDEXES. Параметр обязателен для заполнения.
    - **Начальные размеры для файлов данных табличного пространства DICT** – начальные размеры для файлов данных табличного пространства DICT. Параметр обязателен для заполнения.

- **Размер по умолчанию для экстентов табличного пространства MAIN** – размер по умолчанию для экстентов табличного пространства MAIN. Параметр обязателен для заполнения.

- **Размер по умолчанию для экстентов табличного пространства MESSAGES** – размер по умолчанию для экстентов табличного пространства MESSAGES. Параметр обязателен для заполнения.

- **Размер по умолчанию для экстентов табличного пространства INDEXES** – размер по умолчанию для экстентов табличного пространства INDEXES. Параметр обязателен для заполнения.

- **Размер по умолчанию для экстентов табличного пространства DICT** – размер по умолчанию для экстентов табличного пространства DICT. Параметр обязателен для заполнения.

- **Настройки авторасширения файлов данных** – настройки авторасширения файлов данных. Необходимо выбрать из двух вариантов: **yes** - авторасширение включено, **авторасширение отключено** – авторасширение отключено. Значение по умолчанию: **авторасширение отключено**. В случае выбора варианта **yes** для заполнения отображаются следующие параметры (входящие с группу **Настройки авторасширения файлов данных**):

  - **Размер очередного экстента** – размер очередного экстента. Параметр обязателен для заполнения.

  - **Ограничение на максимальный размер файлов данных** – ограничение на максимальный размер файлов данных. Необходимо выбрать из двух вариантов: **Ограничение отключено** – нет ограничения на максимальный размер файла, **Максимальный размер файла данных** – есть ограничение. Значение по умолчанию: **Ограничение отключено**. В случае выбора варианта **Максимальный размер файла данных** для заполнения отображается параметр **Максимальный размер файла данных** (входит в группу **Ограничение на максимальный размер файлов данных**).

- **Настройки LOB** – настройки хранения больших объектов в СУБД Oracle:

  - **Размеры LOB chunks** – размеры фрагментов больших объектов в СУБД Oracle. Параметр обязателен для заполнения.

  - **Размеры LOB chunks для текстовых частей** – размеры больших объектов в СУБД Oracle для текстовых частей. Параметр обязателен для заполнения.

- **Каталог для внешних скриптов на сервере базы данных** – путь к внешним скриптам на сервере базы данных. Параметр обязателен для заполнения.

- **Параметры автоматического управления файлами данных** – параметры автоматического управления файлами данных:

  - **Добавление файлов данных при уменьшении доступного в ТП MAIN места ниже указанного предела (monitor-reserved-main)** – добавление файлов данных при уменьшении доступного в ТП MAIN места ниже указанного предела. Параметр обязателен для заполнения.

- **Добавление файлов данных при уменьшении доступного в ТП MESSAGES места ниже указанного предела (monitor-reserved-mess)** – добавление файлов данных при уменьшении доступного в ТП MESSAGES места ниже указанного предела. Параметр обязателен для заполнения.

- **Добавление файлов данных при уменьшении доступного в ТП INDEXES места ниже указанного предела (monitor-reserved-indx)** – добавление файлов данных при уменьшении доступного в ТП INDEXES места ниже указанного предела. Параметр обязателен для заполнения.

- **Добавление файлов данных при уменьшении доступного в ТП DICT места ниже указанного предела (monitor-reserved-dict)** – добавление файлов данных при уменьшении доступного в ТП DICT места ниже указанного предела. Параметр обязателен для заполнения.

- **Добавление файлов данных при уменьшении доступного в ТП MAIN места ниже указанного предела (в процентах) (monitor-pct-free-main)** – добавление файлов данных при уменьшении доступного в ТП MAIN места ниже указанного предела (в процентах). Параметр обязателен для заполнения.

- **Добавление файлов данных при уменьшении доступного в ТП MESSAGES места ниже указанного предела (в процентах) (monitor-pct-free-mess)** – добавление файлов данных при уменьшении доступного в ТП MESSAGES места ниже указанного предела (в процентах). Параметр обязателен для заполнения.

- **Добавление файлов данных при уменьшении доступного в ТП INDEXES места ниже указанного предела (в процентах) (monitor-pct-free-indx)** – добавление файлов данных при уменьшении доступного в ТП INDEXES места ниже указанного предела (в процентах). Параметр обязателен для заполнения.

- **Добавление файлов данных при уменьшении доступного в ТП DICT места ниже указанного предела (в процентах) (monitor-pct-free-dict)** – добавление файлов данных при уменьшении доступного в ТП DICT места ниже указанного предела (в процентах). Параметр обязателен для заполнения.

- **Настройки отправки почтовых сообщений из базы данных** – настройки отправки почтовых сообщений из базы данных:

  - **SMTP-сервер для отсылки уведомлений** – SMTP-сервер, выбранный для отсылки уведомлений. Значение по умолчанию: **change_on_install**. Параметр обязателен для заполнения.

Примечание

Для получения уведомлений от СУБД Oracle необходимо заменить значение на имя почтового сервера организации.

- **SMTP-порт для отсылки уведомлений** – SMTP-порт, указанный для отсылки уведомлений. Значение по умолчанию: 25. Параметр обязателен для заполнения.

- **Поле Кому сообщения с уведомлением** – поле **Кому** сообщения с уведомлением. Значение по умолчанию: **dozor**. Параметр обязателен для заполнения.

- **Статистика smap** – определяет статистику **smap**.

  - **История монитора БД** – история монитора БД. Необходимо выбрать из двух вариантов: **ведется** – ведется история монитора БД, **не ведется** – история монитора БД не ведется. В случае выбора варианта **ведется** отображаются следующие параметры для заполнения:

    - **Период добавления данных в историю** – период добавления данных в историю.

    - **Период хранения данных в истории** – период хранения данных в истории.

- **Использование секционирования** (для PostgreSQL) – включает использование секционирования БД. Принимает значения **использовать** и **не использовать**. Значение по умолчанию: **не использовать**. При выборе значения **использовать** отображаются параметры секционирования:

  - **Период секционирования** – интервал времени в неделях, данные за который хранятся в одной секции. Значение по умолчанию: 4 (4 недели).

  - **Количество изначально создаваемых секций** – количество изначально создаваемых секций. Значение по умолчанию: 2.

  - **Интервал опережения при создании секций** – интервал опережения при создании новых секций. Если сумма текущей даты и значения этого параметра больше даты окончания предыдущей секции, то создаётся новая секция. Значение по умолчанию: **8D**.

  - **Автоматическое отключение секций** – предоставляет возможность автоматически отключать секции. Принимает значения **используется** и **не используется**. Значение по умолчанию: **не используется**. При выборе значения **используется** отображаются параметры автоматического отключения:

    - **Время до автоматического отключения секций** – интервал времени, после которого выполняется автоматическое отключение секций. Значение состоит из длительности и размерности интервала, где размерность может быть одним из следующего: **D** – день, **W** – неделя (строго равна 7 дням), **M** – месяц. Например: **1M** – один месяц; **2W** – две недели; **10D** – десять дней. Значение по умолчанию: **3M**.

    - **detach-action** – действие при отключении секций. Принимает следующие значения: **Ручная обработка отключенных секций**, **Автоудаление отключенных секций**, **Автоархивирование отключенных секций**.

      При выборе действия **Автоудаление отключенных секций** отображается параметр **Время до удаления отключенных секций** – интервал времени, через который отключенные секции удаляются из БД архива. Отсчитывается от даты окончания действия секции. Значение по умолчанию **4M**.

Примечание

Под датой окончания действия секции понимается момент времени, в который была или будет прекращена запись данных в секцию.

При выборе действия **Автоархивирование отключенных секций** отображаются следующие параметры:

- **Время до архивации отключенных секций** – интервал времени, через который отключенные секции архивируются (значение по умолчанию **4M**);
- **Путь к области долговременного хранения** – каталог, в который происходит резервное копирование архивов с расширением **dump** (значение по умолчанию **/data/backups**).

- **Параметры хранения данных в БД** – параметры хранения табличных пространств для секций БД архива под управлением СУБД PostgreSQL. Содержит следующие параметры:
  - **Список каталогов для табличных пространств MAIN** – каталог для файлов данных табличного пространства **MAIN**. Если параметр не задан, основные секционированные таблицы будут созданы без указания табличного пространства. Возможно указание нескольких каталогов через запятую без пробелов. Пример:

    ```
    /data2/isim,/data3/isim
    ```

    Если на очередном разделе места недостаточно (меньше чем указано в значении параметра **Минимально допустимое свободное место в каталоге MAIN**), выполняется попытка сохранения данных в следующем разделе по порядку и т.д.
  - **Минимально допустимое свободное место в каталоге MAIN** – минимальное значение объема свободного места в каталоге для файлов данных табличного пространства **MAIN**. Значение по умолчанию: **10M** (10 Мбайт). Допускается использование следующей размерности: **K** – Кб; **M** – Мб; **G** – Гб.
  - **Список каталогов для табличных пространств MESSAGE** – каталог для файлов данных табличного пространства **MESSAGE**. Если параметр не задан, основные секционированные таблицы будут созданы без указания табличного пространства. Возможно указание нескольких каталогов через запятую без пробелов. Пример:

    ```
    /data4/isim,/data5/isim,/data6/isim
    ```

    Если на очередном разделе места недостаточно (меньше чем указано в значении параметра **Минимально допустимое свободное место в каталоге MESSAGE**), выполняется попытка сохранения данных в следующем разделе по порядку и т.д.
  - **Минимально допустимое свободное место в каталоге MESSAGE** – минимальное значение объема свободного места в каталоге для файлов данных

табличного пространства **MESSAGE**. Значение по умолчанию: **10M** (10 Мбайт). Допускается использование следующей размерности: **K** – Кб; **M** – Мб; **G** – Гб.

- **Количество генераторов последовательностей для создания ID сообщений** – размер пула последовательностей, используемых для создания и присвоения идентификаторов сообщениям. Параметр используется при постоянно высокой скорости загрузки сообщений в архив (порядка 1000 в секунду) для уменьшения хаотичности при присвоении идентификаторов сообщениям и уменьшения количества повторных загрузок сообщений в архив. Значение по умолчанию: 0.

- **Проверка подключения не выполнялась** – данное сообщение появляется, если проверка подключения к базе данных не выполнялась. При успешной проверки подключения появляется следующее сообщение **Подключение проверено 01.08.2017 11:43 Проверка прошла успешно**.

Настройки файлового хранилища:

- **Gzip-компрессия при размещении** – включает Gzip-компрессию при закладке писем в файловое хранилище. По умолчанию включена.

- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **filestorage-ng**. Предназначено для диагностики возникающих проблем в работе файлового хранилища. По умолчанию выключено.

- **Режим распределения по хранилищам при переносе** – алгоритм распределения данных по хранилищам при их переносе. Принимает значения: **Приоритет скорости** и **Равномерное распределение**. Значение по умолчанию: **Приоритет скорости**.

  При выбранном значении **Приоритет скорости** данные переносятся в центральные ФХ с той скоростью, с которой они могут быть приняты. Более быстрый сервер забирает на себя больше данных. Неработающие узлы исключаются из переноса. Этот режим наиболее производительный, но может приводить к дисбалансу объемов хранения между хранилищами.

  При выбранном значении **Равномерное распределение** на каждое центральное ФХ переносится одинаковое количество контейнеров. Медленный узел замедляет процесс переноса. Неработающий узел практически останавливает процесс переноса. Этот режим дает равномерное распределение данных по хранилищам, но скорость переноса фактически ограничена скоростью самого медленного узла.

- **Разрешенные часы переноса данных из локального файлового хранилища в центральное** – временные интервалы в часах по переносу данных из локального файлового хранилища в центральное. Включает следующие параметры:

  - **Час начала (timezone сервера)** – час начала переноса данных из локального файлового хранилища в центральное. Значение по умолчанию: 0.

  - **Час окончания (timezone сервера)** – час окончания (включительно, минуты игнорируются) переноса данных из локального файлового хранилища в центральное. Значение по умолчанию: 24.

- **Настройка переноса контейнеров** – параметры переноса контейнеров. Для настроек нового контейнера необходимо щелкнуть мышью на значок  . Для удаления языка необходимо щелкнуть мышью на значок  рядом с нужным полем ввода.

- **Volume Group** – идентификатор группы томов. Значение по умолчанию: **vg-000000**.
- **Время жизни до переноса** – время нахождения сообщений в локальном файловом хранилище до начала переноса в центральное. Задаётся в днях и часах. Значение по умолчанию: **0д, 0ч** (немедленный перенос).

- **Настройка ротации** – содержит следующие параметры ротации контейнеров:
  - **Volume Group** – идентификатор группы томов.
  - **Время жизни до ротации (д)** – время нахождения сообщений в центральном файловом хранилище до начала их ротации. Задаётся в днях. Значение по умолчанию: 30.
  - **Рекомендуемый размер файла архива (МБ)** – максимальный размер файла, формируемый при ротации в режиме **Локальная файловая система**. Если объем передаваемых во внешнее хранилище данных превышает указанное в данном параметре значение, данные разбиваются на несколько архивных файлов, размер каждого из которых не превышает указанное в параметре значение. Указывается в мегабайтах. Значение по умолчанию: 256.
  - **Критический объем свободного места (МБ)** – минимальное значение объема свободного пространства в центральном ФХ. Проверка свободного пространства производится каждые сутки в 3 часа ночи по времени сервера. Если объем свободного пространства в центральном ФХ становится меньше значения этого параметра, производится внеочередная ротация. Указывается в мегабайтах. Значение по умолчанию: 256.
  - **Gzip компрессия архива** – включает gzip-компрессию при ротации в режиме **Локальная файловая система**. По умолчанию выключена.
  - **Режим ротации** – режим ротации. Имеется три режима: удаление данных (**Удалить, не архивировать**), сохранение на локальном носителе (**Локальная файловая система**) и сохранение на внешнем ftp-сервере (**Внешний FTP сервер**). Значение по умолчанию: **Удалить, не архивировать**.

    При значении **Локальная файловая система** данные при ротации будут отключены от ФХ и помещены в каталог, указанный в параметре **Путь**.

    При значении **Внешний FTP сервер** данные при ротации будут отключены от ФХ и помещены заданный каталог на заданном FTP-сервере:

    - **Сетевой адрес** – адрес FTP-сервера организации.
    - **Номер порта** – порт, на котором FTP-сервер ожидает соединения.
    - **Режим FTP** – режим работы, на который настроен FTP-сервер (активный или пассивный).
    - **Пользователь** – имя пользователя для соединения с FTP-сервером.
    - **Пароль** – пароль этого пользователя.
    - **Путь на FTP-сервере** – путь к каталогу на FTP-сервер, в который будут сохраняться данные при ротации.

- **Периодичность ротации** – периодичность выполнения ротации. Имеется три варианта: **Ежедневно**, **Еженедельно** и **Ежемесячно**. Значение по умолчанию: **Ежедневно** (ежедневно).

  Еженедельно включает следующие параметры:

  - **День недели** – день начала ротации. Значение по умолчанию не задано.
  - **Час** – час начала ротации. Значение по умолчанию не задано.
  - **Минута** – минута начала ротации. Значение по умолчанию не задано.

  Ежемесячно включает следующие параметры:

  - **День месяца** – день начала ротации. Значение по умолчанию не задано.
  - **Час** – час начала ротации. Значение по умолчанию не задано.
  - **Минута** – минута начала ротации. Значение по умолчанию не задано.

  Ежедневно включает следующие параметры:

  - **Час** – час начала ротации. Значение по умолчанию не задано.
  - **Минута** – минута начала ротации. Значение по умолчанию не задано.

Тома файлового хранилища:

По умолчанию создано 6 групп томов файлового хранилища, которые характеризуются идентификаторами в базе данных. Идентификатор группы задается автоматически и редактированию не подлежит. Для добавления новой группы следует нажать значок рядом с идентификатором группы, а для удаления – значок . Каждая группа томов содержит набор следующих параметров:

- **Группа томов (Volume Group)** – идентификатор группы томов. Принимает значения:
  - **vg-000000** – для первой группы.
  - **abook** – для второй группы.
  - **agent-media** – для третьей группы.
  - **audio** – для четвертой группы.
  - **screen-video** – для пятой группы.
  - **detective-data** – для шестой группы.
- **Идентификатор тома** – идентификатор тома. Принимает значения:
  - **main** – для первой группы.
  - **abook** – для второй группы.
  - **agent-media** – для третьей группы.

- **audio** – для четвертой группы.
- **screen-video** – для пятой группы.
- **detective-data** – для шестой группы.

- **Только для чтения** – настройка тома только для чтения. По умолчанию выключено.
- **Разрешить ротацию тома** – разрешить ротацию тома. Если том относится к локальному файловому хранилищу, настройка игнорируется. По умолчанию выключено.
- **Путь, по которому размещены данные** – путь, по которому размещены данные файлового хранилища. Принимает значения:
  - **/data/storage/vg-000000/fs-1** – для первой группы.
  - **/data/storage/abook** – для второй группы.
  - **/data/storage/agent-media** – для третьей группы.
  - **/data/storage/audio** – для четвертой группы.
  - **/data/storage/screen-video** – для пятой группы.
  - **/data/storage/detective-data** – для шестой группы.

Сервис хранения и индексации событий и инцидентов:

- **Хранилище инцидентов (PostgreSQL)** – имя схемы соединения с БД, используемой для хранения информации о задачах сервиса **incident-daemon**. Принимает значения **Отсутствует** и **Специальная БД**. Значение по умолчанию: **Отсутствует**. Если выбрано значение **Специальная БД**, доступны параметры:
  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.
  - **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.
  - **Проверка подключения не выполнялась** – данное сообщение появляется, если проверка подключения к БД не выполнялась. При успешной проверки подключения появляется следующее сообщение **Подключение проверено 01.09.2021 11:00 Проверка прошла успешно**.
- **Режим ротации** – режим ротации:
  - Архивировать – архивировать секции в локальный каталог (указанный в параметре **Путь до каталога архивации**), по умолчанию выключен;
  - Удалять (не архивировать) – удалить секции;

- Ротация не производится – выключить режим ротации.

Хранение медиаинформации:

- **Срок хранения снимков (д)** – период хранения метаданных снимков экрана в днях. Значение по умолчанию: 90.
- **Срок хранения снимков демонстрации экрана (ч)** – период хранения снимков демонстрации экрана в часах. Значение по умолчанию: 2160 (90 дней).
- **Срок хранения аудиозаписей (д)** – период хранения метаданных аудиозаписей в днях. Значение по умолчанию: 90.
- **Срок хранения записей экрана (д)** – период хранения метаданных записей экрана/экранов рабочих станций персоны в днях. Значение по умолчанию: 90.
- **Срок хранения списков процессов приложений (д)** – период хранения метаданных запущенных процессов, активного URL и заголовка активного окна. Значение по умолчанию: 90.
- **База данных (PostgreSQL)** – имя схемы соединения с БД, используемой для хранения информации о задачах сервиса **agent-media-server**. Принимает значения **БД по умолчанию** и **Специальная БД**. Значение по умолчанию: **БД по умолчанию**. При значении **БД по умолчанию** сервис подключается к БД политики, настройки которой задаются в разделе GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** > **БД настроек политики и досье**. Если выбрано значение **Специальная БД**, доступны параметры:
  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.
  - **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.
  - **Проверка подключения не выполнялась** – данное сообщение появляется, если проверка подключения к БД не выполнялась. При успешной проверки подключения появляется следующее сообщение **Подключение проверено 01.09.2021 11:00 Проверка прошла успешно**.

A.1.3. Взаимодействие

Сервис доступа к Досье:

- **Автоматическая синхронизация Досье** – включает автоматическую синхронизацию досье с источниками LDAP/AD. По умолчанию выключена.
- **Периодичность запуска синхронизации (ч)** – периодичность запуска в часах автоматической синхронизации досье с источниками LDAP/AD. Значение по умолчанию: 4.

Примечание

Периодичность запуска синхронизации происходит вне зависимости от наступления новой даты.

- **Периодичность запуска синхронизации (м)** – периодичность запуска в минутах автоматической синхронизации досье с источниками LDAP/AD. Значение по умолчанию: 0. Значение добавляется к количеству часов, заданному в предыдущем параметре.

Примечание

Не рекомендуется устанавливать значение периодичности синхронизации меньше 20 минут, т.к. при объемном LDAP-каталоге и большом количестве пользователей для успешного завершения обновления данного времени может быть недостаточно.

При значении 0 часов 0 минут синхронизация работать не будет.

Источники данных досье:

В этой группе параметров может быть задано несколько источников данных. Для добавления новой секции и нового источника следует нажать значок рядом с идентификатором источника. Для удаления следует нажать значок . Источник данных характеризуется идентификатором источника в базе данных. Идентификатор источника (параметр **Описание источника данных**) задается автоматически при добавлении нового источника и редактированию не подлежит. Описание источника данных содержит параметры **Название источника** и **Параметры доступа к источнику**.

- **Синхронизировать** – выполнить синхронизацию с источником.

Примечание

Синхронизация возможна только при выполнении следующих условий:

- *Имеется хотя бы один включенный источник данных (установлен флажок "Синхронизация включена").*
- *Настройки всех источников данных успешно применены.*
- *В данный момент не выполняется другая синхронизация.*

- **Название источника** – название источника данных.
- **Синхронизация включена** – при установленном флажке Досье синхронизируется с источником данных.

  Возможные значения параметра: **true** и **false**. В конфигурации источников, поставляемых с системой (**AD**, **389 Directory Server Example** и **ALD Pro**), синхронизация по умолчанию отключена.

Примечание

При попытке синхронизировать Досье со всеми отключенными источниками данных отображается соответствующее предупреждение.

- **Параметры доступа к источнику данных** – выбираются из раскрывающегося списка. Возможные значения параметра: **ldap** и **file**.

  При выборе значения **ldap** появляется дополнительный набор параметров доступа к данным с LDAP-сервера (перечислены ниже):

  - **DN пользователя** – запись, которая уникально идентифицирует имя пользователя.
  - **Пароль пользователя** – пароль для идентификации пользователя.
  - **URL LDAP сервера** – URL LDAP-сервера.
  - **Базовый DN для поиска** – позволяет переопределить заданную по умолчанию начальную точку поиска.
  - **Число записей на странице** – размер страницы запроса. Измеряется в записях.
  - **Фильтр подразделений** – строковое представление фильтра, применяемого при поиске подразделений.
  - **Фильтр групп** – строковое представление фильтра, применяемого при поиске групп.
  - **Фильтр персон** – строковое представление фильтра, применяемого при поиске персон.
  - **Атрибут, содержащий уникальный идентификатор записи** – имя атрибута, содержащего UUID записи.
  - **Атрибут, содержащий номер последнего изменения записи** – имя атрибута, содержащего номер последнего изменения записи.
  - **Атрибут RootDSE, содержащий идентификатор сервера** – имя атрибута RootDSE, содержащего идентификатор сервера.
  - **Атрибут RootDSE, содержащий номер последнего изменения содержимого** – имя атрибута RootDSE, содержащего номер последнего изменения содержимого.
  - **Список соответствий атрибутов** – список соответствий атрибутов. Может быть задано несколько атрибутов учетной записи и для каждого из них указано соответствие **LDAP-атрибута** и **атрибута адресной книги**.

    Есть возможность выбора из следующего списка атрибутов персоны досье:

    - DN;
    - Уменьшенная фотография;
    - Адрес электронной почты;

- ФИО;
- Группа;
- Фамилия;
- Имя;
- Название компании;
- Должность;
- Номер мобильного телефона;
- Номер телефона;
- Логин;
- Кому подчиняется;
- Дата приема на работу.

Примечание

*Адреса электронной почты пользователей (атрибут **Адрес электронной почты**) могут содержаться в атрибутах **proxyAddresses** и **mail**.*

Также задается **Приоритет источника** – приоритет источника, который учитывается при слиянии персон из нескольких источников. Если при слиянии персон значение уникального атрибута из источника с приоритетом, равным 1, отсутствует, то будет использовано значение этого атрибута из источника с приоритетом, равным 2 и т.д. Если необходимо настроить приоритеты по умолчанию, для атрибута у всех источников устанавливается приоритет, равный 1. Диапазон значений: от 1 до **N**, где **N** – число источников данных Досье.

- **Список соответствий атрибутов групп** – список соответствий атрибутов групп Досье. Может быть задан 1 атрибут группы Досье и для него указано соответствие **LDAP-атрибута** и атрибута группы персон, принимающего значение **Руководитель группы**.

При выборе значения **file** появляется дополнительный набор параметров, предназначенных для настройки импорта данных ОШС из файлов:

- **Каталог с данными ОШС** – каталог для размещения файлов с данными о структуре ОШС. Значение по умолчанию: **/data/spool/abook-daemon/org_structure/**.
- **Файл со списком групп** – имя csv-файла со списком групп. Значение по умолчанию: **groups.csv**.
- **Файл со списком сотрудников** – имя csv-файла со списком персон. Значение по умолчанию: **persons.csv**.

Сервер управления агентами:

- **Настройки LDAP** – настройки взаимодействия сервиса **software-center** с LDAP-сервером. Принимает значения: **Выключено** и **Включено**. По умолчанию параметр выключен. При значении **Включено** доступны следующие параметры:
  - **URL LDAP сервера** – URL LDAP-сервера. Значение по умолчанию: **ldap://nihil.local:3268**.
  - **DN пользователя** – данный параметр предназначен для ввода DN записи с целью подключения к LDAP. Значение по умолчанию: **user@nihil.local**.
  - **Пароль пользователя** – данный параметр предназначен для ввода пароля с целью подключения к LDAP.
  - **Проверка подключения не выполнялась** – данное сообщение появляется, если проверка подключения к БД не выполнялась. При успешной проверки подключения появляется следующее сообщение **Подключение проверено 01.09.2021 11:00 Проверка прошла успешно**.
- **Таймаут удаления временных станций (мин)** – время ожидания удаления временных станций в мин. Значение по умолчанию: 480.

Настройки модуля KEO DLP Traffic Analyzer:

- Группа параметров **Захват сетевого трафика** (содержит параметры настройки используемой технологии захвата трафика с сетевого интерфейса):
  - **Сетевой интерфейс** – список имён сетевых интерфейсов, на которых KEO DLP Traffic Analyzer ожидает зеркалируемый незашифрованный трафик. Имена сетевых интерфейсов перечисляются через запятую без пробелов, например: **eth0,eth2**. Список всех имеющихся сетевых интерфейсов можно получить с помощью команды CLI **ifconfig**.
  - **Низкоуровневый фильтр** – строка, задающая параметры низкоуровневой фильтрации пакетов.

    Значение по умолчанию: **not port 1025**. Рекомендуется использовать следующее значение:

    ```
    not host <IP-адрес> and not host <IP-адрес-2> and ...
    ```

    где **<IP-адрес>>**, **<IP-адрес-2>** и т.д. – IP-адреса узлов кластера KEO DLP, для которых не планируется использование сервиса KEO DLP Traffic Analyzer
  - **Технология захвата** – используемая технология перехвата. Принимает значения **библиотека PF_RING** (выполняются перехваты с сетевого интерфейса модулем **pf_ring**) и **библиотека libpcap** (с помощью библиотеки Pcap). Значение по умолчанию: **библиотека PF_RING**.

    Если через сетевые интерфейсы проходит много данных, лучше выбрать библиотеку PF_RING. Она поможет уменьшить потери при перехвате большого объёма трафика.

    Если трафик поступает в малых объемах или сетевой интерфейс PF_RING не работает, следует использовать **библиотека libpcap**.

- **Асинхронный режим** – включает асинхронный цикл захвата трафика по технологии SPAN, позволяющий снизить нагрузку на процессор при небольшой сетевой активности. Принимает значения: **true** и **false**. Значение по умолчанию: **true**.

  Примечание

  Рекомендуется использовать оставить включенным.

- **Период опроса (мс)** – время приостановки синхронного цикла захвата трафика, необходимое для снижения нагрузки при отсутствии трафика. Значение по умолчанию:0. При высокой нагрузке на систему рекомендуется установить значение 5-10 мс. Используется совместно с параметром **Асинхронный режим**.

- **Минимальный размер буфера для libpcap (Кб)** – ограничение в Кб на размер буфера для библиотеки **libpcap** при захвате и разборе трафика. Значение по умолчанию: 200000.

- **Список фильтруемых сетевых портов** – доступный для редактирования список портов. Значение по умолчанию:

  22,389,443,1010,1025,1344,2266,2269,2272,2344,3000,3001,3003,3004,3006,3010,3030,3268,3900,4444,5001,5434,5439,5440,5445,5558,7001,7199,7837,8008,8080,8090,8123,9000,9001,9042,9160,9200,9201,9301,9302,9400,9401,9666,9998,10000,10050,11344,16379,61616

  Рекомендованные значения параметров **Низкоуровневый фильтр** (**filter**) и **Список фильтруемых портов** (**filter_port_list**) исключают перехват данных на узлах и портах, используемых сервисами KEO DLP. Таким образом, снижается нагрузка на KEO DLP Traffic Analyzer.

  Если изменяется значение порта по-умолчанию, это изменение следует отразить в значении параметра **Список фильтруемых сетевых портов**. Для исключения перехвата прочих сервисов следует добавить порты, используемые этими сервисами, в список.

  Во всех случаях, кроме перехвата ICAP-трафика, поступающего по технологии SPAN, не вносить порты 1344 и 2344 в список фильтруемых портов.

- **Включить nDPI-фильтрацию пакетов** – включает фильтрацию пакетов с помощью библиотеки **nDPI**. Принимает значение **true** и **false**. Значение по умолчанию: **false**.

- **Максимальное количество памяти для nDPI (Мб)** – максимальное количество выделяемой оперативной памяти в Мб под библиотеку **nDPI**. Значение по умолчанию: 512.

- **Сборщик TCP-потоков** (сборка TCP-потоков объединение их в непрерывный поток данных):

  - **Включить поддержку интерфейса с multiqueue** – включает поддержку сетевого интерфейса с multiqueue. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).

- **Максимальное число неподтвержденных сегментов в буфере** – максимальное число неподтвержденных сегментов, находящихся в очереди получения сетевых пакетов. Значение по умолчанию: 64.

  Примечание

  Значение параметра подбирается администратором в соответствии с сетевой инфраструктурой и постепенно увеличивается от 10 до 128 сегментов.

  Примечание

  *Параметр используется при работе KEO DLP Traffic Analyzer в режиме мультиочереди, т.е. совместно с параметром **Включить поддержку интерфейса с multiqueue**.*

- **Не ожидать фазу ESTABLISHED** – включает обработку соединения по стандарту TCP/IP. Принимает значения **true** и **false**. При значении **false** обработка соединения происходит по упрощенной схеме. Значение по умолчанию: **false** (выключено).

- **Показывать предупреждения о потерях пакетов** – запись предупреждений о работе IP-пакетов в журнальный файл. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).

- **Показывать предупреждения о дубликатах пакетов** – включает появление предупреждений о дубликатах пакетов. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).

- **Показывать предупреждения о нарушении порядка пакетов** – включает появление предупреждений о нарушении порядка пакетов. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).

- **Показывать предупреждения о непредсказуемом поведении** – включает появление предупреждений о непредсказуемом поведении сборщика. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).

- **Сборщик IP-фрагментов** (параметры сборщика фрагментированных IP-пакетов):

  - **Включить** – включает сборку IP-фрагментов. Принимает значение **true** и **false**. Значение по умолчанию: **false**.

  - **Выбрасывать фрагментированные пакеты** – включает блокировку IP-фрагментов. Принимает значение **true** и **false**. Значение по умолчанию: **false**.

  - **Максимальный размер пакета (Б)** – максимальный размер пакета в байтах. Значение по умолчанию: 10240.

  - **Максимальное число фрагментов пакета** – максимальное число фрагментов пакета. Значение по умолчанию: 128.

  - **Таймаут сборки пакета (мс)** – время ожидания при сборке пакета в миллисекундах. Значение по умолчанию: 1000000.

- **Максимальный размер IP заголовка (Б)** – максимальный размер заголовка IP-пакета в байт. Значение по умолчанию: 64.

- **Отладка, расширенный лог** – включает расширенное отладочное журналирование. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

- **Отладка, предупреждение медленного старта** – включает записи событий медленного старта в журнал. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

- **Отладка, предупреждение неупорядоченности** – включает записи событий о неупорядоченной доставке IP-пакетов в журнал. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

- **Отбрасывать сборки без начала** – включает игнорирование сборок без заголовков. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

- **Пересчитывать контрольную сумму IP заголовка** – включает пересчет контрольной суммы заголовка IP-пакета. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

- **Максимальное число собираемых пакетов** – максимальное число собираемых пакетов. Значение по умолчанию: 1024.

- Группа параметров **ICAP-сервер** (настройки ICAP-сервера):

  - **Включить ICAP-сервер** (**enable**) – включить анализ данных, поступающих от источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера). Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

  - **Порты ICAP-сервера** – сетевой порт, на котором ICAP-сервер ожидает данные. Значение по умолчанию: 1344.

  - **Режим работы ICAP-сервера** – режим работы ICAP-сервера модуля KEO DLP Traffic Analyzer. Принимает значения **Работа в режиме REQMOD и RESPMOD**, **Работа в режиме REQMOD** и **Работа в режиме совместимости с Blue Coat**. Значение по умолчанию: **Работа в режиме REQMOD и RESPMOD**.

    При значении **Работа в режиме REQMOD и RESPMOD** KEO DLP Traffic Analyzer анализирует запросы и ответы, полученные по протоколу ICAP от источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера). KEO DLP Traffic Analyzer сохраняет в кэш принятые запросы (REQMOD) и ожидает ответы (RESPMOD) в рамках ICAP-сессии. После получения RESPMOD KEO DLP Traffic Analyzer анализирует данные, формирует сообщение-перехват и отправляет его в KEO DLP. Если KEO DLP Traffic Analyzer не получит ответ (RESPMOD), это приведет к потере принятых запросов (REQMOD).

    Если источник не поддерживает отправку ответов (RESPMOD) или анализ ответов (RESPMOD) не требуется, следует выбрать значение **Работа в режиме REQMOD**, при котором KEO DLP Traffic Analyzer, получив запрос, сразу анализирует его и отправляет сформированные сообщения-перехваты в KEO DLP. В этом случае KEO DLP Traffic Analyzer не ожидает ответов (RESPMOD) по протоколу ICAP от источника трафика.

Внимание!

В режиме анализа запросов (REQMOD) не будет перехватываться любая информация, загруженная из сети Интернет, так как для части веб-сервисов она может приходить в ответе сервера (например, скачивание файлов и входящая веб-почта). Также не будет работать связь между различными сетевыми сессиями (например, «авторизация – отправка эл. почты», «сохранение черновика - отправка письма» и т.д.) Кроме того, некоторые облачные хранилища будут разбивать загружаемые файлы объемом более 5 Мб на части, которые перехватываются по отдельности.

Режим **Работа в режиме совместимости с Blue Coat** предназначен для работы с Blue Coat Proxy SG в режиме запросов (REQMOD) и ответов (RESPMOD).

Примечание

*Режим работы ICAP-сервера определяется только параметром **Режим работы ICAP-сервера**. Если модуль KEO DLP Traffic Analyzer использует режим анализа запросов и ответов, в настройках источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера) указывается URL или IP-адрес узла с ролью **Сервис перехвата и анализа сетевого трафика** (Traffic Analyzer). Это необходимо для случая, когда источники ICAP различаются (например, одни поддерживают отправку запросов и ответов, а другие могут работать только в режиме **Reqonly**). Описание взаимодействия KEO DLP Traffic Analyzer с различными прокси-серверами приведено в документе Модуль перехвата и анализа сетевого трафика «Traffic Analyzer». Руководство системного администратора). Поддерживаемые форматы URL:*

- ***icap://ta.isim.local:1344/** или **icap://ta.isim.local:1344/reqresp** – передача запросов и ответов;*
- ***icap://ta.isim.local:1344/reqonly** – передача запросов.*

Примечание

Рекомендуются следующие режимы в зависимости от используемого источника трафика:

- *KEO DLP webProxy или любые другие прокси-серверы, работающие согласно RFC – **Работа в режиме REQMOD и RESPMOD**.*
- *Режим **Работа в режиме совместимости с Blue Coat** предназначен для работы с прокси-сервером Blue Coat Proxy SG одновременно в режимах REQMOD и RESPMOD.*
- *IronPort (Cisco Web Security Appliance) – **Работа в режиме REQMOD** (IronPort может работать только в режиме REQMOD).*

- **Максимальный размер тела HTTP-запроса в ICAP (Б)** – максимальный размер ICAP-сессии в байтах, обработку которой выполняет KEO DLP Traffic Analyzer. Значение по умолчанию: 156314880 Б (149 Мб). При нулевом значении снимается ограничение на размер тела запроса.

Внимание!

Не рекомендуется слишком сильно увеличивать значение параметра по умолчанию в связи с возрастающей нагрузкой KEO DLP Traffic Analyzer на оперативную память и процессор.

- **Не обрабатывать запросы "CONNECT"** – отключает обработку HTTP-запросов вида **CONNECT**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

Внимание!

*Отключение обработки HTTP-запросов вида **CONNECT** позволяет повысить производительность работы KEO DLP Traffic Analyzer, поскольку уменьшается число обрабатываемых запросов.*

- **Максимальное число соединений с ICAP-сервером** – максимальное число попыток соединений с ICAP-сервером. Значение по умолчанию: 1000.
- **Максимальное число используемых ядер** – максимальное число потоков процессора, используемых при обработке трафика. Значение по умолчанию: 1.
- **Тип планировщика** – алгоритм распределения поступающего с прокси-серверов трафика по ядрам (потокам) ICAP-сервера. Общее количество потоков равно значению параметра **Максимальное число используемых ядер** (см. описание выше).

  Принимает значения: **хэш (hash)**, **круговой (rr)**. Значение по умолчанию: **хэш (hash)**.

  При значении **хэш (hash)** каждому ICAP-серверу выделяется отдельный поток. Для IP-адреса ICAP-сервера вычисляется хэш. При таком алгоритме ICAP-сессии упорядоченно распределяются по потокам.

  При значении **круговой (rr)** происходит равномерное распределение сессий по потокам ICAP-сервера. При таком алгоритме возможно неупорядоченное распределение ICAP-сессий по потокам.

  Рекомендуется использовать значение по умолчанию.
- **Включить таймаут приема данных от клиента** – включает ожидание ответа от источника ICAP-трафика (прокси-сервера). Принимает значения **true** и **false**. Значение по умолчанию: **true** (включено).
- **Таймаут приема данных от клиента (с)** – определяет таймаут ожидания ответа в секундах от источника ICAP-трафика. Значение по умолчанию: 90.
- **Включить асинхронный режим ICAP (не буферизировать ответ клиенту)** – включает асинхронный режим работы ICAP-сервера, при котором ответ не сохраняется на KEO DLP Traffic Analyzer. Принимает значения **true** и **false**. Значение по умолчанию: **false**.

Внимание!

*Асинхронный режим работы ICAP-сервера поддерживается при многопоточном функционировании модуля **icap** (значение параметра **Максимальное число используемых ядер** > 0).*

Примечание

*При использовании источников трафика **F5 BIG-IP**, **Bluecoat ProxySG**, **Squid**, **McAfee**, принимающих только ответы с кодом 200, рекомендуется включить асинхронный режим работы ICAP-сервера в секции ICAP-сервер.*

- **Игнорировать ICAP заголовок "Allow 204"** – включает принудительный ответ ICAP-клиенту с кодом 204. Принимает значения **true** и **false**. Значение по умолчанию: **false**.
- **Оптимизировать выдачу ответов ICAP-клиентам** – при включенном параметре источники ICAP-трафика быстрее получают ответы на свои запросы. Принимает значения **true** и **false**. Значение по умолчанию: **true**.
- **Максимальное количество попыток создания сервера** – максимальное число попыток перезапустить ICAP-сервер. Параметр применяется только при включённом многопоточном ICAP-сервере (параметр **max_threads** отличен от нуля). Значение по умолчанию: 256.
- **Включить дополнительные параметры системного вызова bind** – настройки сокета, создающегося при подключении к ICAP-серверу. Значение по умолчанию: 0.

- Группа параметров **ICAPS-сервер**:
  - **Включить ICAPS-сервер** (**enable**) – включить анализ данных, поступающих от источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера) в зашифрованном виде. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.
  - **Порты ICAPS-сервера (через запятую)** – сетевой порт, на котором ICAPS-сервер ожидает данные.
  - **Путь к сертификату icaps** – путь к файлу сертификата шифрования.
  - **Путь к ключу icaps** – путь к файлу закрытого ключа.
  - **Режим работы ICAPS-сервера** – режим работы ICAPS-сервера модуля KEO DLP Traffic Analyzer. Принимает значения **Работа в режиме REQMOD и RESPMOD**, **Работа в режиме REQMOD** и **Работа в режиме совместимости с Blue Coat**. Значение по умолчанию: **Работа в режиме REQMOD и RESPMOD**.

    При значении **Работа в режиме REQMOD и RESPMOD** KEO DLP Traffic Analyzer анализирует запросы и ответы, полученные по протоколу ICAPS от источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера). KEO DLP

Traffic Analyzer сохраняет в кэш принятые запросы (REQMOD) и ожидает ответы (RESPMOD) в рамках ICAP-сессии. После получения RESPMOD KEO DLP Traffic Analyzer анализирует данные, формирует сообщение-перехват и отправляет его в KEO DLP. Если KEO DLP Traffic Analyzer не получит ответ (RESPMOD), это приведет к потере принятых запросов (REQMOD).

Если источник не поддерживает отправку ответов (RESPMOD) или анализ ответов (RESPMOD) не требуется, следует выбрать значение **Работа в режиме REQMOD**, при котором KEO DLP Traffic Analyzer, получив запрос, сразу анализирует его и отправляет сформированные сообщения-перехваты в KEO DLP. В этом случае KEO DLP Traffic Analyzer не ожидает ответов (RESPMOD) по протоколу ICAPS от источника трафика.

Внимание!

В режиме анализа запросов (REQMOD) не будет перехватываться любая информация, загруженная из сети Интернет, так как для части веб-сервисов она может приходить в ответе сервера (например, скачивание файлов и входящая веб-почта). Также не будет работать связь между различными сетевыми сессиями (например, «авторизация – отправка эл. почты», «сохранение черновика - отправка письма» и т.д.) Кроме того, некоторые облачные хранилища будут разбивать загружаемые файлы объемом более 5 Мб на части, которые перехватываются по отдельности.

Режим **Работа в режиме совместимости с Blue Coat** предназначен для работы с Blue Coat Proxy SG в режиме запросов (REQMOD) и ответов (RESPMOD).

Примечание

*Режим работы ICAPS-сервера определяется только параметром **Режим работы ICAPS-сервера**. Если модуль KEO DLP Traffic Analyzer использует режим анализа запросов и ответов, в настройках источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера) указывается URL или IP-адрес узла с ролью **Сервис перехвата и анализа сетевого трафика** (Traffic Analyzer). Это необходимо для случая, когда источники ICAPS различаются (например, одни поддерживают отправку запросов и ответов, а другие могут работать только в режиме **Reqonly**). Описание взаимодействия KEO DLP Traffic Analyzer с различными прокси-серверами приведено в документе Модуль перехвата и анализа сетевого трафика «Traffic Analyzer». Руководство системного администратора). Поддерживаемые форматы URL:*

- ***icap://ta.isim.local:1344/** или **icap://ta.isim.local:1344/reqresp** – передача запросов и ответов;*
- ***icap://ta.isim.local:1344/reqonly** – передача запросов.*

Примечание

Рекомендуются следующие режимы в зависимости от используемого источника трафика:

- *KEO DLP webProxy или любые другие прокси-серверы, работающие согласно RFC – **Работа в режиме REQMOD и RESPMOD**.*

- *Режим **Работа в режиме совместимости с Blue Coat** предназначен для работы с прокси-сервером Blue Coat Proxy SG одновременно в режимах REQMOD и RESPMOD.*
- *IronPort (Cisco Web Security Appliance) – **Работа в режиме REQMOD** (IronPort может работать только в режиме REQMOD).*

- **Максимальное число соединений с ICAPS-сервером** – максимальное число попыток соединений с ICAPS-сервером. Значение по умолчанию: 1000.
- **Максимальное число используемых ядер** – максимальное число потоков процессора, используемых при обработке трафика. Значение по умолчанию: 1.
- **Тип планировщика** – алгоритм распределения поступающего с прокси-серверов трафика по ядрам (потокам) ICAPS-сервера. Общее количество потоков равно значению параметра **Максимальное число используемых ядер** (см. описание выше).

  Принимает значения: **хэш (hash)**, **круговой (rr)**. Значение по умолчанию: **хэш (hash)**.

  При значении **хэш (hash)** каждому ICAPS-серверу выделяется отдельный поток. Для IP-адреса ICAPS-сервера вычисляется хэш. При таком алгоритме ICAPS-сессии упорядоченно распределяются по потокам.

  При значении **круговой (rr)** происходит равномерное распределение сессий по потокам ICAPS-сервера. При таком алгоритме возможно неупорядоченное распределение ICAPS-сессий по потокам.

  Рекомендуется использовать значение по умолчанию.
- **Включить таймаут приема данных от клиента** – включает ожидание ответа от источника ICAP-трафика (прокси-сервера). Принимает значения **true** и **false**. Значение по умолчанию: **true** (включено).
- **Таймаут приема данных от клиента (с)** – определяет таймаут ожидания ответа в секундах от источника ICAP-трафика. Значение по умолчанию: 90.
- **Включить асинхронный режим ICAPS (не буферизировать ответ клиенту)** – включает асинхронный режим работы ICAPS-сервера, при котором ответ не сохраняется на KEO DLP Traffic Analyzer. Принимает значения **true** и **false**. Значение по умолчанию: **false**.

  Внимание!

  *Асинхронный режим работы ICAP-сервера поддерживается при многопоточном функционировании модуля **icaps** (значение параметра **Максимальное число используемых ядер** > 0).*
- **Игнорировать ICAPS заголовок "Allow 204"** – включает принудительный ответ ICAPS-клиенту с кодом 204. Принимает значения **true** и **false**. Значение по умолчанию: **false**.

- **Оптимизировать выдачу ответов ICAP-клиентам** – при включенном параметре источники ICAP-трафика быстрее получают ответы на свои запросы. Принимает значения **true** и **false**. Значение по умолчанию: **true**.

- **Максимальное количество попыток создания сервера** – максимальное число попыток перезапустить ICAPS-сервер. Параметр применяется только при включённом многопоточном ICAPS-сервере (параметр **max_threads** отличен от нуля). Значение по умолчанию: 256.

- **Включить дополнительные параметры системного вызова bind** – настройки сокета, создающегося при подключении к ICAPS-серверу. Значение по умолчанию: 0.

