

INFOWATCH

InfoWatch Traffic Monitor

Руководство администратора

29/10/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Введение 6
1.1 Аудитория 6
1.2 Комплект документов 6
1.3 Техническая поддержка пользователей 6
2 Обзор Traffic Monitor 7
2.1 Функции InfoWatch Traffic Monitor 7
2.1.1 Схема перехвата SMTP-трафика 7
2.2 Состав InfoWatch Traffic Monitor (Astra Linux) 9
2.3 Лицензирование 11
3 Типы установки Системы 15
4 Настройка Системы после установки 16
4.1 Изменение предустановленного пароля 16
4.2 Настройка защиты от подбора паролей 18
4.3 Предварительные настройки 19
4.3.1 Настройка синхронизации времени 19
4.3.2 Конфигурирование работы Sphinx при распределенной установке 19
4.4 Общие настройки 20
4.4.1 Перехват трафика, передаваемого по протоколу ICAP 20
Настройка ICAP 21
Рекомендации по настройке SQUID 22
Рекомендации по настройке UserGate 27
Отключение ICAP 31
4.5 Настройка перехвата трафика 31
4.5.1 Настройка перехвата SMTP-трафика 32
Прием копий с почтового сервера 32
Блокировка "в разрыв" 33
Настройки почтовых серверов для перехвата SMTP-трафика 43
4.5.2 Прием объектов, перехваченных InfoWatch Device Monitor 51
4.6 Автозапуск процессов 51
4.6.1 Проверка автозапуска процессов 51
4.6.2 Включение и выключение автозапуска процессов 54
4.7 Модуль взаимодействия с удаленной базой данных 57
4.7.1 Настройка сбора данных в филиальной сети 57

4.7.2 Настройка клиентской части модуля взаимодействия с удаленной БД ... 57
4.7.3 Настройка серверной части модуля взаимодействия с удаленной БД ... 59
4.8 Настройка OCR-экстракторов ... 59
4.8.1 Поддерживаемые OCR-экстракторы ... 60
Настройки Tesseract ... 61
Настройки Content AI ContentReader Engine ... 62
4.9 Настройка отправки уведомлений пользователям и сотрудникам ... 64
4.10 Ограничение количества найденных событий ... 64
4.11 Настройка межсервисного взаимодействия (служба Consul) ... 64
4.11.1 Запуск и остановка службы ... 65
4.11.2 Регистрация сервисов в Consul ... 65
4.11.3 Распределенная установка ... 67
4.11.4 Настройка сетевых правил доступа в Consul ... 69
4.11.5 Конфигурационный файл consul.json и unit-файл iwtm-consul.service ... 69
4.12 Рекомендации по настройке безопасного окружения ... 72
4.12.1 Порты компонентов ... 73
4.13 Настройка управления вердиктом ... 78
5 Настройки автоматического удаления событий Data Discovery ... 80
6 Мониторинг ... 81
6.1 Настройки подсистемы мониторинга ... 81
6.1.1 Настройка подключения Device Monitor ... 81
6.1.2 Ручная настройка индикаторов ... 82
6.1.3 Настройка адреса сервера синхронизации времени для подсистемы мониторинга ... 82
7 Автоматическая проверка допустимого получателя с помощью выгрузки из базы данных ... 83
8 Администрирование базы данных ... 85
8.1 PostgreSQL ... 85
8.1.1 Табличные пространства в базе данных InfoWatch Traffic Monitor ... 85
Общая информация ... 85
Хранение ... 88
Архивирование ... 88
Удаление ... 88
8.1.2 Управление ежедневными табличными пространствами ... 88
Настройка размещения файлов в файловой системе ... 88
Настройка режимов хранения файлов табличного пространства ... 90
Архивирование ежедневных табличных пространств ... 93
Восстановление ежедневных табличных пространств ... 97

Удаление ежедневных табличных пространств ... 98
Управление ежедневными табличными пространствами с помощью консольной утилиты ... 101
8.1.3 Статистика загруженности ежедневных табличных пространств ... 103
Сценарии работы скрипта ... 104
8.1.4 Резервное копирование базы данных ... 108
Создание резервной копии базы данных ... 108
Восстановление базы данных из резервной копии ... 115
8.1.5 Проведение регламентных работ на сервере базы данных ... 119
8.1.6 Логирование базы данных ... 120
Ротация логов базы данных ... 120
8.2 Восстановление Data Storage ... 120
8.2.1 Получение токена для работы с сервисом Data Storage ... 121
8.2.2 Создание задачи восстановления корзины ... 121
8.2.3 Проверка успешного завершения задачи ... 122
9 Администрирование серверной части InfoWatch Traffic Monitor ... 123
9.1 Процессы серверной части Traffic Monitor ... 123
9.1.1 Список процессов серверной части Traffic Monitor ... 123
9.1.2 Настройка конфигурационных файлов серверной части Traffic Monitor ... 131
9.1.3 Работа с процессами серверной части Traffic Monitor ... 132
9.1.4 Шифрование SSL Thrift ... 134
Подготовка ключа и сертификатов ... 135
Настройки конфигурационных файлов ... 136
9.2 Настройка использования OCR ... 138
9.2.1 Включение использования технологии OCR при внедрении ... 139
9.2.2 Настройка OCR для нескольких нод ... 139
9.2.3 Конфигурационный файл ocr_custom.xml ... 139
9.3 Настройка параметров обработки архивов вложений ... 141
9.3.1 Конфигурационный файл extractors.xml ... 142
9.3.2 Конфигурационный файл extractors_customization.xml ... 146
9.4 Настройка параметров поиска с использованием групповых символов ... 148
9.5 Настройка интеграции с Data Analysis Service ... 149
9.6 Настройка соединения с Data Storage ... 152
9.7 Настройка отправки событий в Платформу ... 154
9.7.1 Переключение способа отправки событий ... 155
9.7.2 Настройка отправки событий в реальном времени ... 156
9.7.3 Настройка отправки событий по расписанию ... 156
9.8 Логирование работы Системы ... 157
9.9 Файловые очереди ... 158
9.10 Восстановление работоспособности системы в аварийных ситуациях ... 161

9.11 Управление языками с поддержкой морфологии ... 162
9.11.1 Добавление нового языка для поиска событий. Морфология и добавление терминов. ... 162
9.11.2 Обновление установленного языка ... 163
9.11.3 Удаление языка для поиска и терминов ... 164
9.12 Настройка передачи информации в SIEM ... 164
9.12.1 Настройки на стороне SIEM ... 165
Табличное представление событий TM ... 165
Табличное представление аудита пользователей ... 174
9.12.2 Настройки на стороне TM ... 180
Управление пользователем siem ... 180
Передача логов в SIEM ... 182
Управление логированием сессий пользователей БД TM ... 183
9.12.3 Типы логов, передаваемых в SIEM ... 183
9.13 Удаление временных файлов ... 184
10 Работа в Traffic Monitor в веб-интерфейсе Центра администрирования (Платформа) ... 185
11 Настройка сквозной аутентификации между продуктами InfoWatch 187
12 Взаимодействие с внешними системами ... 189
13 Приложение A. Рекомендации по составлению имен и паролей ... 190
14 Приложение B. Индикаторы мониторинга ... 191

1 Введение

В настоящем руководстве содержатся сведения по администрированию InfoWatch Traffic Monitor: настройке системы после установки, восстановлению после сбоев, проведению регламентных работ.

1.1 Аудитория

Документ предназначен для администраторов InfoWatch Traffic Monitor Server, знакомых с основами работы в среде операционных систем Microsoft Windows и Linux, а также обладающих навыками администрирования СУБД Oracle и Postgre SQL.

1.2 Комплект документов

В комплект документации по InfoWatch Traffic Monitor входят:

- «*InfoWatch Traffic Monitor. Руководство по установке*»

Содержит описание порядка установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.

- «*InfoWatch Traffic Monitor. Руководство администратора*».

Содержит информацию по администрированию Системы (база данных, серверная часть).

- «*InfoWatch Traffic Monitor. Руководство пользователя*».

Содержит описание порядка работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, составление политик для обработки объектов).

- «*InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*».

Содержит пояснения к часто используемым конфигурационным файлам.

Кроме основных руководств для пользователей и администраторов Системы предусмотрена База знаний lk.infowatch.ru, которая включает материалы по устранению неисправностей и ответы на вопросы. В случае отсутствия доступа к Базе знаний, просьба обращаться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

1.3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера.
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support

2 Обзор Traffic Monitor

В этой главе:

- Функции InfoWatch Traffic Monitor;
- Состав InfoWatch Traffic Monitor;
- Лицензирование.

2.1 Функции InfoWatch Traffic Monitor

InfoWatch Traffic Monitor позволяет контролировать информационные потоки в корпоративной среде для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.