- Группа параметров **Анализатор данных** (настройки обработки перехватываемого потока данных):

  - **Максимальное время на обработку запроса (мс)** – максимальное время на обработку потока в миллисекундах, при превышении которого обработка прекращается. Значение по умолчанию: 200000.

  - **Максимальная длина очереди запросов** – максимальное количество обработанных запросов от прокси-серверов к KEO DLP Traffic Analyzer, которое может находиться в очереди потока. Значение по умолчанию: 200.

  - **Включить отчет о зависании обработки запроса** – включить сбор отладочной информации, если обработка ICAP-сессии занимает очень много времени. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

  - **Добавлять тело запроса в отчет** – включить сбор отладочной информации о теле ICAP-сессии. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

  - **Максимальный размер обрабатываемого запроса (Б)** (**http_body_limit**) – максимальный размер потока в байтах, принимаемого на обработку. При превышении этого размера поток отбрасывается без обработки. Значение по умолчанию: 104857600.

  - **Обработка протокола HTTP over proxy** (**http_redirect**) – в случае использования прокси-сервера включает обработку протокола HTTP. Принимает значение **true** и **false**. Значение по умолчанию: **false**.

  - **Обработка протокола HTTPS over proxy** (**https_redirect**) – в случае использования прокси-сервера включает обработку протокола HTTPS. Принимает значение **true** и **false**. Значение по умолчанию: **false**.

  - **Обработка протокола OSCAR over proxy** (**oscar_redirect**) – в случае использования прокси-сервера включает обработку протокола OCSAR. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

- Группа параметров **Фильтрация сообщений** (настройка общей фильтрации):

  - **Список отключенных детекторов** – список отключенных детекторов из набора отключаемых. Поддерживается отключение детекторов **!generic**, **accounts** и **!file-upload**.

- **Включить фильтр однотипных сообщений** – включает фильтрацию однотипных сообщений. Под однотипными сообщениями понимаются сообщения, в которых совпадают заголовки, идентифицирующие пользователя и его тип действия на ресурсе.

  Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

  Примечание

  Включение фильтрации однотипных сообщений позволяет повысить производительность работы KEO DLP Traffic Analyzer. Рекомендуется оставить параметр включенным.

- **Размер кэша фильтра однотипных сообщений** – размер кэша хранения однотипных сообщений, полученных в результате фильтрации. Измеряется в количестве записей. Значение по умолчанию: 100000. При превышении этого размера происходит ротация кэша – старые записи удаляются.

- **Время жизни записи в кэше фильтра однотипных сообщений (сек)** – максимальное время в секундах, отводимое на хранение записей об однотипных сообщениях в кэше. Значение по умолчанию: 28800 (8 часов). Старые записи удаляются.

  Примечание

  По истечении таймаута необходимо выполнить действие, которое сформирует перехваченное сообщение, отличное от однотипных. После этого возобновятся перехваты однотипных сообщений.

- Группа параметров **Менеджер сообщений** (формирование отчетов):

  - **Максимальное время на запись одного отчёта в спул (с)** – максимальное время в секундах, отводимое на запись одного отчёта в спулы. Значение по умолчанию: 0. Рекомендуется оставить значение по умолчанию.

- Группа параметров **HTTP-спул сообщений** (настройки отправки сообщений в **mailfilter** по протоколу HTTP):

  - **Включить** – включает передачу сообщений по протоколу HTTP. Принимает значение **true** и **false**. Значение по умолчанию: **true**. Следует оставить значение **true**, а в качестве значения параметра **enable** секции **SMTP-спул сообщений** установить **false**.

  - **Адрес сервиса (URL)** – URL-ресурс с компонентом **http_reporter**. Значение по умолчанию: **http://127.0.0.1:3010/spool**.

  - **Отладка** – включение вывода отладочной информации. Принимает значение **true** и **false**. Значение по умолчанию: **false** (вывод отладочной информации выключен).

  - **Таймаут соединения (с)** – время ожидания соединения с HTTP-спулом в секундах. Значение по умолчанию: 10.

- **Таймаут обмена данными (с)** – время ожидания ответа на запросы пользователя в секундах. Значение по умолчанию: 10.

- Группа параметров **SMTP-спул сообщений** (настройка записи в спулы сервиса **sender**):

  - **Включить SMTP-спул** – запись сообщений, генерируемых KEO DLP Traffic Analyzer, в спул сервиса **sender**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**. Следует оставить значение **true**, а в качестве значения параметра **enable** секции **HTTP-спул сообщений** установить **false**.

  - **Путь к каталогу SMTP-спула** – путь к каталогу SMTP-спула. Значение по умолчанию: **${smap-settings/common/smap-home}/spool/smap-send/**.

  - **Иерархические делители SMTP-спула сообщений** – иерархические делители SMTP-спула сообщений. В качестве значения используется убывающий ряд натуральных чисел, разделенных пробелами. Значение по умолчанию: **3600 700 50**.

  - **Слоты SMTP-спула сообщений** – слоты спула. В качестве значения используется ряд имён вида **norm<n>**, разделённых пробелами, где <n> – натуральные числа. Значение по умолчанию: **norm4 norm5 norm6**.

  - **Адрес, записываемый в поле FROM SMTP-конверта при помещении сообщения в спул** – адрес, записываемый в поле FROM SMTP-конверта при помещении сообщения в спул. Значение по умолчанию: **trafficagent@example.com**. Следует установить актуальное значение.

  - **Адрес, записываемый в поле RCPT SMTP-конверта при помещении сообщения в спул** – адрес или адреса, записываемые в поле RCPT SMTP-конверта при помещении сообщения в спул. Значение по умолчанию: **dozor@example.com**. Следует установить актуальное значение.

  - **Адрес SMTP-сервера** – доменное имя или IP-адрес узла кластера KEO DLP, имеющего роль **Фильтр почтового потока**. Значение по умолчанию: **localhost**. Следует установить актуальное значение.

  - **Порт для подключения к узлу server-name** – порт для подключения к узлу, указанному в предыдущем параметре. Значение по умолчанию: 1025. Следует установить актуальное значение порта, на котором почтовый фильтр ожидает соединения (должно совпадать со значением, указанным в конфигурационном файле **smtp-gw.conf**, по умолчанию – 1025).

  - **Протокол SMTP-сервера** – тип сервера, который используется для отправки перехваченных пакетов. Значение по умолчанию **SMTP**. Для зашифрованных соединений можно выбрать расширения **SMTPS** или **STARTTLS**.

  - **Количество повторных попыток подключения при возникновении ошибок** – количество повторных попыток подключения при возникновении ошибок. Значение по умолчанию: 5.

  - **Действие при ошибке отправки** – действие при ошибке. Принимает следующие значения: **Сменить профиль отправки**, **Продолжать попытки отправить**, **Переместить сообщение в очередь ошибок** и **Удалить сообщение**. Значение по умолчанию: **Продолжать попытки отправить** (повторить попытку подключения).

- **Версия заголовков писем в спуле** – версия заголовков писем в спуле. Значение по умолчанию: 2.6.

- Группа параметров **Лицензирование продукта** (параметры соединения с сервером лицензирования):

  - **Адрес сервера лицензий (URL)** – URL для соединения с сервером лицензирования. Следует указать значение вида **https://<master_host>:3004/license/dozor/modules/traffic-agent**, где **<master_host>** – FQDN или IP-адрес master-узла.

A.1.4. Производительность

JVM сервиса выполнения действий над сообщениями в архиве:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти, выделяемой сервису выполнения действий над сообщениями в архиве. Значение по умолчанию: 512.

JVM сервера выполнения действий по обработке медиаданных:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервиса выполнения действий по обработке медиаданных. Значение по умолчанию: 512 Мб.

Производительность сервиса отпечатков краулера:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-snapshot**. Значение по умолчанию: 2048.

Сервис поиска данных краулером:

- **Максимальное время на установку соединения (с)** – максимальное время в секундах на установку соединения с удаленным ресурсом. Значение по умолчанию: 600.

- **Максимальное время ожидания ответа при чтении/записи (с)** – максимальное время ожидания ответа от удаленного ресурса при чтении/записи в секундах. Значение по умолчанию: 120.

- **Таймаут сетевого взаимодействия (с)** – время ожидания в секундах при сетевом взаимодействии с удаленным ресурсом. Значение по умолчанию: 0.

Производительность сервиса поиска данных краулером:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-scanner**. Значение по умолчанию: 2048.

Запись данных в архив:

- **Количество потоков для обработки данных высокого приоритета** – максимальное количество потоков, используемых сервисом **archiver** для чтения и обработки событий информационной безопасности и сообщений, предназначенных для размещения в ФХ и БД архива. Значение по умолчанию: 5.

- **Количество потоков для обработки данных низкого приоритета** – максимальное количество потоков, используемых сервисом **archiver** для чтения и обработки информации об изменении уровня доверия. Значение по умолчанию: 2.

- **Таймаут при взаимодействии с сервисом управления Досье (с)** – время ожидания в секундах при взаимодействии с сервисом управления Досье. Значение по умолчанию: 60.

JVM сервиса анализа поведения:

- **Максимально доступное количество оперативной памяти (МБ)** – максимально доступное количество оперативной памяти в мегабайтах, выделяемой для сервиса анализа поведения. Значение по умолчанию: 4096.

Коннектор сервиса работы с цифровыми отпечатками:

- **Минимальный размер текста для проверки (Б)** – минимальный размер текста для проверки (в байтах). Значение по умолчанию: 1024.

- **Минимальный размер изображения для проверки (Б)** – минимальный размер изображения для проверки (в байтах). Значение по умолчанию: 1024.

- **Минимальный размер таблицы для проверки (Б)** – минимальный размер таблицы для проверки (в байтах). Значение по умолчанию: 1024.

- **Минимальный размер бинарных данных для проверки (Б)** – минимальный размер бинарных данных для проверки (в байтах). Значение по умолчанию: 1024.

Сервис контроля идентификаторов:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти, используемое сервером (в МБ). Значение по умолчанию: 1024. Рекомендуемое значение: 4096 или более. Значение не может быть меньше 512.

- **Максимальное количество одновременно обрабатываемых клиентских запросов** – максимальное количество одновременно обрабатываемых клиентских запросов. Значение по умолчанию: 50.

- **Максимальное количество потоков в пуле** – максимальное количество потоков в пуле. Значение по умолчанию: 50.

- **Размер пула потоков** – количество служебных потоков сервера. Значение по умолчанию: 25.

Производительность сервиса поиска и индексации OpenSearch:

- **Размер памяти (ГБ)** – объём оперативной памяти в гигабайтах, выделяемой для сервиса **opensearch**. Значение по умолчанию: 4. Рекомендуется увеличить это значение на столько, сколько десятков миллионов сообщений содержится в архиве. Максимально допустимое значение – половина оперативной памяти сервера, но не более 128 ГБ.

- **Ограничение direct-памяти (ГБ)** – максимальный объём буфера ввода/вывода клиентских запросов в гигабайтах. Значение по умолчанию: 4.

JVM сервиса индексации сообщений в архиве:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервиса **indexer-ng**. Значение по умолчанию: 2048.

Сервис распознавания текста изображений:

- **Режим распознавания** – способ распознавания текста изображений. Принимает значения **Быстрый** и **Тщательный**. Значение по умолчанию: **Быстрый**.
- **Использовать сервис skvt-cassandra для кэширования результатов распознавания** – включает использование сервиса **skvt-cassandra** для кэширования результатов распознавания. По умолчанию включено.
- **Максимальное количество потоков обработки изображения** – максимальное число потоков, которые могут выполнять обработку изображений одновременно. Значение по умолчанию: 20.
- **Максимальное количество одновременно подключенных клиентов** – максимальное количество одновременно обрабатываемых запросов на распознавание текста (обработку изображений) от сервиса **mailfilter**. Остальные запросы попадают в очередь и остаются там до тех пор, пока не освободится один из потоков, регулируемых параметром **Максимальное количество потоков обработки изображения**. Значение по умолчанию: 1000.

Сервис доступа к Досье:

- **Количество соединений с БД** – количество соединений сервиса **abook-daemon** с БД политики. Значение по умолчанию: 10.

JVM сервиса доступа к Досье:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса доступа к Досье. Значение по умолчанию: 512.

Сервис репликации Досье на подчиненных узлах:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу **abook-slave**. Значение по умолчанию: 1024.

JVM файлового хранилища:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса **filestorage-ng**. Значение по умолчанию: 256.

JVM сервиса хранения и индексации событий и инцидентов:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса хранения и индексации событий и инцидентов. Значение по умолчанию: 512.

Сервис цифровых отпечатков:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса цифровых отпечатков. По умолчанию используется 2048 МБ.

Отладка доступа к сообщениям в архиве:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса **archive-server**. Значение по умолчанию: 512.

JVM сервиса **Расследование**:

- **Максимальное количество оперативной памяти (МБ)** – максимально доступное количество оперативной памяти в мегабайтах, выделяемой для сервиса **Расследование**. Значение по умолчанию: 1024.

JVM веб-сервера:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для веб-сервера. Значение по умолчанию: 512.

Производительность центра управления краулером:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-ccc**. Значение по умолчанию: 2048.

JVM локального веб-сервера:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для локального веб-сервера. Значение по умолчанию: 512.

Сервис распознавания речи:

- **Максимальное количество обработчиков, выполняющих распознавание** – количество экземпляров обработчика, одновременно выполняющих распознавание речи. Для каждого экземпляра организуется очередь сообщений для обработки, максимальное количество сообщений в очереди определяется параметром **Размер очереди заданий**. При использовании ЦП рекомендуется оставить значение по умолчанию. При использовании графических процессоров рекомендуется устанавливать значение, равное количеству графических процессоров. Значение по умолчанию: 1. При значении 0 количество экземпляров обработчика будет равно количеству ядер процессора.

- **Количество потоков для приема сообщений** – количество внутренних сетевых потоков сервиса распознавания речи, используемых для приема сообщений для обработки. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству логических ядер центрального процессора). Рекомендуется использовать значение по умолчанию или меньше.

- **Размер очереди заданий** – максимальное количество сообщений для обработки для каждого экземпляра обработчика. Значение по умолчанию: 0 (фактически будет ис-

пользоваться значение 100). При использовании нескольких экземпляров обработчика и/или графических процессоров рекомендуется устанавливать значение 1000.

- **Количество потоков для работы с обработчиками** – количество внутренних сетевых потоков сервиса распознавания речи, которые отправляют результаты распознавания на вывод во внешний интерфейс. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству логических ядер центрального процессора). Рекомендуется использовать значение по умолчанию или меньше.

- **Количество GPU** – количество графических процессоров, используемых для распознавания речи. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству графических процессоров на сервере).

- **Максимальный размер запроса** – максимально допустимый размер сообщения в мегабайтах, принимаемый сервисом определения речи на обработку. Значение по умолчанию: 100.

- **Время ожидания ответа** – максимальное время (в секундах) ожидания экземпляром обработчика ответа от сервиса распознавания, после которого запрос обработчика будет перезагружен. Значение по умолчанию: 120.

Сервис интеграции:

- **Таймаут взаимодействия с веб-сервером** – таймаут в секундах, в течение которого сервис интеграции ожидает ответа от веб-сервера. Если веб-сервер не успеет ответить – сервис интеграции возвращает внешнему клиенту ошибку HTTP 502. Значение по умолчанию: 60.

- **Таймаут взаимодействия с сервером лицензирования** – таймаут в секундах, в течение которого сервис интеграции ожидает ответа от сервера лицензирования. Если сервис активен, то он запрашивает лицензию раз в час. Если сервис не получил лицензию и/или неактивен, то он запрашивает лицензию раз в пять минут. Неактивный сервис не принимает запросов к API. Значение по умолчанию: 60.

JVM сервиса интеграции:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса интеграции. Значение по умолчанию: 512.

Сервис фильтрации сообщений:

- **Количество потоков обработки спула сообщений** – количество потоков обработки спула сообщений. Значение по умолчанию: 5.

- **Таймаут на обработку сообщения (с)** – таймаут на общую обработку (распаковку, извлечение вложений и обработку политикой) сообщения в секундах. Значение по умолчанию: 600.

- **Доля времени на распаковку сообщения (в процентах от общего времени на обработку)** – доля времени на распаковку сообщения от общего времени на обработку, выраженная в процентах. Значение по умолчанию: 50.

- **Таймаут при взаимодействии с сервером лицензирования (с)** – время ожидания в секундах при взаимодействии с сервером лицензирования. Значение по умолчанию: 60.

- **Таймаут при взаимодействии с Tikaserver (с)** – время ожидания в секундах при взаимодействии с сервером **Tika**. Значение по умолчанию: 60.

- **Таймаут при взаимодействии с сервером определения графических объектов (с)** – время ожидания в секундах при взаимодействии с сервером определения графических объектов. Значение по умолчанию: 60. Рекомендуется задать значение, равное 30.

- **Таймаут при взаимодействии с сервисом управления Досье (с)** – время ожидания в секундах при взаимодействии с сервисом управления Досье. Значение по умолчанию: 60.

- **Максимальное время проверки сообщений типа email** – максимальное время обработки сообщений типа **email** политикой. На все остальные типы сообщений данный параметр не влияет.

  Принимает значения **Выключено** и **Настройки ограничения времени**.

  При значении **Выключено** ограничение отсутствует.

  При значении **Настройки ограничения времени** будет ограничено максимальное время проверки сообщений. Будут доступны следующие параметры:

  - **Максимальное время работы набора условий (с)** – максимальное время работы набора условий. Значение по умолчанию: 30 сек.

  - **Максимальное время работы политики (с)** – максимальное время работы политики. Значение по умолчанию: 600 сек.

  - **Действие по наступлению ограничения** – действие по наступлению ограничения. Возможные следующие варианты:

    - **Отправить, используя профиль отправки** – отправляет письмо, используя профиль отправки, который можно указать в поле, открывающемся при выборе этого действия.

    - **Переместить в очередь ошибок** – приводит к перемещению письма в спул **mailfilter-err**.

    - **Заблокировать с указанием причины** – перед помещением письма в архив на нем устанавливается пометка **заблокировано**, а в логе указывается причина превышения работы политики или условия.

  - **Скрипт для запуска при наступлении ограничения** – скрипт для запуска при наступлении ограничения. Указывается путь к выполняемому скрипту. При выполнении скрипта в качестве параметров ему будет передаваться путь к сообщению на диске. Данная возможность может использоваться для сбора дополнительной информации о проблеме, например для сбора данных о загрузке системы, работающих процессах и т.д.

- **Максимальное время проверки сообщений остальных типов** – максимальное время обработки сообщений от перехватчиков (KEO DLP Endpoint Agent, KEO DLP Traffic Analyzer, File Crawler) политикой.

  Принимает значения **Выключено** и **Настройки ограничения времени**.

  При значении **Выключено** ограничение отсутствует.

  При значении **Настройки ограничения времени** будет ограничено максимальное время проверки сообщений. Будут доступны следующие параметры:

  - **Максимальное время работы набора условий (с)** – максимальное время работы набора условий. Значение по умолчанию: 30 сек.
  - **Максимальное время работы политики (с)** – максимальное время работы политики. Значение по умолчанию: 600 сек.
  - **Действие по наступлению ограничения** – действие по наступлению ограничения. Возможные следующие варианты:
    - **Переместить в очередь ошибок** – приводит к перемещению письма в спул **mailfilter-err**.
    - **Заблокировать с указанием причины** – перед помещением письма в архив на нем устанавливается пометка **заблокировано**, а в логе указывается причина превышения работы политики или условия.
  - **Скрипт для запуска при наступлении ограничения** – скрипт для запуска при наступлении ограничения. Указывается путь к выполняемому скрипту. При выполнении скрипта в качестве параметров ему будет передаваться путь к сообщению на диске. Данная возможность может использоваться для сбора дополнительной информации о проблеме, например для сбора данных о загрузке системы, работающих процессах и т.д.

JVM сервиса фильтрации сообщений:

- **Максимально доступное количество оперативной памяти (МБ)** – максимально доступное количество оперативной памяти в мегабайтах, выделяемой для сервиса фильтрации сообщений. Значение по умолчанию: 4096.

  Внимание!

  *Значение параметра **Максимально доступное количество оперативной памяти (МБ)** должно быть меньше объема оперативной памяти виртуальной машины Java.*

Сервер агентов:

- **Максимальное количество оперативной памяти (МБ)** – максимальный объём памяти в мегабайтах, выделяемой процессу сервера агентов. Значение по умолчанию: 512.

Сервис определения графических объектов:

- **Максимальное количество обработчиков, выполняющих распознавание** – количество экземпляров обработчика, одновременно выполняющих распознавание графических объектов. Для каждого экземпляра организуется очередь сообщений для обработки, максимальное количество сообщений в очереди – 100. Значение по умолчанию: 1. При значении 0 количество экземпляров обработчика будет равно количеству ядер процессора.

- **Количество потоков для приема сообщений** – количество внутренних сетевых потоков сервиса распознавания графических объектов, используемых для приема сообщений для обработки. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству логических ядер центрального процессора). Рекомендуется установить значение по умолчанию или меньше используемых для распознавания ядер процессора.

- **Размер очереди заданий** – максимальное количество сообщений для обработки для каждого экземпляра обработчика. Значение по умолчанию: 0 (фактически будет использоваться значение 100). При использовании нескольких экземпляров обработчика и/или графических процессоров рекомендуется устанавливать значение 1000.

- **Количество потоков для работы с обработчиками** – количество внутренних сетевых потоков сервиса распознавания графических объектов, которые отправляют результаты распознавания на вывод во внешний интерфейс. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству логических ядер центрального процессора). Рекомендуется установить значение по умолчанию или меньше используемых для распознавания ядер процессора.

- **Количество GPU** – количество графических процессоров, используемых для распознавания графических объектов. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству графических процессоров на сервере).

- **Максимальный размер запроса** – максимально допустимый размер сообщения в мегабайтах, принимаемый сервисом определения графических объектов на обработку. Значение по умолчанию: 100.

- **Время ожидания ответа** – максимальное время (в секундах) ожидания экземпляром обработчика ответа от сервиса распознавания, после которого запрос обработчика будет перезагружен. Значение по умолчанию: 0 (фактически будет использоваться значение 120).

- **Настройки ограничений на параметры графических изображений** – настройки ограничений на параметры графических изображений:

  - **Минимальный размер изображения по вертикали, в пикселях** – минимальный размер изображения по вертикали в пикселях. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** ограничение отсутствует.

  - **Минимальный размер изображения по горизонтали (пикселей)** – минимальный размер изображения по горизонтали в пикселях. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** ограничение отсутствует.

- **Максимальная высота изображения (пикселей)** – максимальная высота изображения в пикселях. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** ограничение отсутствует.
- **Максимальная ширина изображения (пикселей)** – максимальная ширина изображения в пикселях. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** ограничение отсутствует.
- **Минимальный размер изображения (байт)** – минимальный размер файла графического изображения в байтах. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** будет действовать максимальное ограничение в 100 МБ.
- **Максимальный размер изображения (байт)** – максимальный размер файла графического изображения в байтах. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** будет действовать максимальное ограничение в 100 МБ.

Сервис обработки данных краулером:

- **Максимальное количество одновременно обрабатываемых ресурсов** – максимальное количество одновременно обрабатываемых ресурсов в рамках работающих задач. Значение по умолчанию: 10.
- **Максимальное количество попыток подключения к ресурсу** – максимальное количество попыток подключения к ресурсу. Значение по умолчанию: 2.
- **Таймаут между попытками подключения (с)** – таймаут в секундах между попытками подключения. Значение по умолчанию: 10.
- **Максимальное время ожидания ответа о результатах обработки** – время ожидания ответа в секундах при обработке файла от сервиса **mailfilter**. Значение по умолчанию: 900.
- **Максимальное время на установку соединения (с)** – максимальное время в секундах на установку соединения с удаленным ресурсом. Значение по умолчанию: 600.
- **Максимальное время ожидания ответа при чтении/записи (с)** – максимальное время ожидания ответа от удаленного ресурса при чтении/записи в секундах. Значение по умолчанию: 120.
- **Таймаут сетевого взаимодействия (с)** – время ожидания в секундах при сетевом взаимодействии с удаленным ресурсом. Значение по умолчанию: 0.

Производительность сервиса обработки данных краулером:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-processor**. Значение по умолчанию: 2048.

JVM сервера управления агентами:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервера управления агентами. Значение по умолчанию: 1024 Мб.

Производительность прокси центра управления краулером:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-pccc**. Значение по умолчанию: 2048.

Сервис отправки сообщений:

- **Количество процессов** – количество потоков, используемых для отправки сообщений. Значение по умолчанию: 2.

JVM сервиса отправки сообщений:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервиса отправки сообщений. Значение по умолчанию: 256.

Прием сообщений:

- **Отвергать сообщения при загрузке системы более** – отвергать сообщения при загрузке системы, превышающей указанное значение. Значение по умолчанию: 20. При достижении этого порога в журнальный файл **$smap_home/log/smtp_gw.log** записывается сообщение вида **Feb 14 12:23:18 bvm193 smtp-gw-1025[8058]: Load average too high: refusing email from 10.31.7.193:42465** и SMTP-прокси перестает принимать новые сообщения.

- **Отвергать соединения при загрузке системы более** – отвергать соединения при загрузке системы, превышающей указанное значение. Значение по умолчанию: 30. При достижении этого порога в журнальный файл **$smap_home/log/smtp_gw.log** записывается сообщение вида **Feb 14 12:22:56 bvm193 smtp-gw-1025[7427]: Load average too high: rejecting connection from 10.31.7.193:42433**, а также отвергается установка новых соединений с SMTP-прокси.

- **Максимальный размер принимаемого сообщения (МБ)** – максимально допустимый размер принимаемого сообщения (в мегабайтах). Данным параметром можно снять ограничение на размер принимаемого сообщения, установив значение 0. Значение параметра по умолчанию: 40 Мб.

- **Количество процессов SMTP-прокси** – количество процессов SMTP-прокси. Значение по умолчанию: 10.

Сервис извлечения текстовых данных:

- **Максимальный размер используемой оперативной памяти (МБ)** – максимальный размер используемой оперативной памяти (МБ). По умолчанию используется 2048 МБ.

Отладка сервиса построения отчетов:

- **Максимальное количество оперативной памяти (Мб)** – максимальное количество оперативной памяти в Мб, потребляемой сервисом **report-server**. Значение по умолчанию: 512.

A.2. Расширенные настройки

A.2.1. Администрирование системы

A.2.1.1. Общее

Сервис лицензирования:

- **Вывод отладочной информации** – вывод отладочной информации о работе сервиса. По умолчанию выключено.
- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервер лицензирования ожидает соединения. Значение по умолчанию: 3004.
- **Директория для хранения данных** – путь к каталогу для хранения данных лицензии. Значение по умолчанию: **/data/spool/dozor/license**.
- **Подсчет активных адресов в архиве** – группа параметров пересчета активных адресов в архиве:
  - **Периодичность пересчета (с)** – периодичность пересчета в секундах. Значение по умолчанию: 86400.

Отладка сервиса лицензирования:

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **license-server** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Сервис отправки диагностической информации:

- **Включение отправки диагностической информации вендору** – использовать отправку диагностической информации вендору. По умолчанию выключено.
- **Адрес отправителя** – информация об отправителе:
  - **Имя владельца почтового ящика** – имя персоны, которой принадлежит почтовый ящик. Допустимо любое значение. Значение по умолчанию не задано.
  - **Имя почтового ящика** – уникальная комбинация букв, цифр и служебных символов, расположенная перед доменом. Следует указать имя актуального почтового ящика, с которого будет вестись отправка диагностической информации. Значение по умолчанию: **dozor**.
  - **Имя почтового домена** – имя домена, в котором находится почтовый ящик, указанный в предыдущем параметре. Значение по умолчанию: **dozor**.
- **Адреса получателей** – информация о получателях (можно задать несколько получателей с помощью кнопки **Добавить**):
  - **Имя владельца почтового ящика** – имя персоны, которой принадлежит почтовый ящик. Допустимо любое значение. Значение по умолчанию не задано.

- **Имя почтового ящика** – уникальная комбинация букв, цифр и служебных символов, расположенная перед доменом. Следует указать имя актуального почтового ящика, с которого будет вестись отправка диагностической информации. Значение по умолчанию: **dozor**.
- **Имя почтового домена** – имя домена, в котором находится почтовый ящик, указанный в предыдущем параметре. Значение по умолчанию: **dozor**.

- **Адрес/порт SMTP-сервера** – информация о SMTP-сервере:
  - **Сетевой адрес** – доменное имя или IP-адрес SMTP-сервера. Значение по умолчанию: 127.0.0.1.
  - **Номер порта** – порт, на котором SMTP-сервер ожидает соединения. Значение по умолчанию: 25.

СУБД Oracle:

- **ORACLE_BASE** – переменная окружения ORACLE_BASE. По умолчанию задано значение: **/usr/lib/oracle**.
- **ORACLE_HOME** – переменная окружения ORACLE_HOME. По умолчанию задано значение: **${smap-settings/oracle/oracle-base}/12.2/client64**.
- **NLS_LANG** – переменная окружения NLS_LANG. По умолчанию задано значение: **RUSSIAN_RUSSIA.AL32UTF8**.
- **NLS_DATE_FORMAT** – переменная окружения NLS_DATE_FORMAT. По умолчанию задан формат: **DD/MM/YYYY**.
- **ORA_NLS33** – переменная окружения ORA_NLS33. По умолчанию задано значение: **${oracle-home}/ocommon/nls/admin/data**.
- **SQL*Plus version verify** – включение/выключение проверки версии клиента Oracle при развертывании схемы. При включенном параметре происходит проверка номера версии скрипта SQL*Plus. В случае если номер версии SQL*Plus меньше, чем 11.2, выводится сообщение об ошибке:

  ```
  Incorrect version of SQL*Plus. Need 11.2 at least
  ```

  и скрипт прекращает свое выполнение. Если же версия SQL*Plus не соответствует версии СУБД, появляется предупреждение о несоответствии версий:

  ```
  SQL*Plus version not equal RDBMS version
  SQL*Plus version: версия клиента
  RDBMS version: версия сервера
  ```

  и выполнение скрипта продолжается. При выключенном параметре развертывание продолжается, несмотря на любые возможные несоответствия. По умолчанию данный параметр включен.

Примечание

Вышеуказанные параметры предназначены для настройки клиента Oracle. За рекомендациями относительно настройки СУБД Oracle следует обращаться к соответствующей документации.

Общие настройки системы:

- **Каталог для временных файлов** – каталог для хранения временных файлов, создаваемых в процессе обработки сообщения. Значение по умолчанию: **/data/temp**.
- **Вывод отладочной информации** – вывод отладочной информации о ходе работы системы. Включение параметра приводит к сбору информации о ходе работы системы. При этом собирается большой объем информации, что может значительно замедлить работу системы. Рекомендуемое время работы с включенным параметром – не более 20 минут. Включение параметра на более продолжительное время сильно увеличит размер отладочного файла журнала.
- **Вывод vID сообщения в каждой строке отладочной информации** – включает вывод vID сообщения в каждой строке отладочной информации (параметр не работает для сервиса **mailfilter**).

  Примечание

  *Сервис **mailfilter** всегда выполняет вывод vID сообщения.*

  Принимает значения **true** (включено) и **false** (выключено). По умолчанию флажок установлен.
- **LANG** – региональные установки, используемые в подсистемах KEO DLP. Значение по умолчанию: **Русский**. Используются значения: **Английский** и **Русский**.
- **LC_MESSAGES** – язык, на котором выводятся сообщения интерфейса KEO DLP. Значение по умолчанию: **ru_RU**.
- **URL для формирования ссылок на систему** – URL для формирования ссылок, использующихся в работе модулей проведения внутренних расследований инцидентов ИБ (**Расследование**) и распознавания речи. По умолчанию указано **https://dozor**.

  Значение задается в соответствии со следующими принципами:

  1. Для активации ссылок в стенограмме с результатами распознавания речи – IP-адрес узла KEO DLP, которому назначены роли **Сервер управления** либо **Локальный веб-сервер**.
  2. Для активации ссылок в схемах и отчетах по делу, которые относятся к модулю **Расследование** – IP-адрес сервера управления KEO DLP.
- **Общая настройка журналирования** – настройки параметров **Уровень журналирования** и **Использование syslog**.

- **Уровень журналирования** – степень детализации ведения журнальных файлов. В качестве значения можно выбрать один из следующих параметров в раскрывающемся списке:
  - Журналирование отключено;
  - Обычный;
  - Повышенный;
  - Отладочный.
- **Использование syslog** – включает ведение журналов с помощью протокола syslog, а также определяет способ использования данного протокола. Значение по умолчанию **отключено** (использование **syslog** отключено). Есть возможность выбора из раскрывающегося списка значения **facility**. Параметр **facility** определяет тип программы, которая выполняет запись сообщений в журнальный файл ОС. При выборе значения **facility** открываются следующие два поля под общим заголовком **facility**:
  - **Служба syslog** – предоставляет выбор значения из следующего списка:
    - LOG_AUTHPRIV – сообщения о безопасности/авторизации
    - LOG_CRON – планировщик
    - LOG_DAEMON – другие системные демоны, кроме планировщика
    - LOG_LOCAL0 – значение зарезервировано
    - LOG_LOCAL1 – значение зарезервировано
    - LOG_LOCAL2 – значение зарезервировано
    - LOG_LOCAL3 – значение зарезервировано
    - LOG_LOCAL4 – значение зарезервировано
    - LOG_LOCAL5 – значение зарезервировано
    - LOG_LOCAL6 – значение зарезервировано
    - LOG_LOCAL7 – значение зарезервировано
    - LOG_MAIL – почтовая подсистема
    - LOG_USER – общие сообщения на уровне пользователя
  - **Префикс программы для вывода syslog** – необходимо задавать вручную. Задание префиксов для различных программных средств дает возможность различать записи этих программных средств в общем файле журналирования. Рекомендуется задавать префикс схожий с именем программного средства.

- **Адрес отправителя в системных сообщениях** – адрес отправителя в системных сообщениях. Например, **dozor@dozor**.

- **Имя владельца почтового ящика** – имя персоны, которой принадлежит почтовый ящик;
- **Имя почтового ящика** – уникальная комбинация букв, цифр и служебных символов, расположенная перед доменом. Значение по умолчанию: **dozor**;
- **Имя почтового домена** – название почтового домена. Значение по умолчанию: **dozor**.

- **Адрес получателей в системных сообщениях** – адреса получателей в системных сообщениях. Можно задать список адресов. Для добавления адреса необходимо нажать кнопку рядом с параметром **Адрес получателей в системных сообщениях**. Для удаления адреса необходимо нажать кнопку рядом с параметром **Адрес получателей в системных сообщениях**.

  Для каждого адреса задаются следующие параметры:

  - **Имя владельца почтового ящика** – имя персоны, которой принадлежит почтовый ящик;
  - **Имя почтового ящика** – уникальная комбинация букв, цифр и служебных символов, расположенная перед доменом. Значение по умолчанию: **dozor**;
  - **Имя почтового домена** – название почтового домена. Значение по умолчанию: **dozor**.

Параметры сервиса журнала journald:

- **Максимальный размер журнала (МБ)** – максимальный размер журнала **journald** в МБ, при превышении которого более старые записи будут удалены. Рекомендуется выделять как минимум половину свободного пространства раздела **/var**. Значение по умолчанию: 4096.

Журнал централизованного обмена сообщениями и планирования задач:

- **Уровень журналирования сервиса** – степень детализации ведения журнальных файлов сервиса. В качестве значения можно выбрать один из следующих параметров в раскрывающемся списке:
  - inherit – наследуемый (или стандартный).
  - Уровень журналирования – предоставляет выбор следующих дополнительных возможностей:
    - Журналирование отключено;
    - Обычный;
    - Повышенный;
    - Отладочный.
- **Использование syslog** – включает ведение журналов с помощью протокола syslog, а также определяет способ использования данного протокола. В качестве значения

параметра необходимо выбрать в раскрывающемся списке режим использования сервиса **syslog**:

- inherit – наследуемый (или стандартный).
- override – переопределяемый. Открывает дополнительное поле **override** со значением по умолчанию **отключено** (использование **syslog** отключено) и возможностью выбора из раскрывающегося списка значения **facility**. Параметр **facility** определяет тип программы, которая выполняет запись сообщений в журнальный файл ОС. При выборе значения **facility** открываются следующие два поля под общим заголовком **facility**:
  - Служба syslog – предоставляет выбор значения из следующего списка:
    - LOG_AUTHPRIV – сообщения о безопасности/авторизации;
    - LOG_CRON – планировщик;
    - LOG_DAEMON – другие системные демоны, кроме планировщика;
    - LOG_LOCAL0 – значение зарезервировано;
    - LOG_LOCAL1 – значение зарезервировано;
    - LOG_LOCAL2 – значение зарезервировано;
    - LOG_LOCAL3 – значение зарезервировано;
    - LOG_LOCAL4 – значение зарезервировано;
    - LOG_LOCAL5 – значение зарезервировано;
    - LOG_LOCAL6 – значение зарезервировано;
    - LOG_LOCAL7 – значение зарезервировано;
    - LOG_MAIL – почтовая подсистема;
    - LOG_USER – общие сообщения на уровне пользователя.
  - Префикс программы для вывода syslog – необходимо задавать вручную. Задание префиксов для различных программных средств дает возможность различать записи этих программных средств в общем файле журналирования. Рекомендуется задавать префикс схожий с именем программного средства.

- **Особый файл журнала для сервиса** – особый файл журнала для сервиса. При выборе из раскрывающегося списка значения параметра **none** (значение по умолчанию) особый файл журнала не используется. При выборе значения параметра **path** появляется дополнительное одноименное поле для ввода пути к файлу журнала.
- **Настройки журналирования по facility** – настройки журналирования по типу программы, которая выполняет запись сообщений в журнальный файл ОС.

Для различных программных средств (facilities) есть возможность устанавливать настройки, отличающиеся от общих. Есть возможность задать следующие настройки журналирования для различных программных средств:

- **Название facility** – название типа программы, которая выполняет запись сообщений в журнальный файл ОС.

- **Уровень журналирования facility** – задание уровня журналирования типа программы. По умолчанию имеет значение **inherit** (наследуемый или стандартный). Из раскрывающегося списка есть возможность выбора значения **override** (переопределяемый). Выбор переопределяемых уровней журналирования аналогичен выбору общих настроек уровня журналирования (описано выше).

- **Использование syslog** – включает ведение журналов с помощью протокола syslog, а также определяет способ использования данного протокола. По умолчанию имеет значение **inherit** (наследуемый или стандартный). Из раскрывающегося списка есть возможность выбора значения **override** (переопределяемый). Выбор переопределяемых параметров использования syslog аналогичен выбору общих настроек использования syslog (описано выше).

- **Особый файл журнала для facility** – задание особого файла журнала для типа программы. По умолчанию имеет значение **inherit** (наследуемый или стандартный). Из раскрывающегося списка есть возможность выбора значения **override** (переопределяемый). При выборе этого значения появляется поле **override** для задания пути к файлу.

A.2.1.2. Интерфейс

Общие настройки системы:

- **Уровень журналирования** – степень детализации ведения журнальных файлов. По умолчанию имеет значение **inherit** (наследуемый или стандартный). Из раскрывающегося списка есть возможность выбора значения **override** (переопределяемый). Выбор переопределяемых уровней журналирования аналогичен выбору общих настроек уровня журналирования (описано выше).

- **Использование syslog** – включает ведение журналов с помощью протокола syslog, а также определяет способ использования данного протокола. По умолчанию имеет значение **inherit** (наследуемый или стандартный). Из раскрывающегося списка есть возможность выбора значения **override** (переопределяемый). Выбор переопределяемых параметров использования syslog аналогичен выбору общих настроек использования syslog (описано выше).

Сервис отображения диаграмм и графиков Grafana:

- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервис **grafana** ожидает соединения. Значение по умолчанию: 3900.

Веб-сервер:

- **HTTPS-порт** – порт, используемый протоколом HTTPS. Значение по умолчанию: 443.

- **Путь к хранилищу ключей и сертификатов** – путь к jks-контейнеру с ключами и сертификатами УЦ организации.

- **Пароль к хранилищу ключей и сертификатов** – пароль от этого контейнера.

Внимание!

*В случае использования параметров **Путь к хранилищу ключей и сертификатов** и **Пароль к хранилищу ключей и сертификатов**, после сохранения и применения конфигурации необходимо вручную перезапустить сервис **webserver**.*

- **Не показывать ошибки в интерфейсе** – включает или выключает отображение ошибок в интерфейсе KEO DLP. По умолчанию флажок установлен.
- **Срок хранения журналов действий** – срок хранения журналов с действиями пользователей. Принимает следующие значения: **Всегда**, **День**, **Неделя**, **Месяц**, **Год**. Значение по умолчанию: **Год**.
- **Запись журналов действий в syslog в формате CEF** – включает запись действий пользователей в БД политики и в журнал ОС syslog в формате CEF, определенном как стандарт для отправки информации в SIEM-системы. CEF использует syslog в качестве транспортного механизма. В общем случае запись CEF имеет вид:

```
CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class
ID|Name|Severity|[Extension]
```

Поле **CEF: Version** является обязательным. Остальная часть формируется с использованием полей, разделенных символом «|». Также CEF позволяет задать свои собственные поля (**Extension**), определив для них имя (**csNLabel**) и значение (**csN**). Принимает значения **true** (включено) и **false** (выключено). Пример записи журнала при включенном параметре:

```
CEF:0|Organisation|KEO DLP|7.1|authorization|login|Low|end=Jan<space>09<space>2018<space>
13:59:34 suser=super_alex src=vm5.isim.local act=login
```

При значении **false** запись действий пользователей происходит только в БД политики. Значение по умолчанию: **false**.

Примечание

При отправке журналов syslog в формате CEF в SIEM-системы накладываются следующие ограничения на размер записи журнала:

1. *передача по протоколу UDP – не более 1000 байт*
2. *передача по протоколу TCP – не более 4000 байт*

При превышении заданных ограничений размеры записей будут уменьшены до 1000 и 4000 байт соответственно – из конца строки будут удалены лишние символы.

JVM веб-сервера:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для веб-сервера. Значение по умолчанию: 512.
- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **webserver** в случае ошибки исчерпания памяти. По умолчанию выключено.

Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

JVM локального веб-сервера:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для локального веб-сервера. Значение по умолчанию: 512.

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **webserver-local** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Локальный веб-сервер:

- **Доменная аутентификация через Kerberos** – включает или выключает аутентификацию в KEO DLP под доменной учетной записью без ввода логина и пароля. Используется механизм аутентификации Kerberos. Принимает значения **true** и **false**.

  При значении **true** станет доступна кнопка **Войти через домен**. Таким образом, вход в KEO DLP можно выполнить локальной и доменной учетными записями. Чтобы войти в KEO DLP под учетной записью AD, следует нажать кнопку **Войти через домен**. В этом случае вводить логин и пароль не требуется, т.к. для аутентификации в KEO DLP используются данные учетной записи, уже выполнившей вход в ОС.

  Если системный администратор организации заблокировал учетную запись пользователя в AD, активный сеанс работы такого пользователя в системе будет завершен. После этого откроется окно авторизации KEO DLP.

  Если доменная учетная запись AD не активна, удалена или заблокирована, доступ в KEO DLP под доменной учетной записью запрещен. В этом случае будет выдано соответствующее сообщение об ошибке.

  При значении **false** аутентификация в KEO DLP выполняется только под локальной учетной записью.

  Значение по умолчанию: **false**.

- **Идентификатор службы Kerberos (SPN)** – имя участника службы для Kerberos-соединений. Задается в формате **HTTP/<dozor.fqdn>@<DOMAIN>**, где **<dozor.fqdn>** – FQDN master-узла KEO DLP, **<DOMAIN>** – имя домена. Используется совместно с параметром **Доменная аутентификация через Kerberos**.

Сервер интерфейса администрирования:

- **HTTPS порт** – HTTPS порт для подключения к веб-интерфейсу. По умолчанию используется порт 443.

- **Время жизни HTTP-сессий (мин)** – Время жизни http-сессий в минутах. Если в течение этого времени администратор не проявляет активности (нет ввода с клавиатуры, не двигается мышь и т.п.), то сессия разрывается, для дальнейшей работы администратора требуется его повторная аутентификация. Значение по умолчанию: 180 мин. Значение **Время жизни HTTP-сессий (мин)** не может быть меньше 10.

- **Максимальный размер потребляемой памяти, по достижении которого процесс будет перезапущен (МБ)** – размер оперативной памяти в мегабайтах, используемой процессом, при превышении которого процесс будет перезапущен. Значение по умолчанию: 8192.

A.2.1.3. Мониторинг

Сервер мониторинга:

- **База данных PostgreSQL** – имя схемы соединения с БД, используемой для хранения информации о задачах сервера мониторинга Zabbix. Принимает значения **БД по умолчанию** и **Специальная БД**. Значение по умолчанию: **БД по умолчанию**. При значении **БД по умолчанию** сервис подключается к БД политики.

  Если выбрано значение **Специальная БД**, доступны параметры:

  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.
  - **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.

  Примечание

  При первом подключении к БД и при изменении значения порта сервера мониторинга ***monitor-server*** *проверяет наличие необходимой для работы БД. Если БД отсутствует, выполняется ее создание.*

- **Порт** – порт сервера мониторинга. Значение по умолчанию: 10051.
- **Производительность** – настройки производительности сервера мониторинга. Включает в себя параметры:

  - **Количество предварительно создаваемых процессов poller** – количество предварительно создаваемых процессов, опрашивающих пассивных агентов мониторинга. Значение по умолчанию: 40.
  - **Количество предварительно создаваемых процессов ICMP pinger** – количество предварительно создаваемых процессов, проверяющих доступность узлов в сети с помощью команды
    ping
    . Значение по умолчанию: 5.
  - **Количество предварительно создаваемых процессов poller unreachable** – количество предварительно создаваемых процессов, опрашивающих недоступных пассивных агентов мониторинга. Значение по умолчанию: 10.

- **Количество предварительно создаваемых процессов trapper** – количество предварительно создаваемых процессов, принимающих данные от **Zabbix sender**, активных агентов мониторинга, узлов и прокси. Значение по умолчанию: 10.
- **Количество предварительно создаваемых процессов discoverer** – количество предварительно создаваемых процессов обнаружения устройств. Значение по умолчанию: 1.
- **Количество предварительно создаваемых процессов dbsyncers** – количество предварительно создаваемых процессов синхронизации базы данных, получающих информацию о различных кэшах памяти сервера мониторинга и перемещающих элементы из кэшей во внутреннюю БД. Значение по умолчанию: 5.
- **Периодичность опроса при потере связи с узлом (с)** – определяет частоту проверки узла сети в секундах при его недоступности. Значение по умолчанию: 20.
- **Время отсутствия связи, после которого узел считается недоступным (с)** – время отсутствия связи с узлом сети в секундах, после которого он считается недоступным. Значение по умолчанию: 50.
- **Размер кэша конфигурации (МБ)** – размер кэша в Мб для хранения конфигурации (данных узлов сети, элементов данных и триггеров). Значение по умолчанию: 100.
- **Размер кэша истории (МБ)** – размер разделяемой памяти в Мб для хранения данных истории. Значение по умолчанию: 100.
- **Размер кэша индекса истории (МБ)** – размер разделяемой памяти в Мб для индексации данных записываемой истории в кэш истории.
- **Размер кэша динамики изменений (МБ)** – размер кэша динамики изменений в Мб. Значение по умолчанию: 100.
- **Размер кэша для хранения истории значений (МБ)** – размер кэша для хранения истории значений в Мб. Значение по умолчанию: 100.
- **Периодичность очистки БД (ч)** – периодичность очистки БД сервера мониторинга, выраженная в часах. Необходима для удаления устаревшей информации. Значение по умолчанию: 1.
- **Максимальное количество строк, удаляемых при очистке БД** – максимальное количество строк, удаляемых при очистке БД. Значение по умолчанию: 5000.

- **Настройки оповещения** – настройки оповещений при возникновении проблем на узлах. Включает в себя параметры:
  - **Адрес/порт SMTP-сервера** – информация о SMTP-сервере:
    - **Сетевой адрес** – доменное имя или IP-адрес SMTP-сервера. Значение по умолчанию:127.0.0.1.
    - **Номер порта** – порт, на котором SMTP-сервер ожидает соединения. Значение по умолчанию: 1025.
  - **Отправитель** – адрес отправителя. Значение по умолчанию: **dozor@local**.

- **Адреса для отправки уведомлений о проблемах чрезвычайной критичности** – адрес для отправки уведомлений о проблемах с чрезвычайным уровнем критичности. Значение по умолчанию: **disaster@example.com**.

- **Адреса для отправки уведомлений о проблемах высокой и средней критичности** – адрес для отправки уведомлений о проблемах с высоким и средним уровнем критичности. Значение по умолчанию: **average@example.com**.

- **Адреса для отправки уведомлений о проблемах низкой критичности** – адрес для отправки уведомлений о проблемах с низким уровнем критичности. Значение по умолчанию: **info@example.com**.

- **Периодичность проверки состояния ресурсов (мин)** – периодичность проверки состояния ресурсов (мин). Значение по умолчанию: 5.

- **Включить активные действия** – при переходе ресурсов, которые относятся к очередям сообщений (см. ниже), в критическое состояние останавливает работу сервисов **smap-smtp-gw** и **mailfilter**. При освобождении места в файловой системе спулов эти ресурсы выходят из критического состояния, и указанные сервисы запускаются вновь. Принимает значения **true** (включено) и **false** (выключено).

  При значении **false** в GUI появляются уведомления о проблемах с чрезвычайным уровнем критичности, при этом сервисы не останавливаются.

- **Проверка наличия процессов - минимальное количество секунд, в течение которых процесс должен существовать, чтобы считаться работающим (process-alive-seconds-threshold)** – проверка наличия процессов. Параметр определяет минимальное количество секунд в течение которых процесс должен существовать, чтобы считаться работающим. Значение по умолчанию: 10.

- **Пороговое значение на свободную оперативную память** – пороговое значение на свободную оперативную память.

  - **Пороговое значение на свободную оперативную память (Гб) - Уровень Critical** – пороговое значение на свободную оперативную память в Гб при уровне Critical. Значение по умолчанию – 1.

  - **Пороговое значение на свободную оперативную память (Гб) - Уровень Warning** – пороговое значение на свободную оперативную память в Гб при уровне Warning. Значение по умолчанию – 3.

- **Пороговое значение на свободное место на файловой системе** – пороговое значение на свободное место на файловой системе.

  - **Пороговое значение на свободное место на файловой системе (%) - Уровень Critical** – пороговое значение на свободное место на файловой системе при уровне Critical, выраженное в процентах. Значение по умолчанию – 4.

  - **Пороговое значение на свободное место на файловой системе (%) - Уровень Warning** – пороговое значение на свободное место на файловой системе при уровне Warning, выраженное в процентах. Значение по умолчанию – 10.

- **Пороговое значение на свободное место в swap** – пороговое значение на свободное место в файле подкачки.

- **Пороговое значение на свободное место в swap (%) - Уровень Critical** – пороговое значение на свободное место в файле подкачки при уровне Critical, выраженное в процентах. Значение по умолчанию – 20.
- **Пороговое значение на свободное место в swap (%) - Уровень Warning** – пороговое значение на свободное место в файле подкачки при уровне Warning, выраженное в процентах. Значение по умолчанию – 30.

- **Пороговое значение на время простоя CPU** – пороговое значение на время простоя CPU в секундах. Значение по умолчанию: 30.
- **Пороговое значение на использование CPU** – пороговое значение на использование CPU в количестве очередей. Значение по умолчанию: 5.
- **Пороговое значение на количество процессов** – пороговое значение на общее количество процессов в системе. Значение по умолчанию: 2500.
- **Пороговое значение на количество исполняющихся процессов** – пороговое значение на общее количество исполняющихся процессов в системе. Значение по умолчанию: 40.
- **Пороговое значение на количество подключенных пользователей** – пороговое значение на количество подключенных к системе пользователей. Значение по умолчанию: 50.
- **Очереди входящих сообщений в спуле хранения** – параметры обработки очереди входящих сообщений в спуле хранения.
  - **Пороговое значение количества сообщений в очереди для состояния Warning** – пороговое значение количества сообщений в очереди для состояния Warning. Значение по умолчанию – 500.
  - **Пороговое значение количества сообщений в очереди для состояния Critical** – пороговое значение количества сообщений в очереди для состояния Critical. Значение по умолчанию – 1000.
  - **Пороговое значение объёма сообщений в очереди для состояния Warning (МБ)** – пороговое значение объёма сообщений в очереди для состояния Warning в Мб. Значение по умолчанию – 15.
  - **Пороговое значение объёма сообщений в очереди для состояния Critical (МБ)** – пороговое значение объёма сообщений в очереди для состояния Critical в Мб. Значение по умолчанию – 30.
- **Очереди сообщений в спуле хранения, возвращённых после ошибок обработки** – параметры производительности очередей сообщений в спуле хранения, возвращенных после ошибок обработки.
  - **Пороговое значение количества сообщений в очереди для состояния Warning** – пороговое значение количества сообщений в очереди для состояния Warning. Значение по умолчанию – 1.
  - **Пороговое значение количества сообщений в очереди для состояния Critical** – пороговое значение количества сообщений в очереди для состояния Critical. Значение по умолчанию – 10.

- **Пороговое значение объёма сообщений в очереди для состояния Warning (МБ)** – пороговое значение объёма сообщений в очереди для состояния Warning в Мб. Значение по умолчанию – 1.

- **Пороговое значение объёма сообщений в очереди для состояния Critical (МБ)** – пороговое значение объёма сообщений в очереди для состояния Critical в Мб. Значение по умолчанию – 5.

- **Очереди входящих сообщений в спуле фильтрации** – параметры обработки очереди входящих сообщений в спуле фильтрации.

  - **Пороговое значение количества сообщений в очереди для состояния Warning** – пороговое значение количества сообщений в очереди для состояния Warning. Значение по умолчанию – 500.

  - **Пороговое значение количества сообщений в очереди для состояния Critical** – пороговое значение количества сообщений в очереди для состояния Critical. Значение по умолчанию – 1000.

  - **Пороговое значение объёма сообщений в очереди для состояния Warning (МБ)** – пороговое значение объёма сообщений в очереди для состояния Warning в Мб. Значение по умолчанию – 15.

  - **Пороговое значение объёма сообщений в очереди для состояния Critical (МБ)** – пороговое значение объёма сообщений в очереди для состояния Critical в Мб. Значение по умолчанию – 30.

- **Очереди сообщений в спуле фильтрации, возвращённых после ошибок обработки** – параметры производительности очередей сообщений в спуле фильтрации, возвращенных после ошибок обработки.

  - **Пороговое значение количества сообщений в очереди для состояния Warning** – пороговое значение количества сообщений в очереди для состояния Warning. Значение по умолчанию – 1.

  - **Пороговое значение количества сообщений в очереди для состояния Critical** – пороговое значение количества сообщений в очереди для состояния Critical. Значение по умолчанию – 10.

  - **Пороговое значение объёма сообщений в очереди для состояния Warning (МБ)** – пороговое значение объёма сообщений в очереди для состояния Warning в Мб. Значение по умолчанию – 1.

  - **Пороговое значение объёма сообщений в очереди для состояния Critical (МБ)** – пороговое значение объёма сообщений в очереди для состояния Critical в Мб. Значение по умолчанию – 5.

- **Очереди входящих сообщений в спуле отправки** – параметры обработки очереди входящих сообщений в спуле отправки.

  - **Пороговое значение количества сообщений в очереди для состояния Warning** – пороговое значение количества сообщений в очереди для состояния Warning. Значение по умолчанию – 500.

- **Пороговое значение количества сообщений в очереди для состояния Critical** – пороговое значение количества сообщений в очереди для состояния Critical. Значение по умолчанию – 1000.

- **Пороговое значение объёма сообщений в очереди для состояния Warning (МБ)** – пороговое значение объёма сообщений в очереди для состояния Warning в Мб. Значение по умолчанию – 15.

- **Пороговое значение объёма сообщений в очереди для состояния Critical (МБ)** – пороговое значение объёма сообщений в очереди для состояния Critical в Мб. Значение по умолчанию – 30.

- **Очереди сообщений в спуле отправки, возвращённых после ошибок обработки** – параметры производительности очередей сообщений в спуле отправки, возвращенных после ошибок обработки.

  - **Пороговое значение количества сообщений в очереди для состояния Warning** – пороговое значение количества сообщений в очереди для состояния Warning. Значение по умолчанию – 1.

  - **Пороговое значение количества сообщений в очереди для состояния Critical** – пороговое значение количества сообщений в очереди для состояния Critical. Значение по умолчанию – 10.

  - **Пороговое значение объёма сообщений в очереди для состояния Warning (МБ)** – пороговое значение объёма сообщений в очереди для состояния Warning в Мб. Значение по умолчанию – 1.

  - **Пороговое значение объёма сообщений в очереди для состояния Critical (МБ)** – пороговое значение объёма сообщений в очереди для состояния Critical в Мб. Значение по умолчанию – 5.

- **Количество таймаутов обработки сообщений за последний час** – количество превышений времени обработки сообщений за последний час. Включает в себя параметр **Количество таймаутов работы политики за последний час** – количество превышений времени работы политики за последний час (см. параметр **Максимальное время работы политики (с)**). Включает дополнительные параметры:

  - **Состояние Warning** – определяет количество таймаутов, при котором ресурс переходит в состояние **Warning**. Значение по умолчанию – 1;

  - **Состояние Critical** – определяет количество таймаутов, при котором ресурс переходит в состояние **Critical**. Значение по умолчанию – 5.

- **Пороговое значение среднего времени фильтрации сообщения (мин)** – пороговое значение среднего времени фильтрации сообщения (мин). Значение по умолчанию: 10.

- **Табличное пространство SMAP_MAIN** – параметры мониторинга табличного пространства SMAP.

  - **Пороговые значения на свободное место (МБ)** – пороговые значения на свободное место (Мб):

    - **Состояние Warning** – состояние Warning. Значение по умолчанию – 100;

- **Состояние Critical** – состояние Critical. Значение по умолчанию – 10.

- **Табличное пространство SMAP_MESSAGES** – параметры мониторинга табличного пространства **smap_messages**.
  - **Пороговые значения на свободное место (МБ)** – пороговые значения на свободное место (Мб):
    - **Состояние Warning** – состояние Warning. Значение по умолчанию – 500;
    - **Состояние Critical** – состояние Critical. Значение по умолчанию – 100.

- **Табличное пространство SMAP_DICT** – параметры мониторинга табличного пространства **SMAP_DICT**.
  - **Пороговые значения на свободное место (МБ)** – пороговые значения на свободное место (Мб):
    - **Состояние Warning** – состояние Warning. Значение по умолчанию – 100;
    - **Состояние Critical** – состояние Critical. Значение по умолчанию – 10.

- **Табличное пространство SMAP_INDEXES** – параметры мониторинга табличного пространства **SMAP_INDEXES**.
  - **Пороговые значения на свободное место (МБ)** – пороговые значения на свободное место (Мб):
    - **Состояние Warning** – состояние Warning. Значение по умолчанию – 500;
    - **Состояние Critical** – состояние Critical. Значение по умолчанию – 100.

- **База данных PostgreSQL** – параметры мониторинга базы данных PostgreSQL.
  - **Пороговые значения на свободное место (МБ)** – пороговые значения на свободное место (МБ):
    - **Состояние Warning** – состояние Warning. Значение по умолчанию – 500. При превышении этого значения отправляется уведомление администратору. Если установить значение этого параметра ниже текущего состояния свободного места в БД системы, сообщение администратору отправляться не будет.
    - **Состояние Critical** – состояние Critical. Значение по умолчанию – 100. При превышении этого значения прекращается архивирование писем.
  - **Максимальное количество сообщений в очереди на индексацию** – максимальное количество сообщений, находящихся в очереди на индексацию. Значение по умолчанию: 10000.

- **Мониторинг количества подключений к базам данных** – параметры мониторинга количества подключений к базам данных.
  - **Пороговое значение на количество подключений (%)** – пороговые значения на количество подключений в процентах:
    - **Состояние Warning** – состояние Warning. Значение по умолчанию – 80;

        - **Состояние Critical** – состояние Critical. Значение по умолчанию – 90.
- **Текущая секция базы данных** – параметры мониторинга текущей секции базы данных.
    - **Пороговые значения на время жизни секции (ч)** – пороговые значения на время жизни секции (ч):
        - **Состояние Warning** – состояние Warning. Значение по умолчанию – 48;
        - **Состояние Critical** – состояние Critical. Значение по умолчанию – 12.
- **ICAP-интерфейс** – параметры мониторинга трафика от ICAP-источников.
    - **Период проверки отсутствия принятых фильтром сообщений** – периодичность в минутах, с которой проверяется отсутствие принятых фильтром сообщений. Значение по умолчанию: **10m** (10 минут).
    - **Период проверки отсутствия обработанных фильтром сообщений** – периодичность в минутах, с которой проверяется отсутствие обработанных фильтром сообщений. Значение по умолчанию: **10m** (10 минут).
    - **Пороговое значение количества ошибок в ответах фильтра** – пороговое значение количества ошибок в ответах фильтра внешнему ICAP-источнику. Значение по умолчанию: 10.
- **Рабочее время, в течение которого следует проверять отсутствие сообщений** – настройки рабочего времени организации, в течение которого KEO DLP проверяет отсутствие сообщений:
    - **Начало рабочего дня (ч)** – час начала рабочего дня. Значение по умолчанию: 0.
    - **Конец рабочего дня (ч)** – час окончания рабочего дня. Значение по умолчанию: 24.
- **Opensearch** – пороговое значение доли используемой памяти сервисом **opensearch**, при превышении которого наступает состояние Critical. Значение по умолчанию: 80.
- **Отображаемое на графике максимальное количество открытых файловых дескрипторов** – максимальное количество открытых файловых дескрипторов, которое может быть отображено на графике монитора ресурсов. Значение по умолчанию: 100000.

Пороговые значения проверок для групп мониторинга:

Для каждой группы мониторинга могут быть заданы конкретные проверки, которые выбираются из раскрывающегося списка:

- **Количество таймаутов работы политики за последний час**;
- **Очереди входящих сообщений в спуле отправки**;
- **Очереди входящих сообщений в спуле фильтрации**;
- **Очереди входящих сообщений в спуле хранения**;
- **Очереди сообщений в спуле отправки, возвращённых после ошибок обработки**;

- **Очереди входящих сообщений в спуле фильтрации, возвращённых после ошибок обработки**;
- **Очереди входящих сообщений в спуле хранения, возвращённых после ошибок обработки**;
- **Пороговое значение на время простоя CPU**;
- **Пороговое значение на использование CPU**;
- **Пороговое значение на количество исполняющихся процессов**;
- **Пороговое значение на количество подключенных пользователей**;
- **Пороговое значение на количество процессов**;
- **Пороговое значение на свободное место в swap**;
- **Пороговое значение на свободное место на файловой системе**;
- **Пороговое значение на свободную оперативную память**;
- **Пороговое значение среднего времени фильтрации сообщения (мин)**.

Агенты мониторинга:

- **Порт** – порт, на котором внешний сервер мониторинга принимает соединения. Значение по умолчанию: 10050.
- **Пользовательский сервер мониторинга (для пассивных проверок)** – пользовательские серверы мониторинга, используемые для пассивных проверок, т.е. упрощенных запросов. В качестве значения задается список перечисленных через запятую IP-адресов или имен узлов, допускается использование маски CIDR в формате **X.X.X.X/N**.

  Примеры значений:

  ```
  127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.domain
  ```

  Если значение не указано, используется сервер мониторинга на master-узле KEO DLP.
- **Пользовательский сервер мониторинга (для активных проверок)** – пользовательские серверы мониторинга, используемые для активных проверок, которые требуют более сложной обработки. В качестве значения задается список перечисленных через запятую пар **IP-адрес:порт** или **Имя узла: порт**. Не допускается использование пробелов. Если значение не указано, активные проверки отключены.
- **Читать системную конфигурацию zabbix-agent (/etc/zabbix/zabbix_agentd.d/)** – включает считывание дополнительных параметров, необходимых для сбора статистики агентом мониторинга, из каталога **/etc/zabbix/zabbix_agentd.d/**. Принимает значения **true** (включено) и **false** (выключено).

  При значении **false** параметры считываются из файла **data/repos/dozor/config-final.git/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/monitor-agent/monitor-agent.conf**,

где **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** – идентификатор узла в кластере KEO DLP. Пример: **0f676af8-e25d-481e-a193-2aaecb2a2eed**

Значение по умолчанию: **false**.

A.2.1.4. Вспомогательные сервисы

Сервис распределенного хранения Cassandra:

- **Имя узла** – имя узла с сервисом **skvt-cassandra**. По умолчанию задано имя **Cassandra${subcluster-id}**.

Подключение к сервису распределенного хранения Cassandra:

- **Автоматическая миграция данных при добавлении новых узлов в кластер** – включение автоматической миграции данных при добавлении новых узлов в кластер. По умолчанию флажок установлен.
- **RPC адрес, на котором сервер будет принимать соединения** – RPC адрес, на котором сервер будет принимать соединения. Есть возможность выбора значения параметра из раскрывающегося списка: **Сетевой адрес** или **IP-адрес**. В зависимости от выбранного значения появляется дополнительный параметр **Сетевой адрес** или **IP-адрес** для указания локального адреса в виде имени хоста или IP. По умолчанию задано значение **Сетевой адрес**: **${node-ip}**. При выборе значения **IP-адрес** установлено значение **0.0.0.0**.
- **Локальный порт, на котором сервер будет принимать соединения** – локальный порт, на котором сервис распределенного хранения Cassandra будет принимать соединения. По умолчанию задано значение: 9042.

Отладка сервиса распределенного хранения:

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **skvt-cassandra** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Выполнение действий по обработке медиаданных:

- **Вывод отладочной информации** – включить вывод отладочной информации о работе сервиса в журнал. По умолчанию выключено.
- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервис ожидает соединения. Значение по умолчанию: 3012.
- **Количество тредов, выполняющих действия** – количество потоков сервиса выполнения действий по обработке медиаданных. Значение по умолчанию: 20.

JVM сервера выполнения действий по обработке медиаданных:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервиса выполнения действий по обработке медиаданных. Значение по умолчанию: 512 Мб

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **media-processor-action-server** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Сервис интеграции:

- **Вывод отладочной информации** – включить вывод отладочной информации о работе сервиса в журнал. По умолчанию выключено.
- **Порт сервиса интеграции** – порт, на котором сервис ожидает соединения от внешнего клиента. Значение по умолчанию: 33033.
- **Использовать защищенное соединение** – принимать запросы от внешнего клиента только после установки защищенного соединения по протоколу HTTPS. По умолчанию включено.
- **Таймаут взаимодействия с веб-сервером** – таймаут в секундах, в течение которого сервис интеграции ожидает ответа от веб-сервера. Если веб-сервер не успеет ответить – сервис интеграции возвращает внешнему клиенту ошибку HTTP 502. Значение по умолчанию: 60.
- **Таймаут взаимодействия с сервером лицензирования** – таймаут в секундах, в течение которого сервис интеграции ожидает ответа от сервера лицензирования. Если сервис активен, то он запрашивает лицензию раз в час. Если сервис не получил лицензию и/или неактивен, то он запрашивает лицензию раз в пять минут. Неактивный сервис не принимает запросов к API. Значение по умолчанию: 60.
- **Интеграционные ключи** – набор строк, используемых для дополнительной авторизации внешнего клиента. Значение по умолчанию не задано.

JVM сервиса интеграции:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса интеграции. Значение по умолчанию: 512.
- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти сервиса интеграции в случае ошибки исчерпания памяти. По умолчанию выключено.
- **Каталог для записи дампов памяти** – путь к каталогу для записи дампов памяти.

БД сервера действий по обработке медиаданных:

- **Настройки соединения с базой** – настройки подключения к БД сервера действий по обработке медиаданных:
  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД. Используемое значение: 5442.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.

- **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.

Очереди сообщений и действий над сообщениями:

- **Адрес** – адрес сервера для подключения к сервису **redis**. Значение по умолчанию: 0.0.0.0.
- **Порт** – порт для подключения к сервису **redis**. Значение по умолчанию: 16379.
- **Каталог хранилища** – путь к каталогу на файловой системе, в котором хранятся очереди сообщений и действий над сообщениями. Значение по умолчанию: **${smap-settings/common/smap-home}/redis**.

Сервис очередей:

- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервер будет принимать соединения. Значение по умолчанию: 61616.

Отладка сервиса очередей:

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **smap-activemq** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Модуль подтверждения отправки:

- **Локальный почтовый домен** – имя домена локальной почты. Значение по умолчанию не задано.
- **Список ldap-Серверов ldap://host:port** – список LDAP-серверов. Указывается в формате **ldap://host:port**. Значение по умолчанию: **ldap://localhost:3268**.
- **Шаблон bind-dn** – шаблон предоставления DN подключения. Значение по умолчанию: **%l**.
- **Шаблон base-dn** – шаблон базы для поиска. Значение по умолчанию: **dc=%c**.
- **Шаблон фильтра** – шаблон фильтра. Значение по умолчанию: **(userPrincipalName=%l)** (указывается заключенным в скобки).
- **Атрибуты с адресами** – атрибуты с адресами. Перечисляются через пробел. Значения по умолчанию: **mail proxyAddresses**.
- **Глубина поиска в LDAP** – глубина поиска в LDAP. В качестве значения параметра необходимо выбрать в раскрывающемся списке один из следующих вариантов:
  - **base** – поиск непосредственно в узле (базе поиска).
  - **onelevel** – поиск по всем узлам, являющимися непосредственными потомками базового в иерархии, то есть расположенным на один уровень ниже базового.
  - **subtree** – поиск по всей области, нижележащей относительно базы поиска (baseDN). Значение по умолчанию.

- **Опции LDAP** – указывается используемая версия протокола LDAP. Значение по умолчанию: **version=3**.
- **Таблица трансляции доменов NETBIOS** – таблица трансляции доменов NETBIOS. Значение по умолчанию: **domain.local=domain subdomain.domain.local=subdomain.domain**.
- **Вывод отладочной информации** – вывод отладочной информации. По умолчанию выключено.
- **Почтовый домен для вывода в окне авторизации** – почтовый домен для вывода в окне авторизации. По умолчанию имеет значение: **domain**.

A.2.2. Настройка модулей перехвата

A.2.2.1. Агенты

Сервис БД для Центра приложений:

- **Настройки соединения с базой** – настройки подключения к БД:
  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД. Используемое значение: 5441.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.
  - **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.

Сервер агентов:

- **Вывод отладочной информации** – включение вывода отладочной информации. По умолчанию вывод выключен.
- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервер будет принимать соединения. Значение по умолчанию: 4444.
- **Максимальное количество оперативной памяти (МБ)** – максимальный объём памяти в мегабайтах, выделяемый процессу сервера агентов. Значение по умолчанию: 512.
- **Директория для хранения данных** – путь к каталогу для хранения данных об агентах. Значение по умолчанию: **/data/spool/dozor/agent-server**.
- **Перехват нажатий клавиш** – параметры перехвата нажатий клавиш:
  - **Интервал сбора перехваченных нажатий клавиш для объединения в сообщение (с)** – интервал в секундах, через который формируется буфер с перехваченными блоками нажатий клавиш. По истечении этого времени формируется почтовое сообщение с перехваченными данными. Значение по умолчанию: 300.

- **Объем перехваченных нажатий клавиш для объединения в сообщение (КБ)** – объем в Кб перехваченных блоков нажатий клавиш, для которых формируется буфер. По достижении значения данного параметра формируется почтовое сообщение с перехваченными данными. Значение по умолчанию: 10.

- **Соединения с сервисом фильтрации сообщений** – определяет параметры соединений с сервисом **mailfilter**. Принимает значения **Определять автоматически** и **Задать в виде списка**. Значение по умолчанию: **Определять автоматически**.

  При значении **Определять автоматически** соединения определяются в конфигурационном файле **/data/repos/dozor/config-final.git/<UUID узла>/agent-server/agent-server.edn**.

  Пример: **/data/repos/dozor/config-final.git/2d5cd12b-428c-4c80-8c18-265777e522da/agent-server/agent-server.edn**.

  При значении **Задать в виде списка** параметры соединений задаются вручную. Для добавления нового соединения необходимо нажать на кнопку **Добавить**. Чтобы дублировать соединение, следует щелкнуть мышью на значок  и ввести характеристики соединения. Для удаления подключения следует нажать на значок  рядом с идентификатором соединения.

  При выборе значения **Задать в виде списка** отображаются следующие параметры соединений с сервисом фильтрации:

  - **Сетевой адрес** – доменное имя или IP-адрес узла с сервисом **mailfilter**.
  - **Номер порта** – порт, на котором узел с сервисом **mailfilter** ожидает соединения.

Отладка сервера агентов:

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **agent-server** в случае ошибки исчерпания памяти. Дамп сохраняется в каталоге **/data/temp/java_dumps/agent-server/**. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Сервер управления агентами:

- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервер будет принимать соединения. Значение по умолчанию: 3006.

- **База данных** – имя схемы соединения с БД, используемой для хранения информации о задачах сервиса **agent-control-ng**. Принимает значения **БД по умолчанию** и **Специальная БД**. Значение по умолчанию: **БД по умолчанию**. При значении **БД по умолчанию** сервис подключается к БД политики. Если выбрано значение **Специальная БД**, доступны параметры:

  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД.
  - **Имя базы данных** – имя БД.

- **Пользователь базы данных** – указывается имя пользователя БД.
- **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.
- **Проверка подключения не выполнялась** – данное сообщение появляется, если проверка подключения к хранилищу Досье не выполнялась. При успешной проверке подключения появляется сообщение **Подключение проверено Проверка прошла успешно**.

Примечание

При переключении с БД по умолчанию на специальную БД информация о группах станций, настройках перехвата и дистрибутивах не сохраняется.

- **Настройки LDAP** – настройки взаимодействия сервиса **software-center** с LDAP-сервером. Принимает значения: **Выключено** и **Включено**. По умолчанию параметр выключен. При значении **Включено** доступны следующие параметры:
  - **URL LDAP сервера** – URL LDAP-сервера. Значение по умолчанию: **ldap://nihil.local:3268**.
  - **DN пользователя** – данный параметр предназначен для ввода DN записи с целью подключения к LDAP. Значение по умолчанию: **user@nihil.local**.
  - **Пароль пользователя** – данный параметр предназначен для ввода пароля с целью подключения к LDAP.
  - **Базовый DN для поиска** – ветка информационного дерева каталога, от которой начинается поиск данных. Атрибут FreeIPA и ALD Pro. Для AD рекомендуется оставить пустым.

    Примечание

    Для отображения описания параметра следует навести курсор мыши на его название.

  - **Фильтр станций** – фильтр LDAP для поиска рабочих станций персоны. Значение по умолчанию: **(objectCategory=computer)**.
  - **Атрибут имени станции** – имя атрибута LDAP, содержащего имя рабочей станции. Значение по умолчанию: **dNSHostName**.
  - **Атрибут организационной единицы** – атрибут ALD Pro, содержащий описание организационной единицы (OU), к которой относится рабочая станция. Для ALD Pro следует задать значение **rbtadp**. Для Microsoft AD и FreeIPA (389 Directory Server) рекомендуется оставить пустым.

Примечание

Для отображения описания параметра следует навести курсор мыши на его название.

После задания настроек подключения следует установить подключение к LDAP-серверу, нажав кнопку **Проверить**. В зависимости от ситуации появляются следующие сообщения:

- **Проверка подключения не выполнялась** – данное сообщение появляется, если проверка подключения к LDAP-серверу не выполнялась.
- При успешной проверке подключения появляется сообщение **Подключение проверено Проверка прошла успешно**.

- **Периодичность синхронизации списка станций (ч)** – промежуток времени в часах, через который список рабочих станций синхронизируется с LDAP-сервером. Значение по умолчанию: 1.

- **Таймаут удаления временных станций (мин)** – время ожидания удаления временных станций в мин. Значение по умолчанию: 480.
- **Максимальное время недоступности агента (дн.)** – промежуток времени в днях, в течение которого Агент считается недоступным. Значение по умолчанию: 14.
- **Автоматическая активация агентов при наличии квоты в лицензии** – отключает автоматическую активацию агентов при наличии квоты в лицензии. Принимает значения **true** и **false**. Если в результате проблем с лицензией полнофункциональные агенты были деактивированы системой и значение параметра равно **true**, они будут активированы автоматически. При значении **false** пользователь активирует агентов самостоятельно. Значение по умолчанию: **true**.
- **Ключи для проверки подлинности загружаемых плагинов** – определяет 5 ключей для проверки подлинности загружаемых в KEO DLP плагинов для перехвата данных в мессенджере Telegram. Один из ключей используется для подписи плагина. Изначально все ключи считаются надёжными и проверенными, так как установлены все соответствующие флажки. Можно указать, какие ключи являются доверенными, а какие – скомпрометированными.

JVM сервера управления агентами:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервера управления агентами. Значение по умолчанию: 1024 Мб.
- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **agent-control-ng** в случае ошибки исчерпания памяти. По умолчанию включено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Глобальные настройки агентов:

- **Время ожидания активности персоны (мин)** – время ожидания активности персоны, выраженное в минутах. Значение по умолчанию: 15.

- **Максимальная длительность сеанса записи (мин)** – максимальная длительность сеанса записи звука в минутах. Значение по умолчанию: 1440. Значение параметра может быть от 1 до 10080 минут.

- **Длительность тишины для приостановки записи (с)** – время в секундах, по истечении которого запись звука будет приостановлена. Значение по умолчанию: 10. Значение параметра может быть от 1 до 600 секунд.

Конфигурации агентов:

Чтобы добавить перехватчик, следует щелкнуть мышью на значок и ввести его характеристики. Чтобы удалить перехватчик, следует нажать на значок рядом с идентификатором перехватчика.

- **ID** – идентификатор набора, который будет использоваться для формирования имени файла. Значение по умолчанию: **default-agent-settings**.

  Внимание!

  *По значению параметра **ID** происходит связь с группой станций, поэтому оно задается один раз и не меняется.*

- **Название набора** – произвольный текст, описывающий набор. Значение по умолчанию: **default-agent-settings**.

- **Максимальное время отправки сообщения на сервер (с)** – максимальное время отправки сообщения на сервер агентов в секундах.

- **Интервал передачи информации об активности пользователя (мин)** – интервал передачи информации серверу агентов об активности пользователя на рабочей станции. Значение по умолчанию: 10.

- **Список доступных агенту endpoint-серверов** – список серверов, доступных агенту. Есть возможность выбора значения **Определять автоматически** или **Задать в виде списка**. Если задано **Определять автоматически**, то в конфигурации агента будет установлен сервер или список серверов, указанных при установке модуля KEO DLP Endpoint Agent на рабочую станцию. При выборе **Задать в виде списка** появляется новый параметр **Задать в виде списка** для задания параметров серверов с KEO DLP Endpoint Agent вручную. Чтобы задать конкретные параметры сервера, необходимо нажать кнопку . В результате появляются параметры **Сетевой адрес** (сетевой адрес сервера) и **Номер порта** (номер порта сервера). Можно задавать параметры для нескольких серверов управления рабочими станциями. Для удаления параметров сервера, заданного вручную, необходимо нажать кнопку .

- **Пропускная способность соединения с сервером агентов в КБ/с. Если значение равно 0, то ограничение отсутствует** – максимальная скорость передачи данных на сервер агентов, выраженная в КБ/с. Если значение равно 0, то ограничение отсутствует.

- **Использовать прокси-серверы для соединения с сервером агентов** – разрешает использование прокси-серверов для установления соединения с сервером управления

рабочими станциями. Принимает значения **true** и **false**. При значении **true** выполняется попытка подключения через прокси. При значении **false** рабочие станции подключаются к серверу управления агентами напрямую. Значение по умолчанию: **false**.

- **Перечень прокси-серверов, используемых для соединения с сервером агентов** – перечень прокси-серверов, которые могут использоваться при установлении соединения с сервером управления рабочими станциями.

- **Использовать прокси-серверы, заданные в настройках рабочей станции** – включает использование прокси-серверов, заданных в настройках рабочей станции. Принимает значения **true** и **false**. При значении **true** поиск прокси-сервера выполняется в конфигурации WinHTTP, которая в свою очередь настраивается в ветви реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\WinHttpSettings** на рабочей станции.

  При значении **false** используются значения параметра **Перечень прокси-серверов, используемых для соединения с сервером агентов**. При пустых списках подключение к серверу агентов будет выполнено напрямую.

  Значение по умолчанию: **false**.

- **Максимальный срок хранения данных во временном хранилище на агенте (сутки)** – максимальный срок хранения данных перехвата на рабочей станции пользователя. Задается в сутках. Переданные в KEO DLP данные сразу удаляются с рабочей станции пользователя. Если значение равно нулю, то ограничение отсутствует.

- **Максимальный размер временного хранилища (в процентах от диска)** – максимальный объем данных перехвата, которые могут храниться на рабочей станции пользователя. Переданные в KEO DLP данные сразу удаляются с рабочей станции пользователя. Если значение равно нулю, то ограничение отсутствует.

- **Уровень журналирования** – степень детализации журналирования перехватчика. В качестве значения можно выбрать один из следующих параметров в раскрывающемся списке:

  - **Журналирование выключено** – не выполняется запись в журнальный файл.
  - **Критичные ошибки** – в журнал записываются критические ошибки.
  - **Предупреждения** – в журнал записываются предупреждения об ошибках.
  - **Информация** – в журнал записываются информационные сообщения.
  - **Отладка** – в журнал записываются отладочные сообщения.

- **Исключить изменение системной конфигурации печати Windows** – флажок отвечает за исключение изменения оригинальных программных файлов печати, влияющих на работу ОС Windows. Применяется к следующим виртуальным принтерам Microsoft:

  - XPS Document Writer;
  - XPS Document Writer4;
  - Print To PDF;

- OneNote;
- Software Printer Driver.

Если флажок установлен, Агент не будет вносить изменения в соответствующие файлы и перехватывать данные, отправленные для печати на вышеуказанных принтерах. Операция блокировки печати при этом остается доступной. По умолчанию флажок снят.

Внимание!

При использовании KEO DLP Endpoint Agent для Windows версии 5.2 и ниже изменения в политике перехвата применятся только после перезагрузки рабочих станций.

Центр приложений агентов:

- **Локальный порт, на котором сервер будет принимать соединения от рабочих станций** – порт, на котором сервер будет принимать соединения от рабочих станций. Значение по умолчанию: 9400.
- **Локальный порт, на котором сервер будет принимать соединения от других сервисов** – порт, на котором центр приложений будет принимать соединения от сервера управления KEO DLP Endpoint Agent. Значение по умолчанию: 9401.
- **Порт для подключения SSH-клиента** – номер порта, на котором рабочая станция будет принимать соединения по протоколу SSH. Значение по умолчанию: 22.
- **WinRM транспорт** – протокол для передачи данных в службе **WinRM**. Принимает значения **HTTP** и **HTTPS**. Значение по умолчанию: **HTTP**.
- **Внешний адрес сервера** – определяет, какой адрес будет отправлен из центра приложений на **Updater Service** в качестве URL. Принимает значения **Определять автоматически** или **Задать вручную**.

  Если задано **Определять автоматически**, то IP-адрес будет автоматически сгенерирован центром приложений.

  При выборе **Задать вручную** появляется новый параметр **Задать вручную** для задания параметров серверов с KEO DLP Endpoint Agent вручную.
- **Путь установки Updater** – путь к каталогу установки средства развертывания (Updater) на рабочей станции. Значение по умолчанию:

  ```
  C:\Windows\785268CBDB964b448A517D7F3ECFE681
  ```

  Изменение параметра вступает в силу только после запуска обновления версии Агента.

  Во избежание конфликтов с антивирусным ПО после изменения каталога установки Updater следует добавить в исключения антивирусного ПО путь к указанному каталогу.
- **Путь установки для агентов** – параметр предназначен для изменения пути установки модуля KEO DLP Endpoint Agent. Каталог для установки агента должен быть пустым.

При изменении пути необходимо задать новый путь в исключениях антивируса. Можно ввести не более 200 символов, при этом допустимы только латинские буквы, цифры, пробел, дефис и символы «/» и «_».

При установке агентов сторонними способами (ручная установка, установка через GPO и т.д.) измененный путь должен задаваться в командной строке.

- **Имя службы управления сервером** – параметр предназначен для изменения названия службы управления сервером.

  Имя службы должно быть указано без расширения. Можно ввести не более 200 символов, при этом допустимы только латинские буквы, цифры, пробел и символ подчеркивания(«_»).

  Не рекомендуется указание названий, совпадающих с другим ПО. При изменении названий служб, в исключениях антивируса необходимо указать новые имена файлов, поскольку меняется и имя исполняемого файла.

  При установке агентов сторонними способами (ручная установка, установка через GPO и т.д.) измененные названия должны задаваться в командной строке.

- **Описание службы управления сервером** – параметр предназначен для изменения описания службы управления сервером.

  Можно ввести не более 200 символов, при этом допустимы только символы кириллицы, латинские буквы и цифры.

  При установке агентов сторонними способами (ручная установка, установка через GPO и т.д.) измененные названия должны задаваться в командной строке.

- **Имя службы обработки контента** – параметр предназначен для изменения названия службы обработки контента.

  Имя службы должно быть указано без расширения. Можно ввести не более 200 символов, при этом допустимы только латинские буквы, цифры, пробел и символ подчеркивания(«_»).

  Не рекомендуется указание названий, совпадающих с другим ПО. При изменении названий служб, в исключениях антивируса необходимо указать новые имена файлов, поскольку меняется и имя исполняемого файла.

  При установке агентов сторонними способами (ручная установка, установка через GPO и т.д.) измененные названия должны задаваться в командной строке.

- **Описание службы обработки контента** – параметр предназначен для изменения описания службы обработки контента.

  Можно ввести не более 200 символов, при этом допустимы только символы кириллицы, латинские буквы и цифры.

  При установке агентов сторонними способами (ручная установка, установка через GPO и т.д.) измененные названия должны задаваться в командной строке.

- **Имя службы контроля трафика** – параметр предназначен для изменения названия службы контроля трафика.

Можно ввести не более 200 символов, при этом допустимы только латинские буквы, цифры, пробел и символ подчеркивания(«_»). Не рекомендуется указание названий, совпадающих с другим ПО.

При изменении названий служб, в исключениях антивируса необходимо указать новые имена файлов, поскольку меняется и имя исполняемого файла.

При установке агентов сторонними способами (ручная установка, установка через GPO и т.д.) измененные названия должны задаваться в командной строке.

- **Описание службы контроля трафика** – параметр предназначен для изменения описания службы контроля трафика.

  Можно ввести не более 200 символов, при этом допустимы только символы кириллицы, латинские буквы и цифры.

  При установке агентов сторонними способами (ручная установка, установка через GPO и т.д.) измененные названия должны задаваться в командной строке.

- **Имя службы контроля целостности** – параметр предназначен для изменения названия службы контроля целостности.

  Можно ввести не более 200 символов, при этом допустимы только латинские буквы, цифры, пробел и символ подчеркивания(«_»). Не рекомендуется указание названий, совпадающих с другим ПО.

  При изменении названий служб, в исключениях антивируса необходимо указать новые имена файлов, поскольку меняется и имя исполняемого файла.

  При установке агентов сторонними способами (ручная установка, установка через GPO и т.д.) измененные названия должны задаваться в командной строке.

- **Описание службы контроля целостности** – параметр предназначен для изменения описания службы контроля целостности.

  Можно ввести не более 200 символов, при этом допустимы только символы кириллицы, латинские буквы и цифры.

  При установке агентов сторонними способами (ручная установка, установка через GPO и т.д.) измененные названия должны задаваться в командной строке.

- **Стандартный таймаут для этапов развертывания (с)** – определяет время развертывания в секундах, по истечении которого центр приложений агентов будет считать данную станцию недоступной. Значение по умолчанию: 300.

- **Таймаут на установку Updater (мин)** – таймаут в минутах на установку Updater. Значение по умолчанию: 1440.

- **Таймаут на перезагрузку станции (мин)** – таймаут в минутах на перезагрузку рабочей станции. Значение по умолчанию: 1440.

- **Период хранения статуса (мин)** – период хранения статуса Агента в минутах. Значение по умолчанию: 1440.

- **Способ загрузки Updater при использовании WinRM** – определяет способ загрузки Updater на рабочую станцию при использовании службы WinRM. Значение по умолчанию: **Определять автоматически**.

  Принимает значения:

  - **По HTTP** – загрузка Updater на рабочую станцию выполняется по протоколу HTTP.
  - **Частями в Base64 через WinRM** – файл **Updater.exe** разбивается на части по несколько килобайт. Далее выполняется преобразование каждой части в формат Base64, после этого части с помощью службы WinRM загружаются на рабочую станцию. Далее загруженные части объединяются обратно в файл.
  - **Выбирать автоматически** – будет использован способ **По HTTP**. В случае возникновения ошибок будет выполнена загрузка Updater на рабочую станцию способом **Частями в Base64 через WinRM**.

- **Вывод отладочной информации** – вывод отладочной информации о работе сервиса **software-center**. По умолчанию выключено.

A.2.2.2. Краулер

Сервис отпечатков краулером:

- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **crawler-snapshot**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Максимальное число попыток подключения к хранилищу** – максимальное количество попыток подключения к БД сервиса отпечатков. Значение по умолчанию: 5.
- **Настройки подключения к хранилищу** – настройки подключения к БД с метазаданиями.
  - **Настройки подключения к базе данных** – настройки подключения к базе данных хранилища.
    - **Хост БД с метазаданиями** – IP-адрес узла БД хранилища.
    - **Имя пользователя БД с метазаданиями** – имя пользователя БД хранилища. Значение по умолчанию: **dozor**.
    - **Пароль пользователя БД с метазаданиями** – пароль пользователя БД хранилища. Значение по умолчанию: **dozor**.
    - **Название БД с метазаданиями** – имя БД хранилища. Значение по умолчанию: **dozor**.

Производительность сервиса отпечатков краулера:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-snapshot**. Значение по умолчанию: 2048.

Сервис поиска данных краулером:

- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **crawler-scanner**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Максимальное количество одновременно сканируемых ресурсов** – максимальное количество одновременно сканируемых ресурсов. Значение по умолчанию: 10.
- **Максимальное количество попыток подключения к ресурсу** – максимальное количество попыток подключения к ресурсу. Значение по умолчанию: 2.
- **Таймаут между попытками подключения (с)** – таймаут в секундах между попытками подключения. Значение по умолчанию: 10.
- **Настройки сканирования сети** – настройки сканирования сети:
  - **Определять доменное имя хоста** – включает определение доменного имени хоста во время сканирования сети. Если параметр **Определять доменное имя хоста** включен, File Crawler выполняет отправку запросов на DNS для определения имени хоста. По умолчанию включено.
  - **Максимальное количество одновременно сканируемых хостов** – максимальное количество одновременно сканируемых хостов в рамках одной задачи. Значение по умолчанию: 10.

    Внимание!

    Так как сканирование сети оказывает большую нагрузку на сеть, для данного параметра не рекомендуется указывать большое значение.

    *Минимальное значение для параметра **Максимальное количество одновременно сканируемых хостов** равно 1.*

- **Настройки транспорта** – настройки транспорта.
  - **Настройки соединения с CCC** – настройки соединения с центром управления crawler.
    - **Адрес хоста сервиса CCC** – адрес узла с центром управления crawler. Значение по умолчанию: **$(node-ip)**.
    - **Порт сервиса CCC** – порт центра управления crawler. Значение по умолчанию: 8080.
- **Настройки подключения по SMB протоколу** – настройки подключения по протоколу SMB.
  - **Версия SMB протокола** – версия протокола SMB. Значение по умолчанию: **smb2**. В данной реализации поддерживаются версии **smb1**, **smb2**.
  - **Максимальное время на установку соединения (с)** – максимальное время в секундах на установку соединения с удаленным ресурсом. Значение по умолчанию: 600.

- **Максимальное время ожидания ответа при чтении/записи (с)** – максимальное время ожидания ответа от удаленного ресурса при чтении/записи в секундах. Значение по умолчанию: 120.
- **Таймаут сетевого взаимодействия (с)** – время ожидания в секундах при сетевом взаимодействии с удаленным ресурсом. Значение по умолчанию: 0.

- **Настройки прокси-сервера** – настройки прокси-сервера.
  - **Прокси-хост** – доменное имя или IP-адрес прокси-сервера. Значение по умолчанию не установлено.
  - **Прокси-порт** – порт, на котором прокси-сервер ожидает соединения. Значение по умолчанию не установлено.
- **Настройки подключения к сервису Snapshot** – настройки подключения к сервису Snapshot.
  - **Хост** – IP-адрес или имя узла с сервисом **smtp-gw**. Значение по умолчанию: 127.0.0.1.

Производительность сервиса поиска данных краулера:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-scanner**. Значение по умолчанию: 2048.