Основные функции InfoWatch Traffic Monitor:

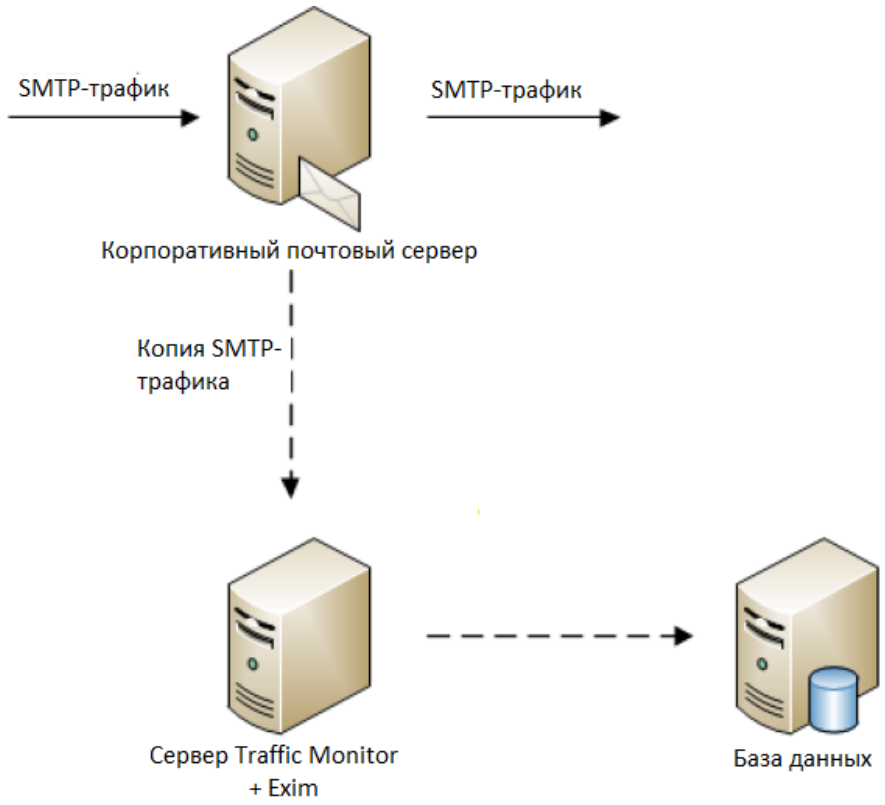
- *перехват в потоке/на шлюзе трафика, передаваемого по протоколу SMTP, с учетом мандатных меток*;
- перехват трафика на рабочих станциях агентами Device Monitor (подробнее см. *InfoWatch Device Monitor. Руководство пользователя)*.

- анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности;
- фильтрация перехваченного трафика путем выдачи разрешения/запрещения на доставку определенных данных.

2.1.1 Схема перехвата SMTP-трафика

Способ №1

На корпоративном почтовом сервере нужно настроить правило, отправляющее скрытую копию (BCC) для каждого отправленного письма. Копия должна отравляться на несуществующий почтовый адрес почтового домена, IP-адрес которого соответствует серверу Traffic Monitor. Данная функция поддерживается большинством почтовых серверов.



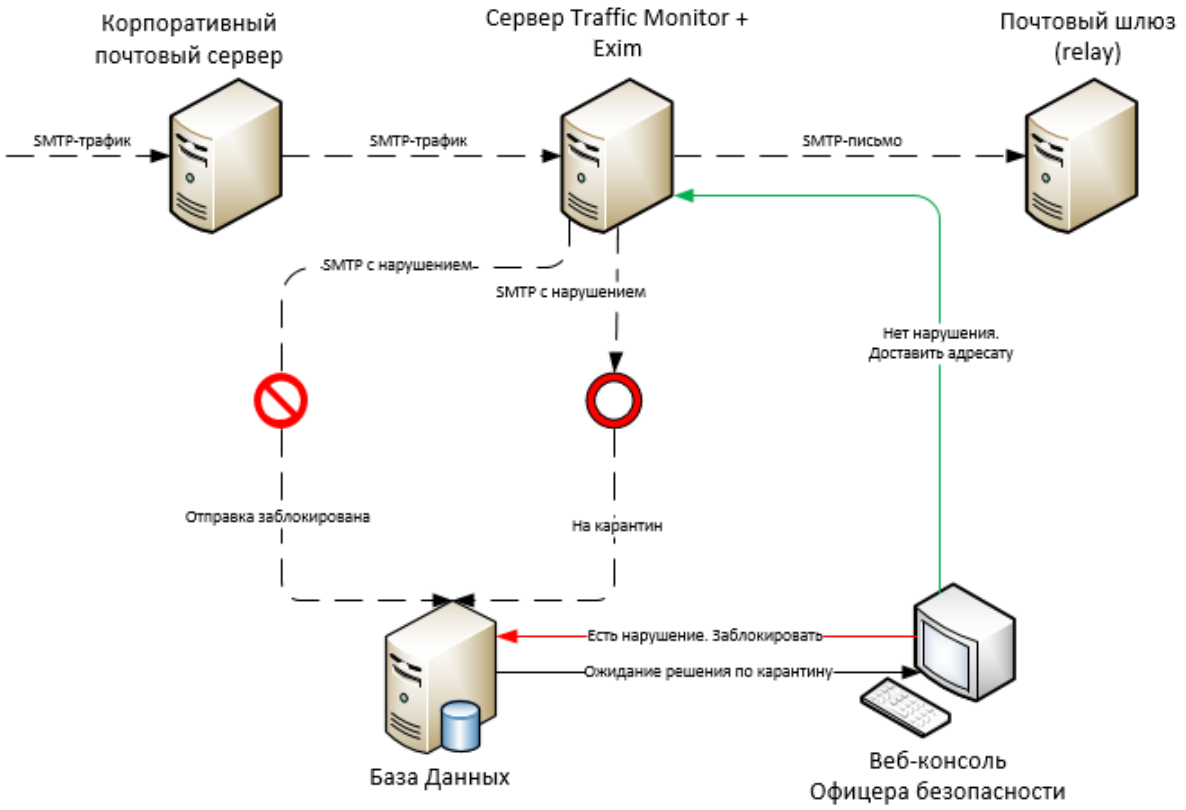
О настройке данного функционала см. *Прием копий с почтового сервера*.
Преимущества:

- позволяет анализировать не только внешнюю, но и внутреннюю переписку компании;
- гарантирует анализ всех писем.

Недостатки:

- требует внесения изменений в настройки корпоративного почтового сервера;
- никак не контролируются внешние почтовые серверы (если их использование разрешено);
- при недоступности сервера Traffic Monitor пользователи получат сообщение об ошибке доставки скрытой копии;
- дополнительная нагрузка на почтовый сервер.

Способ №2
Сервер Traffic Monitor, использующий настроенный почтовый сервер Postfix, выполняет функцию SMTP-ретранслятора и работает в режиме "Блокировка".



О настройке данного функционала см. *Блокировка "в разрыв"*.
Преимущества:

- позволяет включить функционал блокировки почтового трафика.

Недостатки:

- требует внесения изменений в настройки корпоративного почтового сервера;
- никак не контролируются внешние почтовые серверы (если их использование разрешено);
- в случае недоступности сервера Traffic Monitor пользователи не смогут отправлять письма, если не предусмотрено резервирование сервиса (например, через MX-записи).

2.2 Состав InfoWatch Traffic Monitor (Astra Linux)

Подсистема InfoWatch Traffic Monitor	Назначение подсистемы
Подсистема перехвата трафика	Перехват и передача на обработку трафика: объектов или их копий. Состоит из модулей: • Модуль ICAP; • Модуль Device Monitor; • Модуль перехвата почты (SMTP).

Подсистема InfoWatch Traffic Monitor	Назначение подсистемы
Подсистема обработки	Извлечение из перехваченных объектов значимой информации и вложений, определение форматов вложений и передача извлеченных текстов в подсистему анализа. **Примечание:** при создании объекта составляется его XML-контекст – текстовый файл, включающий содержимое объекта и информацию о нем.
Подсистема анализа	Анализ текстовых данных, извлеченных из перехваченных объектов (текстов писем, сообщений, запросов, а также текстов, извлеченных из вложений). Состоит из технологий: • Категории и термины; • Текстовые объекты; • Эталонные документы; • Векторные изображения; • Бланки; • Печати; • Выгрузки из БД; • Графические объекты; • Автолингвист.
Подсистема применения политик	На основе результатов работы подсистемы анализа и подсистемы обработки выносит вердикт о факте нарушения или не нарушения перехваченным объектом политики информационной безопасности. Также обеспечивает привязку данных о получателе или отправителе объекта к записям справочника сотрудников и рабочих станций. Состоит из следующих модулей: Модуль интеграции с Astra Linux Directory, Модуль принятия решений.
Подсистема хранения	Хранение информации о перехваченных объектах, результатах их анализа и применения политик, а также предоставление возможности для просмотра хранящейся информации посредством запросов из консоли управления. Представляет собой базу данных. Состоит из следующих модулей: Модуль взаимодействия с удаленной БД, Модуль загрузки объектов в БД, Модуль хранения настроек системы, Модуль хранения объектов. **Примечание:** перед сохранением объектов в БД они преобразуются из одного внутреннего формата (XML) в другой внутренний формат.
Подсистема мониторинга	Возможность удаленного мониторинга состояния серверов, на которых установлены компоненты InfoWatch Traffic Monitor, и работающих на них служб. Также выполнение общих действий по управлению сервером.