Центр управления краулером:

- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **crawler-ccc**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Параметры подключения к БД хранения метазаданий** – параметры подключения к БД хранения метазаданий.
- **Параметры подключения к БД**:
  - **Хост БД с метазаданиями** – узел с БД метазаданий. Значение по умолчанию: 127.0.0.1.
  - **Имя пользователя БД с метазаданиями** – имя пользователя БД метазаданий. Значение по умолчанию: dozor.
  - **Пароль пользователя БД с метазаданиями** – пароль пользователя БД метазаданий.
  - **Название БД с метазаданиями** – название БД метазаданий. Значение по умолчанию: dozor.
- **Параметры подключения к сервису Snapshot**:
  - **Хост** – узел с сервисом Snapshot. Значение по умолчанию: 127.0.0.1.

Производительность центра управления краулером:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-ccc**. Значение по умолчанию: 2048.

Загрузка сообщений из корпоративных мессенджеров:

- **Уровень журналирования** – требуемая степень подробностей журналируемых данных. Значение по умолчанию: **Информация**. В качестве значения можно выбрать один из следующих параметров в раскрывающемся списке:
  - **Отключен**;
  - **Критические ошибки**;
  - **Ошибки**;
  - **Предупреждения**;
  - **Уведомления**;
  - **Информация**;
  - **Отладка**.
- **Время актуальности данных в кэше (секунд)** – периодичность в секундах, с которой обновляется список участников беседы, для которой выполняется перехват сообщений. Значение по умолчанию: 3600 (один час).
- **Каталог для временных файлов** – каталог для временных файлов сервиса. Значение по умолчанию: **/data/temp**.
- **Настройки прокси-сервера** – принимает значения **Настройка прокси-сервера** и **Прокси-сервер не используется**. Значение по умолчанию: **Прокси-сервер не используется**.

  Если для доступа к адресу **https://webexapis.com/** требуется соединение через прокси-сервер, следует выбрать значение **Настройка прокси-сервера**. При выборе этого значения доступны параметры:
  - **Адрес прокси-сервера** – адрес (IP или FQDN) прокси-сервера, через который предполагается соединяться с узлом **webexapis.com**.
  - **Порт прокси-сервера** – номер порта, на котором этот прокси-сервер ожидает соединения.
  - **Логин для Basic-аутентификации на прокси-сервере** – имя учётной записи пользователя для авторизации на прокси-сервере.
  - **Пароль для Basic-аутентификации на прокси-сервере** – пароль этой учётной записи.
- **Файл с токеном доступа** – путь к файлу **token.json**, необходимому для идентификации опрашивающего сервера KEO DLP на стороне серверов Webex. Значение по умолчанию: **/opt/dozor/share/im-crawler/token.json**.

Внимание!

*Файл **token.json** необходим для идентификации опрашивающего сервера KEO DLP на стороне серверов Webex. При отсутствии обращений серверов KEO DLP к серверам Webex с помощью этого файла в течение более 90 суток, файл становится недействительным. Для создания нового такого файла необходимо обратиться к инструкции, описанной в документе Руководство по установке и настройке.*

- **Client ID** – значение поля **CLIENT_ID**. По умолчанию не заполнено.
- **Client Secret** – значение поля **CLIENT_SECRET**. По умолчанию не заполнено.

Примечание

*Для получения **CLIENT_ID**, **CLIENT_SECRET** и файла **token.json** необходимо выполнить настройку перехвата сообщений из корпоративного мессенджера Cisco Webex Teams согласно документу Руководство по установке и настройке.*

- **Максимальный размер загружаемых файлов (МБ)** – максимальный размер файлов в мегабайтах, передаваемых в беседах, для которых будет выполняться загрузка и фильтрация по политике безопасности. KEO DLP не обрабатывает файлы размером более 500 МБ. Значение по умолчанию: 100.

Примечание

Существует возможность ограничить максимальный размер передаваемых файлов на стороне мессенджера Webex и таким образом обеспечить загрузку и фильтрацию всех переданных в беседах файлов.

- **Загружать историю сообщений за последние** – задать промежуток времени, за который требуется загрузить сообщения из истории. Возможные значения: **1 день**, **5 дней**, **10 дней**, **30 дней**, **60 дней**, **90 дней**, **Все возможные**. Значение по умолчанию: **1 день**.
- **Сообщения и файлы** – выбрать один из двух вариантов:
  - **Только ранее не загруженные (при повторной загрузке дубли в перехватах будут отсутствовать)** – при загрузке истории сообщений будут учтены сообщения, уже имеющиеся в архиве, и повторно загружены не будут. Такой вариант подходит при увеличении выбранного периода истории.
  - **Все за выбранный период (при повторной загрузке возможны дубли сообщений в архиве)** – сообщения за выбранный период истории будут загружены независимо от того, были ли они помещены в архив ранее. Такой вариант можно применить при необходимости перефильтрации сообщений в архиве.
- **Интервал обновления (секунд)** – периодичность в секундах, с которой KEO DLP опрашивает сервер Webex в ожидании новых сообщений. Значение по умолчанию: 3.

Примечание

Производителем корпоративного мессенджера установлено ограничение на количество запросов в единицу времени, отправляемых на сервер Webex. При достижении предела сообщения перестают загружаться в KEO DLP. По умолчанию таймаут загрузки сообщений с сервера действует в течение минуты, при этом производитель может установить более длительный период. По истечении этого времени загрузка сообщений возобновляется.

Сервис обработки данных краулером:

- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **crawler-processor**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Максимальное количество одновременно обрабатываемых ресурсов** – максимальное количество одновременно обрабатываемых ресурсов. Значение по умолчанию: 10.
- **Максимальное количество попыток подключения к ресурсу** – максимальное количество попыток подключения к ресурсу. Значение по умолчанию: 2.
- **Таймаут между попытками подключения (с)** – таймаут в секундах между попытками подключения. Значение по умолчанию: 10.
- **Максимальное время ожидания ответа о результатах обработки** – время ожидания ответа в секундах при обработке файла от сервиса **mailfilter**. Значение по умолчанию: 900.
- **Настройки транспорта** – настройки транспорта.
  - **Настройки соединения с CCC** – настройки соединения с центром управления crawler.
    - **Адрес хоста сервиса CCC** – адрес узла с центром управления crawler. Значение по умолчанию: **${node-ip}**.
    - **Порт сервиса CCC** – порт подключения к центру управления crawler. Значение по умолчанию: 8080.
- **Настройки подключения по SMB протоколу** – настройки подключения по протоколу SMB.
  - **Версия SMB протокола** – версия протокола SMB. Значение по умолчанию: **smb2**. В данной реализации поддерживаются версии **smb1**, **smb2**.
  - **Максимальное время на установку соединения (с)** – максимальное время в секундах на установку соединения с удаленным ресурсом. Значение по умолчанию: 600.
  - **Максимальное время ожидания ответа при чтении/записи (с)** – максимальное время ожидания ответа от удаленного ресурса при чтении/записи в секундах. Значение по умолчанию: 120.

- **Таймаут сетевого взаимодействия (с)** – время ожидания в секундах при сетевом взаимодействии с удаленным ресурсом. Значение по умолчанию: 0.

- **Настройки прокси-сервера** – настройки прокси-сервера.
  - **Прокси-хост** – доменное имя или IP-адрес прокси-сервера. Значение по умолчанию не установлено.
  - **Прокси-порт** – порт, на котором прокси-сервер ожидает соединения. Значение по умолчанию не установлено.

- **Каталог для временных файлов** – временный каталог для хранения загруженных файлов. Значение по умолчанию: **/data/temp/crawler-x/processor/**.

- **Размер блока файла, скачиваемый за одну итерацию загрузки** – размер блока файла, скачиваемый за одну итерацию загрузки. Значение по умолчанию: **128к**.

- **Настройки mailfilter** – определяет параметры соединений с сервисом **mailfilter**. Принимает значения **Определять автоматически** и **Задать вручную**. Значение по умолчанию: **Определять автоматически**.

  При значении **Определять автоматически** соединения описываются в конфигурационном файле **/data/repos/dozor/config-final.git/.../crawler-x-processor/crawler-x-processor-server.conf**.

  При выборе значения **Задать вручную** отображаются следующие параметры соединений с сервисом фильтрации:
  - **Хост** – доменное имя или IP-адрес узла с сервисом **mailfilter**.
  - **Порт** – порт, на котором узел с сервисом **mailfilter** ожидает соединения.

Производительность сервиса обработки данных краулером:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-processor**. Значение по умолчанию: 2048.

Прокси центра управления краулером:

- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **crawler-pccc**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.

- **Параметры подключения к хранилищу** – параметры подключения к БД хранения метазаданий.
  - **Параметры подключения к БД**:
    - **Хост БД с метазаданиями** – узел с БД метазаданий. Значение по умолчанию: 127.0.0.1.
    - **Имя пользователя БД с метазаданиями** – имя пользователя БД метазаданий. Значение по умолчанию: dozor.

- **Пароль пользователя БД с метазаданиями** – пароль пользователя БД метазаданий.
- **Название БД с метазаданиями** – название БД метазаданий. Значение по умолчанию: dozor.

- **Облачные домены организации** – список облачных хранилищ, которые используют сотрудники предприятия. Чтобы добавить облачный домен, следует нажать на кнопку **Добавить** и ввести его характеристики. Чтобы удалить домен из списка, следует нажать на значок рядом с идентификатором домена. Для дублирования домена следует нажать на значок и ввести его характеристики.

  Облачный домен определяется следующими параметрами:

  - **Тенант** – основной домен организации.
  - **Дополнительные домены организации** – дополнительные домены организации.

- **Ротация результатов выполнения задач** – настройки ротации результатов выполнения задач (по умолчанию ротация выключена). При включении ротации появляются следующие параметры:

  - **Ограничение на количество хранимых результатов** – количество сохраненных журналов сервиса **crawler-pccc**. Значение по умолчанию: 1.
  - **Интервал проверки ограничений** – интервал проверки системой вышеуказанного количества журналов. Значение по умолчанию: 1ч.

Производительность прокси центра управления краулером:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой процессу сервиса **crawler-pccc**. Значение по умолчанию: 2048.

Подключение к БД краулера:

- **Порт для сервиса БД Краулера** – порт, на котором БД Краулера ожидает соединения. Значение по умолчанию: 5439.

A.2.2.3. KEO DLP Traffic Analyzer

Настройки модуля KEO DLP Traffic Analyzer:

- Группа параметров **Захват сетевого трафика** (содержит параметры настройки используемой технологии захвата трафика с сетевого интерфейса):
  - **Сетевой интерфейс** – список имён сетевых интерфейсов, на которых KEO DLP Traffic Analyzer ожидает зеркалируемый незашифрованный трафик. Имена сетевых интерфейсов перечисляются через запятую без пробелов, например: **eth0,eth2**. Список всех имеющихся сетевых интерфейсов можно получить с помощью команды CLI **ifconfig**.
  - **Низкоуровневый фильтр** – строка, задающая параметры низкоуровневой фильтрации пакетов.

Значение по умолчанию: **not port 1025**. Рекомендуется использовать следующее значение:

```
not host <IP-адрес> and not host <IP-адрес-2> and ...
```

где **<IP-адрес>>**, **<IP-адрес-2>** и т.д. – IP-адреса узлов кластера KEO DLP, для которых не планируется использование сервиса KEO DLP Traffic Analyzer

- **Технология захвата** – используемая технология перехвата. Принимает значения **библиотека PF_RING** (выполняются перехваты с сетевого интерфейса модулем **pf_ring**) и **библиотека libpcap** (с помощью библиотеки Pcap). Значение по умолчанию: **библиотека PF_RING**.

  Если через сетевые интерфейсы проходит много данных, лучше выбрать библиотеку PF_RING. Она поможет уменьшить потери при перехвате большого объёма трафика.

  Если трафик поступает в малых объемах или сетевой интерфейс PF_RING не работает, следует использовать **библиотека libpcap**.

- **Асинхронный режим** – включает асинхронный цикл захвата трафика по технологии SPAN, позволяющий снизить нагрузку на процессор при небольшой сетевой активности. Принимает значения: **true** и **false**. Значение по умолчанию: **true**.

  Примечание

  Рекомендуется оставить включенным.

- **Период опроса (мс)** – время приостановки синхронного цикла захвата трафика, необходимое для снижения нагрузки при отсутствии трафика. Значение по умолчанию:0. При высокой нагрузке на систему рекомендуется установить значение 5-10 мс. Используется совместно с параметром **Асинхронный режим**.

- **Минимальный размер буфера для libpcap (Кб)** – ограничение в Кб на размер буфера для библиотеки **libpcap** при захвате и разборе трафика. Значение по умолчанию: 200000.

- **Список фильтруемых сетевых портов** – доступный для редактирования список портов. Значение по умолчанию:

  ```
  22,389,443,1010,1025,1344,2266,2269,2272,2344,3000,3001,3003,3004,3006,3010,3030,3268,3900,4444,5001,5434,5439,5440,5445,5558,7001,7199,7837,8008,8080,8090,8123,9000,9001,9042,9160,9200,9201,9301,9302,9400,9401,9666,9998,10000,10050,11344,16379,61616
  ```

  Рекомендованные значения параметров **Низкоуровневый фильтр** (**filter**) и **Список фильтруемых портов** (**filter_port_list**) исключают перехват данных на узлах и портах, используемых сервисами KEO DLP. Таким образом, снижается нагрузка на KEO DLP Traffic Analyzer.

  Если изменяется значение порта по-умолчанию, это изменение следует отразить в значении параметра **Список фильтруемых сетевых портов**. Для исключения перехвата прочих сервисов следует добавить порты, используемые этими сервисами, в список.

Во всех случаях, кроме перехвата ICAP-трафика, поступающего по технологии SPAN, не вносить порты 1344 и 2344 в список фильтруемых портов.

- **Включить nDPI-фильтрацию пакетов** – включает фильтрацию пакетов с помощью библиотеки **nDPI**. Принимает значение **true** и **false**. Значение по умолчанию: **false**.
- **Максимальное количество памяти для nDPI (Мб)** – максимальное количество выделяемой оперативной памяти в Мб под библиотеку **nDPI**. Значение по умолчанию: 512.
- **Сборщик TCP-потоков** (сборка TCP-потоков объединение их в непрерывный поток данных):
  - **Включить поддержку интерфейса с multiqueue** – включает поддержку сетевого интерфейса с multiqueue. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).
  - **Максимальное число неподтвержденных сегментов в буфере** – максимальное число неподтвержденных сегментов, находящихся в очереди получения сетевых пакетов. Значение по умолчанию: 64.

    Примечание

    Значение параметра подбирается администратором в соответствии с сетевой инфраструктурой и постепенно увеличивается от 10 до 128 сегментов.

    Примечание

    *Параметр используется при работе KEO DLP Traffic Analyzer в режиме мультиочереди, т.е. совместно с параметром **Включить поддержку интерфейса с multiqueue**.*
  - **Не ожидать фазу ESTABLISHED** – включает обработку соединения по стандарту TCP/IP. Принимает значения **true** и **false**. При значении **false** обработка соединения происходит по упрощенной схеме. Значение по умолчанию: **false** (выключено).
  - **Показывать предупреждения о потерях пакетов** – запись предупреждений о работе IP-пакетов в журнальный файл. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).
  - **Показывать предупреждения о дубликатах пакетов** – включает появление предупреждений о дубликатах пакетов. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).
  - **Показывать предупреждения о нарушении порядка пакетов** – включает появление предупреждений о нарушении порядка пакетов. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).

- **Показывать предупреждения о непредсказуемом поведении** – включает появление предупреждений о непредсказуемом поведении сборщика. Принимает значения **true** и **false**. Значение по умолчанию: **false** (выключено).

- **Сборщик IP-фрагментов** (параметры сборщика фрагментированных IP-пакетов):

  - **Включить** – включает сборку IP-фрагментов. Принимает значение **true** и **false**. Значение по умолчанию: **false**.

  - **Выбрасывать фрагментированные пакеты** – включает блокировку IP-фрагментов. Принимает значение **true** и **false**. Значение по умолчанию: **false**.

  - **Максимальный размер пакета (Б)** – максимальный размер пакета в байтах. Значение по умолчанию: 10240.

  - **Максимальное число фрагментов пакета** – максимальное число фрагментов пакета. Значение по умолчанию: 128.

  - **Таймаут сборки пакета (мс)** – время ожидания при сборке пакета в миллисекундах. Значение по умолчанию: 1000000.

  - **Максимальный размер IP заголовка (Б)** – максимальный размер заголовка IP-пакета в байт. Значение по умолчанию: 64.

  - **Отладка, расширенный лог** – включает расширенное отладочное журналирование. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

  - **Отладка, предупреждение медленного старта** – включает записи событий медленного старта в журнал. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

  - **Отладка, предупреждение неупорядоченности** – включает записи событий о неупорядоченной доставке IP-пакетов в журнал. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

  - **Отбрасывать сборки без начала** – включает игнорирование сборок без заголовков. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

  - **Пересчитывать контрольную сумму IP заголовка** – включает пересчет контрольной суммы заголовка IP-пакета. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

  - **Максимальное число собираемых пакетов** – максимальное число собираемых пакетов. Значение по умолчанию: 1024.

- Группа параметров **ICAP-сервер** (настройки ICAP-сервера):

  - **Включить ICAP-сервер** (**enable**) – включить анализ данных, поступающих от источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера). Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

  - **Порты ICAP-сервера** – сетевой порт, на котором ICAP-сервер ожидает данные. Значение по умолчанию: 1344.

- **Режим работы ICAP-сервера** – режим работы ICAP-сервера модуля KEO DLP Traffic Analyzer. Принимает значения **Работа в режиме REQMOD и RESPMOD**, **Работа в режиме REQMOD** и **Работа в режиме совместимости с Blue Coat**. Значение по умолчанию: **Работа в режиме REQMOD и RESPMOD**.

  При значении **Работа в режиме REQMOD и RESPMOD** KEO DLP Traffic Analyzer анализирует запросы и ответы, полученные по протоколу ICAP от источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера). KEO DLP Traffic Analyzer сохраняет в кэш принятые запросы (REQMOD) и ожидает ответы (RESPMOD) в рамках ICAP-сессии. После получения RESPMOD KEO DLP Traffic Analyzer анализирует данные, формирует сообщение-перехват и отправляет его в KEO DLP. Если KEO DLP Traffic Analyzer не получит ответ (RESPMOD), это приведет к потере принятых запросов (REQMOD).

  Если источник не поддерживает отправку ответов (RESPMOD) или анализ ответов (RESPMOD) не требуется, следует выбрать значение **Работа в режиме REQMOD**, при котором KEO DLP Traffic Analyzer, получив запрос, сразу анализирует его и отправляет сформированные сообщения-перехваты в KEO DLP. В этом случае KEO DLP Traffic Analyzer не ожидает ответов (RESPMOD) по протоколу ICAP от источника трафика.

  Внимание!

  В режиме анализа запросов (REQMOD) не будет перехватываться любая информация, загруженная из сети Интернет, так как для части веб-сервисов она может приходить в ответе сервера (например, скачивание файлов и входящая веб-почта). Также не будет работать связь между различными сетевыми сессиями (например, «авторизация – отправка эл. почты», «сохранение черновика - отправка письма» и т.д.) Кроме того, некоторые облачные хранилища будут разбивать загружаемые файлы объемом более 5 Мб на части, которые перехватываются по отдельности.

  Режим **Работа в режиме совместимости с Blue Coat** предназначен для работы с Blue Coat Proxy SG в режиме запросов (REQMOD) и ответов (RESPMOD).

  Примечание

  *Режим работы ICAP-сервера определяется только параметром **Режим работы ICAP-сервера**. Если модуль KEO DLP Traffic Analyzer использует режим анализа запросов и ответов, в настройках источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера) указывается URL или IP-адрес узла с ролью **Сервис перехвата и анализа сетевого трафика** (Traffic Analyzer). Это необходимо для случая, когда источники ICAP различаются (например, одни поддерживают отправку запросов и ответов, а другие могут работать только в режиме **Reqonly**). Описание взаимодействия KEO DLP Traffic Analyzer с различными прокси-серверами приведено в документе Модуль перехвата и анализа сетевого трафика «Traffic Analyzer». Руководство системного администратора). Поддерживаемые форматы URL:*

  - ***icap://ta.isim.local:1344/** или **icap://ta.isim.local:1344/reqresp** – передача запросов и ответов;*
  - ***icap://ta.isim.local:1344/reqonly** – передача запросов.*

Примечание

Рекомендуются следующие режимы в зависимости от используемого источника трафика:

- *KEO DLP webProxy или любые другие прокси-серверы, работающие согласно RFC – **Работа в режиме REQMOD и RESPMOD**.*
- *Режим **Работа в режиме совместимости с Blue Coat** предназначен для работы с прокси-сервером Blue Coat Proxy SG одновременно в режимах REQMOD и RESPMOD.*
- *IronPort (Cisco Web Security Appliance) – **Работа в режиме REQMOD** (IronPort может работать только в режиме REQMOD).*

- **Максимальный размер тела HTTP-запроса в ICAP (Б)** – максимальный размер ICAP-сессии в байтах, обработку которой выполняет KEO DLP Traffic Analyzer. Значение по умолчанию: 156314880 Б (149 Мб). При нулевом значении снимается ограничение на размер тела запроса.

Внимание!

Не рекомендуется слишком сильно увеличивать значение параметра по умолчанию в связи с возрастающей нагрузкой KEO DLP Traffic Analyzer на оперативную память и процессор.

- **Не обрабатывать запросы "CONNECT"** – отключает обработку HTTP-запросов вида **CONNECT**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

Внимание!

*Отключение обработки HTTP-запросов вида **CONNECT** позволяет повысить производительность работы KEO DLP Traffic Analyzer, поскольку уменьшается число обрабатываемых запросов.*

- **Максимальное число соединений с ICAP-сервером** – максимальное число попыток соединений с ICAP-сервером. Значение по умолчанию: 1000.
- **Максимальное число используемых ядер** – максимальное число потоков процессора, используемых при обработке трафика. Значение по умолчанию: 1.
- **Тип планировщика** – алгоритм распределения поступающего с прокси-серверов трафика по ядрам (потокам) ICAP-сервера. Общее количество потоков равно значению параметра **Максимальное число используемых ядер** (см. описание выше).

  Принимает значения: **хэш (hash)**, **круговой (rr)**. Значение по умолчанию: **хэш (hash)**.

При значении **хэш (hash)** каждому ICAP-серверу выделяется отдельный поток. Для IP-адреса ICAP-сервера вычисляется хэш. При таком алгоритме ICAP-сессии упорядоченно распределяются по потокам.

При значении **круговой (rr)** происходит равномерное распределение сессий по потокам ICAP-сервера. При таком алгоритме возможно неупорядоченное распределение ICAP-сессий по потокам.

Рекомендуется использовать значение по умолчанию.

- **Включить таймаут приема данных от клиента** – включает ожидание ответа от источника ICAP-трафика (прокси-сервера). Принимает значения **true** и **false**. Значение по умолчанию: **true** (включено).
- **Таймаут приема данных от клиента (с)** – определяет таймаут ожидания ответа в секундах от источника ICAP-трафика. Значение по умолчанию: 90.
- **Включить асинхронный режим ICAP (не буферизировать ответ клиенту)** – включает асинхронный режим работы ICAP-сервера, при котором ответ не сохраняется на KEO DLP Traffic Analyzer. Принимает значения **true** и **false**. Значение по умолчанию: **false**.

Внимание!

*Асинхронный режим работы ICAP-сервера поддерживается при многопоточном функционировании модуля **icap** (значение параметра **Максимальное число используемых ядер** > 0).*

Примечание

*При использовании источников трафика **F5 BIG-IP**, **Bluecoat ProxySG**, **Squid**, **McAfee**, принимающих только ответы с кодом 200, рекомендуется включить асинхронный режим работы ICAP-сервера в секции ICAP-сервер.*

- **Игнорировать ICAP заголовок "Allow 204"** – включает принудительный ответ ICAP-клиенту с кодом 204. Принимает значения **true** и **false**. Значение по умолчанию: **false**.
- **Оптимизировать выдачу ответов ICAP-клиентам** – при включенном параметре источники ICAP-трафика быстрее получают ответы на свои запросы. Принимает значения **true** и **false**. Значение по умолчанию: **true**.
- **Максимальное количество попыток создания сервера** – максимальное число попыток перезапустить ICAP-сервер. Параметр применяется только при включённом многопоточном ICAP-сервере (параметр **max_threads** отличен от нуля). Значение по умолчанию: 256.
- **Включить дополнительные параметры системного вызова bind** – настройки сокета, создающегося при подключении к ICAP-серверу. Значение по умолчанию: 0.

- Группа параметров **ICAPS-сервер**:
  - **Включить ICAPS-сервер** (**enable**) – включить анализ данных, поступающих от источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера) в зашифрованном виде. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.
  - **Порты ICAPS-сервера (через запятую)** – сетевой порт, на котором ICAPS-сервер ожидает данные.
  - **Путь к сертификату icaps** – путь к файлу сертификата шифрования.
  - **Путь к ключу icaps** – путь к файлу закрытого ключа.
  - **Режим работы ICAPS-сервера** – режим работы ICAPS-сервера модуля KEO DLP Traffic Analyzer. Принимает значения **Работа в режиме REQMOD и RESPMOD**, **Работа в режиме REQMOD** и **Работа в режиме совместимости с Blue Coat**. Значение по умолчанию: **Работа в режиме REQMOD и RESPMOD**.

    При значении **Работа в режиме REQMOD и RESPMOD** KEO DLP Traffic Analyzer анализирует запросы и ответы, полученные по протоколу ICAPS от источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера). KEO DLP Traffic Analyzer сохраняет в кэш принятые запросы (REQMOD) и ожидает ответы (RESPMOD) в рамках ICAPS-сессии. После получения RESPMOD KEO DLP Traffic Analyzer анализирует данные, формирует сообщение-перехват и отправляет его в KEO DLP. Если KEO DLP Traffic Analyzer не получит ответ (RESPMOD), это приведет к потере принятых запросов (REQMOD).

    Если источник не поддерживает отправку ответов (RESPMOD) или анализ ответов (RESPMOD) не требуется, следует выбрать значение **Работа в режиме REQMOD**, при котором KEO DLP Traffic Analyzer, получив запрос, сразу анализирует его и отправляет сформированные сообщения-перехваты в KEO DLP. В этом случае KEO DLP Traffic Analyzer не ожидает ответов (RESPMOD) по протоколу ICAPS от источника трафика.

    Внимание!

    В режиме анализа запросов (REQMOD) не будет перехватываться любая информация, загруженная из сети Интернет, так как для части веб-сервисов она может приходить в ответе сервера (например, скачивание файлов и входящая веб-почта). Также не будет работать связь между различными сетевыми сессиями (например, «авторизация – отправка эл. почты», «сохранение черновика - отправка письма» и т.д.) Кроме того, некоторые облачные хранилища будут разбивать загружаемые файлы объемом более 5 Мб на части, которые перехватываются по отдельности.

    Режим **Работа в режиме совместимости с Blue Coat** предназначен для работы с Blue Coat Proxy SG в режиме запросов (REQMOD) и ответов (RESPMOD).

Примечание

*Режим работы ICAPS-сервера определяется только параметром **Режим работы ICAPS-сервера**. Если модуль KEO DLP Traffic Analyzer использует режим анализа запросов и ответов, в настройках источника трафика (модуля KEO DLP Endpoint Agent или внешнего прокси-сервера) указывается URL или IP-адрес узла с ролью **Сервис перехвата и анализа сетевого трафика** (Traffic Analyzer). Это необходимо для случая, когда источники ICAPS различаются (например, одни поддерживают отправку запросов и ответов, а другие могут работать только в режиме **Reqonly**). Описание взаимодействия KEO DLP Traffic Analyzer с различными прокси-серверами приведено в документе Модуль перехвата и анализа сетевого трафика «Traffic Analyzer». Руководство системного администратора). Поддерживаемые форматы URL:*

- ***icap://ta.isim.local:1344/** или **icap://ta.isim.local:1344/reqresp** – передача запросов и ответов;*
- ***icap://ta.isim.local:1344/reqonly** – передача запросов.*

Примечание

Рекомендуются следующие режимы в зависимости от используемого источника трафика:

- *KEO DLP webProxy или любые другие прокси-серверы, работающие согласно RFC – **Работа в режиме REQMOD и RESPMOD**.*
- *Режим **Работа в режиме совместимости с Blue Coat** предназначен для работы с прокси-сервером Blue Coat Proxy SG одновременно в режимах REQMOD и RESPMOD.*
- *IronPort (Cisco Web Security Appliance) – **Работа в режиме REQMOD** (IronPort может работать только в режиме REQMOD).*

- **Максимальное число соединений с ICAPS-сервером** – максимальное число попыток соединений с ICAPS-сервером. Значение по умолчанию: 1000.
- **Максимальное число используемых ядер** – максимальное число потоков процессора, используемых при обработке трафика. Значение по умолчанию: 1.
- **Тип планировщика** – алгоритм распределения поступающего с прокси-серверов трафика по ядрам (потокам) ICAPS-сервера. Общее количество потоков равно значению параметра **Максимальное число используемых ядер** (см. описание выше).

  Принимает значения: **хэш (hash)**, **круговой (rr)**. Значение по умолчанию: **хэш (hash)**.

  При значении **хэш (hash)** каждому ICAPS-серверу выделяется отдельный поток. Для IP-адреса ICAPS-сервера вычисляется хэш. При таком алгоритме ICAPS-сессии упорядоченно распределяются по потокам.

  При значении **круговой (rr)** происходит равномерное распределение сессий по потокам ICAPS-сервера. При таком алгоритме возможно неупорядоченное распределение ICAPS-сессий по потокам.

Рекомендуется использовать значение по умолчанию.

- **Включить таймаут приема данных от клиента** – включает ожидание ответа от источника ICAP-трафика (прокси-сервера). Принимает значения **true** и **false**. Значение по умолчанию: **true** (включено).
- **Таймаут приема данных от клиента (с)** – определяет таймаут ожидания ответа в секундах от источника ICAP-трафика. Значение по умолчанию: 90.
- **Включить асинхронный режим ICAPS (не буферизировать ответ клиенту)** – включает асинхронный режим работы ICAPS-сервера, при котором ответ не сохраняется на KEO DLP Traffic Analyzer. Принимает значения **true** и **false**. Значение по умолчанию: **false**.

  Внимание!

  *Асинхронный режим работы ICAP-сервера поддерживается при многопоточном функционировании модуля **icaps** (значение параметра **Максимальное число используемых ядер** > 0).*

- **Игнорировать ICAPS заголовок "Allow 204"** – включает принудительный ответ ICAPS-клиенту с кодом 204. Принимает значения **true** и **false**. Значение по умолчанию: **false**.
- **Оптимизировать выдачу ответов ICAP-клиентам** – при включенном параметре источники ICAP-трафика быстрее получают ответы на свои запросы. Принимает значения **true** и **false**. Значение по умолчанию: **true**.
- **Максимальное количество попыток создания сервера** – максимальное число попыток перезапустить ICAPS-сервер. Параметр применяется только при включённом многопоточном ICAPS-сервере (параметр **max_threads** отличен от нуля). Значение по умолчанию: 256.
- **Включить дополнительные параметры системного вызова bind** – настройки сокета, создающегося при подключении к ICAPS-серверу. Значение по умолчанию: 0.

- Группа параметров **Анализатор данных** (настройки обработки перехватываемого потока данных):
  - **Обрабатываемые протоколы** – включает многопоточный режим работы протокола/протоколов. Необходимо установить флажки в списке. Доступен выбор следующих значений:
    - **http**;
    - **icap**;
    - **ftp**;
    - **smb**;
    - **cifs**;

- **smtp**;
- **pop3**;
- **imap**;
- **icq**;
- **xmpp**;
- **msn**;
- **mra**;
- **irc**;
- **skype**;
- **oscar**.

- **Максимальное время на обработку запроса (мс)** – максимальное время на обработку потока в миллисекундах, при превышении которого обработка прекращается. Значение по умолчанию: 200000.
- **Максимальная длина очереди запросов** – максимальное количество обработанных запросов от прокси-серверов к KEO DLP Traffic Analyzer, которое может находиться в очереди потока. Значение по умолчанию: 200.
- **Включить отчет о зависании обработки запроса** – включить сбор отладочной информации, если обработка ICAP-сессии занимает очень много времени. Принимает значение **true** и **false**. Значение по умолчанию: **true**.
- **Добавлять тело запроса в отчет** – включить сбор отладочной информации о теле ICAP-сессии. Принимает значение **true** и **false**. Значение по умолчанию: **true**.
- **Включить трассировку выполнения запросов (отладочный режим)** – включить сбор отладочной информации об обработке выполнения всех запросов (учитывается метод запроса и URL) в реальном времени вне зависимости от того, занимает ли ICAP-сессия очень много времени или нет. Этот параметр доступен только в интерфейсе командной строки.
- **Максимальный размер обрабатываемого запроса (Б)** (**http_body_limit**) – максимальный размер потока в байтах, принимаемого на обработку. При превышении этого размера поток отбрасывается без обработки. Значение по умолчанию: 104857600.
- **Обработка протокола HTTP over proxy** (**http_redirect**) – в случае использования прокси-сервера включает обработку протокола HTTP. Принимает значение **true** и **false**. Значение по умолчанию: **false**.
- **Обработка протокола HTTPS over proxy** (**https_redirect**) – в случае использования прокси-сервера включает обработку протокола HTTPS. Принимает значение **true** и **false**. Значение по умолчанию: **false**.

- **Обработка протокола OSCAR over proxy** (**oscar_redirect**) – в случае использования прокси-сервера включает обработку протокола OCSAR. Принимает значение **true** и **false**. Значение по умолчанию: **true**.

- Группа параметров **Фильтрация сообщений** (настройка общей фильтрации):

  - **Список отключенных детекторов** – список отключенных детекторов из набора отключаемых. Поддерживается отключение детекторов **!generic**, **accounts** и **!file-upload**.

  - **Включить фильтр однотипных сообщений** – включает фильтрацию однотипных сообщений. Под однотипными сообщениями понимаются сообщения, в которых совпадают заголовки, идентифицирующие пользователя и его тип действия на ресурсе.

    Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

    Примечание

    Включение фильтрации однотипных сообщений позволяет повысить производительность работы KEO DLP Traffic Analyzer. Рекомендуется оставить параметр включенным.

  - **Размер кэша фильтра однотипных сообщений** – размер кэша хранения однотипных сообщений, полученных в результате фильтрации. Измеряется в количестве записей. Значение по умолчанию: 100000. При превышении этого размера происходит ротация кэша – старые записи удаляются.

  - **Время жизни записи в кэше фильтра однотипных сообщений (сек)** – максимальное время в секундах, отводимое на хранение записей об однотипных сообщениях в кэше. Значение по умолчанию: 28800 (8 часов). Старые записи удаляются.

    Примечание

    По истечении таймаута необходимо выполнить действие, которое сформирует перехваченное сообщение, отличное от однотипных. После этого возобновятся перехваты однотипных сообщений.

- Группа параметров **Менеджер сообщений** (формирование отчетов):

  - **Максимальное время на запись одного отчёта в спул (сек)** – максимальное время в секундах, отводимое на запись одного отчёта в спулы. Значение по умолчанию: 0. Рекомендуется оставить значение по умолчанию.

- Группа параметров **HTTP-спул сообщений** (настройки отправки сообщений в **mailfilter** по протоколу HTTP):

  - **Включить** – включает передачу сообщений по протоколу HTTP. Принимает значение **true** и **false**. Значение по умолчанию: **true**. Следует оставить значение **true**, а в

качестве значения параметра **enable** секции **SMTP-спул сообщений** установить **false**.

- **Адрес сервиса (URL)** – URL-ресурс с компонентом **http_reporter**. Значение по умолчанию: **http://127.0.0.1:3010/spool**.
- **Отладка** – включение вывода отладочной информации. Принимает значение **true** и **false**. Значение по умолчанию: **false** (вывод отладочной информации выключен).
- **Таймаут соединения (с)** – время ожидания соединения с HTTP-спулом в секундах. Значение по умолчанию: 10.
- **Таймаут обмена данными (с)** – время ожидания ответа на запросы пользователя в секундах. Значение по умолчанию: 10.

- Группа параметров **SMTP-спул сообщений** (настройка записи в спулы сервиса **sender**):
  - **Включить SMTP-спул** – запись сообщений, генерируемых KEO DLP Traffic Analyzer, в спул сервиса **sender**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**. Следует оставить значение **true**, а в качестве значения параметра **enable** секции **HTTP-спул сообщений** установить **false**.
  - **Путь к каталогу SMTP-спула** – путь к каталогу SMTP-спула. Значение по умолчанию: **${smap-settings/common/smap-home}/spool/smap-send/**.
  - **Иерархические делители SMTP-спула сообщений** – иерархические делители SMTP-спула сообщений. В качестве значения используется убывающий ряд натуральных чисел, разделенных пробелами. Значение по умолчанию: **3600 700 50**.
  - **Слоты SMTP-спула сообщений** – слоты спула. В качестве значения используется ряд имён вида **norm<n>**, разделённых пробелами, где <n> – натуральные числа. Значение по умолчанию: **norm4 norm5 norm6**.
  - **Адрес, записываемый в поле FROM SMTP-конверта при помещении сообщения в спул** – адрес, записываемый в поле FROM SMTP-конверта при помещении сообщения в спул. Значение по умолчанию: **trafficagent@example.com**. Следует установить актуальное значение.
  - **Адрес, записываемый в поле RCPT SMTP-конверта при помещении сообщения в спул** – адрес или адреса, записываемые в поле RCPT SMTP-конверта при помещении сообщения в спул. Значение по умолчанию: **dozor@example.com**. Следует установить актуальное значение.
  - **Адрес SMTP-сервера** – доменное имя или IP-адрес узла кластера KEO DLP, имеющего роль **Фильтр почтового потока**. Значение по умолчанию: **localhost**. Следует установить актуальное значение.
  - **Порт для подключения к узлу server-name** – порт для подключения к узлу, указанному в предыдущем параметре. Значение по умолчанию: 1025. Следует установить актуальное значение порта, на котором почтовый фильтр ожидает соединения (должно совпадать со значением, указанным в конфигурационном файле **smtp-gw.conf**, по умолчанию – 1025).

- **Протокол SMTP-сервера** – тип сервера, который используется для отправки перехваченных пакетов. Значение по умолчанию **SMTP**. Для зашифрованных соединений можно выбрать расширения **SMTPS** или **STARTTLS**.

- **Количество повторных попыток подключения при возникновении ошибок** – количество повторных попыток подключения при возникновении ошибок. Значение по умолчанию: 5.

- **Действие при ошибке отправки** – действие при ошибке. Принимает следующие значения: **Сменить профиль отправки**, **Продолжать попытки отправить**, **Переместить сообщение в очередь ошибок** и **Удалить сообщение**. Значение по умолчанию: **Продолжать попытки отправить** (повторить попытку подключения).

- **Версия заголовков писем в спуле** – версия заголовков писем в спуле. Значение по умолчанию: 2.6.

- Группа параметров **Лицензирование продукта** (параметры соединения с сервером лицензирования):

  - **Адрес сервера лицензий (URL)** – URL для соединения с сервером лицензирования. Следует указать значение вида **https://<master_host>:3004/license/dozor/modules/traffic-agent**, где **<master_host>** – FQDN или IP-адрес master-узла.

- Группа параметров **Расширенные настройки** (содержит параметры обработки перехватываемого потока данных):

  - **Используемые ядра процессора** – идентификаторы потоков, в которых функционирует KEO DLP Traffic Analyzer. Принимает значения: **all** и **half**. При значении **all** используются все процессорные ресурсы, а при значении **half** – половина.

  - **Планировщик задач** – алгоритм работы балансировщика задач. Принимает значения: **SCHED_FIFO** и **SCHED_RR**. Значение по умолчанию: **SCHED_FIFO**. При значении **SCHED_FIFO** задачи размещаются в очереди и их выборка происходит по алгоритму FIFO. При значении **SCHED_RR** выбор выполняемых задач из списка выполняется случайным образом. Рекомендуется использовать значение по умолчанию.

  - **Базовый приоритет планировщика задач** – относительный уровень приоритета, от которого отсчитываются приоритеты задач KEO DLP Traffic Analyzer. Значение по умолчанию: 1.

  - **Максимальное время сборки сообщения MessageStream (с)** – максимальное время сборки сообщения детектором, выраженное в секундах. Значение по умолчанию: 300.

  - **Размер кэша хранения одновременных потоков данных (Б)** – размер кэша хранения одновременных потоков зеркалируемого незашифрованного трафика. Значение по умолчанию: 10000.

  - **Время жизни потока данных (с)** – максимальное время в секундах, отводимое на хранение потока зеркалируемого незашифрованного трафика в кэше без обращений к нему. Значение по умолчанию: 300.

- **Максимальных размер потока данных (Б)** – максимальный размер потока зеркалируемого незашифрованного трафика в байтах, при превышении которого поток отбрасывается. Значение по умолчанию: 2000000000.
- **Максимальное время обработки потока данных (с)** – максимальное время в секундах, отводимое на обработку одного пакета в потоке данных. Значение по умолчанию: 300.
- **Максимальный размер используемой виртуальной памяти (МБ)** – ограничение на размер используемой оперативной памяти в мегабайтах. Значение по умолчанию: 0 (нет ограничения).
- **Оповещение о превышении максимального размера используемой виртуальной памяти** – журналировать событие превышения ограничения на размер оперативной памяти. По умолчанию выключено.
- **Получение дампов потоков анализатора** – сохранение дампа памяти процесса **tragent** в случае превышения потоком анализатора данных установленного времени выполнения. По умолчанию включено.

Примечание

*Получение дампов не будет работать, если параметр **kernel.yama.ptrace_scope** установлен в значение 3.*

A.2.3. Настройка средств фильтрации перехваченных данных и детектирования критичной информации

A.2.3.1. Прием сообщений

Балансировка трафика:

Чтобы добавить конфигурацию балансировки трафика, необходимо нажать на кнопку **Добавить**. Чтобы дублировать конфигурацию, следует щелкнуть мышью на значок  и ввести ее характеристики. Для удаления конфигурации следует нажать на значок  рядом с идентификатором конфигурации.

Конфигурация балансировки трафика определяется следующими параметрами:

- **Название конфигурации балансировки** – название конфигурации балансировки трафика.
- **Порт для внешних соединений** – порт, на котором сервис балансировки трафика ожидает соединения. Значение по умолчанию 1010.
- **Время ожидания запроса от клиента (с)** – время ожидания запроса от клиента, выраженное в секундах. Значение по умолчанию 10.

Примечание

В качестве клиента выступают внешние системы, например SMTP/HTTP/ICAP-серверы.

- **Время ожидания запроса от сервера (с)** – время ожидания запроса от серверов фильтрации, которые задаются в параметре **Узлы для балансировки**. Выражено в секундах. Значение по умолчанию по умолчанию 10.
- **Максимальное количество соединений** – максимальное количество соединений, которое принимает балансировщик от клиента (по умолчанию 1000).
- **Метод балансировки** – алгоритм балансировки трафика. Принимает значения: **roundrobin**, **leastconn** и **source**.

  При значении **roundrobin** нагрузка будет распределена равномерно в соответствии с весом каждого сервера фильтрации KEO DLP, если такой указан ниже. При значении **leastconn** запросы будут передаваться серверу с наименьшим количеством подключений. При значении **source** сервер для соединения назначается на основании хэша IP-адреса отправителя запроса и весов серверов.

  Значение по умолчанию **roundrobin**.
- **Узлы для балансировки** – узлы, по которым распределяется трафик. Принимает значения:
  - **Автоматическое определение доступных mailfilter (HTTP)** – автоматически определяются узлы с сервисом **mailfilter**, ожидающие трафик по HTTP-интерфейсу.
  - **Автоматическое определение доступных mailfilter (ICAP)** – автоматически определяются серверы фильтрации, ожидающие ICAP-трафик.
  - **Автоматическое определение доступных smtp-gw** – автоматически определяются узлы с сервисом **smtp-gw**.
  - **Указать вручную** – узлы для балансировки задаются вручную. При выборе **Указать вручную** следует задать следующие параметры:
    - **Тип балансировки** – протокол, по которому распределяется нагрузка между узлами.
    - **Узлы** – добавить одну или несколько записей резервных узлов, предназначенных для балансировки. Запросы от внешних систем будут перенаправляться на эти узлы при недоступности серверов фильтрации KEO DLP. Для добавления новой записи необходимо нажать на кнопку **Добавить**. Чтобы дублировать запись, следует щелкнуть мышью на значок  и ввести характеристики. Для удаления записи следует нажать на значок  рядом с идентификатором записи.

      Запись резервного узла имеет следующие параметры:

      - **Сетевой адрес** – FQDN или IP-адрес резервного узла.
      - **Номер порта** – номер порта, на котором резервный узел будет ожидать соединения.
      - **Вес балансировки** – коэффициент, помогающий балансировщику распределять нагрузку между серверами фильтрации. Узел с большим весом будет получать большее число запросов.

Пример: сервер с весовым коэффициентом 2 будет получать в 2 раза больше запросов, чем сервер с весом, равным 1.

Пример 2: имеется 3 сервера фильтрации A, B и C. Сервера A и B имеют вес, равный 1, а третий сервер имеет весовой коэффициент 2. При недоступности сервера C нагрузка распределится равномерно между серверами A и B. При восстановлении своей работоспособности сервер C будет получать в 2 раза больше запросов, чем сервера A и B.

Прием сообщений:

- **Порт** – номер порта, на котором будет принимать почту SMTP-прокси. Значение по умолчанию: 1025.
- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **smtp-gw**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Отвергать сообщения при загрузке системы более** – отвергать сообщения при загрузке системы, превышающей указанное значение. Значение по умолчанию: 20. При достижении этого порога в журнальный файл **$smap_home/log/smtp_gw.log** записывается сообщение вида **Feb 14 12:23:18 bvm193 smtp-gw-1025[8058]: Load average too high: refusing email from 10.31.7.193:42465** и SMTP-прокси перестает принимать новые сообщения.
- **Отвергать соединения при загрузке системы более** – отвергать соединения при загрузке системы, превышающей указанное значение. Значение по умолчанию: 30. При достижении этого порога в журнальный файл **$smap_home/log/smtp_gw.log** записывается сообщение вида **Feb 14 12:22:56 bvm193 smtp-gw-1025[7427]: Load average too high: rejecting connection from 10.31.7.193:42433**, а также отвергается установка новых соединений с SMTP-прокси.
- **Максимальный размер принимаемого сообщения (МБ)** – максимально допустимый размер принимаемого сообщения (в мегабайтах). Данным параметром можно снять ограничение на размер принимаемого сообщения, установив значение, равное 0. Значение параметра по умолчанию: 40 Мб.
- **Таймаут при приеме (с)** – максимальный тайм-аут при приеме сообщений, в секундах. Значение по умолчанию: 100.
- **Количество процессов SMTP-прокси** – максимальное число порожденных процессов SMTP-прокси. Значение по умолчанию: 10.
- **Поддержка BINARY MIME** – поддержка BINARY MIME. Данный параметр включает поддержку обработки частей сообщения, у которых поле **Content-Transfer-Encoding** имеет значение **BINARY**. По умолчанию параметр включен.
- **Использовать настройки anti-relay** – определяет, нужно ли выполнять настройку **anti-relay** для SMTP-прокси. В типовой конфигурации данная опция не активирована. В случае активации необходимо задавать такие параметры, как **Список внутренних сетей** и др.

- **Список внутренних сетей** – список адресов внутренних сетей. Адреса задаются в виде сеть/маска, например: 192.168.10.0/24, 192.168.10.0/255.255.255.0, и разделяются пробелами.

- **Список внутренних почтовых доменов** – отвечает за входящую почту и определяет список почтовых доменов, доступных для отправки сообщений в KEO DLP. Элементы списка разделяются пробелами или запятыми.

- **Проверять адреса в DNS для внутренних пользователей** – определяет, нужно ли выполнять проверку адреса пользователя внутренней сети в DNS. По умолчанию такая проверка не выполняется.

- **Проверять адреса в DNS для внешних пользователей** – определяет, нужно ли выполнять проверку адреса пользователя внешней сети в DNS. По умолчанию в типовой конфигурации такая проверка выполняется.

- **Имя голосующей зоны ORBS** – определяет имя системы предотвращения получения спама на основе анализа почтовых адресов. Подробная информация представлена на сайте Mail Abuse Prevention System LLC. В том случае, если параметр не используется, задается пустая строка.

- **Ответ, означающий принадлежность к спамерским доменам** – строка, при получении которой сообщение будет считаться спамом. Задается строка, означающая принадлежность к спамерским доменам. Значение по умолчанию: **127.0.0.2**.

- **Что делать с сообщением из спамерского домена** – определяет действие, производимое над сообщениями, являющимися спамом. Возможны два значения: **Добавить заголовок** и **Отказать**. Значение по умолчанию: **Отказать**.

- **Использовать SPF** – включение/выключение использования технологии SPF для проверки подлинности домена отправителя. Настраиваемый служебный параметр. По умолчанию не активирован.

- **Использовать Greylisting** – включение/выключение использования технологии Greylisting для фильтрации спама. Настраиваемый служебный параметр. По умолчанию не активирован.

- **Использовать базу Cassandra для Greylisting** – включение/выключение использования базы Cassandra в технологии Greylisting.

- **Файл базы данных Greylisting** – параметр, определяющий файл БД технологии Greylisting. Значение по умолчанию: **${smap-settings/common/smap-home}/graylist/grey.db**.

- **Начальная задержка Greylisting** – параметр, определяющий начальную задержку технологии Greylisting. Значение по умолчанию: 0.

- **Время жизни новых записей Greylisting** – параметр, определяющий период хранения новых записей Greylisting. Значение по умолчанию: 0.

- **Время жизни активных записей Greylisting** – параметр, определяющий период хранения активных записей Greylisting. Значение по умолчанию 0.

- **Список высокоприоритетных отправителей** – список отправителей, имеющих высокий приоритет. Сообщения, отправленные с адресов, удовлетворяющих какому-

либо элементу списка, помещаются в спул **mailfilter-high** и обрабатываются вне очереди. Элементы списка разделяются пробелами или запятыми. Элементами списка могут быть конкретные почтовые адреса (например, **support@example.com**), любые адреса из конкретного домена (например, **@example.com**), или любые адреса из конкретного домена и всех его поддоменов (например, **example.com**).

- **Список высокоприоритетных получателей** – список получателей, имеющих высокий приоритет. Сообщения, отправляемые на адреса, удовлетворяющие какому-либо элементу списка, помещаются в спул **mailfilter-high** и обрабатываются вне очереди. Параметр задаётся аналогично параметру **Список высокоприоритетных отправителей**.

- **Настроить параметры SSL** – включение/выключение приема писем по протоколу SMTPS. При значении **SSL включен** параметры SSL становятся доступными для редактирования. Значение по умолчанию: **SSL выключен**.

  - **Файл, содержащий X.509 сертификат сервера в формате PEM** – путь к файлу сертификата сервера в формате PEM.

  - **Файл, содержащий Закрытый Ключ в формате PEM** – путь к файлу закрытого ключа в формате PEM.

  - **Файл, содержащий параметры алгоритма DH в формате PEM (необязателен)** – путь к файлу параметров алгоритма Диффи-Хеллмана в формате PEM. Необязательно для заполнения.

  - **Задает имя Эллиптической Кривой для алгоритмов ECDH, например secp384r1 (необязателен) (sslparam-ecdhcurve)** – имя эллиптической кривой для алгоритма Диффи-Хеллмана. Необязательно для заполнения.

  - **Список разрешенных шифров и протоколов шифрования (необязателен)** – список разрешенных шифров и протоколов шифрования. Необязательно для заполнения. Значение по умолчанию: **all:!anull:!enull:!sslv2:!export:!rc2:!des**.

  - **Включить SSL при старте (использовать SMTPS протокол)** – при включении этого параметра, порт сервиса **smtp-gw** работает как порт SMTPS. По умолчанию выключено.

A.2.3.2. Обработка сообщений

Настройки снижения уровня доверия участников переписки:

- **Коэффициент величины снижения уровня доверия получателя сообщения** – коэффициент, понижающий уровень доверия участников переписки. Значение по умолчанию: 0.2.

Хранилище ключей S/MIME:

- **Директория для ключей и сертификатов S/MIME** – расположение закрытых ключей и сертификатов получателей сообщений. Значение по умолчанию: **/opt/dozor/etc/keystores**.

- **Пароль по умолчанию для хранилищ ключей S/MIME** – пароль по умолчанию для хранилищ ключей и сертификатов S/MIME. Значение по умолчанию: **password**.

Сервис распознавания речи:

- **Локальный порт, на котором сервер будет принимать соединения** – локальный порт, на котором сервис распознавания речи будет принимать соединения. Значение по умолчанию: 9304.

- **Асинхронное журналирование** – асинхронное ведение журнала. Рекомендуется использовать для повышения пропускной способности сервиса распознавания речи. При использовании асинхронного журналирования вывод журнала может задерживаться, а последний журнальный файл может быть утерян в случае аварийной остановки сервиса. По умолчанию выключено.

- **Максимальное количество обработчиков, выполняющих распознавание** – количество экземпляров обработчика, одновременно выполняющих распознавание речи. Для каждого экземпляра организуется очередь сообщений для обработки, максимальное количество сообщений в очереди определяется параметром **Размер очереди заданий**. При использовании ЦП рекомендуется оставить значение по умолчанию. При использовании графических процессоров рекомендуется устанавливать значение, равное количеству графических процессоров. Значение по умолчанию: 1. При значении 0 количество экземпляров обработчика будет равно количеству ядер процессора.

- **Количество потоков для приема сообщений** – количество внутренних сетевых потоков сервиса распознавания речи, используемых для приема сообщений для обработки. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству логических ядер центрального процессора). Рекомендуется использовать значение по умолчанию или меньше.

- **Размер очереди заданий** – максимальное количество сообщений для обработки для каждого экземпляра обработчика. Значение по умолчанию: 0 (фактически будет использоваться значение 100). При использовании нескольких экземпляров обработчика и/или графических процессоров рекомендуется устанавливать значение 1000.

- **Количество потоков для работы с обработчиками** – количество внутренних сетевых потоков сервиса распознавания речи, которые отправляют результаты распознавания на вывод во внешний интерфейс. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству логических ядер центрального процессора). Рекомендуется использовать значение по умолчанию или меньше.

- **Количество GPU** – количество графических процессоров, используемых для распознавания речи. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству графических процессоров на сервере).

- **Максимальный размер запроса** – максимально допустимый размер сообщения в мегабайтах, принимаемый сервисом распознавания речи на обработку. Значение по умолчанию: 100.

- **Время ожидания ответа** – максимальное время (в секундах) ожидания экземпляром обработчика ответа от сервиса распознавания, после которого запрос обработчика будет перезагружен. Значение по умолчанию: 120.

- **Режим работы модели** – режим работы сервиса распознавания речи. Принимает значения: **CPU** (работа на серверах с центральным процессором) и **GPU** (ускоренная работа на серверах с графическими процессорами). Значение по умолчанию: **CPU**.

Внимание!

Настоятельно рекомендуется использовать сервер с графическими процессорами. Чем больше графических процессоров будет на сервере – тем производительнее будет сервис распознавания речи. При отсутствии сервера с графическими процессорами следует выделить сервер с наибольшим количеством запаса производительности центрального процессора.

- **Уровень журналирования** – степень детализации журналирования. Значение по умолчанию: **Предупреждения**. В качестве значения можно выбрать один из следующих параметров в раскрывающемся списке:
  - **Отключен** – журналирование отключено;
  - **Критические ошибки** – журналировать только критические ошибки;
  - **Ошибки** – журналировать все ошибки;
  - **Предупреждения** – журналировать все ошибки и предупреждения о работе модуля;
  - **Уведомления** – журналировать все ошибки, предупреждения и уведомления о работе модуля;
  - **Информация** – журналировать все ошибки, предупреждения, уведомления и информацию о работе модуля;
  - **Отладка** – журналировать все ошибки, предупреждения, уведомления и полную отладочную информацию.
- **Каталог для временных файлов** – временный каталог для хранения аудиозаписей из раздела **Записи с микрофона** большой карточки персоны. Значение по умолчанию: **/data/temp/stt**.

Сервис фильтрации сообщений:

- **Вывод отладочной информации** – включает вывод отладочной информации.

  Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Порт HTTP-интерфейса** – значение порта HTTP-интерфейса. Значение по умолчанию: 3010.
- **Время ожидания завершения работы сервиса перед принудительной остановкой** – время ожидания завершения работы сервиса фильтрации сообщений перед принудительной остановкой, необходимое для завершения обработки принятых сообщений. Сервис **mailfilter**, находящийся в режиме ожидания, останавливает прием сообщений и отправляет источникам трафика ответ с кодом 503. Значение по умолчанию: 60 секунд.
- **Количество потоков обработки спула сообщений** – количество потоков обработки спула сообщений. Значение по умолчанию: 5.

- **Таймаут на обработку сообщения (с)** – таймаут на общую обработку (распаковку, извлечение вложений и обработку политикой) сообщения в секундах. Значение по умолчанию: 600.
- **Доля времени на распаковку сообщения (в процентах от общего времени на обработку)** – доля времени на распаковку сообщения от общего времени на обработку, выраженная в процентах. Значение по умолчанию: 50.
- Группа параметров **ICAP-интерфейс** (настройки обработки ICAP-трафика от различных прокси-серверов, выполняется дополнительная фильтрация HTTP-трафика по протоколу ICAP):
  - **Включить ICAP-интерфейс** – включение ICAP-интерфейса. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
  - **Порт ICAP-интерфейса** – порт, на котором ICAP-интерфейс ожидает соединения. Значение по умолчанию: 1344.
  - **Обрабатывать только указанные MIME-типы** – включает обработку MIME-типов, указанных в параметре **MIME-типы**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.
  - **MIME-типы** – определяет список MIME-типов сообщений, проверяемых ICAP-интерфейсом. Для добавления типа содержимого необходимо нажать кнопку рядом с элементом списка. Для удаления типа содержимого необходимо нажать кнопку рядом с элементом списка.

    По умолчанию проверяются следующие регулярные выражения, соответствующие типам сообщений:

    - **multipart/form-data** – HTML-формы с бинарными данными
    - **^application/msexcel** – документы MS Excel
    - **^application/msword** – документы MS Word
    - **^application/msaccess** – документы MS Access
    - **^application/mspowerpoint** – презентации MS PowerPoint
    - **^application/vnd.visio** – схемы MS Visio
    - **^application/vnd.ms-** – любые документы MS Office
    - **^application/vnd.oasis.opendocument** – текстовые документы OpenOffice
    - **^application/vnd.openxmlformats-officedocument** – любые документы формата OpenXML (MS Office 2010)
    - **^application/x-compressed** – любые архивы
    - **^application/x-sfx** – SFX-файлы
    - **application/zip** – ZIP-архивы

- **application/x-bzip2** – BZIP2-архивы
- **application/x-cpio** – архивы RMP-пакетов
- **application/x-tar** – TAR-архивы
- **application/x-gtar** – GTAR-архивы
- **application/x-iscab** – CAB-архивы
- **application/x-mscab** – CAB-архивы
- **application/x-7z-compressed** – 7ZIP-архивы
- **application/x-rar-compressed** – RAR-архивы
- **^text/** – текстовые документы
- **^application/pdf** – документы PDF
- **application/postscript** – страницы на языке PostScript
- **application/rtf** – документы RTF
- **image/x-djvu** – документы DjVu
- **message/rfc822** – сообщения электронной почты
- **message/x-emlx** – сообщения электронной почты (расширенный формат)

- **Не обрабатывать сообщения с пустым телом** – отключает обработку ICAP-сообщений, у которых отсутствует тело. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.
- **Выдавать ответ с кодом 200/204 при ошибках обработки** – включает получение ответов от ICAP-клиента с кодами 200/204 при ошибках обработки. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

- Группа параметров **ICAP-источники** (настройки идентификации ICAP-трафика от внешних источников):
  - **Метка источника** – название, отражающее реалии ICAP-источника.
  - **Имя заголовка** – имя заголовка, определяющего источник.
  - **Значение заголовка (точное совпадение или регулярное выражение)** – ввести значение заголовка, определяющего источник. Может использоваться точное совпадение или регулярное выражение.

Примечание

*Чтобы добавить конфигурацию источника, следует нажать на кнопку **Добавить**. Чтобы дублировать конфигурацию, следует щелкнуть мышью на значок*  *и ввести*

ее характеристики. Для удаления конфигурации следует нажать на значок  *рядом с идентификатором конфигурации.*

- **Использовать дополнительные методики извлечения текстов** – включает использование дополнительных алгоритмов извлечения текстов. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Определять журнальные файлы** – включает определение наличия журнальных данных в текстовых файлах.

  Сервис **mailfilter** выполняет проверку вложения с типом **TEXT/PLAIN** на наличие признаков регулярной структуры журнального файла, например, столбцов. Если такая структура присутствует, вложению присваивается тип **APPLICATION/LOG-DATA**, недоступный для просмотра в KEO DLP.

  Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.
- **Минимальный размер файла для определения журнальных файлов (Кб)** – минимальный размер файла в Кб, необходимый для определения наличия журнальных данных в текстовых файлах.

  Текстовые файлы, размер которых больше или равен значению параметра **Минимальный размер файла для определения журнальных файлов (Кб)**, будут определены, как журнальные файлы типа **APPLICATION/LOG-DATA**.

  Используется совместно с параметром **Определять журнальные файлы** для исключения просмотра текстовых файлов большого размера. Значение по умолчанию: 512.
- Группа параметров **Проверка сообщений с помощью антивируса** (настройка взаимодействия с внешним антивирусом по протоколу ICAP):
  - **Включить проверку с помощью антивируса** – включение антивируса. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
  - **Действие антивируса** – действие антивируса. Принимает значения: **Вылечить** и **Сканировать**. Значение по умолчанию: **Вылечить**.
  - **Имя хоста** – имя сервера с установленным антивирусом. Параметр обязателен для заполнения. Значение по умолчанию: **127.0.0.1**.
  - **URL** – значение URL антивируса. Значение по умолчанию: **/avscanresp?action=SCANREPAIRDELETE**.
  - **Порт** – сетевой порт сервера с установленным антивирусом. Параметр обязателен для заполнения. Значение по умолчанию: 1344.
- Группа параметров **Спул сообщений** (настройка спула сообщений):
  - **Каталог для входящей почты** – определяет каталог (спул), в котором хранятся исходные данные. Значение по умолчанию: **${smap-settings/common/smap-home}/spool/smap**.

- **Слоты в каталоге для входящей почты** – определяет количество слотов в каталоге для сообщений входящей почты с нормальным приоритетом. Значение по умолчанию: 0 1 2 3 4 5. Это значит, что для чтения сообщений доступно шесть слотов - каталоги с именами **/spool/smap/norm0**, **/spool/smap/norm1**, **/spool/smap/norm2**, **/spool/smap/norm3**, **/spool/smap/norm4** и **/spool/smap/norm5**.

- **Слоты для сообщений высокого приоритета в каталоге для входящей почты** – определяет слоты для сообщений входящей почты с высоким приоритетом. Значение по умолчанию: 0 1. Это значит, что имеется два слота с именами **spool/smap/high0** и **spool/smap/high1**.

- **Слоты, доступные для чтения** – определяет слоты, доступные для чтения сообщений с нормальным приоритетом. Значение по умолчанию: 0 1 2 3 4 5. Это значит, что для чтения сообщений доступно шесть слотов - каталоги с именами **/spool/smap/norm0**, **/spool/smap/norm1**, **/spool/smap/norm2**, **/spool/smap/norm3**, **/spool/smap/norm4** и **/spool/smap/norm5**.

- **Слоты, доступные для чтения сообщений высокого приоритета** – определяет слоты, доступные для чтения сообщений с высоким приоритетом. Значение по умолчанию: 0 1. Это значит, что в каталоге для входящих сообщений имеются два слота для сообщений высокого приоритета, из которых возможно чтение, с именами **/spool/smap/high0** и **/spool/smap/high1**.

- **Слоты, доступные для записи** – определяет слоты, доступные для записи сообщений с нормальным приоритетом. Значение по умолчанию: 0 1 2 3 4 5. Это значит, что для записи сообщений доступны шесть слотов - каталоги с именами **/spool/smap/norm0**, **/spool/smap/norm1**, **/spool/smap/norm2**, **/spool/smap/norm3**, **/spool/smap/norm4** и **/spool/smap/norm5**.

- **Слоты, доступные для записи сообщений высокого приоритета** – определяет слоты, доступные для записи сообщений с высоким приоритетом. Значение по умолчанию: 0 1. Это значит, что имеется два слота с именами **spool/smap/high0** и **spool/smap/high1**.

- **Пауза перед перечитыванием спула (с)** – периодичность обработки спула сообщений сервисом **mailfilter** в секундах. Значение по умолчанию: 5.

- Группа параметров **Спул ошибок** (настройка хранилища ошибок обработки сообщений):

  - **Каталог для входящей почты** – каталог для входящей почты. Значение по умолчанию: **${smap-settings/common/smap-home}/spool/smap**.

  - **Слоты, доступные для записи** – слоты, доступные для записи. Значение по умолчанию: 0. Это значит, что для записи сообщений доступны четыре слота, т.е. каталоги с именами **/spool/smap/norm0**.

  - **Сохранять логи в спул ошибок** –включает запись ошибок обработки сообщений в файл вида **<vid>.err**. Файл данного вида сохраняется в **error-spool**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

- **Перемещать обрабатываемые сообщения в спул ошибок при аварийном завершении процесса фильтрации** – используется для защиты от постоянного аварийного завершения работы сервиса **mailfilter** в том случае, если в очереди есть сообщения,

приводящие к аварийному завершению. Принимает значения **true** (включено) и **false** (выключено).

Если значение равно **true**, при восстановлении фильтра после аварийного сбоя сообщения перемещаются в спул ошибок. При аварийном завершения работы фильтра, сообщения, находящиеся в очереди, будут обработаны еще раз. Если попытка обработки сообщений завершится аварийным сбоем сервиса **mailfilter**, сообщения попадут в спул ошибок. Значение по умолчанию: **false**.

- **Перепаковывать архивы при удалении файлов** – устанавливает тип обработки архивов при реконструкции. По умолчанию параметр отключен, и в случае истинности условия проверки при реконструкции весь архив будет удален. При включенном параметре удалены будут только отдельные файлы, входящие в архив, удовлетворяющие условиям фильтрации, после чего архив будет переупакован заново в формате ZIP. Значение по умолчанию: **false**.

- **Таймаут при взаимодействии с сервером лицензирования (с)** – время ожидания в секундах при взаимодействии с сервером лицензирования. Значение по умолчанию: 60.

- **Таймаут при взаимодействии с Tikaserver (с)** – время ожидания в секундах при взаимодействии с сервером **Tika**. Значение по умолчанию: 60.

- **Таймаут при взаимодействии с сервером определения графических объектов (с)** – время ожидания в секундах при взаимодействии с сервером определения графических объектов. Значение по умолчанию: 60. Рекомендуется задать значение, равное 30.

- **Распознавать QR-коды** – при установленном флажке включает распознавание QR-кодов на изображениях. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.

- **Таймаут при взаимодействии с сервисом управления Досье (с)** – время ожидания в секундах при взаимодействии с сервисом управления Досье. Значение по умолчанию: 60.

- **Определять тип сообщений Exchange** – включает распознавание сообщений **Exchange**. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**. При значении **false** сообщения **Exchange** определяются как сообщения типа **Email**.

- **Значения RCPT TO для журнальных сообщений Exchange 2003** – данный параметр определяет значения заголовков **rcpt to** для журнальных сообщений, которые будут обрабатываться парсером **exchange 2003** (только для Exchange 2003). В качестве значения параметра следует указать соответствующий почтовый адрес или адреса, разделенные пробелом.

  При получении сообщения на один из указанных адресов, сервис **mailfilter** выполняет над сообщением следующие действия:

  1. Устанавливает значение типа сообщения равным **Exchange**.

  2. Удаляет из заголовков сообщения адреса отправителя и получателя, указанные в значении параметра **Значения RCPT TO для журнальных сообщений Exchange**

2003. Атрибуты **Источник** и **Назначение**, которые не содержат адресов SMTP-сервера, остаются.

3. Устанавливает для сообщения пометку **Преобразовано из журнала Exchange**.

- **Использовать syslog для журналирования операций над сообщениями?** – включает использование протокола syslog для журналирования операций над сообщениями и информации о нарушении целостности Агента. Принимает значения **true** (включено) и **false** (выключено). По умолчанию флажок не установлен.

- **Журналировать операции над сообщениями в файл?** – включает запись операций над сообщениями в журнальный файл. Принимает значения **true** (включено) и **false** (выключено). По умолчанию флажок не установлен.

- **Максимальное количество адресов, выводимых при журналировании операций над сообщениями** – определяет максимальное количество адресов, выводимых в поля **SolarDozorSrc** и **SolarDozorDst** журнальных файлов **syslog** и **message.log**. Значение по умолчанию: 0 (ограничение отсутствует).

- **Ограничение на размер заголовка при журналировании операций над сообщениями (в символах)** – определяет максимальную длину заголовка в символах, выводимого в поля **SolarDozorTo**, **SolarDozorFrom**, **SolarDozorCc** и **SolarDozorBcc** журнальных файлов **syslog** и **message.log**. Значение по умолчанию: 0 (ограничение отсутствует).

- **Использовать формат CEF при журналирования операций над сообщениями?** – включает запись действий над сообщениями в журнал в формате CEF. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

- **Выдавать ответ с кодом 503 при отсутствии свободных тредов** – включает отправку ответа с кодом 503 источникам HTTP/ICAP-трафика при отсутствии свободных потоков обработки. Параметр можно использовать для обеспечения балансировки трафика с учетом занятости серверов фильтрации. Если все потоки заняты и использование параметра выключено, фильтр удерживает соединение, помещает сообщение в очередь и ожидает освобождения хотя бы одного потока. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.

- **Применение политики в цикле по получателям сообщения** – режим работы фильтра при обработке сообщений с несколькими получателями. Используется для применения политики для каждого из получателей в цикле (с первого и далее по списку). По умолчанию выключен.

  - При снятом флажке проверка правил завершается для всех получателей после того как для очередного получателя из списка сработает какое-либо правило из набора. Действие, установленное в сработавшем правиле, выполняется для всех получателей.

  - При установленном флажке проверка правил завершается только для текущего получателя, для которого сработало правило из набора. Проверка правил для остальных получателей продолжается. Действия, установленные для правил, сработавших для разных получателей, помещаются в очередь и выполняются после завершения применения политики для всех получателей из списка. В результате для каждого из получателей могут выполняться различные действия.

- **Максимальный размер тела сообщения для помещения в архив (МБ)** – максимальный размер тела сообщения в Мб, по достижении которого сообщение без тела помещается в архив с пометкой следующего вида:

  Превышен лимит на размер тела сообщения (#dict.label-type.body-too-large): 545,10 ≥ 0 (Mb)

  Значение по умолчанию: 0.

- **Остановить распаковку, если суммарный размер частей превысит (МБ)** – максимальный размер всех частей сообщения в Мб, при достижении которого процесс распаковки останавливается. Значение по умолчанию: 2048.

- **Максимальное количество распаковываемых частей** – максимальное количество всех частей сообщения, при достижении которого процесс распаковки останавливается. Значение по умолчанию: 1000.

- **Использовать exiftool для извлечения содержимого медиафайлов** – включает модуль **exiftool** для извлечения содержимого бинарных атрибутов (тегов) медиафайлов (рисунки, фотографии, видеофайлы и звуковые файлы). Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

- **Пароли для распаковки архивов** – определяет пароли, которые указываются для распаковки запароленных (защищенных паролями) архивов. Поддерживаются следующие типы архивов: **zip**, **7z**, **rar**.

  Подбор пароля для запароленного архива будет выполняться до тех пор, пока для него не сработает какой-либо пароль из списка (выполняется проверка паролей сверху вниз по списку). При правильно подобранном пароле KEO DLP успешно выполнит распаковку такого архива.

  Если пароль не подобран, KEO DLP не сможет распаковать содержимое этого архива. В этом случае для сообщения с таким архивом будет установлена пометка **Ошибка при распаковке**. В журналах сервиса **mailfilter** появится запись об ошибке вида:

  Unpack error: Cannot open with specified passwords

  Примечание

  В системе присутствует ограничение на максимальное количество паролей – 100 шт.

  Вид сообщения может различаться в зависимости от типа архива.

  Чтобы добавить пароль, следует нажать кнопку **Добавить** и щелкнуть мышью на значок  , далее ввести пароль. Чтобы удалить пароль, следует нажать на значок  рядом с идентификатором пароля. Значение по умолчанию не установлено.

- **Минимальный размер текстового представления части, обрабатываемого политикой (байт)** – определяет минимальный размер текстового представления части, обрабатываемого политикой, который выражен в байтах. Текстовые представления части меньше этого размера не будут обработаны. Значение по умолчанию: 0 (проверяются части любого размера). Рекомендуемое значение: 7-10 байт.

- **Кэшировать индексы частей сообщения при проверках шаблонов документов** – включает кэширование индексов частей сообщения при проверках шаблонов документов. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

- **Максимальное количество одновременно закэшированных индексов частей сообщения** – максимальное количество одновременно закэшированных индексов частей сообщения при проверках шаблонов документов. Значение по умолчанию: 100.

JVM сервиса фильтрации сообщений:

- **Максимально доступное количество оперативной памяти (МБ)** – максимально доступное количество оперативной памяти в мегабайтах, выделяемой для сервиса фильтрации сообщений. Значение по умолчанию: 4096.

  Внимание!

  *Значение параметра **Максимально доступное количество оперативной памяти (МБ)** должно быть меньше объёма оперативной памяти виртуальной машины Java.*

- **Снимать дампы памяти при критических ошибках** – включает сохранение дампа памяти процесса **mailfilter** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

- **Каталог для записи дампов памяти** – расположение журнального файла с записями дампов памяти. Значение по умолчанию: **/data/temp/java_dumps/mailfilter**.

- **Сбор расширенной диагностики (JFR)** – параметры записи работы JVM для процесса **mailfilter**:

  - **Запись данных JFR** – включает сбор данных диагностики инструментом Java Flight Recorder. Принимает значения **true** (включено) и **false** (выключено).

    Внимание!

    Ответственность за включение параметра возлагается на инженеров поддержки KEO DLP.

  - **Время ожидания перед началом записи JFR (сек)** – время ожидания перед началом сбора данных диагностики, выраженное в секундах.

  - **Длительность записи одной сессии JFR (сек)** – длительность записи одной сессии JFR в секундах.

Примечание

*Параметры **Время ожидания перед началом записи JFR (сек)** и **Длительность записи одной сессии JFR (сек)** настраиваются в соответствии с целью сбора статистики, продолжительностью вывода Java Flight Recorder и ресурсами сервера.*

- **Каталог для сохранения файлов JFR** – временный каталог для сохранения файлов Java Flight Recorder.

Примечание

Сохраненные файлы JFR следует незамедлительно передавать инженерам поддержки KEO DLP.

Схемы преобразования:

В этой группе параметров по умолчанию задано 7 схем, описывающих соответствие заголовков внешних источников трафика и заголовков KEO DLP. Для добавления новой схемы/правила преобразования следует нажать кнопку **Добавить**, а для дублирования – значок рядом с идентификатором схемы/правила. Для удаления схемы/правила следует нажать значок .

Табл. A.1. Схема Dozor email

Параметр	Значение
Имя схемы преобразования	Dozor email
Применять схему	Включено по умолчанию
Имя опорного заголовка	X-Dozor-Mapping-Schema
Значение опорного заголовка	dozor-email
Правила преобразования	Табл.A.2

Табл. A.2. Схема Dozor email: правила сверху вниз

Правило	Поле сообщения	Правило
[:address-info :sender]	Отправитель	:header “x-dozor-sender” :as-email
[:address-info :recipient]	Получатель	:header “x-dozor-recipients” :as-list :as-email
[:address-info :source]	Источник сообщения	:header “x-dozor-sender” :as-email
[:address-info :destination]	Назначение	:header “x-dozor-recipients” :as-list :as-email
[:address-info :source]	Источник сообщения	:header “x-dozor-src-email” :as-list :as-email
[:address-info :source]	Источник сообщения	:header “from” :as-list :as-email
[:address-info :source]	Источник сообщения	:header “sender” :as-list :as-email
[:address-info :destination]	Назначение	:header “x-dozor-dst-email” :as-list :as-email
[:address-info :destination]	Назначение	:header “to” :as-list :as-email
[:address-info :destination]	Назначение	:header “cc” :as-list :as-email
[:address-info :destination]	Назначение	:header “bcc” :as-list :as-email
[:subject]	Тема	:header “subject”
[:subject]	Тема	:header “x-dozor-subject”

Правило	Поле сообщения	Правило
[:recv-date]	Дата получения	:header “date” :or-now :as-date
[:recv-date]	Дата получения	:header “x-dozor-received-date” :or-now :as-date
[:type]	Тип сообщения	:const “email”

Табл. А.3. Схема Dozor messenger

Параметр	Значение
Имя схемы преобразования	Dozor messenger
Применять схему	Включено по умолчанию
Имя опорного заголовка	X-Dozor-Mapping-Schema
Значение опорного заголовка	dozor-im
Правила преобразования	Табл.А.4

Табл. А.4. Схема Dozor messenger: правила сверху вниз

Правило	Поле сообщения	Правило
[:address-info :source]	Источник сообщения	:header "x-dozor-src-login" :as-login
[:address-info :source]	Источник сообщения	:header "x-dozor-src-domain-login" :as-login
[:address-info :source]	Источник сообщения	:header "x-dozor-src-im" :as-im
[:address-info :source]	Источник сообщения	:header "x-dozor-src-email" :as-email
[:address-info :source]	Источник сообщения	:header "x-dozor-src-sid" :as-sid
[:address-info :source]	Источник сообщения	:header "x-dozor-src-hostname" :as-hostname
[:address-info :source]	Источник сообщения	:header "x-dozor-src-ip" :as-ip
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-login" :as-list :as-login
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-domain-login" :as-list :as-login
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-im" :as-list :as-im
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-email" :as-list :as-email
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-sid" :as-list :as-sid
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-hostname" :as-list :as-hostname
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-ip" :as-list :as-ip
[:headers]	Заголовки сообщения	:header "x-dozor-application" :as-header "x-agent-application-name";
[:headers]	Заголовки сообщения	:header "x-dozor-process" :as-header "x-agent-application-name"
[:headers]	Заголовки сообщения	:header "x-dozor-chat-id" :as-header "x-agent-chat-id"
[:subject]	Тема сообщения	:header "subject"
[:subject]	Тема сообщения	:header "x-dozor-subject"
[:filename]	Имя передаваемого файла	:header "filename"
[:filename]	Имя передаваемого файла	:header "x-dozor-filename"
[:recv-date]	Дата получения	:header "date" :or-now :as-date
[:recv-date]	Дата получения	:header “x-dozor-received-date” :or-now :as-date
[:type]	Тип сообщения	:const "endpoint/im"
[:comm-channel]	Канал коммуникации	:const "im"

Табл. A.5. Схема Dozor file

Параметр	Значение
Имя схемы преобразования	Dozor file
Применять схему	Включено по умолчанию
Имя опорного заголовка	X-Dozor-Mapping-Schema
Значение опорного заголовка	dozor-file
Правила преобразования	Табл.A.6

Табл. A.6. Схема Dozor file: правила сверху вниз

Правило	Поле сообщения	Правило
[:address-info :source]	Источник сообщения	:header "x-dozor-src-login" :as-login
[:address-info :source]	Источник сообщения	:header "x-dozor-src-domain-login" :as-login
[:address-info :source]	Источник сообщения	:header "x-dozor-src-im" :as-im
[:address-info :source]	Источник сообщения	:header "x-dozor-src-email" :as-email
[:address-info :source]	Источник сообщения	:header "x-dozor-src-sid" :as-sid
[:address-info :source]	Источник сообщения	:header "x-dozor-src-hostname" :as-hostname
[:address-info :source]	Источник сообщения	:header "x-dozor-src-ip" :as-ip
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-login" :as-list :as-login
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-domain-login" :as-list :as-login
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-im" :as-list :as-im
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-email" :as-list :as-email
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-sid" :as-list :as-sid
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-hostname" :as-list :as-hostname
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-ip" :as-list :as-ip
[:headers]	Заголовки сообщения	:header "x-dozor-application" :as-header "x-agent-application-name";
[:headers]	Заголовки сообщения	:header "x-dozor-process" :as-header "x-agent-application-name"
[:subject]	Тема сообщения	:header "filename"
[:subject]	Тема сообщения	:header "x-dozor-filename"
[:filename]	Имя передаваемого файла	:header "filename"
[:filename]	Имя передаваемого файла	:header "x-dozor-filename"
[:recv-date]	Дата получения	:header "date" :or-now :as-date
[:recv-date]	Дата получения	:header “x-dozor-received-date” :or-now :as-date
[:type]	Тип сообщения	:const "file"
[:comm-channel]	Канал коммуникации	:const "storage"

Табл. A.7. Схема Dozor message

Параметр	Значение
Имя схемы преобразования	Dozor message
Применять схему	Включено по умолчанию
Имя опорного заголовка	X-Dozor-Mapping-Schema
Значение опорного заголовка	dozor-message

Параметр	Значение
Правила преобразования	Табл.А.8

Табл. А.8. Схема Dozor message: правила сверху вниз

Правило	Поле сообщения	Правило
[:address-info :source]	Источник сообщения	:header "x-dozor-src-login" :as-login
[:address-info :source]	Источник сообщения	:header "x-dozor-src-domain-login" :as-login
[:address-info :source]	Источник сообщения	:header "x-dozor-src-im" :as-im
[:address-info :source]	Источник сообщения	:header "x-dozor-src-email" :as-email
[:address-info :source]	Источник сообщения	:header "x-dozor-src-sid" :as-sid
[:address-info :source]	Источник сообщения	:header "x-dozor-src-hostname" :as-hostname
[:address-info :source]	Источник сообщения	:header "x-dozor-src-ip" :as-ip
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-login" :as-list :as-login
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-domain-login" :as-list :as-login
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-im" :as-list :as-im
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-email" :as-list :as-email
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-sid" :as-list :as-sid
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-hostname" :as-list :as-hostname
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-ip" :as-list :as-ip
[:headers]	Заголовки сообщения	:header "x-dozor-application" :as-header "x-agent-application-name";
[:headers]	Заголовки сообщения	:header "x-dozor-process" :as-header "x-agent-application-name"
[:headers]	Заголовки сообщения	:header "x-dozor-chat-id" :as-header "x-agent-chat-id"
[:subject]	Тема сообщения	:header "subject"
[:subject]	Тема сообщения	:header "x-dozor-subject"
[:filename]	Имя передаваемого файла	:header "filename"
[:filename]	Имя передаваемого файла	:header "x-dozor-filename"
[:comp-date]	Дата создания сообщения	:header "x-dozor-created-date" :as-date
[:recv-date]	Дата получения	:header "date" :or-now :as-date
[:recv-date]	Дата получения	:header “x-dozor-received-date” :or-now :as-date
[:type]	Тип сообщения	:header "x-dozor-message-type""
[:comm-channel]	Канал коммуникации	:header "x-dozor-comm-channel"

Табл. А.9. Схема TrueConf

Параметр	Значение
Имя схемы преобразования	TrueConf
Применять схему	Включено по умолчанию
Имя опорного заголовка	X-Dozor-Mapping-Schema
Значение опорного заголовка	TrueConf
Правила преобразования	Табл.А.10

Табл. А.10. Схема TrueConf: правила сверху вниз

Правило	Поле сообщения	Правило
[:address-info :source]	Источник сообщения	:header "x-dozor-src-login" :as-login
[:address-info :source]	Источник сообщения	:header "x-dozor-src-domain-login" :as-login
[:address-info :source]	Источник сообщения	:header "x-dozor-src-im" :as-im
[:address-info :source]	Источник сообщения	:header "x-dozor-src-email" :as-email
[:address-info :source]	Источник сообщения	:header "x-dozor-src-sid" :as-sid
[:address-info :source]	Источник сообщения	:header "x-dozor-src-hostname" :as-hostname
[:address-info :source]	Источник сообщения	:header "x-dozor-src-ip" :as-ip
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-login" :as-list :as-login
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-domain-login" :as-list :as-login
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-im" :as-list :as-im
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-email" :as-list :as-email
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-sid" :as-list :as-sid
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-hostname" :as-list :as-hostname
[:address-info :destination]	Назначение сообщения	:header "x-dozor-dst-ip" :as-list :as-ip
[:headers]	Заголовки сообщения	:header "x-dozor-application" :as-header "x-agent-application-name";
[:headers]	Заголовки сообщения	:header "x-dozor-process" :as-header "x-agent-application-name"
[:headers]	Заголовки сообщения	:header "x-dozor-chat-id" :as-header "x-agent-chat-id"
[:subject]	Тема сообщения	:const "Личное сообщение. Мессенджер: TrueConf. Тип: текст."
[:subject]	Тема сообщения	:if-header-exists "x-dozor-filename" [:const "Личное сообщение. Мессенджер: TrueConf. Тип: файл."]
[:subject]	Тема сообщения	:if-header-exists "x-dozor-chat-title" [:make-string [:header "x-dozor-chat-title"] ". Мессенджер: TrueConf. Тип: текст."]
[:subject]	Тема сообщения	:if-header-exists "x-dozor-chat-title" [:if-header-exists "x-dozor-filename" [:make-string [:header "x-dozor-chat-title"] ". Мессенджер: TrueConf. Тип: файл."]]
[:filename]	Имя передаваемого файла	:header "filename"
[:filename]	Имя передаваемого файла	:header "x-dozor-filename"
[:recv-date]	Дата получения	:header "date" :or-now :as-date
[:recv-date]	Дата получения	:header “x-dozor-received-date” :or-now :as-date
[:type]	Тип сообщения	:const "endpoint/im"
[:comm-channel]	Канал коммуникации	:const "im"

Табл. А.11. Схема Express

Параметр	Значение
Имя схемы преобразования	Express
Применять схему	Включено по умолчанию

Параметр	Значение
Имя опорного заголовка	X-Dozor-Mapping-Schema
Значение опорного заголовка	Express
Правила преобразования	Табл.А.12

Табл. А.12. Схема Express: правила сверху вниз

Правило	Поле сообщения	Правило
[:address-info :source]	Источник сообщения	:header "x-plain-authenticated-user" :extract #".+\\(.+)" :as-login
[:address-info :source]	Источник сообщения	:header "x-plain-authenticated-user" :extract #".+\\(.+)" :as-im
[:address-info :source]	Источник сообщения	:header "x-plain-authenticated-user" :extract #"(^[1-9]+[0-9]*$)" :as-im
[:address-info :destination]	Назначение сообщения	:header "x-recipient-user-login" :as-list :extract #".+\\(.+)" :as-login
[:address-info :destination]	Назначение сообщения	:header "x-recipient-user-login" :as-list :extract #".+\\(.+)" :as-im
[:address-info :destination]	Назначение сообщения	:header "x-recipient-user-login" :as-list :extract #"(^[1-9]+[0-9]*$)" :as-im
[:subject]	Тема сообщения	:header "subject"
[:subject]	Тема сообщения	:header "x-dozor-subject"
[:headers]	Заголовки сообщения	:header "x-application" :as-header "x-agent-application-name";
[:headers]	Заголовки сообщения	:header "x-dozor-chat-id" :as-header "x-agent-chat-id"
[:recv-date]	Дата получения	:header “x-message-date” :or-now :as-date
[:comp-date]	Дата создания сообщения	:header "x-message-date" :or-now :as-date
[:type]	Тип сообщения	:const "endpoint/im"
[:comm-channel]	Канал коммуникации	:const "im"
[:filename]	Имя передаваемого файла	:header "x-file-name"

Табл. А.13. Схема DAG

Параметр	Значение
Имя схемы преобразования	DAG
Применять схему	Включено по умолчанию
Имя опорного заголовка	X-Dozor-Mapping-Schema
Значение опорного заголовка	dag-message
Правила преобразования	Табл.А.14

Табл. А.14. Схема DAG: правила сверху вниз

Правило	Поле сообщения	Правило
[:comm-channel]	Канал коммуникации	:const "storage"
[:type]	Тип сообщения	:const "file"
[:filename]	Имя передаваемого файла	:header "filename"
[:headers]	Заголовки сообщения	:header "x-agent-destination-files" :extract #"//(.+?)/" :as-header "x-dar-host"

Правило	Поле сообщения	Правило
[:headers]	Заголовки сообщения	:header "x-agent-destination-files" :extract #"//.+?(/.+)$" :as-header "x-dar-path"

Сервис определения графических объектов:

- **Локальный порт, на котором сервер будет принимать соединения** – локальный порт, на котором сервис определения графических объектов будет принимать соединения. Значение по умолчанию: 9303.

- **Асинхронное журналирование** – асинхронное ведение журнала. Рекомендуется использовать для повышения пропускной способности сервиса определения графических объектов. При использовании асинхронного журналирования вывод журнала может задерживаться, а последний журнальный файл может быть утерян в случае аварийной остановки сервиса. По умолчанию выключено.

- **Максимальное количество обработчиков, выполняющих распознавание** – количество экземпляров обработчика, одновременно выполняющих распознавание графических объектов. Для каждого экземпляра организуется очередь сообщений для обработки, максимальное количество сообщений в очереди определяется параметром **Размер очереди заданий**. При использовании графических процессоров рекомендуется устанавливать значение, равное количеству графических процессоров. Значение по умолчанию: 1. При значении 0 количество экземпляров обработчика будет равно количеству ядер процессора.

- **Количество потоков для приема сообщений** – количество внутренних сетевых потоков сервиса распознавания графических объектов, используемых для приема сообщений для обработки. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству логических ядер центрального процессора). Рекомендуется использовать значение по умолчанию или меньше.

- **Размер очереди заданий** – максимальное количество сообщений для обработки для каждого экземпляра обработчика. Значение по умолчанию: 0 (фактически будет использоваться значение 100). При использовании нескольких экземпляров обработчика и/или графических процессоров рекомендуется устанавливать значение 1000.

- **Количество потоков для работы с обработчиками** – количество внутренних сетевых потоков сервиса распознавания графических объектов, которые отправляют результаты распознавания на вывод во внешний интерфейс. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству логических ядер центрального процессора). Рекомендуется использовать значение по умолчанию или меньше.

- **Количество GPU** – количество графических процессоров, используемых для распознавания графических объектов. Значение по умолчанию: 0 (фактически будет использоваться значение, равное количеству графических процессоров на сервере).

- **Максимальный размер запроса** – максимально допустимый размер сообщения в мегабайтах, принимаемый сервисом определения графических объектов на обработку. Значение по умолчанию: 100.

- **Время ожидания ответа** – максимальное время (в секундах) ожидания экземпляром обработчика ответа от сервиса распознавания, после которого запрос обработчика

будет перезагружен. Значение по умолчанию: 0 (фактически будет использоваться значение 120).

- **Уровень журналирования** – степень детализации журналирования. В качестве значения можно выбрать один из следующих параметров в раскрывающемся списке:
  - **Отключен** – журналирование отключено;
  - **Критические ошибки** – журналировать только критические ошибки;
  - **Ошибки** – журналировать все ошибки;
  - **Предупреждения** – журналировать все ошибки и предупреждения о работе модуля;
  - **Уведомления** – журналировать все ошибки, предупреждения и уведомления о работе модуля;
  - **Информация** – журналировать все ошибки, предупреждения, уведомления и информацию о работе модуля;
  - **Отладка** – журналировать все ошибки, предупреждения, уведомления и полную отладочную информацию.
- **Каталог для временных файлов** – временный каталог для хранения изображений графических объектов. Значение по умолчанию: **/data/temp/god**.
- **Настройки ограничений на параметры графических изображений** – настройки ограничений на параметры графических изображений:
  - **Минимальный размер изображения по вертикали, в пикселях** – минимальный размер изображения по вертикали в пикселях. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** ограничение отсутствует.
  - **Минимальный размер изображения по горизонтали (пикселей)** – максимальный размер изображения по горизонтали в пикселях. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** ограничение отсутствует.
  - **Максимальная высота изображения (пикселей)** – максимальная высота изображения в пикселях. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** ограничение отсутствует.
  - **Максимальная ширина изображения (пикселей)** – максимальная ширина изображения в пикселях. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** ограничение отсутствует.
  - **Минимальный размер изображения (байт)** – минимальный размер файла графического изображения в байтах. Принимает значения **Ограничен значением** и **Не ограничен значением**. При значении **Не ограничен значением** будет действовать максимальное ограничение в 100 МБ.
  - **Максимальный размер изображения (байт)** – максимальный размер файла графического изображения в байтах. Принимает значения **Ограничен значением** и

Не ограничен значением. При значении **Не ограничен значением** будет действовать максимальное ограничение в 100 МБ.

Сервис извлечения текстовых данных:

- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервис **smap-tikaserver** ожидает соединения. Значение по умолчанию: 9998.
- **Максимальный размер используемой оперативной памяти (МБ)** – максимальный размер используемой оперативной памяти в Мб. По умолчанию используется 2048 Мб.
- **Определяемые языки** – определяемые языки. Для добавления языка необходимо щелкнуть мышью на значок  и в появившемся поле ввода ввести обозначение для языка, например, **uk** – для английского. Для удаления языка необходимо щелкнуть мышью на значок  рядом с нужным полем ввода.
- **Уровень отладки** – уровень вывода отладочной информации в журнальный файл сервиса. По умолчанию используется уровень журналирования **info**.
- **Определять кодировку UTF-7** – включает определение кодировки UTF-7. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.
- **Каталог для временных файлов** – каталог для хранения временных файлов. Значение по умолчанию: **/data/temp/tikaserver**.
- **Удалять некорректные символы при нормализации кодировки** – если флажок установлен, при нормализации кодировки некорректные символы удаляются, а при снятом флажке вместо них используются символы замены. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **true**.