Подсистема InfoWatch Traffic Monitor	Назначение подсистемы
	Работа с подсистемой осуществляется администратором через веб-интерфейс.
Подсистема аудита	Возможность настраивать поисковые фильтры (по персоне, действию, объекту, датам), получать краткую наглядную информацию по событиям и нарушениям согласно установленным фильтрам, а также устанавливать период хранения событий в Системе. Работа с подсистемой осуществляется администратором через веб-интерфейс.
Подсистема «Консоль управления»	Обеспечение работы графического пользовательского интерфейса, с помощью которого производится администрирование, настройка и использование Traffic Monitor. Состоит из модулей: • Модуль мониторинга; • Модуль контроля; • Модуль настройки.

2.3 Лицензирование

После установки Системы нужно также установить лицензию.
Для этого запросите файл лицензионного ключа (см. *InfoWatch Traffic Monitor. Руководство пользователя. Запрос лицензии*).
Лицензия определяет срок действия, количество пользователей, набор модулей перехвата и анализа, а также возможность взаимодействия со сторонними системами.

Лицензионный ключ представляет собой файл формата LIC.
При установке и использовании лицензионного ключа нужно учитывать следующее:

- если период действия лицензии истек, работа перехватчиков будет остановлена. Для возобновления работы Системы установите новую лицензию;
- если нужно изменить настройки передачи трафика согласно новой схеме развертывания, замените лицензионный ключ с учетом новых перехватчиков.

При полной переустановке операционной системы или системы InfoWatch Traffic Monitor вам потребуется заново установить лицензию. Поэтому рекомендуем сохранить файл лицензионного ключа на каком-либо носителе.

> **Важно!**
>
> О проверке валидности лицензии и об управлении лицензиями см. *InfoWatch Traffic Monitor. Руководство пользователя. Управление лицензиями*.

Ниже приведены списки модулей, которые используются в продукте.

Модули перехвата, разработанные компанией InfoWatch		
Подсистема	Тип событий	Протокол
TM	Электронная почта	POP3 IMAP SMTP NRPC
	Веб-сообщение	HTTP HTTPS
	Веб-почта	HTTP HTTPS
	ICQ	OSCAR
	Data Discovery	-
DM	Электронная почта	POP3 IMAP Outlook SMTP
	Веб-сообщение	HTTP HTTPS
	Веб-почта	HTTP HTTPS
	Печать	-
	Skype	SKYPE
	XMPP	XMPP
	Mail.Ru Агент	MMP
	FTP	FTP
	Буфер обмена	-

Модули перехвата, разработанные компанией InfoWatch		
Подсистема	Тип событий	Протокол
	Снимки экрана	-
	Съемные устройства	-
	Сетевые ресурсы	-
	Терминальная сессия	-
	Облачное хранилище	HTTPS
	Telegram	-
	Ввод с клавиатуры	-
	VK (ВКонтакте)	HTTPS
	Facebook	HTTPS
	WhatsApp	-
Adapters	MS Lync	SIP
	Электронная почта (Lotus)	NRPC
	Веб-сообщение (ICAP)	ICAP
	Веб-почта (ICAP)	ICAP

Модули перехвата сторонних разработчиков	
Тип событий	Протокол
Электронная почта	POP3 MAPI SMTP/ESMTP IMAP NRPC
Веб-почта	HTTP HTTPS ICAP

Модули перехвата сторонних разработчиков	
Тип событий	Протокол
ICQ	OSCAR
Mail.ru Агент	MMP
Skype	Skype
XMPP	XMPP
MS Lync	SIP
Веб-сообщение	HTTP HTTPS ICAP
FTP	FTP
Съемные устройства	-
Печать	-
SmartLogger	XMPP

Модули анализа:

1. Лингвистический анализ.
2. Детектор эталонных документов.
3. Детектор векторных изображений.
4. Детектор текстовых объектов.
5. Детектор выгрузок из баз данных.
6. Детектор форм.
7. Графический анализ.
8. Детектор печатей.
9. Автолингвист.

Дополнительные возможности:

1. Модули автообновления эталонных выгрузок.
2. Экспорт в сторонние системы анализа.

Ограничение:

Технология блокирования каналов утечки на рабочих станциях по результатам анализа не лицензируется.

3 Типы установки Системы

Развертывание Системы осуществляется следующими способами, исходя из расчетной нагрузки на аппаратные средства и цели внедрения (подробнее см. *InfoWatch Traffic Monitor. Руководство по установке*. *Схемы развертывания Системы и выбор типа установки*):

- *"Все-в-одном" (All-in-one) Standard* – базовый тип установки всех компонентов Системы на один компьютер с использованием СУБД PostgreSQL. Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Установка TM Enterprise и TM Standard в режиме "Все-в-одном";*
- *"Все-в-одном" (All-in-one) Enterprise* – тип установки Системы с расширенными возможностями, включая: использование СУБД PostgreSQL, настройку масштабируемости, тонкий контроль за рабочими станциями. Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Установка TM Enterprise и TM Standard в режиме "Все-в-одном"*;
- *Распределенная установка TM Enterprise (*компоненты Traffic Monitor и СУБД устанавливаются на разные машины*)* – тип установки Системы для функционирования под большой нагрузкой и работой с большим объемом данных. Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Распределенная установка TM Enterprise*.

Важно!

В случае распределенной установки Системы на разные серверы (или при создании кластера серверов) вводится ряд дополнительных ограничений и настроек:

- нужно настроить сетевые параметры поисковика Sphinx (см. *Конфигурирование работы Sphinx при распределенной установке*);
- некоторые процессы серверной части (**iw_adlibitum, iw_deliver, iw_indexer, iw_is, iw_image_autoling, iw_text_autoling**) и пользовательской консоли (**iw_kicker, iw_configerator**) должны быть запущены в единственном экземпляре на кластере (см. *Список процессов серверной части Traffic Monitor*).

Каждый из типов установки, в зависимости от приобретаемой лицензии, может включать установку перехватчиков Системы:

- InfoWatch Device Monitor – предназначен для настройки схем безопасности, системы мониторинга компьютеров, контроля доступа к компьютерам компании и др. (см. *InfoWatch Device Monitor (Windows). Руководство по установке, конфигурированию и администрированию* или *InfoWatch Device Monitor (Linux). Руководство по установке*).
- Adapters – модули перехвата для интеграции со сторонними системами.

4 Настройка Системы после установки

После установки Системы выполняются следующие настройки, необходимые для штатного функционирования Системы:

- *Настройка синхронизации времени* – о включении автоматической синхронизации времени на серверах;
- *Конфигурирование работы Sphinx при распределенной установке* – о настройках для распределенной установки;
- *Настройка перехвата трафика* – особенности настроек для различных типов перехватываемого трафика;

- *Общие настройки* – порядок настроек для перехвата трафика, передаваемого по протоколу ICAP;

- *Автозапуск процессов* – перечень системных процессов и описание необходимости и порядка включения и отключения их автозапуска;
- *Настройка OCR-экстракторов* – порядок установки пакетов, необходимых для распознавания текста в перехваченных событиях;
- *Настройка отправки уведомлений пользователям и сотрудникам* – обязательные настройки для поддержки почтовых уведомлений, отправляемых в результате срабатывания тех или иных правил в политиках (см. *InfoWatch Traffic Monitor. Руководство пользователя*);
- *Ограничение количества найденных событий* – изменение максимального количества событий, выводимых в Консоли управления;
- Настройка Сервера InfoWatch Device Monitor – настройки отдельных модулей Сервера Device Monitor и изменение настроек протоколирования (см. *InfoWatch Device Monitor (Windows). Руководство по установке, конфигурированию и администрированию* или *InfoWatch Device Monitor (Linux). Руководство по установке*);
- *Настройка сбора данных в филиальной сети* – настройки конфигурационных файлов служб, осуществляющих сбор данных в филиальной сети;
- *Настройка межсервисного взаимодействия (служба Consul)* – настройки конфигурационного файла и службы, осуществляющей управление процессами Системы;
- Обнаружение рабочих станций для установки агентов – сканирование сети на наличие рабочих станций вне Active Directory (см. *InfoWatch Device Monitor. Руководство пользователя*).