Отладка сервиса извлечения текстовых данных:

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **tikaserver** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объем на дисковом пространстве.

A.2.3.3. Политика

Коннектор сервиса контроля идентификаторов:

- **Максимальное время ожидания ответа от сервера (с)** – максимальное время ожидания ответа от сервиса контроля идентификаторов в секундах. Значение по умолчанию: 60.

Коннектор сервиса цифровых отпечатков:

- **Максимальное время ожидания ответа от сервера (с)** – максимальное время ожидания ответа от сервиса работы с цифровыми отпечатками в секундах. Значение по умолчанию: 10.
- **Вставлять совпавший текст в пометку** – включать в пометку, устанавливаемую на сообщение, для которого выполняется проверка цифровых отпечатков, текст, совпа-

дающий у проверяемого сообщения и эталона. К пометке добавляются первые 200 символов совпавшего текста.

- **Проверка по двоичной сигнатуре (binary)** – проверка по двоичной сигнатуре.
- **Проверка текста (plain_text)** – проверка текста.
- **Проверка изображений (image)** – проверка изображений.
- **Проверка содержимого таблиц (table)** – проверка содержимого таблиц.
- **Минимальный размер текста для проверки (Б)** – минимальный размер текста для проверки (в байтах). Значение по умолчанию: 1024.
- **Минимальный размер изображения для проверки (Б)** – минимальный размер изображения для проверки (в байтах). Значение по умолчанию: 1024.
- **Минимальный размер таблицы для проверки (Б)** – минимальный размер таблицы для проверки (в байтах). Значение по умолчанию: 1024.
- **Минимальный размер бинарных данных для проверки (Б)** – минимальный размер бинарных данных для проверки (в байтах). Значение по умолчанию: 1024.
- **Вычисление результатов распознавания** – выбор способа вычисления результатов распознавания:
  - Наибольший из результатов проверки (maximum base.matching и self.matching).
  - Результат сравнения с базой эталонов (base.matching).

Параметры, ограничивающие минимальные размеры данных (**Минимальный размер текста для проверки (Б)**, **Минимальный размер изображения для проверки (Б)**, **Минимальный размер таблицы для проверки (Б)**, **Минимальный размер бинарных данных для проверки (Б)**), задаются для возможного снижения нагрузки за счет уменьшения количества обращений.

Сервис контроля идентификаторов:

- **Локальный порт, на котором сервер будет принимать соединения** – локальный порт, на котором сервер будет принимать соединения. Значение по умолчанию: 9302.
- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти, используемое сервером (в МБ). Значение по умолчанию: 1024. Рекомендуемое значение: 4096 или более. Значение не может быть меньше 512.
- **Размер пула потоков** – количество служебных потоков сервера. Значение по умолчанию: 25.
- **Каталог для временных файлов** – каталог для хранения временных файлов сервиса контроля идентификаторов. Значение по умолчанию: **/data/temp/idid**.
- **Максимальный размер, при превышении которого содержимое обрабатываемого документа сбрасывается на диск (Б)** – максимальный размер в байтах, при превышении которого содержимое обрабатываемого документа сбрасывается на диск. Значение по умолчанию: 1048576.

Сервис цифровых отпечатков:

- **Локальный порт, на котором сервер будет принимать соединения** – локальный порт, на котором сервер будет принимать соединения. Значение по умолчанию: 9301.
- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти, используемое сервисом DIFI (в Мб). Значение по умолчанию: 2048.
- **Каталог для временных файлов** – каталог для хранения временных файлов. Значение по умолчанию: **/data/temp/difi**.
- **Рассчитывать hash для отраженного изображения** – рассчитывать хэш для отраженного изображения при загрузке в базу эталонов и при сравнении документов. Включение этого параметра увеличивает время обработки изображений в 2-3 раза. По умолчанию выключено.
- **Мультипликатор для нахождения ближайшего вектора дескрипторов в алгоритме сравнения отпечатков** – мультипликатор для нахождения ближайшего вектора дескрипторов в алгоритме сравнения отпечатков. Влияет на быстродействие при сравнении отпечатков изображений (чем больше – тем быстрее) и на точность сравнения (чем меньше – тем точнее). Значение по умолчанию: 3.
- **Вывод отладочной информации** – включает вывод отладочной информации.

Отладка сервиса цифровых отпечатков:

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **smap-difi** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Сервис категоризации:

- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервер будет принимать соединения. Значение по умолчанию: 3002.

A.2.4. Настройка средств мониторинга и анализа нарушений

A.2.4.1. События и инциденты

Сервис хранения и индексации событий и инцидентов:

- **HTTPS порт** – локальный HTTPS-порт, на котором сервер будет принимать соединения. Значение по умолчанию: 2272.
- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса. По умолчанию выключено.
- **Хранилище инцидентов (PostgreSQL)** – имя схемы соединения с БД, используемой для хранения информации о задачах сервиса **incident-daemon**. Принимает значения **Отсутствует** и **Специальная БД**. Значение по умолчанию: **Отсутствует**. При значении **БД по умолчанию** сервис не подключается к БД. Если выбрано значение **Специальная БД**, доступны параметры:

- **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
- **Сетевой порт сервера базы данных** – сетевой порт сервера БД.
- **Имя базы данных** – имя БД.
- **Пользователь базы данных** – указывается имя пользователя БД.
- **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.
- **Проверка подключения не выполнялась** – данное сообщение появляется, если проверка подключения к базе данных не выполнялась. При успешной проверки подключения появляется следующее сообщение **Подключение проверено 01.09.2021 11:45 Проверка прошла успешно**.

- **Ротация хранилища инцидентов** – настройки ротации хранилища инцидентов:
  - **Путь до каталога архивации** – путь к каталогу архивации.
  - **Путь до каталога восстановления архивов** – путь к каталогу восстановления архивов.
  - **Размер блока данных при выполнении ротации** – размер блока данных при выполнения ротации секций в БД событий и инцидентов. Значение по умолчанию: 30000.
  - **Журналировать обработку каждого n-го блока данных** – журналировать обработку каждого n-го блока данных при выполнении ротации секций (значение n). Значение по умолчанию: 2.
  - **Режим ротации** – режим ротации:
    - **Архивировать** – архивировать секции в локальный каталог (указанный в параметре **Путь до каталога архивации**), по умолчанию выключен;
    - **Удалять (не архивировать)** – удалить секции;
    - **Ротация не производится** – выключить режим ротации.
- **Порог журналирования медленных запросов (мс)** – порог журналирования медленных запросов (миллисекунды), выраженный в миллисекундах. Значение по умолчанию: 5000.
- **Количество shard-ов** – количество шардов OpenSearch (подробнее о шардах и прочих настройках ES см. документ *Руководство по установке и настройке*). Значение по умолчанию: 1.
- **Число копий** – число копий индексов OpenSearch. Значение по умолчанию 0.
- **Периодичность обновления индекса (с)** – интервал времени в секундах между помещением индекса в базу данных OpenSearch и его отображением (доступностью для использования). Значение по умолчанию: 30.
- **Журналировать регистрацию событий** – использовать механизм журналирования в системный журнал вместо журнала сервиса **incident-daemon** для регистрации собы-

тий и инцидентов ИБ. По умолчанию выключено. При включении параметра появляется следующая группа параметров:

  - **Журналировать изменение статуса событий и инцидентов** – при любом изменении полей **status** или **state** в БД событий и инцидентов будет выполняться журналирование этих событий.

  - **Журналировать в syslog в формате CEF** – при журналировании будет использоваться формат CEF.

  - **Уровень критичности событий и инцидентов** – уровень критичности тех событий и инцидентов ИБ, которые будут журналироваться.

- **Предпочитаемый язык** – язык, используемый при журналировании регистрации событий и инцидентов ИБ.

- **Разделять оперативные и исторические данные** – использование механизма раздельной индексации событий и инцидентов ИБ в зависимости от их возраста. Принимает значение **Разделять** и **Не разделять**. При использовании значения **Разделять** становится доступен параметр **Период хранения в оперативном архиве**, определяющий максимальный возраст события или инцидента в неделях до его перехода из оперативных в исторические. При использовании значения **Не разделять** все события и инциденты считаются оперативными.

- **Ежедневная фоновая миграция устаревших индексов** – параметры фоновой миграции более неактуальных для KEO DLP индексов событий и инцидентов:

  - **Включена** – включить фоновую миграцию. По умолчанию выключено.

  - **Время начала** – час начала ежедневной миграции.

  - **Время окончания** – час окончания ежедневной миграции.

JVM сервиса хранения и индексации событий и инцидентов:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса хранения и индексации событий и инцидентов. Значение по умолчанию: 512.

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **incident-daemon** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

A.2.4.2. Поиск

Сервис поиска и индексации OpenSearch:

- **Порт для подключения по HTTP** – порт для подключения к OpenSearch по протоколу HTTP. Значение по умолчанию: 9200.

- **Транспортный TCP-порт** – транспортный порт к OpenSearch по протоколу HTTP. Значение по умолчанию: 9201.

- **Периодичность проверки доступности узлов (сек)** – периодичность проверки доступности узлов (в секундах). Значение по умолчанию: 1.
- **Таймаут при проверке доступности (сек)** – таймаут при проверке доступности узла (в секундах). Значение по умолчанию: 30.
- **Количество сбоев, после которого узел считается недоступным** – количество сбоев, после которого узел считается недоступным. Значение по умолчанию: 3.
- **Таймаут запросов поиска по умолчанию (сек)** – таймаут запросов поиска сервисом OpenSearch в секундах. Значение по умолчанию: 300 сек.
- **Каталог для хранения индексов** – каталог для хранения индексов OpenSearch. Можно добавить несколько значений с помощью кнопки  .
- **Разделяемая файловая система для хранения snapshot'ов индексов** – каталоги для хранения резервных копий индексов почтового архива. Можно добавить несколько значений с помощью кнопки  .
- **Прекратить размещение новых индексов, если свободного места меньше (Мб)** – минимальный размер свободного места на файловой системе в мегабайтах, при котором происходит размещение новых индексов. Значение по умолчанию: 1024.
- **Переносить данные на другие узлы, если свободного места меньше (Мб)** – максимальный размер свободного места на файловой системе в мегабайтах, при котором происходит перенос данных на другие узлы. Значение по умолчанию: 512.
- **Перейти в режим "только для чтения", если свободного места меньше (Мб)** – минимальный размер свободного места на файловой системе в мегабайтах, при котором сервис **opensearch** не переходит в режим **read-only**. При размере ниже минимального сервис **opensearch** для предотвращения аварийной остановки системы перейдет в режим **read-only**.

Примечание

*В территориально-распределённой схеме работы каждый из параметров **Прекратить размещение новых индексов, если свободного места меньше (Мб)**, **Переносить данные на другие узлы, если свободного места меньше (Мб)**, и **Перейти в режим "только для чтения", если свободного места меньше (Мб)** должен иметь одинаковые значения внутри подкластера, поэтому параметры настраиваются для каждого узла подкластера. В иной схеме работы каждый из этих параметров должен иметь одинаковые значения внутри кластера OpenSearch, поэтому параметры настраиваются для всего кластера KEO DLP, т.е. выбрано **Общая конфигурация** в списке **Конфигурация/Узел**.*

- **Репликация с учётом размещения серверов в стойках** – при включении этого параметра копии индексов ES сохраняются на узлах с учетом их физического размещения в серверных стойках. На узлах, размещённых в одной стойке, совокупно будет находиться одна полная копия индексов или её часть, без дублирования. Принадлежность узла к той или иной стойке следует указать в разделе GUI **Система > Узлы и роли**, открыв вспомогательное меню этого узла и выбрав пункт **Атрибуты**. Количество копий индексов ES не должно превышать количество стоек, содержащих узлы кластера

OpenSearch. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.

Производительность сервиса поиска и индексации OpenSearch:

- **Размер памяти (ГБ)** – объём оперативной памяти в гигабайтах, выделяемой для сервиса **opensearch**. Значение по умолчанию: 4. Рекомендуется увеличить это значение на столько, сколько десятков миллионов сообщений содержится в архиве. Максимально допустимое значение – половина оперативной памяти сервера, но не более 32 ГБ.

- **Ограничение direct-памяти (ГБ)** – максимальный объём буфера ввода/вывода клиентских запросов в гигабайтах. Значение по умолчанию: 4.

Индексация сообщений в архиве:

- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса. По умолчанию выключено.

- Группа параметров **Индексация**:

  - **Период плановой индексации (Ч)** – периодичность плановой индексации сообщений в архиве. Задается в часах. Значение по умолчанию: 1.

  - **HTTP-порт** – порт HTTP-сервера. Значение по умолчанию: 7837.

  - **Размер индексируемой части сообщения (символов)** – размер индексируемой части сообщения. Значение по умолчанию: 20000000.

  - **Максимальное количество индексируемых частей сообщения** – максимальное количество индексируемых частей сообщения. Значение по умолчанию: 10000.

  - **Глубина индексации** – ограничение глубины индексации в неделях. Принимает значения **Задать** и **Не ограничена** (неограниченная глубина). При значении **Задать** появляется дополнительный параметр **Недель** – индексы старше заданного количества недель удаляются. Значение по умолчанию: **Не ограничена**.

  - **Максимальное количество соединений с БД** – максимальное число подключений к БД сервиса **indexer-ng**. Значение по умолчанию: 12.

  - **Настройки потоков индексации**:

    - **Количество потоков индексации для каждой БД** – число параллельных потоков обработки метаданных сообщений. Значение по умолчанию: 5.

  - **Максимальная длительность цикла обхода архива (мин)** – таймаут в минутах, по истечении которого процесс индексации прерывается и запускается заново, что позволяет получить более новые сообщения. Значение по умолчанию: 1440.

  - **Глубина индексации для сервиса UBA (д)** – ограничение глубины индексации для сервиса **uba-server**. Задается в днях.

  - **Настройки индексов**:

- **Параметры индекса сообщений** – параметры индексирования архива сообщений:
  - **Порог журналирования медленных запросов (миллисекунды)** – порог журналирования медленных запросов в миллисекундах.
  - **Количество shard-ов** – количество шардов OpenSearch. Значение по умолчанию: 1.
  - **Число копий** – число копий индексов OpenSearch. Значение по умолчанию 0.
  - **Периодичность обновления индекса (сек)** – интервал времени в секундах между помещением индекса в базу данных OpenSearch и его отображением (доступностью для использования). Значение по умолчанию: 30.
  - **Поддержка поиска по точному совпадению** – включает поддержку поиска по точному совпадению.
- **Параметры индекса бесед** – параметры индексирования архива бесед:
  - **Порог журналирования медленных запросов (миллисекунды)** – порог журналирования медленных запросов в миллисекундах.
  - **Количество shard-ов** – количество шардов ES. Значение по умолчанию: 6.
  - **Число копий** – число копий индексов ES. Значение по умолчанию 0.
  - **Периодичность обновления индекса (сек)** – интервал времени в секундах между помещением индекса в базу данных OpenSearch и его отображением (доступностью для использования). Значение по умолчанию: 30.
- **Параметры индекса структуры каталогов** – параметры индексирования структуры каталогов:
  - **Порог журналирования медленных запросов (миллисекунды)** – порог журналирования медленных запросов в миллисекундах.
  - **Количество shard-ов** – количество шардов ES. Значение по умолчанию: 1.
  - **Число копий** – число копий индексов ES. Значение по умолчанию 0.
  - **Периодичность обновления индекса (сек)** – интервал времени в секундах между помещением индекса в базу данных OpenSearch и его отображением (доступностью для использования). Значение по умолчанию: 30.

- **Ежедневная фоновая миграция устаревших индексов сообщений** – параметры фоновой миграции более неактуальных для KEO DLP индексов сообщений, бесед и устройств:
  - **Включена для сообщений** – включить фоновую миграцию для устаревших индексов сообщений и устройств. По умолчанию выключено.
  - **Включена для бесед** – включить фоновую миграцию для устаревших индексов бесед. По умолчанию выключено.

- **Время начала** – час начала ежедневной миграции.
- **Время окончания** – час окончания ежедневной миграции.

- **Разделять оперативные и исторические данные** – использование механизма раздельной индексации сообщений в архиве в зависимости от их возраста. Принимает значение **Разделять** и **Не разделять**. При использовании значения **Разделять** становится доступен параметр **Период хранения в оперативном архиве**, определяющий максимальный возраст сообщения в неделях до его перехода из оперативных в исторические. При использовании значения **Не разделять** все сообщения в архиве считаются оперативными.

JVM сервиса индексации сообщений в архиве:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервиса **indexer-ng**. Значение по умолчанию: 2048.
- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти сервиса индексации сообщений в архиве в случае ошибки исчерпания памяти. По умолчанию включено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

A.2.4.3. Досье

Сервис доступа к Досье:

- **HTTPS-порт** – порт, на котором сервис **abook-daemon** ожидает соединения по протоколу HTTPS. Значение по умолчанию: 2269.
- **БД для хранения настроек политики и досье** – имя схемы соединения с БД, используемой для хранения информации сервиса **abook-daemon**. Принимает значения **БД по умолчанию** и **Специальная БД**. Значение по умолчанию: **БД по умолчанию**. При значении **БД по умолчанию** сервис подключается к БД политики, настройки которой задаются в разделе GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** > **БД настроек политики и досье**. Если выбрано значение **Специальная БД**, доступны параметры:
  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.
  - **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.
  - **Проверка подключения не выполнялась** – данное сообщение появляется, если проверка подключения к базе данных не выполнялась. При успешной проверки подключения появляется следующее сообщение **Подключение проверено 01.09.2021 11:45 Проверка прошла успешно**.

- **Режим работы** – режим работы системы Досье на узле. Принимает значения: **Главный** и **Подчиненный**. Настройка синхронизации Досье описана в *Руководстве по установке и настройке* в разделе *Настройка синхронизации Досье*.

  Если Досье кластера KEO DLP использует один или несколько внешних источников данных, следует выбрать значение **Главный**. В этом случае доступны следующие параметры:

  - Группа параметров **Настройки уровня доверия** – настройки уровня доверия:

    - **Рассчитывать уровень доверия** – включает сбор данных, необходимых для рассчета уровня доверия. Принимает значения: **true** и **false**. Значение по умолчанию: **true**.

    - **Минимальное значение уровня доверия** – минимальное значение уровня доверия. Значение по умолчанию: -1000.

    - **Максимальное значение уровня доверия** – максимальное значение уровня доверия. Значение по умолчанию: 1000.

    - **Начальное значение уровня доверия (DTL) для персон** – начальное значение уровня доверия (DTL) для персоны или адреса. Фактически, DTL означает максимально допустимое значение уровня доверия для данной персоны или адреса. Значение по умолчанию: 0.

    - **Начальное значение уровня доверия (DTL) для адресов, не принадлежащих персонам** – начальное значение уровня доверия (DTL) для адресов, не принадлежащих персонам. Значение по умолчанию: 0.

    - **Допустимое ежедневное отклонение уровня доверия (DTLp)** – допустимое ежедневное отклонение уровня доверия (DTLp). Значение по умолчанию: 300.

    - **Порог уровня доверия warning** – порог уровня доверия warning. Значение по умолчанию: -700.

    - **Порог уровня доверия critical** – порог уровня доверия critical. Значение по умолчанию: -850.

    - **Порог уровня доверия адреса для автоматического создания персоны** – порог уровня доверия адреса для автоматического создания персоны. Значение по умолчанию: -600.

    - **Период хранения истории изменения уровня доверия (в днях)** – период хранения истории изменения уровня доверия (в днях). Значение по умолчанию: 365.

    - **Период истории, за который рассчитываются статистические показатели (в днях)** – период истории, за который рассчитываются статистические показатели (в днях). Значение по умолчанию: 30.

  - **Настройка работы в режиме главного сервера Досье** – настройки автоматической синхронизации досье с заданными в системе источниками LDAP/AD:

    - **Автоматическая синхронизация Досье** – включает автоматическую синхронизацию досье с источниками LDAP/AD. По умолчанию выключена.

- **Периодичность запуска синхронизации (ч)** – периодичность запуска в часах автоматической синхронизации досье с источниками LDAP/AD. Значение по умолчанию: 4.

  Примечание

  Периодичность запуска синхронизации происходит вне зависимости от наступления новой даты.

- **Периодичность запуска синхронизации (м)** – периодичность запуска в минутах автоматической синхронизации досье с источниками LDAP/AD. Значение по умолчанию: 0. Значение добавляется к количеству часов, заданному в предыдущем параметре.

  Примечание

  Не рекомендуется устанавливать значение периодичности синхронизации меньше 20 минут, т.к. при объемном LDAP-каталоге и большом количестве пользователей для успешного завершения обновления данного времени может быть недостаточно.

  При значении 0 часов 0 минут синхронизация работать не будет.

- **Метод синхронизации** – метод синхронизации с источниками данных. Принимает значения: **internal** и **internal (new ldap)**. Значение по умолчанию: **internal**.

  При значении **internal** синхронизация выполняется с использованием встроенного LDAP-клиента виртуальной машины Java, а при значении **internal (new ldap)** – с использованием клиента UnboundID LDAP SDK.

  Примечание

  *Рекомендуется применять метод **internal**. Если в процессе синхронизации появляется сообщение об ошибке **Connection reset**, следует использовать **internal (new ldap)**.*

- **Количество соединений с БД** – количество соединений сервиса **abook-daemon** с БД политики. Значение по умолчанию: 10.

  Рекомендуется указывать по следующей формуле: 5 + **<количество узлов с ролью abook-slave>** + **<количество инсталляций KEO DLP или KEO DLP webProxy с подчиненным Досье>** + **<количество узлов с ролью abook-slave на инсталляциях KEO DLP или KEO DLP webProxy с подчиненным Досье>** + **<количество БД архива на инсталляциях KEO DLP или KEO DLP webProxy с подчиненным Досье>**. Если полученная величина меньше 10, рекомендуется оставить значение по умолчанию.

Примечание

После увеличения значения параметра следует проверить ограничение на общее число соединений к БД политики. Для этого следует обратиться к специалистам, обеспечивающим устойчивую работу KEO DLP.

При использовании Досье другого кластера KEO DLP или KEO DLP webProxy, следует выбрать значение **Подчиненный**. В этом случае доступны следующие параметры:

- **Настройки подключения к master-системе Досье**:
  - **Сетевой адрес** – FQDN master-узла кластера KEO DLP или KEO DLP webProxy, с Досье которого будет выполняться синхронизация.
  - **Номер порта** – порт, на котором кластера с Досье ожидает соединения.

    После задания настроек подключения следует установить подключение к Досье стороннего кластера, нажав кнопку **Проверить**. В зависимости от ситуации появляются следующие сообщения:

    Проверка подключения не выполнялась – данное сообщение появляется, если проверка подключения к хранилищу Досье не выполнялась. При успешной проверке подключения появляется сообщение **Подключение проверено Проверка прошла успешно**.

    Примечание

    *Сохранение и применение конфигураций доступно также без установления подключения к Досье стороннего кластера. После нажатия кнопки **Применить** не подключенные друг к другу кластеры Досье, работающие в главном и подчиненном режимах, предпринимают попытки выполнить соединение раз в минуту. В журналах сервиса **abook-daemon** появляются записи об ошибках. В зависимости от типа ошибки конкретный вид записи может различаться.*
  - **Настройка работы в режиме главного сервера Досье** – см. описание выше.
- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса. По умолчанию выключено.

JVM сервиса доступа к Досье:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервиса доступа к Досье. Значение по умолчанию: 512 Мб.
- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **abook-daemon** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Источники данных досье (определяет настройки источников данных досье):

В этой группе параметров может быть задано несколько источников данных. Для добавления новой секции и нового источника следует нажать значок  рядом с идентификатором источника. Для удаления следует нажать значок  . Источник данных характеризуется идентификатором источника в базе данных. Идентификатор источника (параметр **Описание источника данных**) задается автоматически при добавлении нового источника и редактированию не подлежит. Описание источника данных содержит параметры **Название источника** и **Параметры доступа к источнику**.

- **Синхронизировать** – выполнить синхронизацию с источником.

  Примечание

  Синхронизация возможна только при выполнении следующих условий:

  - *Имеется хотя бы один включенный источник данных (установлен флажок "Синхронизация включена").*
  - *Настройки всех источников данных успешно применены.*
  - *В данный момент не выполняется другая синхронизация.*

- **Название источника** – название источника данных.
- **Синхронизация включена** – при установленном флажке Досье синхронизируется с источником данных.

  Возможные значения параметра: **true** и **false**. В конфигурации источников, поставляемых с системой (**AD**, **389 Directory Server Example** и **ALD Pro**), синхронизация по умолчанию отключена.

  Примечание

  При попытке синхронизировать Досье со всеми отключенными источниками данных отображается соответствующее предупреждение.

- **Параметры доступа к источнику данных** – выбираются из раскрывающегося списка. Возможные значения параметра: **ldap** и **file**.

  При выборе значения **ldap** появляется дополнительный набор параметров доступа к данным с LDAP-сервера (перечислены ниже):

  - **DN пользователя** – запись, которая уникально идентифицирует имя пользователя.
  - **Пароль пользователя** – пароль для идентификации пользователя.
  - **URL LDAP сервера** – URL LDAP-сервера.
  - **Базовый DN для поиска** – позволяет переопределить заданную по умолчанию начальную точку поиска.
  - **Число записей на странице** – размер страницы запроса. Измеряется в записях.

- **Фильтр подразделений** – строковое представление фильтра, применяемого при поиске подразделений.
- **Фильтр групп** – строковое представление фильтра, применяемого при поиске групп.
- **Фильтр персон** – строковое представление фильтра, применяемого при поиске персон.
- **Атрибут, содержащий уникальный идентификатор записи** – имя атрибута, содержащего UUID записи.
- **Атрибут, содержащий номер последнего изменения записи** – имя атрибута, содержащего номер последнего изменения записи.
- **Атрибут RootDSE, содержащий идентификатор сервера** – имя атрибута RootDSE, содержащего идентификатор сервера.
- **Атрибут RootDSE, содержащий номер последнего изменения содержимого** – имя атрибута RootDSE, содержащего номер последнего изменения содержимого.
- **Список соответствий атрибутов** – список соответствий атрибутов. Может быть задано несколько атрибутов учетной записи и для каждого из них указано соответствие **LDAP-атрибута** и **атрибута адресной книги**.

  Есть возможность выбора из следующего списка атрибутов персоны досье:

  - DN;
  - Уменьшенная фотография;
  - Адрес электронной почты;
  - ФИО;
  - Группа;
  - Фамилия;
  - Имя;
  - Название компании;
  - Должность;
  - Номер мобильного телефона;
  - Номер телефона;
  - Логин;
  - Кому подчиняется;
  - Дата приема на работу.

Примечание

*Адреса электронной почты пользователей (атрибут **Адрес электронной почты**) могут содержаться в атрибутах **proxyAddresses** и **mail**.*

Также задается **Приоритет источника** – приоритет источника, который учитывается при слиянии персон из нескольких источников. Если при слиянии персон значение уникального атрибута из источника с приоритетом, равным 1, отсутствует, то будет использовано значение этого атрибута из источника с приоритетом, равным 2 и т.д. Если необходимо настроить приоритеты по умолчанию, для атрибута у всех источников устанавливается приоритет, равный 1. Диапазон значений: от 1 до **N**, где **N** – число источников данных Досье.

- **Список соответствий атрибутов групп** – список соответствий атрибутов групп Досье. Может быть задан 1 атрибут группы Досье и для него указано соответствие **LDAP-атрибута** и атрибута группы персон, принимающего значение **Руководитель группы**.

При выборе значения **file** появляется дополнительный набор параметров, предназначенных для настройки импорта данных ОШС из файлов:

- **Каталог с данными ОШС** – каталог для размещения файлов с данными о структуре ОШС. Значение по умолчанию: **/data/spool/abook-daemon/org_structure/**.
- **Файл со списком групп** – имя csv-файла со списком групп. Значение по умолчанию: **groups.csv**.
- **Файл со списком сотрудников** – имя csv-файла со списком персон. Значение по умолчанию: **persons.csv**.

Сервис репликации Досье на подчиненных узлах:

- **Максимальное количество оперативной памяти (Мб)** – максимальное количество оперативной памяти в мегабайтах, которую может использовать процесс сервиса **abook-slave**. Значение по умолчанию: 1024.
- **Каталог для временных файлов** – каталог для хранения временных файлов. Значение по умолчанию: **/data/temp/abook-slave**.
- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **abook-slave**. По умолчанию выключено.
- **Снимать дампы памяти при критических ошибках** – включает сохранение дампа памяти процесса **abook-slave** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Сопоставление загружаемых данных из разных источников – определяет атрибуты персоны, по которым происходит сопоставление данных Досье, загружаемых из разных источников):

- **Параметры сопоставления карточек персон из нескольких источников** – может быть задано несколько атрибутов. Есть возможность выбора из следующего списка атрибутов персоны досье:
  - DN;
  - ICQ;
  - Windows SID;
  - Адрес электронной почты;
  - Город, нас. пункт;
  - Группа;
  - Дата изменения;
  - Дата приема на работу;
  - Дата увольнения;
  - День рождения;
  - Должность;
  - Домашняя страница;
  - Замечания, комментарий;
  - Имя;
  - Имя хоста рабочей станции;
  - Кому подчиняется;
  - Логин;
  - Название компании;
  - Название улицы, номер дома;
  - Номер автомашины;
  - Номер комнаты;
  - Номер мобильного телефона;
  - Номер офисного телефона;
  - Номер телефона;
  - Номер факса;
  - Область, регион;
  - Подразделение;

- Почтовый индекс;
- Страна;
- Уменьшенная фотография;
- ФИО;
- Фамилия;
- Фотография;
- Чем руководит.

Для добавления нового атрибута следует нажать кнопку **Добавить**. Для дублирования атрибута следует нажать значок рядом с названием параметра **Список соответствий атрибутов**. Для удаления атрибута следует нажать значок рядом с его названием.

Примеры по сопоставлению (слиянию) персон приведены в разделе 6.19.1.

A.2.4.4. Отчеты

Сервис построения отчетов:

- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервер будет принимать соединения. Значение по умолчанию: 9000.
- **Путь для сохранения результатов выполнения отчетов** – путь для сохранения результатов построения отчетов. Значение по умолчанию: **/data/spool/report-server**.
- **Email, с которого будут отправляться уведомления о завершении и результаты отчёта** – адрес электронной почты, с которого будут отправляться уведомления о завершении и результаты отчёта.

  Содержит параметры:

  - **Имя владельца почтового ящика** – имя персоны, которой принадлежит почтовый ящик. По умолчанию не заполняется.
  - **Имя почтового ящика** – уникальная комбинация букв, цифр и служебных символов, расположенная перед доменом. Значение по умолчанию: **dozor**.
  - **Имя почтового домена** – часть почтового ящика после символа **@**. Значение по умолчанию: **localhost**.
- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **report-server**. По умолчанию выключено.

Отладка сервиса построения отчетов:

- **Максимальное количество оперативной памяти (Мб)** – максимальное количество оперативной памяти в Мб, потребляемой сервисом **report-server**. Значение по умолчанию: 512.

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **report-server** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

A.2.4.5. Анализ поведения (UBA)

Сервис анализа поведения:

- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервис **uba-server** будет принимать соединения. Значение по умолчанию: 3030.
- **Таймаут соединения с Clickhouse (с)** –таймаут соединения с Clickhouse в секундах. Значение по умолчанию: 600.
- **Параметры расчета** – параметры расчеты показателей поведения персон:
  - **Исторический период для анализа (в днях)** – промежуток времени в днях, в течении которого хранится история поведения персоны. Значение по умолчанию: 90.
  - **Время буферизации сообщений (в секундах)** – время буферизации сообщений в секундах.
  - **Рамки устойчивого поведения: чувствительность к аномалиям** – определяет пороговое значение, при котором персона может выйти из ожидаемого интервала персональных показателей. Интервалы рассчитываются на основе персональной истории. Значение по умолчанию 1.2. Допустимые значения от 0.1 (больше аномалий) до 2.0 (меньше аномалий).
  - **Рамки устойчивого поведения: условие устойчивости** – определяет диапазон значений показателей поведения персон. Значение по умолчанию: 0.18. Допустимы значения от 0.05 (строгое условие – меньше аномалий) до 0.5 (слабое условие – больше аномалий).

    Примечание

    Значения персональных показателей не всегда устойчивы. При большом диапазоне значений показатели поведения считаются неустойчивыми и для них не выводятся аномалии.

  - **Расчетная точность** – степень близости показателей поведения персон к некоторому действительному значению. Чем меньше значение точности, тем вероятнее система обнаружит аномалию отклонения от нулевого значения. Значение по умолчанию: 0.03. Допустимы значения от 0 до 0.5.

JVM сервиса анализа поведения:

- **Максимальное количество оперативной памяти (МБ)** – максимально доступное количество оперативной памяти в мегабайтах, выделяемой для сервиса анализа поведения. Значение по умолчанию: 4096.

Внимание!

*Значение параметра **Максимально доступное количество оперативной памяти (МБ)** должно быть меньше объёма оперативной памяти виртуальной машины Java.*

- **Снимать дампы памяти при критических ошибках** – включает сохранение дампа памяти процесса **uba-server** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

- **Каталог для записи дампов памяти** – расположение журнального файла с записями дампов памяти. Значение по умолчанию: **/data/temp/java_dumps/uba-server**.

A.2.4.6. Расследование

Сервис **Расследование**:

- **Вывод отладочной информации** – включение вывода отладочной информации. По умолчанию вывод выключен.

- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервис **detective-server** будет принимать соединения. Значение по умолчанию: 8300.

- **Максимальный размер одного файла, прикрепляемого к делу (МБ)** – максимальный размер файла, прикрепляемого к делу в качестве материала. Значение по умолчанию: 50 Мб.

- **Максимальный совокупный размер всех файлов по делу (МБ)** – максимальный суммарный размер всех файлов, прикрепляемых к делу в качестве материала. Значение по умолчанию: 10240 Мб.

- **Частота репликации (с)** – частота в секундах, с которой данные о пользователях системы, их ролях и типах угроз копируются из БД политики в БД сервиса **Расследование**. Значение по умолчанию: 300.

- **Частота проверки файлов в БД в статусе "Ожидается загрузка файла" (с)** – частота проверки БД сервиса **Расследование** на наличие файлов, находящихся в статусе "Ожидается загрузка файла". Значение по умолчанию: 300.

- **Время ожидания загрузки файла (с)** – время, отведенное на загрузку файла на сервер. По истечении этого времени статус файла меняется на "Не удалось загрузить". Значение по умолчанию: 300.

JVM сервиса **Расследование**:

- **Максимальное количество оперативной памяти (МБ)** – максимально доступное количество оперативной памяти в мегабайтах, выделяемой для сервиса **Расследование**. Значение по умолчанию: 1024.

- **Снимать дампы памяти при критических ошибках** – включает сохранение дампа памяти процесса **detective-server** в случае ошибки исчерпания памяти. По умолчанию

выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

БД сервиса Расследование:

- **Настройки соединения с базой** – настройки подключения к БД:
  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД. Используемое значение: 5443.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.
  - **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.

A.2.5. Настройка обеспечивающих средств

A.2.5.1. Хранение

Выполнение действий над сообщениями в архиве:

- **Вывод отладочной информации** – вывод отладочной информации о работе сервиса **action-server**. По умолчанию выключено.
- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервер будет принимать соединения. Значение по умолчанию: 3001.
- **Количество тредов, выполняющих действия** – количество потоков сервиса действий. Значение по умолчанию: 3.
- **Количество тредов, выполняющих быстрые действия** – количество потоков, выполняющих "быстрые" действия. Значение по умолчанию: 3.
- **Ограничение на количество объектов для быстрых действий** – максимальное количество объектов, с которыми выполняются "быстрые" действия. Значение по умолчанию: 25.
- **Таймаут перезапуска действия (с)** – время в секундах от начала выполнения какого-либо задания, на которые разбивается действие, после которого это задание перезапускается. Значение по умолчанию: 3600.
- **Директория для хранения результатов выполнения действий** – путь к каталогу для хранения результатов выполнения действий. Значение по умолчанию: **/data/spool/dozor/actions**.
- **Таймаут взаимодействия с сервером распознавания речи (с)** – таймаут взаимодействия с сервером распознавания речи в секундах. Значение по умолчанию: 120.
- **Перепаковывать архивы при удалении файлов** – устанавливает тип обработки архивов при реконструкции. По умолчанию параметр отключен, и в случае истинности условия проверки при реконструкции весь архив будет удален. При включенном пара-

метре удалены будут только отдельные файлы, входящие в архив, удовлетворяющие условиям фильтрации, после чего архив будет переупакован заново в формате ZIP. Значение по умолчанию: **false**.

JVM сервиса выполнения действий над сообщениями в архиве:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервиса выполнения действий над сообщениями в архиве. Значение по умолчанию: 512 Мб.
- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **action-server** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Запись данных в архив:

- **Каталог спула** – путь к каталогу спула архиватора. Значение по умолчанию: **${smap-settings/common/smap-home}/spool/smap-db**.
- **Слоты спула** – слоты спула архиватора. Значение по умолчанию: 0 1 2 3 4 5.
- **Слоты, доступные для чтения** – слоты спула архиватора, доступные для чтения. Значение по умолчанию: 0 1 2 3 4 5.
- **Слоты, доступные для записи** – слоты спула архиватора, доступные для записи. Значение по умолчанию: 0 1 2 3 4 5.
- **Количество потоков для обработки данных высокого приоритета** – максимальное количество потоков, используемых сервисом **archiver** для чтения и обработки событий информационной безопасности и сообщений, предназначенных для размещения в ФХ и БД архива. Значение по умолчанию: 5.
- **Количество потоков для обработки данных низкого приоритета** – максимальное количество потоков, используемых сервисом **archiver** для чтения и обработки информации об изменении уровня доверия. Значение по умолчанию: 2.
- **Пауза перед повторным считыванием спула (с)** – таймаут в секундах между попытками чтения из спула, если в спуле отсутствуют данные. Значение по умолчанию: 5.
- **Пауза при ошибке соединения с целевыми сервисами (с)** – таймаут в секундах в случае возникновения ошибки при взаимодействии архиватора с каким-либо сервисом. Значение по умолчанию: 5.
- **Таймаут взаимодействия с целевыми сервисами (с)** – включает в себя таймаут на чтение или запись в файловое хранилище и таймаут на установление соединения с файловым хранилищем в секундах. При превышении таймаута в журнал архиватора записывается сообщение об ошибке, а сам архиватор продолжает работу с другими сервисами. Значение по умолчанию: 180.

Примечание

*При появлении сообщения **Read timed out** в журналах сервиса **archiver** требуется увеличить значение параметра **Таймаут взаимодействия с целевыми сервисами (с)**.*

- **Таймаут при взаимодействии с сервисом управления Досье (с)** – время ожидания в секундах при взаимодействии с сервисом управления Досье. Значение по умолчанию: 60.

БД сервера действий:

- **Настройки соединения с базой** – настройки подключения к БД сервера действий:
  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД. Используемое значение: 5440.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.
  - **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.

БД настроек политики и досье:

- **Настройки соединения с базой** – настройки подключения к БД политики:
  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД. Используемое значение: 5434.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.
  - **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.
- **Конфигурация сервера PostgreSQL** – параметры конфигурации сервера PostgreSQL. Принимает значения **По умолчанию** и **Задана**. При значении **По умолчанию** используются значения из конфигурационного файла **postgresql.conf**. При значении **Задана** доступна настройка следующих параметров:
  - **Объем временной памяти сессии (МБ)** – максимальный объём памяти в Мб, который будет использоваться во внутренних операциях при обработке запросов (например, для сортировки или хеш-таблиц), прежде чем будут задействованы временные файлы на диске. Значение по умолчанию: 32 Мб.
  - **Объем буферов разделяемой памяти (МБ)** – объём памяти в Мб, который будет использовать сервер баз данных для буферов в разделяемой памяти. Значение по умолчанию: 256 Мб.

- **Максимальное число соединений** – максимальное число одновременных подключений к серверу БД. Значение по умолчанию: 400.

Схемы соединений с БД:

- **Идентификатор соединения с базой данных** – идентификатор соединения с базой данных. Проставляется автоматически.
- **Подкластер** – подкластер, ресурсы которого использует выбранная БД. Выбирается из раскрывающегося списка. По умолчанию ничего не выбрано.

Примечание

Подкластеры могут настраиваться при наличии работающего модуля централизованного управления системой.

- **Имя схемы соединения с базой данных** – имя схемы соединения с базой данных. Параметр обязателен для заполнения.
- **Признак активности соединения** – необходимо включить параметр, чтобы активировать соединение. По умолчанию выключен.
- **Настройки использования соединения с БД** – настройки использования данного соединения:
  - **Использовать БД для поиска по архиву** – включает использование хранилища для поиска по архиву. Необходимо включить параметр, чтобы использовать хранилище для поиска по архиву. По умолчанию выключено.
  - **Использовать БД для архивирования сообщений** – включает использование хранилища для архивирования сообщений. Необходимо включить параметр, чтобы использовать хранилище для архивирования сообщений. По умолчанию выключено.
  - **Использовать БД для архивирования по умолчанию** – включает использование хранилища для архивирования сообщений, если в профиле архивирования не указано имя схемы соединения с БД. Может быть включено в нескольких схемах соединения (в этом случае БД для архивирования сообщения определяется случайным образом). По умолчанию включено.
- **Ротация данных** – включает выполнение действий по удалению старых сообщений, в т. ч. помеченных как важные, из БД архива, в которой не используется секционирование. Принимает значения: **Выключена** и **Включена**. По умолчанию параметр выключен. При значении **Включена** доступны следующие параметры:
  - **Ограничение на количество сообщений** – определяет ограничение на количество сообщений. При превышении этого количества старые записи удаляются. Принимает значения **Включено** и **Выключено**. При значении **Выключено** ограничение отсутствует. При значении **Включено** можно задать ограничение.
  - **Ограничение на суммарный объем сообщений (МБ)** – при превышении этого размера наиболее старые сообщения будут удалены. Принимает значения **Включено** и **Выключено**. При значении **Выключено** ограничение отсутствует. При значении **Включено** можно задать ограничение.

- **Не удалять сообщения с пометкой "Важное"** – при включенном параметре сообщения в архиве, помеченные как важные, не удаляются при очистке БД архива. При выключенном параметре в процессе удаления сообщений из архива (при превышении их количества или объема) сообщения с пометкой **Важное сообщение** также удаляются. По умолчанию параметр выключен.

- **Интервал проверки ограничений** – интервал проверки ограничений на количество и суммарный объем сообщений. Значение по умолчанию: **0 дн. 12 ч.**

- **Тип базы данных** – тип используемой СУБД: Oracle или PostgreSQL, выбирается из списка. В зависимости от выбора типа СУБД отображаются разные настройки соединения с базой данных. Ниже описаны отдельно параметры для настройки базы данных PostgreSQL и Oracle.

- **Настройки соединения с базой** – настройки соединения с базой (для PostgreSQL):

  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД PostgreSQL, обязательно для заполнения. Параметр обязателен для заполнения.

  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД PostgreSQL. Параметр обязателен для заполнения.

  - **Имя базы данных** – имя базы данных PostgreSQL. Параметр обязателен для заполнения.

  - **Пользователь базы данных** – указывается имя пользователя базы данных, заданное при установке. Параметр обязателен для заполнения.

  - **Пароль пользователя базы данных** – пароль пользователя для доступа к базе данных. В данном поле указывается пароль пользователя, заданный при установке.

- **Использование секционирования** (для PostgreSQL) – включает использование секционирования БД. Принимает значения **использовать** и **не используется**. Значение по умолчанию: **не используется**. При выборе значения **использовать** отображаются параметры секционирования:

  - **Период секционирования** – интервал времени в неделях, данные за который хранятся в одной секции. Значение по умолчанию: 4 (4 недели).

  - **Количество изначально создаваемых секций** – количество изначально создаваемых секций. Значение по умолчанию: 2.

  - **Интервал опережения при создании секций** – интервал опережения при создании новых секций. Если сумма текущей даты и значения этого параметра больше даты окончания предыдущей секции, то создаётся новая секция. Формат значений такой же, как и у **Период секционирования**. Значение по умолчанию: **8D**.

  - **Автоматическое отключение секций** – предоставляет возможность автоматически отключать секции. Принимает значения **используется** и **не используется**. Значение по умолчанию: **не используется**. При выборе значения **используется** отображаются параметры автоматического отключения:

    - **Время до автоматического отключения секций** – интервал времени, после которого выполняется автоматическое отключение секций. Значение состоит из длительности и размерности интервала, где размерность может быть одним из

следующего: **D** – день, **W** – неделя (строго равна 7 дням), **M** – месяц . Например: **1M** – один месяц; **2W** – две недели; **10D** – десять дней. Значение по умолчанию: **3M**.

- **detach-action** – действие при отключении секций. Принимает следующие значения: **Ручная обработка отключенных секций**, **Автоудаление отключенных секций**, **Автоархивирование отключенных секций**.

- **Параметры хранения данных в БД** – параметры хранения табличных пространств для секций БД архива под управлением СУБД PostgreSQL. Содержит следующие параметры:

  - **Список каталогов для табличных пространств MAIN** – каталог для файлов данных табличного пространства **MAIN**. Если параметр не задан, основные секционированные таблицы будут созданы без указания табличного пространства. Возможно указание нескольких каталогов через запятую без пробелов. Пример:

    ```
    /data2/isim,/data3/isim
    ```

    Если на очередном разделе места недостаточно (меньше чем указано в значении параметра **Минимально допустимое свободное место в каталоге MAIN**), выполняется попытка сохранения данных в следующем разделе по порядку и т.д.

  - **Минимально допустимое свободное место в каталоге MAIN** – минимальное значение объема свободного места в каталоге для файлов данных табличного пространства **MAIN**. Значение по умолчанию: **10M** (10 Мбайт). Допускается использование следующей размерности: **K** – Кб; **M** – Мб; **G** – Гб.

  - **Список каталогов для табличных пространств MESSAGE** – каталог для файлов данных табличного пространства **MESSAGE**. Если параметр не задан, основные секционированные таблицы будут созданы без указания табличного пространства. Возможно указание нескольких каталогов через запятую без пробелов. Пример:

    ```
    /data4/isim,/data5/isim,/data6/isim
    ```

    Если на очередном разделе места недостаточно (меньше чем указано в значении параметра **Минимально допустимое свободное место в каталоге MESSAGE**), выполняется попытка сохранения данных в следующем разделе по порядку и т.д.

  - **Минимально допустимое свободное место в каталоге MESSAGE** – минимальное значение объема свободного места в каталоге для файлов данных табличного пространства **MESSAGE**. Значение по умолчанию: **10M** (10 Мбайт). Допускается использование следующей размерности: **K** – Кб; **M** – Мб; **G** – Гб.

- **Настройки соединения с базой** – настройки соединения с базой данных (для Oracle):

  - **TNS имя** – имя службы TNS. Параметр обязателен для заполнения.

  - **Пользователь базы данных** – имя учетной записи пользователя базы данных. Параметр обязателен для заполнения.

- **Пароль пользователя базы данных** – пароль пользователя базы данных. Параметр обязателен для заполнения.

- **Настройки пользователя для мониторинга базы данных** – настройки пользователя для мониторинга базы данных (для Oracle).
  - **Пользователь базы данных** – монитор: имя учетной записи пользователя базы данных. Параметр обязателен для заполнения.
  - **Пароль пользователя базы данных** – монитор: пароль пользователя базы данных. Параметр обязателен для заполнения.

- **Обслуживание базы данных** – признак обслуживания базы данных (для Oracle). Необходимо выбрать из двух вариантов: **Настройки обслуживания базы данных** или **База данных не обслуживается**. В случае выбора варианта **Настройки обслуживания базы данных** отображаются следующие параметры для заполнения:
  - **Использование секционирования** – включает использование секционирования БД. Необходимо выбрать из двух вариантов: **используется** или **не используется**. Значение по умолчанию: **не используется**. в случае выбора варианта **используется** для заполнения отображаются следующие параметры (входящие с группу **использование секционирования**):
    - **Период секционирования** – период секционирования, то есть интервал времени, данные за который хранятся в одной секции. Значение состоит из длительности и размерности интервала, где размерность может быть одним из следующего: **D** – день, **W** – неделя (строго равна 7 дням), **M** – месяц. Например: **1M** – один месяц; **2W** – две недели; **10D** – десять дней. Значение по умолчанию: **1M**.
    - **Количество изначально создаваемых секций** – количество изначально создаваемых секций. Значение по умолчанию: 2.
    - **Номер первой секции. Нумерация начинается с этого числа** – номер первой созданной секции. Значение по умолчанию: 10000.
    - **Конец диапазона первой секции** – конец диапазона первой секции (созданной при создании БД).
    - **Использование внешнего обработчика операций с секциями** – использование внешнего обработчика операций с секциями. Необходимо включить параметр, чтобы обеспечить использование обработчика. По умолчанию выключен.
    - **Скрипт обработчика, вызывается при выполнении операций с секциями** – скрипт обработчика, который вызывается при выполнении операций с секциями. Значение по умолчанию: **/opt/oracle/bin/parthook.sh**.
    - **Добавлять секции автоматически** – позволяет добавлять секции автоматически. Необходимо включить параметр, чтобы секции автоматически добавлялись. По умолчанию включен.
    - **Добавление секций за указанное время до окончания последней** – добавление секций за указанное время до окончания последней. Значение состоит из длительности и размерности интервала, где размерность может быть одним из следующего: **D** – день, **W** – неделя (строго равна 7 дням), **M** – месяц. Например:

1M – один месяц; **2W** – две недели; **10D** – десять дней. Значение по умолчанию: **1D**.

- **Автоматическое отключение секций** – предоставляет возможность автоматически отключать секции. Принимает значения **используется** и **не используется**. Значение по умолчанию: **не используется**. При выборе значения **используется** отображаются параметры автоматического отключения:
  - **Максимальное количество online-секций** – максимальное количество online-секций. Значение по умолчанию: 999.
  - **Час автоматического отключения секций** – час автоматического отключения секций. Значение по умолчанию: 3.
  - **detach-action** – действие при отключении секций. Принимает следующие значения: **Ручная обработка отключенных секций**, **Автоудаление отключенных секций**, **Автоархивирование отключенных секций**.
  - **Полный путь к файлу скрипта на сервере Oracle, который запускается после автоматического отключения секции (detach-part-script)** – расположение файла скрипта на сервере Oracle. Скрипт запускается после автоматического отключения секции. По умолчанию: **/opt/oracle/parthook.sh**.
- **Использование TTS** – включает использование переносимых табличных пространств (Transportable Tablespaces) в СУБД Oracle. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Каталог для файлов TTS** – каталог, в который выгружаются файлы Transportable Tablespaces. Значение по умолчанию: **/tmp**.

- **Количество генераторов последовательностей для создания ID сообщений** – размер пула последовательностей, используемых для создания и присвоения идентификаторов сообщениям. Параметр используется при постоянно высокой скорости загрузки сообщений в архив (порядка 1000 в секунду) для уменьшения хаотичности при присвоении идентификаторов сообщениям и уменьшения количества повторных загрузок сообщений в архив. Значение по умолчанию: 0.
- **Инсталляция в конфигурации RAC** – включает установку Oracle Real Application Cluster. Используется в случае установки СУБД Oracle на нескольких узлах.
- **Параметры хранения данных в базе** – параметры хранения данных в базе:
  - **Параметры создания новых файлов данных** – параметры создания новых файлов данных.
    - **Каталог для файлов данных табличного пространства MAIN** – каталог для файлов данных табличного пространства MAIN. Параметр обязателен для заполнения. Возможно указание нескольких каталогов через запятую или запятую и пробел.
    - **Каталог для файлов данных табличного пространства MESSAGES** – каталог для файлов данных табличного пространства MESSAGES. Параметр обязателен для заполнения. Возможно указание нескольких каталогов через запятую или запятую и пробел.

- **Каталог для файлов данных табличного пространства INDEXES** – каталог для файлов данных табличного пространства INDEXES. Параметр обязателен для заполнения. Возможно указание нескольких каталогов через запятую или запятую и пробел.
- **Каталог для файлов данных табличного пространства DICT** – каталог для файлов данных табличного пространства DICT. Параметр обязателен для заполнения. Возможно указание нескольких каталогов через запятую или запятую и пробел.
- **Начальные размеры для файлов данных табличного пространства MAIN** – начальные размеры для файлов данных табличного пространства MAIN. Параметр обязателен для заполнения.
- **Начальные размеры для файлов данных табличного пространства MESSAGES** – начальные размеры для файлов данных табличного пространства MESSAGES. Параметр обязателен для заполнения.
- **Начальные размеры для файлов данных табличного пространства INDEXES** – начальные размеры для файлов данных табличного пространства INDEXES. Параметр обязателен для заполнения.
- **Начальные размеры для файлов данных табличного пространства DICT** – начальные размеры для файлов данных табличного пространства DICT. Параметр обязателен для заполнения.
- **Размер по умолчанию для экстентов табличного пространства MAIN** – размер по умолчанию для экстентов табличного пространства MAIN. Параметр обязателен для заполнения.
- **Размер по умолчанию для экстентов табличного пространства MESSAGES** – размер по умолчанию для экстентов табличного пространства MESSAGES. Параметр обязателен для заполнения.
- **Размер по умолчанию для экстентов табличного пространства INDEXES** – размер по умолчанию для экстентов табличного пространства INDEXES. Параметр обязателен для заполнения.
- **Размер по умолчанию для экстентов табличного пространства DICT** – размер по умолчанию для экстентов табличного пространства DICT. Параметр обязателен для заполнения.

- **Настройки авторасширения файлов данных** – настройки авторасширения файлов данных. Необходимо выбрать из двух вариантов: **yes** - авторасширение включено, **авторасширение отключено** – авторасширение отключено. Значение по умолчанию: **авторасширение отключено**. В случае выбора варианта **yes** для заполнения отображаются следующие параметры (входящие с группу **Настройки авторасширения файлов данных**):
  - **Размер очередного экстента** – размер очередного экстента. Параметр обязателен для заполнения.
  - **Ограничение на максимальный размер файлов данных** – ограничение на максимальный размер файлов данных. Необходимо выбрать из двух вариан-

тов: **Ограничение отключено** – нет ограничения на максимальный размер файла, **Максимальный размер файла данных** – есть ограничение. Значение по умолчанию: **Ограничение отключено**. В случае выбора варианта **Максимальный размер файла данных** для заполнения отображается параметр **Максимальный размер файла данных** (входит в группу **Ограничение на максимальный размер файлов данных**).

- **Настройки LOB** – настройки хранения больших объектов в СУБД Oracle:
  - **Размеры LOB chunks** – размеры фрагментов больших объектов в СУБД Oracle. Параметр обязателен для заполнения.
  - **Размеры LOB chunks для текстовых частей** – размеры больших объектов в СУБД Oracle для текстовых частей. Параметр обязателен для заполнения.
- **Каталог для внешних скриптов на сервере базы данных** – путь к внешним скриптам на сервере базы данных. Параметр обязателен для заполнения.
- **Параметры автоматического управления файлами данных** – параметры автоматического управления файлами данных:
  - **Добавление файлов данных при уменьшении доступного в ТП MAIN места ниже указанного предела (monitor-reserved-main)** – добавление файлов данных при уменьшении доступного в ТП MAIN места ниже указанного предела. Параметр обязателен для заполнения.
  - **Добавление файлов данных при уменьшении доступного в ТП MESSAGES места ниже указанного предела (monitor-reserved-mess)** – добавление файлов данных при уменьшении доступного в ТП MESSAGES места ниже указанного предела. Параметр обязателен для заполнения.
  - **Добавление файлов данных при уменьшении доступного в ТП INDEXES места ниже указанного предела (monitor-reserved-indx)** – добавление файлов данных при уменьшении доступного в ТП INDEXES места ниже указанного предела. Параметр обязателен для заполнения.
  - **Добавление файлов данных при уменьшении доступного в ТП DICT места ниже указанного предела (monitor-reserved-dict)** – добавление файлов данных при уменьшении доступного в ТП DICT места ниже указанного предела. Параметр обязателен для заполнения.
  - **Добавление файлов данных при уменьшении доступного в ТП MAIN места ниже указанного предела (в процентах) (monitor-pct-free-main)** – добавление файлов данных при уменьшении доступного в ТП MAIN места ниже указанного предела (в процентах). Параметр обязателен для заполнения.
  - **Добавление файлов данных при уменьшении доступного в ТП MESSAGES места ниже указанного предела (в процентах) (monitor-pct-free-mess)** – добавление файлов данных при уменьшении доступного в ТП MESSAGES места ниже указанного предела (в процентах). Параметр обязателен для заполнения.
  - **Добавление файлов данных при уменьшении доступного в ТП INDEXES места ниже указанного предела (в процентах) (monitor-pct-free-indx)** –

добавление файлов данных при уменьшении доступного в ТП INDEXES места ниже указанного предела (в процентах). Параметр обязателен для заполнения.

- **Добавление файлов данных при уменьшении доступного в ТП DICT места ниже указанного предела (в процентах) (monitor-pct-free-dict)** – добавление файлов данных при уменьшении доступного в ТП DICT места ниже указанного предела (в процентах). Параметр обязателен для заполнения.

- **Настройки отправки почтовых сообщений из базы данных** – настройки отправки почтовых сообщений из базы данных:

  - **SMTP-сервер для отсылки уведомлений** – SMTP-сервер, выбранный для отсылки уведомлений. Значение по умолчанию: **change_on_install**. Параметр обязателен для заполнения.

    Примечание

    Для получения уведомлений от СУБД Oracle необходимо заменить значение на имя почтового сервера организации.

  - **SMTP-порт для отсылки уведомлений** – SMTP-порт, указанный для отсылки уведомлений. Значение по умолчанию: 25. Параметр обязателен для заполнения.

  - **Поле Кому сообщения с уведомлением** – поле **Кому** сообщения с уведомлением. Значение по умолчанию: **dozor**. Параметр обязателен для заполнения.

- **Статистика smap** – определяет статистику **smap**.

  - **История монитора БД** – история монитора БД. Необходимо выбрать из двух вариантов: **ведется** – ведется история монитора БД, **не ведется** – история монитора БД не ведется. В случае выбора варианта **ведется** отображаются следующие параметры для заполнения:

    - **Период добавления данных в историю** – период добавления данных в историю.

    - **Период хранения данных в истории** – период хранения данных в истории.

Использование файлового хранилища:

- **Использовать ФХ** – включает использование файлового хранилища. При включенном параметре сообщения при архивировании будут помещаться в файловое хранилище.

Настройки файлового хранилища:

- **Настройки HTTPS**:

  - **HTTPS-порт сервера файлового хранилища** – HTTPS-порт сервера файлового хранилища. Значение по умолчанию: 2266.

- **Gzip-компрессия при размещении** – Gzip-компрессия при закладке писем в файловое хранилище. По умолчанию включена.

- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервиса **filestorage-ng**. Предназначено для диагностики возникающих проблем в работе файлового хранилища. По умолчанию выключено.

- **Режим распределения по хранилищам при переносе** – алгоритм распределения данных по хранилищам при их переносе. Принимает значения: **Приоритет скорости** и **Равномерное распределение**. Значение по умолчанию: **Приоритет скорости**.

  При выбранном значении **Приоритет скорости** данные переносятся в центральные ФХ с той скоростью, с которой они могут быть приняты. Более быстрый сервер забирает на себя больше данных. Неработающие узлы исключаются из переноса. Этот режим наиболее производительный, но может приводить к дисбалансу объемов хранения между хранилищами.

  При выбранном значении **Равномерное распределение** на каждое центральное ФХ переносится одинаковое количество контейнеров. Медленный узел замедляет процесс переноса. Неработающий узел практически останавливает процесс переноса. Этот режим дает равномерное распределение данных по хранилищам, но скорость переноса фактически ограничена скоростью самого медленного узла.

- **Разрешенные часы переноса данных из локального файлового хранилища в центральное**:

  - **Час начала (timezone сервера)** – час начала переноса данных из локального файлового хранилища в центральное. Значение по умолчанию: 0.

  - **Час окончания (timezone сервера)** – час окончания (включительно, минуты игнорируются) переноса данных из локального файлового хранилища в центральное. Значение по умолчанию: 24.

- **Настройка переноса контейнеров** – параметры переноса контейнеров. Для настроек нового контейнера необходимо щелкнуть мышью на значок  . Для удаления языка необходимо щелкнуть мышью на значок  рядом с нужным полем ввода.

  - **Volume Group** – идентификатор группы томов. Значение по умолчанию: **vg-000000**.

  - **Время жизни до переноса** – время нахождения сообщений в локальном файловом хранилище до начала переноса в центральное. Задаётся в днях и часах. Значение по умолчанию: **0д, 0ч** (немедленный перенос).

- **Настройка ротации** – параметры ротации.

  - **Volume Group** – идентификатор группы томов. Значения:

    - **agent-media** – для первой конфигурации ротации.

    - **audio** – для второй конфигурации ротации.

  - **Время жизни до ротации (дней)** – время нахождения сообщений в центральном файловом хранилище до начала их ротации. Задаётся в днях. Значение по умолчанию: 30.

  - **Рекомендуемый размер файла архива (Мб)** – максимальный размер файла, формируемый при ротации в режиме **Локальная файловая система**. Если объем

передаваемых во внешнее хранилище данных превышает указанное в данном параметре значение, данные разбиваются на несколько архивных файлов, размер каждого из которых не превышает указанное в параметре значение. Указывается в мегабайтах. Значение по умолчанию: 256.

- **Критический объем свободного места (Мб)** – минимальное значение объема свободного пространства в центральном ФХ. Проверка свободного пространства производится каждые сутки в 3 часа ночи по времени сервера. Если объем свободного пространства в центральном ФХ становится меньше значения этого параметра, производится внеочередная ротация. Указывается в мегабайтах. Значение по умолчанию: 256.

- **Gzip компрессия архива** – включает gzip-компрессию при ротации в режиме **Локальная файловая система**. По умолчанию выключена.

- **Режим ротации** – режим ротации. Имеется три режима: удаление данных (**Удалить, не архивировать**), сохранение на локальном носителе (**Локальная файловая система**) и сохранение на внешнем ftp-сервере (**Внешний FTP сервер**). Значение по умолчанию: **Удалить, не архивировать**.

  При значении **Локальная файловая система** данные при ротации будут отключены от ФХ и помещены в каталог, указанный в параметре **Путь**.

  При значении **Внешний FTP сервер** данные при ротации будут отключены от ФХ и помещены заданный каталог на заданном FTP-сервере:

  - **Сетевой адрес** – адрес FTP-сервера организации.
  - **Номер порта** – порт, на котором FTP-сервер ожидает соединения.
  - **Режим FTP** – режим работы, на который настроен FTP-сервер (активный или пассивный).
  - **Пользователь** – имя пользователя для соединения с FTP-сервером.
  - **Пароль** – пароль этого пользователя.
  - **Путь на FTP-сервере** – путь к каталогу на FTP-сервер, в который будут сохраняться данные при ротации.

- **Периодичность ротации** – периодичность ротации. Имеется три варианта: **Ежедневно**, **Еженедельно** и **Ежемесячно**. Значение по умолчанию: **Ежедневно** (ежедневно).

Тома файлового хранилища:

По умолчанию создано 6 групп томов файлового хранилища, которые характеризуются идентификаторами в базе данных. Идентификатор группы задается автоматически и редактированию не подлежит. Для добавления новой группы следует нажать значок рядом с идентификатором группы, а для удаления – значок . Каждая группа томов содержит набор следующих параметров:

- **Группа томов (Volume Group)** – идентификатор группы томов. Принимает значения:

- **vg-000000** – для первой группы.
- **abook** – для второй группы.
- **agent-media** – для третьей группы.
- **audio** – для четвертой группы.
- **screen-video** – для пятой группы.
- **detective-data** – для шестой группы.

- **Идентификатор тома** – идентификатор тома. Принимает значения:
  - **main** – для первой группы.
  - **abook** – для второй группы.
  - **agent-media** – для третьей группы.
  - **audio** – для четвертой группы.
  - **screen-video** – для пятой группы.
  - **detective-data** – для шестой группы.
- **Только для чтения** – настройка тома только для чтения. По умолчанию выключено.
- **Разрешить ротацию тома** – разрешить ротацию тома. Если том относится к локальному файловому хранилищу, настройка игнорируется. По умолчанию выключено.
- **Путь, по которому размещены данные** – путь, по которому размещены данные файлового хранилища. Принимает значения:
  - **/data/storage/vg-000000/fs-1** – для первой группы.
  - **/data/storage/abook** – для второй группы.
  - **/data/storage/agent-media** – для третьей группы.
  - **/data/storage/audio** – для четвертой группы.
  - **/data/storage/screen-video** – для пятой группы.
  - **/data/storage/detective-data** – для шестой группы.

JVM файлового хранилища:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса **filestorage-ng**. Значение по умолчанию: 256.
- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **filestorage-ng** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Доступ к сообщениям в архиве:

- **Вывод отладочной информации** – включает вывод отладочной информации в журнальный файл сервера архива сообщений. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.
- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервер будет принимать соединения. Значение по умолчанию: 3000.
- **Максимальное количество одновременно обрабатываемых клиентских запросов** – максимальное количество клиентских запросов, которые сервер архива может выполнять одновременно. Значение по умолчанию: 50.
- **Директория для хранения построенных отчетов** – путь к каталогу для хранения построенных отчётов. Значение по умолчанию: **/data/spool/dozor/reports**.
- **Максимальное количество выполняемых одновременно отчетов для каждой БД** – максимальное количество отчётов, одновременно составляемых для каждой БД. Значение по умолчанию: 3.
- **Настройки пула соединений с БД** – настройки пула соединений сервера архива с базами данных архива:
  - **Максимальное количество соединений** – максимальное количество соединений, создаваемых для каждой БД. Значение по умолчанию: 15.

Отладка доступа к сообщениям в архиве:

- **Максимальное количество оперативной памяти (Мб)** – максимальное количество оперативной памяти в Мб, потребляемой сервисом **archive-server**. Значение по умолчанию: 512.
- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **archive-server** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Хранение медиаинформации:

- **Вывод отладочной информации** – включение вывода отладочной информации. По умолчанию вывод включен.
- **Локальный порт, на котором сервер будет принимать соединения** – порт, на котором сервер будет принимать соединения. Значение по умолчанию: 3003.
- **Срок хранения снимков (д)** – период хранения метаданных снимков экрана в днях. Значение по умолчанию: 90.
- **Срок хранения снимков демонстрации экрана (ч)** – период хранения снимков демонстрации экрана в часах. Значение по умолчанию: 2160 (90 дней).
- **Срок хранения аудиозаписей (д)** – период хранения метаданных аудиозаписей в днях. Значение по умолчанию: 90.

- **Срок хранения записей экрана (д)** – период хранения метаданных записей экрана/экранов рабочих станций персоны в днях. Значение по умолчанию: 90.
- **Срок хранения списков процессов приложений (д)** – период хранения метаданных запущенных процессов, активного URL и заголовка активного окна. Значение по умолчанию: 90.
- **База данных (PostgreSQL)** – имя схемы соединения с БД, используемой для хранения информации о задачах сервиса **agent-media-server**. Принимает значения **БД по умолчанию** и **Специальная БД**. Значение по умолчанию: **БД по умолчанию**. При значении **БД по умолчанию** сервис подключается к БД политики, настройки которой задаются в разделе GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** > **БД для хранения настроек политики и досье**. Если выбрано значение **Специальная БД**, доступны параметры:
  - **Сетевое имя сервера базы данных** – имя сервера с установленной БД.
  - **Сетевой порт сервера базы данных** – сетевой порт сервера БД.
  - **Имя базы данных** – имя БД.
  - **Пользователь базы данных** – указывается имя пользователя БД.
  - **Пароль пользователя базы данных** – пароль пользователя для доступа к БД. В данном поле указывается пароль пользователя, заданный при установке.
  - **Проверка подключения не выполнялась** – данное сообщение появляется, если проверка подключения к базе данных не выполнялась. При успешной проверки подключения появляется следующее сообщение **Подключение проверено 01.09.2021 11:45 Проверка прошла успешно**.
- **Настройки индексации медиаинформации** – настройки индексации медиаинформации:
  - **Порог журналирования медленных запросов (мс)** – порог журналирования медленных запросов в миллисекундах. Значение по умолчанию: 1000.
  - **Число копий** – число копий индексов OpenSearch. Значение по умолчанию: 0.
  - **Периодичность обновления индекса (с)** – интервал времени в секундах между помещением индекса в базу данных OpenSearch и его отображением (доступностью для использования). Значение по умолчанию: 30.
  - **Число записей в блоке для индексации** – максимальное количество записей в блоке, обрабатываемом за один шаг индексирования. Значение по умолчанию: 100.
  - **Пауза между индексацией блоков (с)** – таймаут в секундах между шагами индексирования. Значение по умолчанию: 60.
  - **Количество потоков индексации** – максимальное количество потоков, используемых сервисом **agent-media-server** для индексации медиаинформации. Значение по умолчанию: 1.

Отладка хранения медиаинформации:

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти процесса **agent-media-server** в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Сервер БД Clickhouse:

- **Локальный порт, на котором сервер будет принимать соединения** – локальный порт, на котором сервер будет принимать соединения. Значение по умолчанию: 9001.
- **Порт для подключения к Clickhouse по HTTP** – порт для подключения к серверу БД Clickhouse по протоколу HTTP. Значение по умолчанию: 8123.
- **Уровень отладки** – степень детализации журналирования. Значение по умолчанию: **warning**. В качестве значения можно выбрать один из следующих параметров в раскрывающемся списке:
  - **none** – ничего не журналировать.
  - **fatal** – журналировать только критические ошибки с уровнем **FATAL**.
  - **critical** – журналировать только критические ошибки с уровнем **CRITICAL**.
  - **error** – журналировать все ошибки.
  - **warning** – журналировать все ошибки и предупреждения.
  - **notice** – журналировать все ошибки, предупреждения, информацию и уведомления о работе модуля.
  - **information** – журналировать все ошибки, предупреждения и информацию о работе модуля.
  - **debug** – журналировать все ошибки, предупреждения, информацию о работе модуля и общую отладочную информацию.
  - **trace** – журналировать все ошибки, предупреждения, информацию о работе модуля и полную отладочную информацию.
- **Максимальное число тредов** – максимальное число потоков, в которых функционирует БД. Задается в диапазоне от 1 до 100 включительно. Рекомендуется установить равным числу процессоров. При выборе оптимального значения необходимо учитывать наличие на узле другого ПО, интенсивно использующего ЦП. Значение по умолчанию: 4.
- **Максимальное количество оперативной памяти (МБ)** – максимальный объем памяти в МБ, потребляемой СУБД Clickhouse. Значение по умолчанию: 10000.

A.2.5.2. Отправка

Сервис отправки сообщений:

- **Вывод отладочной информации** – записывать в журнал сервиса отправки отладочную информацию. По умолчанию выключено.

- **Количество процессов** – количество потоков, используемых для отправки сообщений. Значение по умолчанию: 2.

- **Размер сегмента** – максимальное количество почтовых сообщений, отправляемых в пределах одной SMTP-сессии. Значение по умолчанию: 100.

- **Таймаут на сетевое взаимодействие при использовании SMTP** – время ожидания сетевого взаимодействия в секундах при отправке сообщений по протоколу SMTP. Значение по умолчанию: 60.

- **Каталог для почты, ожидающей отправки** – каталог для сообщений, ожидающих отправки. Значение по умолчанию: **${smap-settings/common/smap-home}/spool/smap-send**.

- **Слоты в каталоге для почты, ожидающей отправки** – слоты в каталоге для сообщений, ожидающих отправки. Значение по умолчанию: 0 1 2 3. Это значит, что в каталоге для сообщений, ожидающих отправки, доступны четыре слота - каталоги с именами **/spool/smap-send/norm0**, **/spool/smap-send/norm1**, **/spool/smap-send/norm2** и **/spool/smap-send/norm3**.

- **Слоты, доступные для записи** – слоты, доступные для записи. Значение по умолчанию: 0 1 2 3. Это значит, что для записи сообщений доступны четыре слота - каталоги с именами **/spool/smap-send/norm0**, **/spool/smap-send/norm1**, **/spool/smap-send/norm2** и **/spool/smap-send/norm3**.

- **Слоты, доступные для чтения** – слоты, доступные для чтения. Значение по умолчанию: 0 1 2 3. Это значит, что для чтения сообщений доступны четыре слота - каталоги с именами **/spool/smap-send/norm0**, **/spool/smap-send/norm1**, **/spool/smap-send/norm2** и **/spool/smap-send/norm3**.

- **Слоты для сообщений высокого приоритета в каталоге для почты, ожидающей отправки** – слоты для сообщений с высоким приоритетом в каталоге для сообщений, ожидающих отправки. Значение по умолчанию: 0 1. Это значит, что в каталоге для сообщений, ожидающих отправки, имеется два слота для сообщений высокого приоритета с именами **/spool/smap-send/high0** и **/spool/smap-send/high1**.

- **Слоты, доступные для записи сообщений высокого приоритета** – слоты для сообщений с высоким приоритетом, ожидающих отправки, доступные для записи сообщений. Значение по умолчанию: 0 1. Это значит, что в каталоге для сообщений, ожидающих отправки, имеются два слота для сообщений высокого приоритета, в которые возможна запись, с именами **/spool/smap-send/high0** и **/spool/smap-send/high1**.

- **Слоты, доступные для чтения сообщений высокого приоритета** – слоты для сообщений с высоким приоритетом, ожидающих отправки, доступные для чтения сообщений. Значение по умолчанию: 0 1. Это значит, что в каталоге для сообщений, ожидающих отправки, имеются два слота для сообщений высокого приоритета, из которых возможно чтение, с именами **/spool/smap-send/high0** и **/spool/smap-send/high1**.

JVM сервиса отправки сообщений:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в Мб, выделяемой для сервиса отправки сообщений. Значение по умолчанию: 256.

- **Снимать дампы памяти при критических ошибках** – сохранение дампа памяти сервиса отправки сообщений в случае ошибки исчерпания памяти. По умолчанию выключено. Рекомендуется использовать с осторожностью, поскольку файл дампа занимает значительный объём на дисковом пространстве.

Наборы параметров отправки сообщений:

- **Параметры отправки** – определяют настройки наборов параметров отправки сообщений. Для соединения с сервисом отправки сообщений по умолчанию используется первый набор в списке.

  Можно добавить несколько значений, нажав кнопку **Добавить**. Для удаления набора параметров следует нажать значок  . Для дублирования набора параметров следует нажать значок  .

  - **ID** – идентификатор набора параметров отправки.
  - **Название набора параметров** – имя набора параметров отправки. Значение по умолчанию: **default**.
  - **Метод доставки** – метод доставки: **Sendmail**, **SMTP** или **Скрипт**. В случае **Sendmail** сообщение передается на локальный MTA, а в случае **SMTP** KEO DLP отправляет сообщение на указанный SMTP-сервер. Значение по умолчанию: SMTP. В случае **Скрипт** сообщение обрабатывается с помощью команд, описанных в файле скрипта.

    Если выбран метод **Sendmail**, то доступны следующие параметры:

    - **Файл конфигурации sendmail** – конфигурационный файл Sendmail. Необязательный параметр.
    - **Путь к программе sendmail** – путь к программе Sendmail.
    - **Использовать sendmail с опцией -bs** – использование Sendmail с ключом **–bs**. Можно использовать Sendmail либо с ключом **–bs**, либо без него.

    Если выбран метод **smtp**, можно задать несколько SMTP-соединений, нажав кнопку **Добавить**. Для удаления значения следует нажать значок  . Для дублирования SMTP-соединения следует нажать значок  . Доступны следующие параметры в группе **Соединения SMTP**:

    - **Протокол SMTP-сервера** – протокол SMTP-сервера. Параметр определяет протокол работы SMTP-сервера. Возможные варианты выбираются из раскрывающегося списка: **SMTP**, **SMTPS**, **SMTP over TLS**. Значение по умолчанию: **SMTP**.
    - **SMTP-сервер** – значение SMTP-сервера. Значение по умолчанию: **localhost**.
    - **SMTP-порт** – номер SMTP-порта. Значение по умолчанию: 1025.
    - **Использовать режим BINARY MIME** – включает передачу 8-битных данных на SMTP-сервер. Принимает значения **true** (включено) и **false** (выключено). Значение по умолчанию: **false**.

Если выбран метод **Скрипт**, то доступен параметр **Скрипт** – определяет расположение скрипта.

A.2.5.3. Безопасность

Правила аутентификации:

- **Минимальная длина пароля** – минимальная длина пароля. Значение по умолчанию: 6.
- **Максимальная длина пароля (2-12)** – максимальная длина пароля. Возможные значения от 2 до 12. Значение по умолчанию: 12.
- **Минимальная допустимая сложность пароля (2-10)** – минимальная допустимая сложность пароля. Сложность пароля выражается числом от 2 до 10. Значение по умолчанию: 6.
- **Двойное поле для ввода пароля** – двойное поле для ввода пароля. При включенном параметре в процессе авторизации администратора используется раздельный пароль, для ввода которого используется два поля ввода. По умолчанию флажок не установлен.
- **Двухфакторная аутентификация** – если флажок установлен, для входа в систему под локальной или доменной учетной записью с включенной двухэтапной проверкой необходимо дополнительно отсканировать QR-код и ввести одноразовый код. При повторном входе достаточно ввести только одноразовый код. По умолчанию флажок не установлен.
- **Время блокировки учётной записи после исчерпания попыток входа, мин.** – время в минутах, на которое блокируется учётная запись после неудачного/неверного ввода данных для авторизации. Значение по умолчанию: 15. Допустимое значение – от 15 до 1440.
- **Период времени, в течение которого подсчитываются неудачные попытки аутентификации, мин.** – период времени в минутах, в течение которого подсчитываются неудачные попытки входа пользователя. Значение по умолчанию: 60. Допустимое значение – от 60 до 1440.
- **Доменная аутентификация через Kerberos** – включает или выключает аутентификацию в KEO DLP под доменной учетной записью без ввода логина и пароля. Используется механизм аутентификации Kerberos. Принимает значения **true** и **false**.

  При значении **true** станет доступна кнопка **Войти через домен**. Таким образом, вход в KEO DLP можно выполнить локальной и доменной учетными записями. Чтобы войти в KEO DLP под учетной записью AD, следует нажать кнопку **Войти через домен**. В этом случае вводить логин и пароль не требуется, т.к. для аутентификации в KEO DLP используются данные учетной записи, уже выполнившей вход в ОС.

  Если системный администратор организации заблокировал учетную запись пользователя в AD, активный сеанс работы такого пользователя в системе будет завершен. После этого откроется окно авторизации KEO DLP.

  Если доменная учетная запись AD не активна, удалена или заблокирована, доступ в KEO DLP под доменной учетной записью запрещен. В этом случае будет выдано соответствующее сообщение об ошибке.

При значении **false** аутентификация в KEO DLP выполняется только под локальной учетной записью.

Значение по умолчанию: **false**.

- **Идентификатор службы Kerberos (SPN)** – имя участника службы для Kerberos-соединений. Задается в формате **HTTP/<dozor.fqdn>@<DOMAIN>**, где **<dozor.fqdn>** – FQDN master-узла KEO DLP, **<DOMAIN>** – имя домена. Используется совместно с параметром **Доменная аутентификация через Kerberos**.

Локальный веб-сервер:

- **Доменная аутентификация через Kerberos** – включает или выключает аутентификацию в KEO DLP под доменной учетной записью без ввода логина и пароля. Используется механизм аутентификации Kerberos. Принимает значения **true** и **false**.

  При значении **true** станет доступна кнопка **Войти через домен**. Таким образом, вход в KEO DLP можно выполнить локальной и доменной учетными записями. Чтобы войти в KEO DLP под учетной записью AD, следует нажать кнопку **Войти через домен**. В этом случае вводить логин и пароль не требуется, т.к. для аутентификации в KEO DLP используются данные учетной записи, уже выполнившей вход в ОС.

  Если системный администратор организации заблокировал учетную запись пользователя в AD, активный сеанс работы такого пользователя в системе будет завершен. После этого откроется окно авторизации KEO DLP.

  Если доменная учетная запись AD не активна, удалена или заблокирована, доступ в KEO DLP под доменной учетной записью запрещен. В этом случае будет выдано соответствующее сообщение об ошибке.

  При значении **false** аутентификация в KEO DLP выполняется только под локальной учетной записью.

  Значение по умолчанию: **false**.

- **Идентификатор службы Kerberos (SPN)** – имя участника службы для Kerberos-соединений. Задается в формате **HTTP/<dozor.fqdn>@<DOMAIN>**, где **<dozor.fqdn>** – FQDN master-узла KEO DLP, **<DOMAIN>** – имя домена. Используется совместно с параметром **Доменная аутентификация через Kerberos**.

Приложение В. Описание журнала обработки сообщений

Журнал обработки сообщений (**message-stat.log**) создан для интеграции с SIEM-системами и позволяет отслеживать важные шаги в обработке сообщения. Используется аналогично другим журналам системы, но имеет свой формат, более удобный для обработки внешними средствами. В файл **message-stat.log** записывается только определенный набор шагов обработки, поэтому он остается управляемым даже если в системе включен debug на фильтрации, что удобно и при ручном мониторинге системы. Для точной диагностики лучше использовать журнал сервиса **mailfilter**, а просматривать статистику удобнее в журнале обработки сообщений.

Журнал обработки сообщений записывается в файл **/opt/dozor/var/log/message-stat.log**. Ротация выполняется стандартными средствами. Просмотр журнала возможен как через интерфейс, так и с помощью скрипта **seelog**. По умолчанию запись операций над сообщениями в журнальный файл отключена, для ее включения необходимо установить флажок **Журналировать операции над сообщениями в файл?** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений**, секция **Настройки сервиса фильтрации сообщений**)

Каждый сервис записывает в журнал обработки сообщений информацию об определенных действиях. Запись состоит из набора параметров. Некоторые параметры присутствуют в каждой записи (общие), другие только в записях об определенных действиях. Есть также параметры, специфичные для определенных типов сообщений.

Общие параметры журнала обработки сообщений представлены в таблице Табл.В.1.

Табл. В.1. Общие параметры журнала обработки сообщений

Параметр	Расшифровка параметра	Комментарий
SolarSecurityDozorSrv	Сервис, выполняющий действие	Используются значения: • mailfilter; • sender; • archive
SolarSecurityDozorVid	vID сообщения	
SolarSecurityDozorType	Тип сообщения	Используются значения: • email; • network; • http; • file; • exchange; • endpoint.
SolarSecurityDozorSrc	Источник	Количество выводимых адресов регулируется параметром **Максимальное количество адресов, выводимых при журналировании операций над сообщениями** (раздел GUI **Система > Конфигурация**

Параметр	Расшифровка параметра	Комментарий
		> Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений секция **Настройки сервиса фильтрации сообщений**)
SolarSecurityDozorDst	Назначение	Количество выводимых адресов регулируется параметром **Максимальное количество адресов, выводимых при журналировании операций над сообщениями** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений** секция **Настройки сервиса фильтрации сообщений**)
SolarSecurityDozorAct	Выполненное действие	• получено; • обрабатывается; • расшифровано; • зашифровано; • удалено; • отправлено <профиль>; • архивируется <профиль>; • отправлено с реконструкцией <профиль>; • архивируется с реконструкцией <профиль>; • заблокировано <правило>; • отправлено уведомление <шаблон>; • ошибка <содержимое ошибки> (если действие над сообщением завершилось с ошибкой); • инцидент: уровень серьезности инцидента, значение свойства **Влияние** инцидента, название сработавших правил и условия инцидента; • и другие действия.

Примечание

Если значение какого-либо параметра не определено, параметр не выводится.

Описание действий в журнале обработки сообщений приведено в Табл.В.2.

Табл. В.2. Действия журнала обработки сообщений

Код	Описание	Пояснение	Параметры, характерные для действия
101	**received**	Сообщение получено. Выводится в самом начале обработки сервисом **mailfilter**, здесь тип сообщения, источник и назначение еще не определены.	См. таблицу Табл.В.1.
102	**processing**	Сообщение принято в обработку. Выводится после разбора заголовков, определения типа сообщения, а также источника и назначения (для этого действия выводится отдельное сообщение для каждого адреса назначения).	• **SolarSecurityDozorDstCount** – количество уникальных адресов назначения (если адресов несколько, то они разделяются через запятую); • **SolarSecurityDozorSubject** – тема сообщения; • **SolarSecurityDozorCompdate** – дата написания сообщения в формате SMTP (например, например, Tue, 08 Apr 2014 17:51:28 +0400); • **SolarSecurityDozorSize** – размер сообщения; • параметры, специфичные для типа сообщения (например, для типа email это параметры **from**, **to** и **cc**, в которые записываются только адреса через запятую и без пробелов); • **SolarSecurityDozorXMailer** – информация о почтовом клиенте; • **SolarSecurityDozorMimeVersion** – версия MIME; • **SolarSecurityDozorMessageId** – идентификатор сообщения.
103	**unpacked**	Сообщение распаковано. Выводится информация о файлах, распакованных в процессе фильтрации	• **SolarSecurityDozorFilesCount** – количество вложенных файлов (если сообщение не содержит вложений, то система должна выводить нулевое значение [files-count:0]); • **SolarSecurityDozorFilesAttached** – имя вложенного файла
104	**unpacked attachment**	Вложение сообщения распаковано. Выводится информация о вложенных файлах, распакованных в процессе фильтрации.	• **SolarSecurityDozorFile** – имя вложенного файла; • **SolarSecurityDozorMd5** – md5-сумма вложенного файла; • **SolarSecurityDozorFileSize** – размер вложенного файла.
105	**processed**	Сообщение обработано. Выводится по окончании обработки сервисом **mailfilter**.	• **SolarSecurityDozorArc** – **Y** (отправлено в архив), **N** (обработано без архивации);

Код	Описание	Пояснение	Параметры, характерные для действия
			• **SolarSecurityDozorSent** – **Y** (отправлено по назначению), **N** (не отправлено); • **SolarSecurityDozorTime** – время обработки; • **SolarSecurityDozorStime** – время ожидания в спуле перед обработкой; • параметры, специфичные для типа сообщения; • **SolarSecurityDozorLabels** – пометки.
106	**deleted**	Сообщение удалено. Выводится после действия **обработано** в случае, если не было архивирования или отправки, т.е. **arc** = N и **sent** = N	• **SolarSecurityDozorSubject** – тема сообщения; • **SolarSecurityDozorSize** – размер сообщения; • **SolarSecurityDozorLabels** – пометки; • параметры, специфичные для типа сообщения.
108	**error**	Возникли ошибки обработки сообщения, сообщение помещено в спул ошибок. Выводится информация об ошибках обработки сообщения.	**SolarSecurityDozorError** – текст ошибки
109	**log**	Выводится информация о записи в журнальном файле.	**SolarSecurityDozorText** – текст записи
110	**archive**	Сообщение помещено в архив. Выводится информация об UUID профиля архивации.	• **SolarSecurityDozorStorageProfile** – UUID профиля архивации; • **SolarSecurityDozorLabels** – пометки.
	archive-with-reconstruction	Сообщение помещено в архив с реконструкцией. Выводится информация об UUID профиля архивации и шаблона реконструкции.	• **SolarSecurityDozorStorageProfile** – UUID профиля архивации; • **SolarSecurityDozorRecTemplate** – UUID шаблона реконструкции; • **SolarSecurityDozorLabels** – пометки.
	blocked	Сообщение заблокировано. Выводится информация о наборах условий и правил.	• **SolarSecurityDozorRuleSet** – имя набора правил на котором сработало действие блокировки; • **SolarSecurityDozorRule** – имя правила на котором сработало действие блокировки; • **SolarSecurityDozorConditionSet** – имя набора условий на котором сработало действие блокировки; • **SolarSecurityDozorLabels** – пометки.
	sent-notify	Сообщение отправлено с уведомлением. Выводится информация	• **SolarSecurityDozorRelayProfile** – UUID профиля отправки;

Код	Описание	Пояснение	Параметры, характерные для действия
		об UUID профиля отправки и шаблона уведомления.	• **SolarSecurityDozorTemplate** – UUID шаблона уведомления; • **SolarSecurityDozorLabels** – пометки.
	incident	Создано событие информационной безопасности.	• **SolarSecurityDozorSeverity** – критичность события ИБ; • **SolarSecurityDozorImpact** – импакт события ИБ; • **SolarSecurityDozorRuleSet** – имя набора правил на котором сработало действие блокировки; • **SolarSecurityDozorCondSet** – имя набора условий, на котором сработало действие блокировки; • **SolarSecurityDozorLabels** – пометки.
	relay	Сообщение отправлено. Выводится информация об UUID профиля отправки.	• **SolarSecurityDozorRelayProfile** – UUID профиля отправки; • **SolarSecurityDozorLabels** – пометки.
	relay-with-reconstruction	Сообщение отправлено с реконструкцией. Выводится информация об UUID профиля отправки и шаблона реконструкции.	• **SolarSecurityDozorRelayProfile** – UUID профиля отправки; • **SolarSecurityDozorRecTemplate** – UUID шаблона реконструкции; • **SolarSecurityDozorLabels** – пометки.

Описание действий, выполняемых сервисами **archiver** и **sender** приведено в таблице.

Табл. В.3. Действия сервисов archiver и sender

Сервис	Действие	Параметры, характерные для действия
archiver	**архивировано**	• **arc-id** – ИД сообщения в архиве; • **time** – время обработки; • **stime** – время ожидания в спуле перед обработкой.
sender	**отправлено**	• **smtp-rep** – ответ smtp-сервера в случае отправки по протоколу SMTP; • **time** – время обработки; • **stime** – время ожидания в спуле перед обработкой.

Формат вывода информации в журнал обработки сообщений имеет следующий вид:

[Дата-время события с сообщением] заголовок <Комплекс, Приоритет, PID> [srv:<значение>] [vid:<значение>] [type:<значение>] [src:<source>] [dst:<destination>] [act:<значение>] [параметры действия:<значения>]

Примеры записей в журнале **message-stat.log** (syslog):

1. Пример журнала обработки сообщения.

   - Сообщение передано системой в обработку, отслеживается по VID:

     # seelog message-stat.log content | grep e13748b6-d6ae-11e3-baa0-000c29c8e096

     ```
     [08.05.2014 16:47:23] support:info (20264) [srv:mailfilter]
     [vid:e13748b6-d6ae-11e3-baa0-000c29c8e096]
           [src:agent-server@domain.loc] [dst:x@local.net] [act:received]
     ```

   - Начата обработка сообщения:

     ```
     [08.05.2014 16:47:23] support:info (20264) [srv:mailfilter]
     [vid:e13748b6-d6ae-11e3-baa0-000c29c8e096] [type:endpoint/screenshot]
     [src:PC-ROZENKNOP\Администратор@pc-rozenknop.isim.local] [dst:screenshot] [act:processing]
      [dst-count:1] [subject:10.31.88.240 - Удаленный рабочий стол]
     [comp-date: Mon, 01 Sep 2014 17:51:28 +0400] [size:283998]
     [userid:S-1-5-21-951517777-2834940289-1444498753-500] [hostname:pc-rozenknop]
     [domain:isim.local] [datatype:screenshot]
     ```

   - Обработка закончена, доступен список установленных пометок и список основных действий, предпринятых системой:

     ```
     [08.05.2014 16:47:23] support:info (20264) [srv:mailfilter]
     [vid:e13748b6-d6ae-11e3-baa0-000c29c8e096] [type:endpoint/screenshot]
     [src:PC-ROZENKNOP\Администратор@pc-rozenknop.isim.local] [dst:screenshot] [act:processed]
      [subject:10.31.88.240 - Удаленный рабочий стол] [size:283998]
     [labels:"Получено":"";"Применен набор правил":"Архивировать все сообщения";"Удовлетворяет
      набору условий":"агент! (Архивировать все сообщения: Агентские условия 2)";
     "Помещено в архив":"Поместить в архив";"Удовлетворяет набору условий":"Все сообщения
      (Архивировать все сообщения: действие по умолчанию. 13)"] [arc:Y] [sent:N] [stime:9]
     [time:350] [userid:S-1-5-21-951517777-2834940289-1444498753-500] [hostname:pc-rozenknop]
      [domain:isim.local] [datatype:screenshot]
     ```

   - Сообщение успешно помещено в хранилище:

     ```
     [08.05.2014 16:47:27] support:info (22762) [srv:archiver]
     [vid:e13748b6-d6ae-11e3-baa0-000c29c8e096] [type:endpoint/screenshot]
     [src:PC-ROZENKNOP\Администратор@pc-rozenknop.isim.local] [dst:screenshot] [act:archived]

     [labels:"Получено":"";"Применен набор правил":"Архивировать все сообщения";"Удовлетворяет
      набору условий":"агент!
     (Архивировать все сообщения: Агентские условия 2)";"Помещено в архив":"Поместить в
     архив";"Удовлетворяет набору условий":"Все сообщения
     (Архивировать все сообщения: действие по умолчанию. 13)"] [arc-id:2.201405081643041248]
      [time:2] [stime:2]
     ```

2. Примеры действия распаковано:

```
[13.09.2014, 03:04:57] support:info (29211) [srv:mailfilter]
[vid:336d7854-3ad1-11e4-9b6b-005056990065]
[type:email] [src:spamer@dozor] [dst:admin@dozor] [act:unpacked] [files-count:0]
```

```
[26.06.2014 19:03:12] support:info (22898) [srv:mailfilter]
[vid:f200c662-fd42-11e3-a63b-deadd01b0eb0] [type:email] [src:pmi_test@isim.local]
[dst:pse@ss.ru;dv.klimov@isim.local] [act:unpacked] [file:attach_full.txt]
[md5:eccbde04eb47ad1b440d857c29871006]
[26.06.2014 19:03:12] support:info (22898) [srv:mailfilter]
[vid:f200c662-fd42-11e3-a63b-deadd01b0eb0] [type:email] [src:pmi_test@isim.local]
[dst:pse@ss.ru;dv.klimov@isim.local] [act:unpacked] [file:Ваше резюме показалось нам очень
интересным.txt] [md5:09adbb75c98506bdb9261522149976a0]
```

3. Пример действия инцидент:

```
[01.07.2015 14:55:56] support:info (3639) [srv:mailfilter] [vid:1fc8a272-1fe8-11e5-bf3f-005056921005]

[type:email] [src:kosh@isim.local,staff@isim.local] [dst:staff@isim.local] [act:incident]
[labels:"Получено":"";"Внешнее сообщение":"";"Применен набор правил":"Архивировать все
сообщения";
"Удовлетворяет набору условий":"текстовое условие (Архивировать все сообщения: проверка
 по ключевым словам)
-> \"Приказ N 14.0706\\t\\t\\t\\t\\t09 Июля 2014 \\n\\n...\"";"Зарегистрировано событие ИБ":"Категория:
 Намерения,
Уровень критичности: critical";"Удовлетворяет набору условий":"Все сообщения (Архивировать
 все сообщения:
Головное правило) -> #t";"Зарегистрировано событие ИБ":"Категория: Неправомерное
использование ресурсов,
Уровень критичности: info"]
[severity:critical] [impact:8] [rule-set:Архивировать все сообщения] [cond-set:текстовое условие]
```

Для включения записи событий в формате CEF необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений**.