Рекомендуем:

- изменить предустановленные в Системе пароли, следуя требованиям информационной безопасности (см. *Изменение предустановленного пароля*);
- настроить защиту от подбора паролей при авторизации в консолях Traffic Monitor и Device Monitor (см. *Настройка защиты от подбора паролей*);
- настроить сетевой экран, чтобы предотвратить несанкционированный доступ к компонентам Системы (см. *Рекомендации по настройке безопасного окружения*).

4.1 Изменение предустановленного пароля

Для учетных записей в Системе предустановлен стандартный пароль – xxXX1234 (см. *InfoWatch Traffic Monitor. Руководство по установке. Предустановленные серверные параметры*). В процессе эксплуатации Системы его нужно заменить, следуя требованиям информационной безопасности. Стабильная и безопасная работа Системы требует хранить пароли в надежном, недоступном для

других месте. Стандартный пароль изменяется в конфигурационных файлах Системы. Чтобы заменить предустановленный пароль на новый:

1. Остановите процессы Traffic Monitor:

```
iwtm stop
```

2. Выполните команду:

```
egrep -lir --include=\*.{cfg,conf,pgpass} --exclude-dir=\*{etc_conf_backup,config_merge}\*
'xxXX1234' /  | xargs -l sed -i -e 's/xxXX1234/<new_pass>/g'
```

   где `<new_pass>` – новый пароль.
3. Проверьте, что новый пароль установлен во всех конфигурационных файлах:

```
egrep -lir --include=.{cfg,conf,pgpass} --exclude-dir={etc_conf_backup,config_merge}*
'<new_pass>' /
```

4. Измените пароль для подключения к базе данных:
   a. Подключитесь к СУБД PostgreSQL:

```
psql postgres iwtm
```

   b. Получите список пользователей:

```
\du
```

   c. Измените пароли всех пользователей, включая пользователя `postgres`:

```
alter user <iw_user> with password '<new_pass>';
```

      где `<iw_user>` – выбранный пользователь базы данных, а `<new_pass>` – новый пароль для этого пользователя.
   d. Отключитесь от СУБД PostgreSQL:

```
\q
```

5. Запустите процессы Traffic Monitor:

```
iwtm start
```

Требования к паролям

Пароль может состоять из следующих символов:

- прописные буквы латинского алфавита (A–Z);

- строчные буквы латинского алфавита (a–z);
- арабские цифры (0–9);
- специальные символы: "@", "%", ":", "^", "-", "_", "+", "/", ".", ",".

4.2 Настройка защиты от подбора паролей

Для защиты Системы реализована блокировка авторизации пользователя при повторяющихся неудачных попытках авторизации. Защита от подбора паролей настраивается в базе данных.

По умолчанию защита отключена.

Настройка выполняется отдельно для InfoWatch Traffic Monitor и для InfoWatch Device Monitor.

Чтобы включить защиту для сервера Traffic Monitor:

1. Подключитесь напрямую к базе данных, которую использует сервер Traffic Monitor.
2. Найдите таблицу `SETTING`.
3. Найдите 3 параметра, которые отвечают за настройку защиты:
   - **`web_logon_attempts_count`** – количество допустимых неудачных попыток авторизации;
   - **`web_logon_blocking_period`** – время, на которое будет заблокирована возможность авторизации для пользователя, в секундах;
   - **`web_logon_attempts_period`** – период неудачных попыток авторизации, в секундах.
4. Задайте значения всех трех параметров в соответствии с требованиями безопасности.

   > **Важно!**
   >
   > Если любому из параметров задано некорректное значение или 0, защита будет отключена.

5. Для применения настроек достаточно сохранить изменения в базе данных. Перезагрузка сервера не требуется, поддерживается динамическое изменение настроек защиты.

При блокировании авторизации в разделе **Управление - Аудит** консоли управления Traffic Monitor будет создано соответствующее событие, в котором будет указано время разблокировки.
При очередной попытке авторизации заблокированный пользователь будет уведомлен о превышении числа неудачных попыток входа.

Пример настроек защиты для Traffic Monitor:

- `web_logon_attempts_count - 5`
- `web_logon_blocking_period - 300`
- `web_logon_attempts_period - 120`

При данных настройках, если в течение 2 минут (120 секунд) от имени пользователя будут выполнены 5 неудачных попыток авторизации, для данного пользователя будет заблокирована возможность авторизации на 5 минут (300 секунд). Отсчет периода неудачных попыток начинается с первой. Если за 120 секунд пользователь совершит только 4 неудачные попытки, следующая попытка будет первой в новом периоде.

4.3 Предварительные настройки

После установки системы нужно выполнить следующие настройки:

- *Настройка синхронизации времени*;
- *Конфигурирование работы Sphinx при распределенной установке*.

4.3.1 Настройка синхронизации времени

1. Установите системное время с помощью команды `date`. Например, для установки 11 сентября 2013 13:30 запустите команду со следующими параметрами:
   `date 09111330`
2. Скопируйте системное время для настройки аппаратных часов с помощью команды:
   `hwclock --systohc`
3. Проверьте, что системное и аппаратное время настроены корректно:
   `hwclock ; date`
4. Время должно быть одинаковым. Допустимы небольшие отклонения.
   Остановите службу chronyd:
   `systemctl stop chronyd`
5. Определите сервер синхронизации времени. Вы можете использовать любую службу точного времени, работающую по протоколу NTP и доступную из вашей сети: как сетевое оборудование, так и контроллеры домена Windows (сервер Active Directory). Чтобы проверить, поддерживает ли сервер NTP, воспользуйтесь командой `chronyd -q 'server <IP> iburst'`, (где `IP` – адрес проверяемого сервера). Например:
   ```
   chronyd -q 'server 10.10.0.98 iburst'
   2024-09-11T10:30:17Z chronyd version 4.3 starting (+CMDMON +NTP +REFCLOCK
   +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 -DEBUG)
   2024-09-11T10:30:17Z Initial frequency -19.107 ppm
   2024-09-11T10:30:22Z System clock wrong by 8551737.490761 seconds (step)
   2024-12-19T09:59:19Z chronyd exiting
   ```
6. Настройте синхронизацию, указав сервер NTP-синхронизации в файле **/etc/chrony/chrony.conf**. Для этого добавьте запись вида (укажите IP-адрес вашего NTP-сервера):
   `server 10.10.0.98 iburst`
   Запустите службу chronyd:
   `systemctl start chronyd`
7. Проверьте состояние службы chronyd с помощью команды:
   `systemctl status chronyd`
8. Проверьте синхронизацию времени. Для этого выполните команду:
   `chronyc -N sources`