2. В секции **Настройки сервиса фильтрации сообщений** установить флажок для параметра **Использовать формат CEF при журналирования операций над сообщениями?**.

3. Нажать кнопку **Сохранить** для применения настроек.

Поля событий заполняются в соответствии со словарем CEF (действия и соответствующие им параметры описаны выше). Подробнее о формате CEF см. соответствующую документацию.

Примеры записей журнала **message-stat.log** в формате CEF:

1. Пример журнала обработки сообщения (сообщение отслеживается по VID):

```
[16.02.2018 12:07:41] support:info (12945) CEF:0|Organisation|KEO DLP|6.6.0-685|101|
received|Medium|SolarSecurityDozorSrv=mailfilter
SolarSecurityDozorVid=d53dd9f0-12f8-11e8-b70c-344af418bbed
SolarSecurityDozorType= SolarSecurityDozorSrc= SolarSecurityDozorDst=
SolarSecurityDozorAct=received
```

2. Пример действия распаковано:

```
[16.02.2018 12:07:47] support:info (12945) CEF:0|Organisation|KEO DLP|6.6.0-685|103|
unpacked|Medium|SolarSecurityDozorSrv=mailfilter
SolarSecurityDozorVid=d53dd9f0-12f8-11e8-b70c-344af418bbed
SolarSecurityDozorType=email SolarSecurityDozorSrc=vm1@dsdomain.com
SolarSecurityDozorDst=SolarSecurityDozorDst=vm13@dsdomain.com
SolarSecurityDozorAct=unpacked SolarSecurityDozorFilesCount=1
SolarSecurityDozorFilesAttached=Unpack_result.xls
```

3. Пример действия инцидент:

```
[16.02.2018 12:21:13] support:info (12945) CEF:0|Organisation|KEO DLP|6.6.0-685|110|
action|Medium|SolarSecurityDozorRuleSet=основное правило SolarSecurityDozorImpact=4
SolarSecurityDozorSrc=vm1@dsdomain.com SolarSecurityDozorSrv=mailfilter
SolarSecurityDozorType=email
SolarSecurityDozorDst=vm2@dsdomain.com
SolarSecurityDozorVid=7bc0f500-12f9-11e8-b70c-344af418bbed
SolarSecurityDozorSeverity=high SolarSecurityDozorAct=incident
SolarSecurityDozorCondSet=Конфиденциальный текст
```

Приложение С. Требования к паролям учетных записей пользователей

При создании пароля необходимо соблюдать следующие правила:

1. Допустимая длина пароля по умолчанию – от шести до двенадцати символов.
2. Пароль может содержать символы из следующих наборов:
   - буквы раскладки основной латиницы верхнего регистра (latin1) – 26 символов;
   - буквы раскладки основной латиницы нижнего регистра (latin1) – 26 символов;
   - арабские цифры – 10 символов;
   - служебные символы: «~», «!», «@», «#», «$», «%», «^», «&». «*», «(», «)», «+», «-», «=», «`», «'», «_», «/», «\», «|», «"».

При создании пароля KEO DLP рассчитывает уровень его устойчивости (от 0 до 10). Уровень устойчивости пустого пароля равен 0. Расчёт уровня устойчивости пароля выполняется следующим образом:

1. Если длина пароля равна или больше минимальной, прибавляется 1.

   Например, в KEO DLP в настройках установлена минимальная (6 символов) и максимальная (10 символов) длина пароля. В случае если для пользователя задаётся пароль длиной 8 символов из одного набора (например, **ggggssss**), то устойчивость пароля равна 1.

2. Если длина пароля максимальная, прибавляется 2.

   Для указанного выше примера (в п.1) в случае задания для пользователя пароля длиной 10 символов из одного набора (например, **ggggssssff**) к уровню устойчивости пароля прибавляется 2. В итоге устойчивость пароля будет равна 3.

3. Если пароль содержит символы из двух наборов, прибавляется 1.

   Для указанного выше примера в случае задания для пользователя пароля, содержащего символы из двух наборов (например, **ggggssss44**), к уровню устойчивости пароля прибавляется 1. В итоге устойчивость пароля будет равна 4.

4. Если пароль содержит символы из трёх наборов, прибавляется 1.

   Для указанного выше примера в случае задания для пользователя пароля, содержащего символы из трех наборов (например, **gggg4444##**), к уровню устойчивости пароля прибавляется 1. В итоге устойчивость пароля будет равна 5.

5. Если пароль содержит символы из четырёх наборов, прибавляется 1.

   Для указанного выше примера в случае задания для пользователя пароля, содержащего символы из четырёх наборов (например, **ggSS4444##**), к уровню устойчивости пароля прибавляется 1. В итоге устойчивость пароля будет равна 6.

6. Если пароль не содержит более двух символов из одного набора подряд, прибавляется 1.

Для указанного выше примера в случае задания для пользователя пароля с чередованием символов из четырёх наборов через каждые 2 символа (например, **ggSS44##77**), к уровню устойчивости пароля прибавляется 1. В итоге устойчивость пароля будет равна 7.

7. Если пароль не содержит более одного символа из одного набора подряд, прибавляется 2.

   Для указанного выше примера в случае задания для пользователя пароля с чередованием символов из четырёх наборов через 1 символ (например, **gG7#7G#g7#**), к уровню устойчивости пароля прибавляется 2. В итоге устойчивость пароля будет равна 9.

8. Если количество разных символов больше минимальной длины пароля, прибавляется 1.

   Для указанного выше примера в случае задания для пользователя пароля с количеством разных символов, превышающим установленную минимальную длину пароля (6 символов), (например, **gS4#7N@f8$**), к уровню устойчивости пароля прибавляется 1. В итоге устойчивость пароля будет равна 10.

9. Если пароль выполняет условия пунктов 1, 5, 7, 8, прибавляется 1.

   Для указанного выше примера в случае задания для пользователя пароля с выполнением условий пунктов 1, 5, 7, 8 (например, **gS4#7N@f8$**), к уровню устойчивости пароля прибавляется 1. В итоге сумма условий больше 10.

   Если сумма условий больше 10, уровень устойчивости пароля считается равным 10.

По умолчанию в настройках KEO DLP указаны: минимальная длина пароля – 6, максимальная длина пароля – 12, минимальная допустимая устойчивость пароля – 6.

Таким образом, если уровень устойчивости создаваемого пароля меньше 6, KEO DLP не позволит создать такой пароль и на экран будет выдано соответствующее сообщение об ошибке.

Соблюдение указанных выше правил должно быть обеспечено организационными мерами.

При наличии соответствующих прав можно изменить настройки парольной политики по умолчанию. Для этого необходимо перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройки обеспечивающих средств > Безопасность** и отредактировать в секции **Правила аутентификации** значения следующих параметров:

- **Минимальная длина пароля** – минимальная длина пароля.
- **Максимальная длина пароля (2-12)** – максимальная длина пароля (2-12 символов).
- **Минимальная допустимая сложность пароля (2-10)** – минимальная допустимая устойчивость пароля (2-10 символов).
- **Двойное поле для ввода пароля** – двойное поле для ввода пароля. При включенном параметре в процессе авторизации администратора используется раздельный пароль, для ввода которого используется два поля ввода. По умолчанию флажок не установлен.

Приложение D. Инструкция по настройке входа в KEO DLP под учетными записями AD

D.1. Вход с использованием главного веб-сервера

Пользователи могут выполнить вход в KEO DLP с использованием главного веб-сервера под доменной учетной записью без ввода логина и пароля. Аутентификация таких пользователей выполняется через механизм Kerberos, для настройки которой следует выполнить действия:

1. Войти на контроллер домена и создать новую учетную запись пользователя в **Active Directory Users and Computers**. При создании необходимо снять флажок **User must change password at next logon** и выбрать:
   - **User cannot change password**;
   - **Password never expires**.
2. В свойствах объекта пользователя (вызывается щелчком правой кнопкой мыши) перейти на вкладку **Учетная запись**, в поле **Account options** установить флажки **This account supports Kerberos AES 128 bit encryption** и **This account supports Kerberos AES 256 bit encryption** и нажать кнопку **ОК**.
3. С помощью CLI на контроллере домена создать ключ, выполнив следующую команду:

   # ktpass -princ HTTP/dozor.fqdn@DOMAIN -mapuser <user> -pass Pa$$word \ -ptype KRB5_NT_PRINCIPAL -crypto AES256-SHA1 -out C:\Temp\dozor.keytab

   подменяя значения:
   - **dozor.fqdn** – полное доменное имя master-узла KEO DLP.

     Внимание!

     Использование IP-адреса в текущей команде не поддерживается.
   - **DOMAIN** – имя домена в верхнем регистре.
   - **<user>** – имя учетной записи, созданной на шаге 1. Имя указывается вместе с доменом (например – **n-petrov@organization.local**).
   - **Pa$$word** – пароль учетной записи, указанной в предыдущем параметре.

     В результате выполнения этой команды будет создан ключ аутентификации. Ключ будет находиться в месте, указанном после ключа **-out**, в данном примере – **C:\Temp\dozor.keytab**
4. Скопировать ключ и поместить его в каталог **/opt/dozor/etc** на master-узел KEO DLP.
5. Перейти по адресу **https://<dozor-master>**, где **<dozor-master>** – адрес master-узла KEO DLP (IP или FQDN).

6. Ввести в соответствующие поля логин и пароль администратора.

7. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройки обеспечивающих средств > Безопасность** и в секции **Правила аутентификации** задать для параметров значения:

   - **Доменная аутентификация через Kerberos** – установить флажок.
   - **Идентификатор службы Kerberos (SPN)** – имя участника службы для Kerberos-соединений в формате **HTTP/<dozor.fqdn>@<DOMAIN>**, где **<dozor.fqdn>** – FQDN master-узла KEO DLP, **<DOMAIN>** – имя домена.

8. Нажать кнопки **Сохранить** и **Применить**.

9. Перезапустить сервис **webserver**, выполнив следующую команду:

   # dsctl restart webserver

10. Настроить Kerberos-аутентификацию в браузерах.

Внимание!

*Следует учитывать, что по умолчанию Kerberos-аутентификация в браузере Firefox выключена. Для ее включения следует ввести в адресной строке **about:config** и в значении параметра **network.negotiate-auth.trusted-uris** указать полное доменное имя master-узла KEO DLP. При использовании браузера Google Chrome следует убедиться, что master-узел KEO DLP относится к внутренней сети (Local Intranet).*

Для организации доменного доступа пользователя в KEO DLP необходимо настроить соответствующий режим для такого пользователя (см. документ *Руководство пользователя*).

Для входа в GUI KEO DLP следует ввести в адресной строке браузера адрес **https://<доменное имя master-узла KEO DLP>**, и подтвердить исключение сертификата безопасности. Появится окно авторизации (см. **Рис.D.1**).

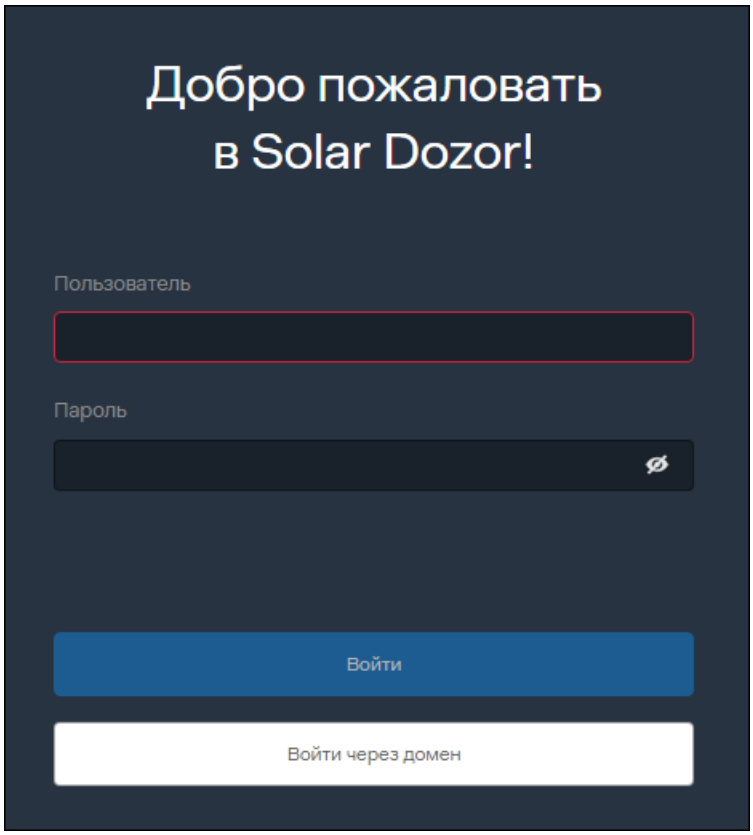


Рис. D.1. Окно авторизации при входе в систему

Внимание!

Вход в интерфейс KEO DLP по IP-адресу не поддерживается. Рекомендуется указывать полное доменное имя узла в формате FQDN.

В окне авторизации следует нажать кнопку **Войти через домен**. В случае корректной настройки Kerberos-аутентификации после входа в систему откроется **Рабочий стол**. Описание работы с разделом GUI **Рабочий стол** приведено в документе *Руководство пользователя* и разделе 5.1.

Если браузер использует NTLM-аутентификацию вместо Kerberos-аутентификации, появится дополнительное окно ввода пароля. В этом случае попытки входа в интерфейс KEO DLP завершатся с ошибкой **Доменная аутентификация не настроена. Обратитесь к администратору** (см. Рис.D.2).

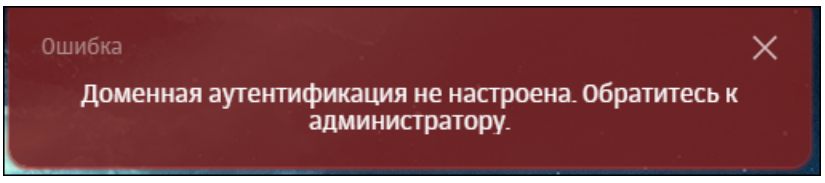


Рис. D.2. Ошибка доменной аутентификации

Приложение Е. Модуль разбора сообщений на составляющие

Е.1. Общие положения

Любая часть сообщения распаковывается в рамках рекурсивного процесса. Конкретная процедура распаковки подбирается в зависимости от типа содержимого (**content-type**) объекта. Тип объекта определяется с помощью специально разработанной библиотеки **file-ng**. Список объектов сообщения, распаковываемых KEO DLP, приведен в разделе **Объекты сообщения, распаковываемые KEO DLP** документа *Справочник пользователя*. Типы данных, распознаваемые KEO DLP, приведены в документе *Справочник пользователя*, раздел **Типы данных, которые распознает KEO DLP**.

В процессе распаковки может быть задействован сервис распаковки и конвертирования (извлечения) данных **smap-tikaserver**.

Программный модуль распаковки содержит:

- реализацию процедур-распаковщиков для каждого из известных типов объектов сообщения, а также реализацию процедур извлечения текста и служебной метаинформации из файлов известного типа.
- таблицы соответствия типа объекта сообщения процедуре-распаковщику, процедурам извлечения текста и метаинформации.

Процедура извлечения текста извлекает текстовую информацию из объектов соответствующих типов и помещает ее во временные файлы в кодировке UTF-8. Исходная кодировка текста распознается с помощью специально разработанной системы определения кодировок. Распознаются кодировки:

- русского языка: CP1251, EUK-KR, GB2312, IBM866, ISO-2022-JP, ISO-8859-5, KOI8-R, UTF-8, UTF-16, UTF-16BE, UTF-16le, UTF-32, UTF-32BE, UTF-32LE.
- арабского языка: ISO-8859-6, MacArabic, UTF-8, WINDOWS-1256, UTF-16, UTF-16BE, UTF-16le, UTF-32, UTF-32BE, UTF-32LE.

Процедура извлечения текста применяется для следующих объектов:

- текстовые части сообщений;
- файлы документов MS Office и OpenOffice;
- XML-файлы;
- файлы архивов (из них извлекается перечень содержимого и комментарий);
- файлы PDF;
- исполняемые файлы;
- изображения.

Полный список объектов сообщения, из которых KEO DLP извлекает текстовую информацию, приведен в разделе **Форматы файлов, из которых KEO DLP извлекает текст** документа *Справочник пользователя*.

Для извлечения текстовой информации из офисных документов используется сервис **smap-tikaserver**. **smap-tikaserver** позволяет извлечь текстовую информацию из офисных документов, а также получить составляющие офисного документа (OLE-объекты, изображения).

Процедура извлечения служебной метаинформации применяется для следующих объектов:

- текстовые части сообщений;
- файлы форматов аудио и видео;
- файлы документов MS Office и OpenOffice.

Для анализа документов, обрабатываемых в офисных приложениях, KEO DLP:

- определяет наличие исправлений, которые не были применены (при работе с документом в режиме правки);
- извлекает информацию из комментариев и связывает текст документа с комментариями (при работе в режиме правки);
- извлекает информацию об авторе комментариев и правок и определяет ее связь с метаданными документа.

Список свойств документов, которые KEO DLP извлекает в виде метаинформации, приведен в документе *Справочник пользователя*, раздел **Свойства документов, извлекаемых KEO DLP**.

Для извлечения метаинформации из медиа-форматов используется внешнее ПО exiftool. Извлеченные данные сохраняются в файлах, располагающихся во временном каталоге.

E.2. Работа с дополнительными методиками извлечения текстов

Параметр конфигурации **Использовать дополнительные методики извлечения текстов (use-detext)** включает программу **detext**, которая реализует различные методы извлечения закодированных данных из полученных в результате обработки текстов сообщений (поддерживает кодировки **uuencode**, **quoted-printable**, **base64**). Примером таких данных может служить архив, закодированный в последовательность ASCII символов (например в **base64**), вставленный прямо в текст сообщения, а не как вложение.

Внимание!

*Программа **detext** производит анализ всех текстов в полном объеме, использует дополнительные методики извлечения текстов и имеет довольно сложный алгоритм, создающий большую нагрузку на процессор и память. В совокупности это может негативно сказаться на скорости обработки потока сообщений. Использование программы полезно для анализа обычной почты с сообщениями небольшого размера. Поэтому рекомендуется отключать*

*параметр **Использовать дополнительные методики извлечения текстов (use-detext)** в следующих ситуациях:*

- *пересылка сообщений большого размера;*
- *обработка ASCII текстов регулярной структуры (например, журнальные файлы).*

Программа **detext** входит в состав KEO DLP и не требует дополнительной лицензии.

Включение/выключение параметра выполняется в секции **Сервис фильтрации сообщений** раздела GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений**. Для включения/отключения параметра необходимо установить/снять флажок **Использовать дополнительные методики извлечения текстов (use-detext)**. По умолчанию параметр выключен.

Для проверки работоспособности программы **detext** следует отправить сообщение, содержащее неоформленные (закодированные) данные, и проверить их обнаружение поиском по тексту.

E.3. Модуль распаковки файлов конструкторской документации в KEO DLP

В KEO DLP можно распаковать файлы конструкторской документации без загрузки и установки соответствующих приложений, например AutoCAD. Информация, извлеченная из таких файлов, необходима администраторам безопасности KEO DLP для дальнейшего анализа.

KEO DLP в соответствии с настройками, заданными в конфигурационном файле **/opt/dozor/etc/mailfilter.edn**, использует внешний сервис **Convert Service.exe** и выполняет извлечение текста из файлов конструкторской документации.

Примечание

*Служба **Convert Service.exe** не входит в комплект дистрибутива KEO DLP. Для получения файлов службы необходимо связаться с вендором KEO DLP.*

Типы файлов конструкторской документации, извлекаемые в KEO DLP, представлены в таблице ниже.

Табл. E.1. Типы файлов конструкторской документации

Тип файла	Тип данных	Описание
.dwg	application/x-dwg	Файл AutoCAD 2000/2001/2002/2013/2014/2015/2016
.dxf	application/x-dxf	Файл AutoCAD Drawing eXchange Format (var.2)

Для настройки распаковки файлов конструкторской документации в KEO DLP следует выполнить действия:

1. Установить на АРМ системного администратора KEO DLP службу **Convert Service.exe**. Для этого на АРМ запустить командную строку от имени администратора и выполнить команду
   InstallUtil.exe ConvertSvc.exe
   .

2. При необходимости отредактировать конфигурационный файл **CovertSvc.exe.config** и заменить значения, выделенные жирным:

```
<ArrayOfString xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <string>http://127.0.0.1:8080/</string>
        <string>http://127.0.0.1:80/</string>
</ArrayOfString>
```

3. Открыть пункт меню **Пуск > Панель управления > Все элементы панели управления > Администрирование > Службы** и запустить службу **Convert Service.exe**.

4. Подключиться к узлу KEO DLP с сервисом **mailfilter** по протоколу SSH.

5. Убедиться, что служба **Convert Service.exe** работает. Для этого отправить запрос, например:

   **curl -o <filename> -X PUT http://<Convert Service IP>:8080/GetText **
   -T <dwg_path> -H "Content-Type:<Data_Type>"

   где

   - **<filename>** – имя файла, содержащего текст из переданного файла. Например, если указать **resp.txt**, будет создан файл **resp.txt**.
   - **<Convert Service IP>** – IP-адрес узла с запущенной службой **Convert Service.exe**
   - **<dwg_path>** – путь к файлу конструкторской документации. Например: **/tmp/CAD_files/equip_pipe.dwg**.
   - **<Data_Type>** – тип данных вложенного файла, например: **application/x-dwg**.

   В случае успешного выполнения данного запроса от **Convert Service.exe** будет получен ответ вида:

```
%  Total   % Received % Xferd   Average  Speed  Time    Time     Time    Current
                          Dload   Upload  Total  Spent   Left   Speed
100 375K   0    377  100 375K    377     375K  0:00:01 --:--:-- 0:00:01 1095k
```

   В домашнем каталоге, из которого была выполнена команда, будет создан текстовый файл **<filename>**.

6. Скопировать файл **/opt/dozor/etc/template-mailfilter.edn** в **/opt/dozor/etc/mailfilter.edn**.

7. Открыть созданный файл **/opt/dozor/etc/mailfilter.edn**, скопированный на предыдущем шаге. Найти строку

```
:extra-mime-unpackers []
```

8. Отредактировать данный файл, указав необходимые параметры распаковщиков MIME-типов. Например:

```
:extra-mime-unpackers
    [[["application/x-dwg" "application/x-autocad" "application/x-dxf"]
  {:name "AutoCAD extractor"
   :method :put
   :url "http://<Convert Service IP>:8080/GetText"
   :result :text}]]
```

   где **<Convert Service IP>** – IP-адрес узла с запущенной службой **Convert Service.exe**, например **10.199.30.164**

   Сохранить и закрыть файл.

9. Запустить командную оболочку KEO DLP, выполнив следующую команду:

   # /opt/dozor/bin/shell

10. Перезапустить сервис **mailfilter**, выполнив команду:

    # dsctl restart mailfilter

    Убедиться, что сервис был перезапущен без ошибок.

Для проверки распаковки следует отправить через KEO DLP на соответствующий адрес несколько сообщений с вложенными файлами конструкторской документации. При успешной распаковке вывод журнала сервиса **mailfilter** будет иметь вид:

```
2019-02-12 11:50:10.723659500 debug (1423) <spool-mailfilter-worker-0>
{25da8dec-2ea3-11e9-a5e4-005056882710} Unpack with External service [AutoCAD extractor] unpacker
2019-02-12 11:50:10.724403500 debug (1423) <spool-mailfilter-worker-0>
{25da8dec-2ea3-11e9-a5e4-005056882710} External service request [ :put
http://10.199.30.164:8080/GetText ]:
/opt/dozor/smap/tmp/mailfilter-tmpdir/mf-25da8dec-2ea3-11e9-a5e4-005056882710-10323173189566717O7/Котел
 Эван 72 кВт.dwg
timeout: 60000 headers: {"Content-Type" "APPLICATION/X-DWG"}
2019-02-12 11:50:11.254152500 debug (1423) <spool-mailfilter-worker-0>
{25da8dec-2ea3-11e9-a5e4-005056882710} External service response success [ :put
http://10.199.30.164:8080/GetText ]: 200 OK
2019-02-12 11:50:11.257724500 debug (1423) <spool-mailfilter-worker-0>
{25da8dec-2ea3-11e9-a5e4-005056882710} External service [AutoCAD extractor] unpacked successfully
```

Далее следует войти в GUI KEO DLP, перейти в раздел **Поиск** и выполнить запрос на просмотр всех сообщений. Убедиться, что в архиве находятся сообщения с вложенными DWG/WDX-файлами. При открытии дополнительной информации о сообщении будет отображено окно с распознанным текстом, содержащимся в файле.

Приложение F. Аудит действий пользователей KEO DLP

Для регистрации событий, связанных с учётными записями пользователей KEO DLP, используется таблица **user_action** БД политики фильтрации. В ней хранятся следующие данные:

- идентификатор действия;
- дата и время выполнения действия;
- логин пользователя системы, выполнившего действие;
- результат выполнения действия пользователя системы. Возможные значения: **success**/**error**.

  Если действие выполнить не удалось, в журнале отобразятся сведения об ошибке (**error**), например:

  ```
  error:  Connections could not be acquired from the underlying database!
  ```

- действие, которое выполнил пользователь системы,
- дополнительное описание атрибутов.
- IP-адрес рабочей станции, с которой пользователь выполнил действие,
- назначенные пользователю роли.

Для просмотра информации в таблице **user_action** следует выполнить действия:

1. Подключиться по протоколу SSH к узлу, на котором функционирует БД политики фильтрации.
2. Подключиться к БД политики, выполнив команду:

   # psql -U dozor -h localhost -p 5434
3. Выполнить команду:

   select * from user_action;

Можно, например, отобразить:

- Все действия конкретного пользователя.

  Пример команды:

  select * from user_action where login = 'ie.kalinkin';
- Все действия, имеющие конкретный результат выполнения.

  Пример команды:

  select * from user_action where status = 'success';

Получить информацию о действиях пользователей системы также можно в разделе GUI **Пользователи > Контроль действий > Журнал** на вкладке **Действия** (см. документ *Руководство пользователя*).

В Табл.F.1 приведено подробное описание действий.

Табл. F.1. Описание действий

№	Вид действия	Название действия	Атрибут	Описание атрибута	Примеры записей в журнале
1.	Вход и выход из системы	Вход в систему	-	-	-
		Выход из системы	-	-	-
2.	Поиск информации в системе (к поиску относится как непосредственно поиск, так и просмотр любой информации, например, на **Рабочем столе**)	Поиск	name	Наименование поискового запроса	**name**: События и инциденты| 24 часа;
		Запуск поиска (для расширенного поиска и/или поиска по шаблонам)	obj	Объект поиска: events (события и инциденты)/ messages (сообщения/ нажатия клавиш)/ files (вложенные файлы)/ endpoints (участники переписки)/ chats (беседы)	**obj**: events;
		Просмотр результатов поиска	type	Тип поиска: quick (быстрый поиск)/ template (шаблоны поиска)/ extended (расширенный поиск)	**type**: quick;
3.	Управление информационными объектами	Создание информационного объекта	name	Наименование информационного объекта	**name**: Выписки;
		Изменение информационного объекта			
		Удаление информационного объекта			
4.	Работа с почтовыми сообщениями в системе	Просмотр почтового сообщения	vid	Уникальный идентификатор сообщения (vID)	**vid**: 235cb402-0000-0000-0000-000000203097;
			url	URL сообщения	**url**: https://dozor1#archive/message&id%7B%22card%b959;
			src	Адрес источника сообщения (возможно множество значений)	**src**: email:ta.polkanov@sevtrad.ru;
			subject	Тема сообщения	**subject**: Движение по карьерной лестнице;
			datatime	Дата и время сообщения	**datetime**: Март 15 2017 17:57:00;
			size	Размер сообщения (в байтах)	**size**: 1596;

№	Вид действия	Название действия	Атрибут	Описание атрибута	Примеры записей в журнале
		Удаление почтового сообщения	vid	Уникальный идентификатор сообщения (vID)	**vid**: 675vg312-0000-0000-0000-000000206787;
		Запуск удаления сообщений по запросу	name	Наименование поискового запроса	**name**: Сообщения | 1 час;
			object	Объект поиска	**obj**: messages;
			type	Тип поиска	**type**: quick;
		Отправка почтового сообщения из архива	vid	Уникальный идентификатор сообщения (vID)	**vid**: a51a39b2-25e5-11e8-b959-00505688370e;
			url	URL сообщения	**url**: https://dozor1#archive/messageId%7B%22cardId%b959;
			scr	Адрес источника сообщения (возможно множество значений)	**scr**: email:dozor@localhost;
			subject	Тема сообщения	**subject**: [fan][12.03.2018 13:00 - 12.03.2018 15:00][Все][Записей: 2];
			datatime	Дата и время сообщения	**datetime**: Март 12 2018 14:08:08;
			size	Размер сообщения (в байтах)	**size**: 1352
			recipient	Адрес получателя (возможно множество значений)	**recipient**: email:a.filimohin@isim.local;
5.	Управление учетными записями пользователей системы	Создание пользователя	login	Логин пользователя системы	**login**: lexey;
			name	Имя пользователя системы	**name**: Кравцев Иван Петрович;
		Изменение пользователя	login	Логин пользователя системы	**login**: lub_ta;
			name	Имя пользователя системы	**name**: Любушкина Татьяна Валерьевна;
		Удаление пользователя	login	Логин пользователя системы	**login**: admin;
			name	Имя пользователя системы	**name**: Администратор;
6.	Управление ролями пользователей системы	Создание роли пользователей	role	Роль пользователей (при выполнении действия "Импорт ролей" возможно множество значений)	**role**: Администраторы;
		Изменение роли пользователей			
		Удаление роли пользователей			
		Импорт ролей			
7.	Настройка набора правил политики	Создание набора правил политики	name	Наименование набора правил политики	**name**: Внутренняя передача;
		Изменение набора правил политики			
		Удаление набора правил политики			

№	Вид действия	Название действия	Атрибут	Описание атрибута	Примеры записей в журнале
8.	Настройка набора условий политики	Создание набора условий политики	name	Наименование набора условий политики	**name**: Временная передача;
		Изменение набора условий политики			
		Удаление набора условий политики			
9.	Управление инструментами политики	Создание инструмента политики	name	Наименование инструмента политики	**name**: template_note_for_admin;
			type	Тип инструмента политики	**type**: rec-template;
		Изменение инструмента политики	name	Наименование инструмента политики	**name**: Правило из досье;
			type	Тип инструмента политики	**type**: monitored-group-rule;
		Удаление инструмента политики	name	Наименование инструмента политики	**name**: Поиск работы;
			type	Тип инструмента политики	**type**: ban-text;
10.	Управление шаблонами и профилями	Создание шаблона/профиля	name	Наименование шаблона/профиля	**name**: icap-шаблон;
			type	Тип шаблона/профиля	**type**: icap-block-template;
		Изменение шаблона/профиля	name	Наименование шаблона/профиля	**name**: Шаблон уведомления;
			type	Тип шаблона/профиля	**type**: mail-template;
		Удаление шаблона/профиля	name	Наименование шаблона/профиля	**name**: Шаблон каталога;
			type	Тип шаблона/профиля	**type**: directory-template;
11.	Применение политики	Применение политики	-	-	-
12.	Импорт политики в систему	Импорт политики	name	Наименование импортируемого файла	**name**: Временная передача;
13.	Управление справочниками	Создание элемента справочника	name	Наименование элемента справочника	**name**: Запретная переписка;
			type	Тип элемента справочника	**type** : label-types;
		Изменение элемента справочника	name	Наименование элемента справочника	**name**: Авария-отказ;
			type	Тип элемента справочника	**type** : event-category;
		Удаление элемента справочника	name	Наименование элемента справочника	**name**: Приложения;

№	Вид действия	Название действия	Атрибут	Описание атрибута	Примеры записей в журнале
			type	Тип элемента справочника	**type** : apps;
14	Изменение конфигурации системы	Изменение конфигурации системы	type	Название сервиса, в который внесено изменение	**type** : incident-daemon;

По умолчанию записи в журнале действий хранятся в системе 1 год с момента их появления. При необходимости срок можно изменить, указав требуемое значение параметра **Срок хранения журналов действий** в секции **Параметры сервера веб-интерфейса** раздела GUI **Система > Конфигурация > Расширенные настройки > Администрирование > Интерфейс**.

Приложение G. Схемы преобразования данных из внешних систем

G.1. Назначение

Внешние системы отправляют информацию в KEO DLP по протоколам ICAP и HTTP. Чтобы полученные данные корректно обрабатывались, необходимо привести их к формату, применяемому в KEO DLP. Это делается с помощью указания соответствия заголовков внешних источника трафика и заголовков KEO DLP в специальных схемах преобразования. С их помощью можно:

- определить тип сообщения и канал связи;
- получить адреса отправителя и получателя;
- установить дату перехвата сообщения;
- сформировать тему сообщения.

G.2. Порядок применения

Схемы преобразования настраиваются в разделе GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений > Схемы преобразования**. В каждой схеме описывается опорный заголовок и правила преобразования. Полученное KEO DLP сообщение сравнивается с опорными заголовками схем преобразования, начиная с первой схемы. Если ни одного совпадения не найдено, используется базовая (поставляемая с KEO DLP) схема преобразования.

G.3. Опорный заголовок

Чтобы система понимала, каким образом представить передаваемую информацию, необходимо указать схему преобразования сообщения в опорном заголовке, представляющем собой поле **X-Dozor-Mapping-Schema**. Значения заголовка, по умолчанию указанные в разделе GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений > Схемы преобразования**:

- **dozor-email** – для передаваемых почтовых сообщений;
- **dozor-im** – для передаваемых с помощью мессенджеров сообщений и файлов;
- **dozor-file** – для передаваемых файлов;
- **dozor-message** – для передаваемых сообщений, которые не укладываются в категории **dozor-email**, **dozor-im** и **dozor-file**;
- **TrueConf** – для сообщений, передаваемых через ПО для видеоконференцсвязи (ВКС) TrueConf Server;
- **Express** – для сообщений, передаваемых через корпоративный мессенджер Express;
- **dag-message** – для сообщений, передаваемых через DAG.

Опорный заголовок также может иметь индивидуальное значение, если используется специальная схема преобразования, созданная пользователем для решения конкретных задач.

В зависимости от выбранной схемы преобразования KEO DLP будет искать необходимую информацию об отправителе, получателях, типе, дате создания и теме сообщения.

G.4. Правило преобразования

G.4.1. Общие сведения

Каждое правило состоит из следующих частей:

- **Поле сообщения** – элемент, необходимый для заполнения (например, **Отправитель почтового сообщения**);
- **Правило преобразования** – выражение, преобразующее исходный заголовок сообщения в требуемый формат.

Примечание

Правила выполняются последовательно. Если поле допускает несколько значений (например, адреса), новые данные добавляются к существующим. При ошибке преобразования используется предыдущее значение. Пустые значения игнорируются.

В качестве примера представлено сообщение:

X-Dozor-Source: admin/ivanov

X-Dozor-Subject: Сообщение от Иванова

Subject: Message from Ivanov

From: i.ivanov@example.com

К нему применены в схеме преобразования следующие правила:

Адрес источника – :header "From" :as-email

Адрес источника – :header "X-Dozor-Source" :as-im

Тема сообщения – :header "Subject"

Тема сообщения – :header "X-Dozor-Subject"

*В результате источник сообщения будет содержать адреса **i.ivanov@example.com** и **admin/ivanov**, а тема сообщения примет вид **Сообщение от Иванова**.*

G.4.2. Поля сообщения

В конфигурации схем преобразования представлен выбор следующих полей сообщения:

- **Дата получения сообщения** – дата, фиксируемая модулем перехвата в момент, когда сообщение передаётся в KEO DLP;
- **Дата создания сообщения** – дата, фиксируемая при создании сообщения;

- **Заголовки сообщения** – список полей сообщения;
- **Имя передаваемого файла** – имя файла первой части сообщения;
- **Источник сообщения** – адреса отправителей;
- **Канал коммуникации** – тип коммуникации;
- **Назначение сообщения** – адреса получателей;
- **Отправитель почтового сообщения** – адреса отправителей почты;
- **Получатель почтового сообщения** – адреса получателей почты;
- **Тема сообщения** – тема сообщения;
- **Тип сообщения** – тип сообщения, определяемый KEO DLP.

Примечание

Важные рекомендации по заполнению полей:

- *Для полей с адресами необходимо использовать параметры **:as-list**, **:as-list-split**.*
- *Преобразования следует завершать приведением к нужному типу (параметры **:as-email**, **:as-ip**).*
- *Для дат необходимо использовать формат **:as-date** и параметр **:or-now**.*
- *Для корректной работы системы следует использовать только стандартные названия каналов и типов.*

Сведения о каналах коммуникации и типах сообщений, которые перехватываются по конкретному каналу приведены в документах «Программный комплекс «KEO DLP». Руководство пользователя» и «Программный комплекс «KEO DLP». Справочник пользователя».

G.4.3. Синтаксис правил преобразования

G.4.3.1. Ключевые слова

Ключевые слова начинаются с символа **":"** .

Примеры:

:const

:as-list

G.4.3.2. Строки

Строки заключаются в двойные кавычки. Текст в строках должен быть в кодировке UTF-8. Как правило, перед строкой следует ключевое слово.

Примеры:

"X-Dozor-Header"

"Пример строки"

G.4.3.3. Регулярные выражения

Регулярные выражения начинаются с символа "**#**" и заключаются в кавычки.

Примеры:

#".*"

#"admin/(\w+)"

G.4.3.4. Группировка

С помощью группировки можно объединить несколько команд вместе, чтобы они выполнялись как единое целое. Для этого используются квадратные скобки.

Примеры:

:make-string "Агент: " [:header "X-Dozor-Vid"]

:if-header-match #"X-Dozor-.*" [:make-string "Сообщение от Дозора"] [:make-string "Внешнее сообщение"]

G.4.3.5. Постоянное значение

Указывается постоянное значение.

Примеры:

Тема сообщения - :const "Важное сообщение"

Канал-коммуникации - :const "im"

G.4.3.6. Получение значения по имени заголовка

Указывается выражение вида **:header "{ИМЯ ЗАГОЛОВКА}"**

Примеры:

Тема сообщения - :header "X-Dozor-Subject"

Тип сообщения - :header "X-Message-Type"

G.4.3.7. Извлечение отдельной части

Указывается выражение вида **:extract #"{РЕГУЛЯРНОЕ ВЫРАЖЕНИЕ}"**

Примеры:

Тема сообщения - :header "Subject" :extract #"из системы\s(.+)."

Адрес источника - :header "From" :extract #"domain\\(\w+)"

G.4.3.8. Работа со списками

Указываются выражения вида:

:as-list – разбивает по запятой или точке с запятой,

:as-list-split – разбивает по указанному разделителю.

Пример:

:header "To" :as-list :as-im

G.4.3.9. Приведение адреса к типу

Чтобы строка адресной информации корректно обрабатывалась, ее необходимо привести к одному из типов адресов. Если значение не соответствует ни одному из допустимых форматов, правило проверки не сработает, и адрес не пройдет проверку. Поэтому каждое правило обработки адресов должно заканчиваться специальным ключевым словом, которое указывает, какой именно формат адреса ожидается получить в результате:

- **:as-login** – преобразование в логин;
- **:as-sid** – преобразование в SID;
- **:as-email** – преобразование в адрес электронной почты;
- **:as-ip** – преобразование в IP-адрес;
- **:as-hostname** – преобразование в **hostname**;
- **:as-im** – преобразование в логин мессенджера;
- **:as-url** – преобразование в URL.

G.4.3.10. Добавление заголовков

Выражение вида **:as-header** добавляет поле в заголовок сообщения, используя результат предыдущего преобразования. Это полезно, когда KEO DLP ожидает определённые поля заголовка, которых нет в сообщении. Оригинальное сообщение не изменяется, только его представление в KEO DLP.

Пример:

:header "X-Dozor-Chat-Id" :as-header "X-Agent-Chat-Id"

В этом примере значение поля заголовка **X-Dozor-Chat-Id** будет перенесено в новый заголовок **X-Agent-Chat-Id**.

G.4.3.11. Работа с датами

В системе есть следующие поля для работы с датами: **Дата получения сообщения** и **Дата создания сообщения**. Их назначение описано в разделе G.4.2.

Необходимо учитывать следующие особенности:

- Форматы дат должны соответствовать стандартам ISO 8601, RFC 5322 или RFC 3339;
- Используются ключевые слова:
  - **:as-date** – преобразует строку в формат даты системы;

- **:or-now** – если дата не найдена, используется текущая дата.

Пример:

:header "X-Dozor-Receive-Date" :or-now :as-date

G.4.3.12. Формирование строк

Указывается выражение вида **:make-string**, объединяющее несколько строк и значений.

Пример:

:make-string "Агент: " [:header "X-Dozor-Agent-Id"] ", передает сообщение " [:header "X-Dozor-Message-Id"]

G.4.3.13. Условные конструкции

Указываются выражения вида:

- **:if-header-exists** – проверяет существование заголовка;
- **:if-header-matches** – проверяет соответствие регулярному выражению;
- **:if-header-value-matches** – проверяет значение заголовка по регулярному выражению.

Примеры:

:if-header-value-exists "x-agent-protocol" [:const "Сообщение от агента"] [:const "Сообщение от внешнего источника"]

:if-header-value-matches "x-agent-protocol" #"file|email" [:const "Передаем файл или письмо"]

G.4.4. Пример правила

Ниже приведены правила преобразования для сообщения типа **dozor-message** (см. раздел G.3):

```
Источник сообщения – :header "x-dozor-src-login" :as-login;
Источник сообщения - :header "x-dozor-src-domain-login" :as-login
Источник сообщения - :header "x-dozor-src-im" :as-im
Источник сообщения - :header "x-dozor-src-email" :as-email
Источник сообщения - :header "x-dozor-src-sid" :as-sid
Источник сообщения - :header "x-dozor-src-hostname" :as-hostname
Источник сообщения - :header "x-dozor-src-ip" :as-ip
Назначение сообщения - :header "x-dozor-dst-login" :as-list :as-login
Назначение сообщения - :header "x-dozor-dst-domain-login" :as-list :as-login
Назначение сообщения - :header "x-dozor-dst-im" :as-list :as-im
Назначение сообщения - :header "x-dozor-dst-email" :as-list :as-email
Назначение сообщения - :header "x-dozor-dst-sid" :as-list :as-sid
Назначение сообщения - :header "x-dozor-dst-hostname" :as-list :as-hostname
Назначение сообщения - :header "x-dozor-dst-ip" :as-list :as-ip
Заголовки сообщения - :header "x-dozor-application" :as-header "x-agent-application-name"
Заголовки сообщения - :header "x-dozor-process" :as-header "x-agent-application-name"
Заголовки сообщения - :header "x-dozor-chat-id" :as-header "x-agent-chat-id"
Тема сообщения - :header "x-dozor-subject"
Тема сообщения - :header "subject"
```

```
Имя файла - :header "x-dozor-filename"
Имя файла - :header "filename"
Дата создания сообщения - :header "x-dozor-created-date" :as-date
Дата получения сообщения - :header "x-dozor-received-date" :or-now :as-date
Дата получения сообщения - :header "date" :or-now :as-date
Тип сообщения - :header "x-dozor-message-type"
Канал коммуникации - :header "x-dozor-comm-channel"
```

Процесс обработки сообщения указанной схемой включает в себя следующие этапы:

1. Извлечение всех возможных типов адресов из полей заголовка **X-Dozor-Src-*** и **X-Dozor-Dst-***.
2. Определение приложения или процесса, связанного с сообщением, на основе значений полей **X-Dozor-Application** или **X-Dozor-Process**.
3. Добавление поля заголовка **X-Agent-Application-Name** для связи со справочником приложений.
4. Добавление поля заголовка **X-Agent-Chat-Id** для построения бесед на основе значения поля **X-Dozor-Chat-Id**.
5. Выбор темы сообщения из полей заголовка **X-Dozor-Subject** или **Subject**.
6. Выбор имени файла первой части из полей заголовка **X-Dozor-Filename** или **Filename**.
7. Определение даты создания сообщения на основе поля заголовка **X-Dozor-Created-Date**.
8. Определение даты получения сообщения на основе полей **X-Dozor-Received-Date** или **Date**.
9. Присвоение типа сообщения на основе поля заголовка **X-Dozor-Message-Type**.
10. Присвоение канала коммуникаций на основе поля **X-Dozor-Comm-Channel**.

Лист контроля версий

03/09/2025-15:37