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================
^* 10.10.0.98                    4   6    37    19    -14us[ -102us] +/-   39ms
```

4.3.2 Конфигурирование работы Sphinx при распределенной установке

При полнотекстовом поиске по запросам в Traffic Monitor используется механизм Sphinx. Служба **sphinx** устанавливается в режиме All-in-one или при установке шаблона "Индексер". Сведения о режимах

установки Системы приведены в документе *InfoWatch Traffic Monitor. Руководство по установке. Схемы развертывания Системы и выбор типа установки*.

Распределенной считается установка, при которой компоненты Traffic Monitor установлены на разных серверах.

> **Примечание:**
>
> При наличии нескольких серверов укажите IP-адрес сервера, на котором запущена служба **sphinx** (сервер с шаблоном "Индексер"). IP-адрес указывается в параметре `hostname` секции `search` конфигурационного файла **web.conf** на сервере с шаблоном "Веб-консоль".

4.4 Общие настройки

Раздел содержит информацию о настройке Системы и ее компонентов:

- *Перехват трафика, передаваемого по протоколу ICAP*.

4.4.1 Перехват трафика, передаваемого по протоколу ICAP

Прокси-сервер с поддержкой протокола ICAP перехватывает HTTP-трафик и передает его на сервер Traffic Monitor для анализа и загрузки в базу данных.

В данной схеме на сервере Traffic Monitor используется автоматически устанавливаемый модуль **iw_icap**, который обрабатывает перехваченные данные, поступившие через proxy-сервер.

Схема поддерживает обработку данных пользователя при следующих методах аутентификации: NTLM, LDAP, Basic, Digest.

> **Важно!**
>
> Сервер Traffic Monitor и прокси-сервер с ICAP-клиентом должны находиться в одной подсети. На каждой рабочей станции браузер должен быть настроен так, чтобы HTTP(S)-трафик проходил через прокси-сервер SQUID. Информацию по настройке вы можете получить из документации к браузеру.

В зависимости от схемы работы (**Копия** или **Блокировка**) возможны следующие варианты движения HTTP-трафика:

- Режим **Копия** – копия HTTP-трафика передается на сервер Traffic Monitor для анализа. При этом трафик проходит через прокси-сервер к следующему звену сети, в зависимости от инфраструктуры организации.
- Режим **Блокировка** – HTTP-трафик анализируется системой Traffic Monitor. В зависимости от наличия нарушений, возможны следующие варианты движения трафика:
  - если нарушение отсутствует, на прокси-сервер возвращается сообщение, разрешающее передачу трафика. Далее трафик от прокси-сервера направляется к следующему звену сети, в зависимости от инфраструктуры организации;

- если обнаруживается нарушение, на прокси-сервер возвращается сообщение, запрещающее передачу трафика. Трафик блокируется, а пользователь, отправивший трафик, получает сообщение с предупреждением.

> **Примечание:**
>
> Текст сообщения с предупреждением содержится в файле **error.html**, расположенном в директории `/opt/iw/tm5/etc`.

В этом разделе:

- *Настройка ICAP*
- *Рекомендации по настройке SQUID*
- *Отключение ICAP*

Настройка ICAP

Модуль ICAP автоматически устанавливается вместе с сервером Traffic Monitor (установка All-in-one или шаблон "Перехватчики").При выборе шаблона "Перехватчики" автозапуск процесса **iw_icap** на сервере Traffic Monitor выключен по умолчанию.
Перехват HTTP- и HTTPS-трафика осуществляется с использованием одних и тех же средств Системы, но различается настройка сторонних механизмов (см. ниже).

Для обеспечения перехвата HTTP(S)-трафика, передаваемого по протоколу ICAP, нужно настроить параметры перехвата HTTP- и HTTPS-запросов на прокси-сервере.

> **Важно!**
>
> На каждой рабочей станции браузер должен быть настроен так, чтобы HTTP(S)-трафик проходил через прокси-сервер SQUID. Информацию по настройке вы можете найти в документации к используемому браузеру.

Возможны следующие варианты настройки ICAP:

1. Чтобы трафик передавался в режиме "Копия":
   a. В конфигурационном файле **luaengined.conf**, расположенном в директории `/opt/iw/tm5/etc`, в секции `TransportModes` в свойстве `Icap` укажите действительное FQDN-имя сервера Traffic Monitor (например, `tm-server1.local`) и значение режима `Copy`. Допускается указывать несколько пар значений:
   `"Icap": [{"Server": "tm-server1.local", "Mode": "Copy"}, {"Server":"tm-server2.local", "Mode": "Copy"}]`
   b. Сохраните изменения в файле **luaengined.conf**.
2. Чтобы трафик передавался вне зависимости от вынесенного вердикта:
   a. В коде, приведенном выше, задайте значение режима: `Transparent`.
   b. Сохраните изменения в файле **luaengined.conf**.
3. Чтобы трафик передавался в режиме "Блокировка":
   a. В коде, приведенном выше, задайте значения режима: `Normal`.
   b. Сохраните изменения в файле **luaengined.conf**.
4. В конфигурационном файле **icap.conf**, расположенном в директории `/opt/iw/tm5/etc/`, укажите значение параметра `AsyncCheck` секции `Icap:`

- `true` – режим "Копия";
- `false` – режим "Блокировка".

5. Сохраните конфигурационный файл.
6. Перезапустите сервер Traffic Monitor:
   `iwtm restart`

Настройте параметры перехвата HTTP- и HTTPS-запросов на прокси-сервере.

> **Примечание:**
>
> Данная настройка зависит от модификации прокси-сервера. Актуальную информацию по настройке вы можете получить из документации к прокси-серверу.
>
> См. *Рекомендации по настройке SQUID*.

Рекомендации по настройке SQUID

Документация содержит информацию о настройке прокси-сервера SQUID для авторизации пользователей из MS AD, перехвата SSL (ssl-bump) и проверки трафика через ICAP.

В этой главе:

- *Установка SQUID*
- *Настройка ICAP*
- *Настройка перехвата и раскрытия SSL*
- *Настройка аутентификации пользователей*

Установка SQUID

Перед установкой прокси-сервера SQUID нужно скачать rpm-пакет или архив (с последующей распаковкой) из репозитория или CD/DVD. В нашем примере будет использован rpm-пакет `squid-3.4.0.2-2.el6.x86_64.rpm` .

Чтобы установить rpm-пакет прокси-сервера SQUID, войдите в Систему под именем `root` и введите следующую команду:

```
rpm -i squid-3.4.0.2-2.el6.x86_64.rpm
```

При успешной установке пакета вы увидите:

```
Preparing...        ##################  [100%]
1:squid             ##################  [100%]
```

Для доступа к конфигурационному файлу введите:

```
cd /etc/squid/
mcedit squid.conf
```

Настройка ICAP

Для настройки ICAP выполните:

1. Добавьте в конфигурационный файл `squid.conf` строки для обработки ICAP:

```
icap_enable on
icap_service service_req reqmod_precache bypass=1 icap://10.60.7.7:1344/request
adaptation_access service_req allow all
icap_send_client_ip on
icap_send_client_username on
```

2. Чтобы настроить работы с ICAP-сервером **UserGate Web Filter**, добавьте в файл `squid.conf` фрагмент:

```
icap_enable on
icap_preview_enable on
icap_preview_size 4096
icap_send_client_ip on
icap_service service_req reqmod_precache bypass=0 icap://10.0.3.10:1344/request
adaptation_access service_req allow all
icap_service service_resp respmod_precache bypass=0 icap://10.0.3.10:1344/response
adaptation_access service_resp allow all http_port 8080 transparent
```

где `10.0.3.10` – адрес сервера **UserGate Web Filter**.

> **Важно!**
>
> Сервер UserGate Web Filter не поддерживает режим `icap_preview_enable off`. Работа с HTTPS-трафиком в данный момент не поддерживается.

3. Перезапустите Squid:

```
sudo service squid3 restart
```

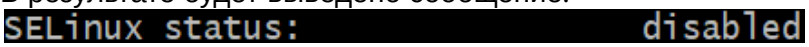
Настройка перехвата и раскрытия SSL

Режим SSL-Bump используется для перехвата содержимого зашифрованных HTTPS-сеансов. При поступлении первого перехватываемого HTTPS-запроса, SQUID осуществляет SSL-соединение с сервером и получает его сертификат. После этого SQUID использует имя хоста из реального полученного от сервера сертификата и создает фиктивный сертификат, при помощи которого имитирует запрошенный сервер при взаимодействии с клиентом, продолжая при этом использовать SSL-соединение, установленное с сервером. Кроме HTTPS-соединений, указанная схема может использоваться для перехвата большинства HTTP-запросов с методом CONNECT.

Для настройки режима SSL-Bump выполните следующие действия:

1. Отключите систему контроля доступа SELinux. Для этого:
   a. Выполните команду:
      `sudo sed -i 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config`
   b. Перезагрузите сервер с помощью команды:
      `reboot`
   c. Проверьте статус системы SELinux с помощью команды:
      `sestatus`

В результате будет выведено сообщение:



2. Создайте каталог для хранения сертификатов SQUID:
   `mkdir /etc/squid/ssl_cert`
3. Сгенерируйте корневой сертификат для браузеров рабочих станций, трафик с которых будет прослушиваться:
   `openssl req -new -newkey rsa:2048 -days <количество дней> -nodes -x509 -keyout /etc/squid/ssl_cert/IW.key -out /etc/squid/ssl_cert/IW.crt`
   `openssl x509 -in /etc/squid/ssl_cert/IW.crt -outform DER -out /etc/squid/ssl_cert/IW.der`
4. Скопируйте файл с расширением **.der** на рабочие станции и установите его как доверенный сертификат в хранилище компьютера.
5. Настройте работу браузеров рабочих станций для использования нового прокси-сервера SQUID.
6. Сгенерируйте файл параметров для алгоритма Diffie-Hellman:
   `openssl dhparam -outform PEM -out /etc/squid/ssl_cert/IW_dhparam.pem 2048`
7. Сделайте пользователя **squid** владельцем директории `/etc/squid/ssl_cert` и для обеспечения безопасности измените права доступа к файлам:
   `chown -R squid:squid /etc/squid/ssl_cert && chmod 400 /etc/squid/ssl_cert/IW*`
8. Определите версию SQUID, используемую на вашем сервере. Для этого выполните команду:
   `squid -v`
   Информация об используемой версии отобразится в следующем формате:
   `Squid Cache: Version <версия>`
9. Остановите SQUID:
   `systemctl stop squid`
10. Если вы используете прокси-сервер Squid версии 3, выполните следующие действия:
    a. Создайте базу данных для подменяемых сертификатов и сделайте пользователя **squid** ее владельцем:
       `mkdir -p /var/lib/squid`
       `rm -rf /var/lib/squid/ssl_db`
       `/usr/lib64/squid/ssl_crtd -c -s /var/lib/squid/ssl_db`
       `chown -R squid:squid /var/lib/squid`
    b. В конфигурационном файле **/etc/squid/squid.conf** закомментируйте настройку `http_port` и добавьте следующие параметры генерации сертификатов:
       `#http_port 3128`
       `http_port 3128 tcpkeepalive=60,30,3 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=20MB cert=/etc/squid/ssl_cert/IW.crt key=/etc/squid/ssl_cert/IW.key cipher=HIGH:MEDIUM:!LOW:!RC4:!SEED:!IDEA:!3DES:!MD5:!EXP:!PSK:!DSS options=NO_TLSv1,NO_SSLv3,NO_SSLv2,SINGLE_DH_USE,SINGLE_ECDH_USE tls-dh=prime256v1:/etc/squid/ssl_cert/IW_dhparam.pem`
       `sslproxy_flags DONT_VERIFY_PEER`
       `sslproxy_cert_error allow all`
       `always_direct allow all`
       `ssl_bump client-first all`
       `ssl_bump server-first all`
       `ssl_bump none all`

`sslcrtd_program /usr/lib64/squid/ssl_crtd -s /var/lib/squid/ssl_db -M 20MB`

11. Если вы используете прокси-сервер Squid версии 4 и выше, выполните следующие действия:
    a. Создайте базу данных для подменяемых сертификатов и сделайте пользователя **squid** ее владельцем:
    ```
    mkdir -p /var/lib/squid
    rm -rf /var/lib/squid/ssl_db
    /usr/lib64/squid/security_file_certgen -c -s /var/lib/squid/ssl_db -M 20MB
    chown -R squid:squid /var/lib/squid
    ```
    b. В конфигурационном файле **/etc/squid/squid.conf** :
        i. Перед первым правилом `http_access` добавьте строки:
        ```
        acl intermediate_fetching transaction_initiator certificate-fetching
        http_access allow intermediate_fetching
        ```
        ii. Закомментируйте настройку `http_port` и добавьте следующие параметры генерации сертификатов:
        ```
        #http_port 3128
        http_port 3128 tcpkeepalive=60,30,3 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=20MB tls-cert=/etc/squid/ssl_cert/IW.crt tls-key=/etc/squid/ssl_cert/IW.key cipher=HIGH:MEDIUM:!LOW:!RC4:!SEED:!IDEA:!3DES:!MD5:!EXP:!PSK:!DSS options=NO_TLSv1,NO_SSLv3,SINGLE_DH_USE,SINGLE_ECDH_USE tls-dh=prime256v1:/etc/squid/ssl_cert/IW_dhparam.pem
        sslproxy_cert_error allow all
        ssl_bump stare all
        sslcrtd_program /usr/lib64/squid/security_file_certgen -s /var/lib/squid/ssl_db -M 20MB
        sslcrtd_children 8
        ```
12. Запустите SQUID:
    ```
    systemctl start squid
    ```

Настройка аутентификации пользователей

Работа SQUID по аутентификации заключается в декодировании HTTP заголовка `Authorization` и передаче декодированной информации стороннему модулю. Если эта информация верна, то доступ пользователю предоставляется, если же она не верна или отсутствует, то SQUID возвращает клиенту HTTP ошибку с кодом 407. Таким образом, всю основную работу по проверке подлинности пользователей выполняют сторонние модули. Расположение этих модулей зависит от операционной системы и версии SQUID. Например, в ОС Debian с установленным SQUID версии 3 они расположены в каталоге `/usr/lib/squid3` , в ОС Red Hat Enterprise Linux – в `/usr/lib64/squid` . Чтобы просмотреть, какие методы проверки подлинности поддерживает SQUID, размещение сторонних модулей и многие другие параметры, используйте команду `squid -v` :

```
squid -v
Squid Cache: Version 3.4.0.2
configure options: '--host=x86_64-redhat-linux-gnu' '--build=x86_64-redhat-linux-gnu' '--program-prefix='
'--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin'
'--sysconfdir=/etc' '--datadir=/usr/share'
'--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec'
```

```
'--sharedstatedir=/var/lib'
 '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--exec_prefix=/usr' '--
libexecdir=/usr/lib64/squid'
 '--localstatedir=/var' '--datadir=/usr/share/squid' '--sysconfdir=/etc/squid'
 '--with-logdir=$(localstatedir)/log/squid' '--with-pidfile=$(localstatedir)/
run/squid.pid'
 '--disable-dependency-tracking' '--enable-eui' '--enable-follow-x-forwarded-
for' '--enable-auth'
 '--enable-auth-basic=DB,LDAP,MSNT,MSNT-multi-
domain,NCSA,NIS,PAM,POP3,RADIUS,SASL,SMB,getp
 wnam' '--enable-auth-ntlm=smb_lm,fake' '--enable-auth-
digest=file,LDAP,eDirectory'
 '--enable-auth-negotiate=kerberos,wrapper'
 '--enable-external-acl-helpers=wbinfo_group,kerberos_ldap_group,AD_group' '--
enable-cache-digests'
 '--enable-cachemgr-hostname=localhost' '--enable-delay-pools' '--enable-epoll'
'--enable-icap-client'
 '--enable-ident-lookups' '--enable-linux-netfilter' '--enable-removal-
policies=heap,lru' '--enable-snmp'
 '--enable-ssl' '--enable-ssl-crtd' '--enable-storeio=aufs,diskd,ufs,rock' '--
enable-wccpv2' '--enable-esi'
 '--with-aio' '--with-default-user=squid' '--with-filedescriptors=16384' '--
with-dl' '--with-openssl' '--with-pthreads'
 '--disable-arch-native' 'build_alias=x86_64-redhat-linux-gnu'
'host_alias=x86_64-redhat-linux-gnu'
 'CFLAGS=-O2 -g' 'CXXFLAGS=-O2 -g -fPIC'
 'PKG_CONFIG_PATH=/usr/lib64/pkgconfig:/usr/share/pkgconfig'
```

Взаимодействие и описание настроек сторонних модулей аутентификации производится с помощью параметра `auth_param`. Клиент будет поочередно пытаться использовать схемы аутентификации в том порядке, в котором они заданы в конфигурационном файле `squid.conf`. Новая настроенная схема аутентификации вступит в силу после перезапуска SQUID. Чтобы изменить существующие схемы без перезапуска сервиса, используйте команду `squid -k reconfigure`.

Для контроля доступа в интернет:

1. Добавьте в начало конфигурационного файла `/etc/squid/squid.conf` настройку используемой аутентификации `auth_param` согласно схеме:
   `auth_param схема_аутентификации параметры_схемы [значения_параметров]`
2. Создайте список управления доступом, который будет задействовать настроенный модуль аутентификации. В конфигурационном файле список управления доступом обозначается как `acl`. В поле `тип_отбора` он должен иметь значение `proxy_auth`, `proxy_auth_regex` или `external` с использованием переменной `%LOGIN`. Например:
   `acl auth proxy_auth REQUIRED`
3. Установите для заданного списка управления доступом разрешение в параметре `http_access`. Например:
   `http_access allow auth`

> **Примечание:**
>
> Подробнее о настройке аутентификации пользователей можно узнать из документации к прокси-серверу SQUID.

Пример настройки Basic-аутентификации:

На сервере с установленным SQUID выполните следующие действия:

1. Добавьте в начало файла `/etc/squid/squid.conf` следующие строки:
   ```
   auth_param basic program /usr/lib64/squid/basic_ldap_auth -R -b "dc=<доменное имя второго уровня>,dc=<доменное имя первого уровня>" -D "<имя пользователя>@<домен Active Directory>" -w "<пароль пользователя>" -f "sAMAccountName=%s" <IP-адрес контроллера домена Active Directory>
   auth_param basic children 10
   auth_param basic realm Squid proxy-caching web server
   auth_param basic casesensitive off
   auth_param basic credentialsttl 1 minute
   acl auth proxy_auth REQUIRED
   http_access allow auth
   ```
2. Чтобы включить запись событий в журнал в режиме отладки, в файле `/etc/squid/squid.conf` добавьте параметр `-d` в первую строку. Например:
   ```
   auth_param basic program /usr/lib64/squid/basic_ldap_auth -R -d -b "dc=<доменное имя второго уровня>,dc=<доменное имя первого уровня>" -D "<имя пользователя>@<домен Active Directory>" -w "<пароль пользователя>" -f "sAMAccountName=%s" <IP-адрес контроллера домена Active Directory>
   ```
   События отладки будут записаны в файл `/var/log/squid/cache.log`.
3. Перезагрузите сервис Squid, выполнив команду:
   ```
   service squid restart
   ```

Рекомендации по настройке UserGate

UserGate, как ICAP-клиент, позволяет передавать HTTP/HTTPS и почтовый SMTP- и POP3-трафик на ICAP-сервер в Traffic Monitor. Чтобы настроить работу UserGate с ICAP-сервером, выполните следующие шаги:

1. Создайте ICAP-сервер:
   i. Перейдите в раздел **Политики безопасности -> ICAP-серверы**.
   ii. Нажмите **Добавить** и создайте один или более ICAP-серверов, выполнив действия:

Поле	Действие
Название	Введите название ICAP-сервера.
Описание	Укажите описание ICAP-сервера (необязательное поле).
Адрес сервера	Введите IP-адрес ICAP-сервера.
Порт	Введите TCP-порт ICAP-сервера. Значение по умолчанию: `1344`
Максимальный размер сообщения	Определяет максимальный размер сообщения, передаваемого на ICAP-сервер (в килобайтах). Установите размер сообщения больше 0. **Пример:** `35840`

Поле	Действие
Период проверки доступности сервера ICAP	Устанавливает время в секундах, через которое UserGate посылает OPTIONS-запрос на ICAP-сервер, чтобы убедиться, что сервер доступен. Задайте значение от 100 до 600 секунд. **Пример:** `100`
Пропускать при ошибках	Если эта опция включена, то UserGate не будет посылать данные на ICAP-сервер в случаях, когда он недоступен (не отвечает на запрос OPTIONS). Включение не требуется.
Reqmod путь	Включите использование режима Reqmod, установив флаг **Вкл**. Далее задайте **Путь на сервере ICAP для работы в режиме Reqmod** вида: `icap://icap-server:port/path` – указание полного URI для режима reqmod. **Пример:** `icap://FQDN:1344/reqmod`
Respmod путь	Включение режима Respmod не требуется.
Посылать имя пользователя	Установите флаг **Вкл**, чтобы включить отсылку имени пользователя на ICAP-сервер. Далее задайте **Название заголовка**, которое будет использоваться для отправки имени пользователя на ICAP-сервер. Значение по умолчанию: `X-Authenticated-User` При необходимости выберите **Кодировать в base64** – кодировать имя пользователя в base64. Это может потребоваться, если имена пользователей содержат символы национальных алфавитов.
Посылать IP-адрес	Если установлен флаг **Вкл**, то включается отсылка IP-адреса пользователя на ICAP-сервер. Далее задайте **Название заголовка**, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. Значение по умолчанию: `X-Client-Ip` Включение не требуется.
Посылать MAC-адрес	Если установлен флаг **Вкл**, то включается отсылка MAC-адреса пользователя на ICAP-сервер.

Поле	Действие
	Далее задайте **Название заголовка**, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. Значение по умолчанию: `X-Client-Mac` Включение не требуется.

2. Создайте правило балансировки на ICAP-серверы (опционально):
   a. Перейдите в раздел **Политики сети -> Балансировка нагрузки**.
   b. Выберите **Добавить -> Балансировщик ICAP** и заполните поля:

Поле	Описание
Вкл/Выкл	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
ICAP-серверы	Список ICAP-серверов, созданных на предыдущем шаге, на которые будет распределяться нагрузка.

3. Создайте правило ICAP:
   a. Перейдите в раздел **Политики безопасности -> Правила ICAP**.
   b. Нажмите **Добавить** и заполните поля:

Поле	Описание
Вкл/Выкл	Включает или отключает правило.
Название	Название правила.
Описание	Описание правила.
Действие	Возможны следующие варианты: • **Пропустить** – не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP; • **Переслать** – переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера. Стандартный режим работы ICAP-серверов; • **Переслать и игнорировать** – переслать данные на ICAP-сервер и игнорировать ответ от ICAP-сервера. В этом случае, вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика.

Поле	Описание
ICAP-серверы	Список ICAP-серверов, созданных на предыдущем шаге, на которые будет распределяться нагрузка.
Источник	Зона источника трафика и/или списки IP-адресов источника трафика.
Пользователи	Список пользователей и групп, для которых применяется данное правило. Могут быть использованы пользователи типов: **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** нужно настроить идентификацию пользователей.
Назначение	Зона назначения трафика и/или списки IP-адресов назначения трафика.
MIME-типы контента	Списки MIME-типов. Предусмотрена возможность управления видео-контентом, аудио-контентом, изображениями, исполняемыми файлами и другими типами. Также администратор может создать собственные группы MIME-типов.
Категории	Списки категорий UserGate URL filtering.
URL	Списки URL.
HTTP-метод	Метод, используемый в HTTP-запросах. Как правило, это POST или GET.
Сервис	Возможны варианты: • **HTTP** – веб-трафик; • **SMTP** – почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа; • **POP3** – почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа.

Важно!

Правила ICAP применяются сверху вниз в том порядке, в котором они указаны в консоли. Выполняется всегда только первое правило, для которого совпали условия, указанные в правиле. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Используйте кнопки **Вверх**/**Вниз** для изменения порядка применения правил.

Отключение ICAP

Если перехват HTTP/HTTPS-запросов по протоколу ICAP больше не требуется, вы можете отключить модуль **iw_icap**.
Чтобы отключить модуль iw_icap:

1. Остановите процессы Traffic Monitor:
   `iwtm stop`
2. Отключите автозапуск процесса **iw_icap**:
   `iwtm disable iw_icap`
3. Запустите процессы Traffic Monitor:
   `iwtm start`
4. Проверьте состояние процессов Traffic Monitor:
   `iwtm status`

После отключения модуля верните исходные настройки прокси-сервера.

4.5 Настройка перехвата трафика

В Системе доступен перехват данных, передаваемых по протоколу SMTP.

SMTP (Simple Mail Transfer Protocol) – почтовый протокол, используемый почтовым клиентом для отправки исходящих сообщений электронной почты на сервер.

В ОС Astra Linux Special Edition "Смоленск" реализовано мандатное управление доступом.
Для этого используется мандатная метка, которая определяется:

1. Мандатным уровнем конфиденциальности (от 0 до 255).
2. Мандатным уровнем целостности.
3. Мандатной категорией.

> **Примечание:**
>
> Более детальное описание мандатного управления доступом и контроля целостности см. в документации к операционной системе Astra Linux.

Traffic Monitor может учитывать мандатные метки при перехвате SMTP-трафика.

В зависимости от типа перехватываемого трафика и способа перехвата Система настраивается следующими способами:

- *Настройка перехвата SMTP-трафика*
- *Прием объектов, перехваченных InfoWatch Device Monitor*

> **Важно!**
>
> Предполагается, что Система уже установлена до начала настройки. Сведения об установке для каждой из схем развертывания приведены в документе *InfoWatch Traffic Monitor. Руководство по установке*.
>
> После настройки перехвата трафика нужно настроить параметры анализа объектов (см. *InfoWatch Traffic Monitor. Руководство пользователя*).

4.5.1 Настройка перехвата SMTP-трафика

Раздел содержит информацию о том, как настроить перехват SMTP-трафика:

- *Прием копий с почтового сервера*
- *Блокировка "в разрыв"*
- *Настройки почтовых серверов для перехвата SMTP-трафика*

Подробное описание схемы перехвата SMTP-трафика см. в статье *Схема перехвата SMTP-трафика*.

Прием копий с почтового сервера

На корпоративном почтовом сервере требуется настроить правило, отправляющее скрытую копию (BCC) для каждого отправленного письма. Копия должна отравляться на несуществующий почтовый адрес несуществующего почтового домена, IP-адрес которого соответствует серверу Traffic Monitor. Данная функция поддерживается большинством почтовых серверов.

Интеграция сервера Traffic Monitor с почтовым сервером Exim4 реализуется следующим образом. Почтовый сервер Exim4, встроенный в Систему Traffic Monitor, получает копии писем, отправленных по SMTP-протоколу. Копии писем поступают на **25**-й порт и передаются процессу **iw_smtpd** на порт **2025**. В Системе создается событие для каждого из писем, информация о которых затем помещается в базу данных.

Чтобы настроить прием копий с почтового сервера, выполните следующие действия:

1. Убедитесь, что включен автозапуск процесса **iw_smtpd** (см. *Автозапуск процессов*).
2. Если нужно, чтобы Traffic Monitor перехватывал письма с мандатным уровнем конфиденциальности выше 0, настройте работу SMTPD:
   a. Установите `exim4`, учитывающий мандатные метки. Для этого выполните команду:
      `apt-get install exim4-daemon-heavy`
   b. Убедитесь, что в конфигурационном файле **smtpd.conf**, расположенном в директории `/opt/iw/tm5/etc/`, указано:
      `"EnablePrivSock": true,`
   c. Установите права пользователю **iwtm**, выполнив команду:
      `usercaps -m 0x100 iwtm`
   d. Выйдите из системы и пройдите повторную авторизацию.
   e. Выполните команду:
      `/etc/init.d/iwtm restart smtpd`
   f. Выполните команду:
      `/etc/init.d/exim4 restart`
3. На почтовом сервере настройте пересылку скрытых копий SMTP-сообщений (BCC – Blind Carbon Copy) на сервер Traffic Monitor. Настройка Exim4 для отправки скрытых копий приведена в статье *Настройка пересылки скрытых копий Exim4*.
4. Настройте встроенный в Систему Exim4 (см. *Настройка сервера Exim4 в системе Traffic Monitor*).
5. Убедитесь, что включен автозапуск для процессов, участвующих в перехвате и обработке почты:
   exim4, **iw_smtpd**, **iw_messed**, **iw_warpd**, **iw_luaengined**, **iw_cas**, **iw_pas**, **iw_x2x**, **iw_x2db**, **iw_tech-tools** (см. *Автозапуск процессов*).
6. Убедитесь, что в `/opt/iw/tm5/etc/luaengined.conf` в параметре `"TransportModes" / " Sm tp"` установлен режим `Copy` или пустое значение.

Все письма, полученные по правилу пересылки скрытой копии или журналирования, будут содержать постоянного получателя, например `"iwtm-mon@local"`. Для его удаления настройте параметр `SmtpTmBccList` в файле **luaengined.conf**.

Блокировка "в разрыв"

Сервер Traffic Monitor используется как промежуточный почтовый сервер. В его состав входит почтовый сервер Postfix/Exim.

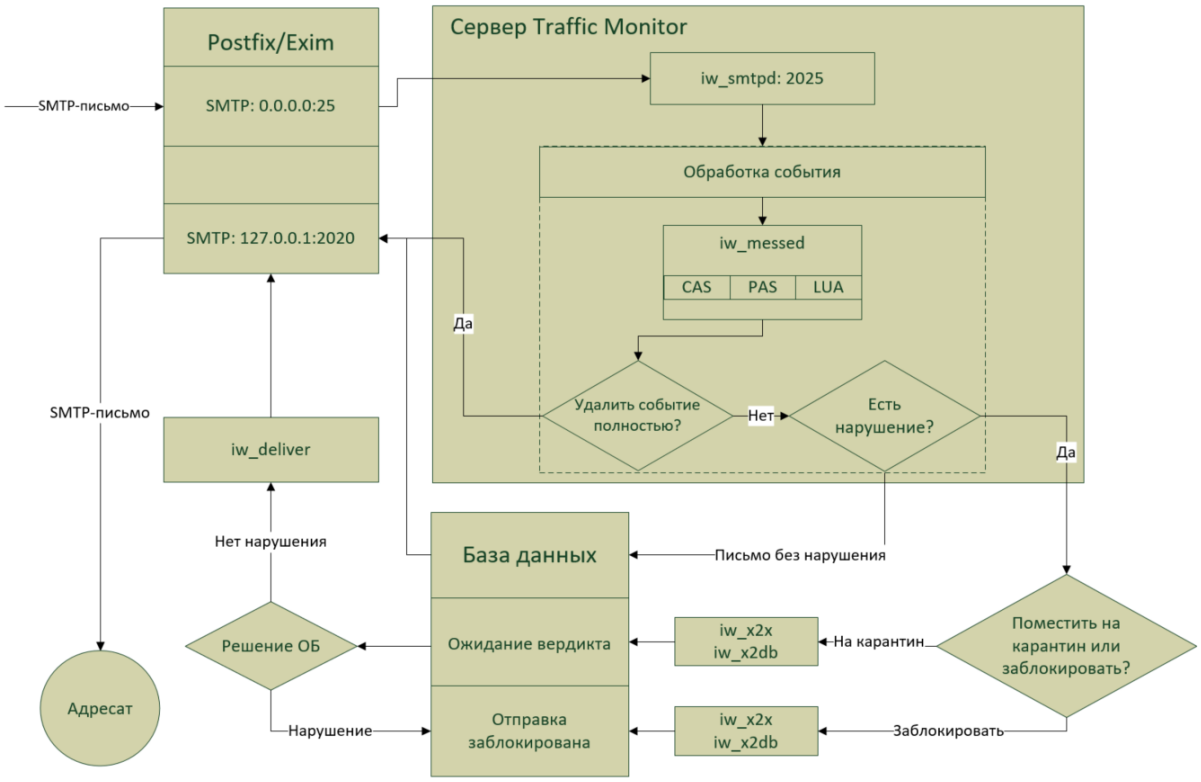
Интеграция сервера Traffic Monitor с почтовым сервером реализуется следующим образом. Почтовый сервер Postfix/Exim, встроенный в систему Traffic Monitor, принимает входящие SMTP-письма на **25** порт. Далее входящие SMTP-письма передаются процессу **iw_smtpd** на порт **2025**. В Системе создаются события для каждого из писем. Письма помещаются в базу данных Traffic Monitor, кроме случая, когда в политике в правиле передачи выбрано действие *Удалить событие полностью.* При этом событие не попадет в Базу данных, а письмо будет отправлено адресату без анализа в Traffic Monitor.

В режиме **Блокировка** SMTP-трафик анализируется системой Traffic Monitor, и:

- если нарушение отсутствует, SMTP-трафик с помощью встроенного сервера Postfix/Exim передается адресату или следующему relay-серверу в почтовой системе организации. Доставка осуществляется так: процесс `iw_messed` передает письма на порт **2020** почтового сервера Postfix/Exim. Почтовый сервер Postfix/Exim либо напрямую доставляет письма адресатам, либо передает их следующему почтовому relay-серверу;
- если обнаружено нарушение и в политиках указан вердикт *Поместить на карантин*, то Система выставляет письму вердикт *Карантин*. Письмо будет доставлено только в том случае, если Офицер безопасности выставит решение пользователя *Нет нарушения,* разрешая доставку письма в Консоли управления (см. *InfoWatch Traffic Monitor. Руководство пользователя*). Доставка осуществляется следующим образом: процесс `iw_deliver` передает письма на порт **2020** почтового сервера Postfix, встроенного в Систему. Почтовый сервер Postfix либо напрямую доставляет письма адресатам, либо передает их следующему почтовому relay-серверу;
- если обнаружено нарушение и в политиках указан вердикт *Заблокировать*, то Система выставляет письму вердикт *Заблокировано*. Доставка письма в этом случае выполнена не будет.

Вы также можете настроить:

- автоматическую блокировку событий с вердиктом *Карантин* в случае истечения заданного срока ожидания. См. *Автоматическая блокировка событий с вердиктом Карантин*.
- приостановку отправки письма до дополнительного подтверждения сотрудником, отправившим его. См. *Приостановка отправки письма до подтверждения сотрудником*.



Чтобы настроить работу "в разрыв" для SMTP-перехватчика, выполните следующие действия:

1. Убедитесь, что включен автозапуск процессов **`iw_smtpd`** и **`iw_deliver`** (см. *Автозапуск процессов*).
2. В файле `/etc/exim4/`**`update-exim4.conf.conf`** включите использование раздельных файлов конфигурации и укажите активные интерфейсы для почтового сервера. Для этого отредактируйте две следующие строки:

```
dc_local_interfaces='0.0.0.0.25 ; 127.0.0.1.2020'
dc_use_split_config='true'
```

> **Примечание:**
>
> Следует обратить внимание, что:
>
> - в файле конфигурации Exim номера портов отделены от IP-адресов символом "." , а не ":".
> - пример приведен для использования протокола IPv4. При необходимости получения писем по протоколу IPv6 значение параметра `dc_local_interfaces` нужно поменять на соответствующее.

3. Создайте файлы с настройками для перенаправления входящих писем на анализ в Traffic Monitor:
   a. Файл с рекомендуемым именем `/etc/exim4/conf.d/transport/`**`45_exim4-config_iwtm_smtp_check`** и содержимым:

```
iwtm_smtp_check:
  driver = smtp
  port = 2025
  delay_after_cutoff = false
  command_timeout = 5m
  final_timeout = 10m
```

Параметры со значениями тайм-аутов `command_timeout` и `final_timeout` указаны в минутах. Они могут потребоваться, чтобы настроить схему перехвата, если Exim и Traffic Monitor установлены на разных серверах.

b. Файл с рекомендуемым именем `/etc/exim4/conf.d/router/`**`050_exim4-config_iwtm`** и содержимым:

```
send_to_iwtm:
  driver = manualroute
  domains = !+local_domains
  self = send
  condition = ${if and {{! match {$sender_host_address}{\N^(|127\.0\.0\.1)$\N}}{eq
{$interface_port}{25}}}{yes}{no}}
  transport = iwtm_smtp_check
  route_list = * 127.0.0.1
  address_test = false
```

В данном примере на анализ в Traffic Monitor отправляется вся почта, приходящая на порт **25** с внешних хостов, кроме писем, направляемых на локальный домен. Минимальная безопасность данной конфигурации обеспечивается путем привязки порта **2020** строго к локальному интерфейсу с адресом **127.0.0.1**, чтобы письма нельзя было пересылать в обход проверки Traffic Monitor.

4. Настройте досылку писем через выделенный почтовый relay. Для этого:
   a. Создайте файл с рекомендуемым именем `/etc/exim4/conf.d/router/`**`051_exim4-config_rela y`** и содержимым:

```
send_to_relay:
  driver = manualroute
  domains = !+local_domains
  transport = remote_smtp
  route_list = * 10.20.30.40
  address_test = false
```

где `route_list` – это IP-адрес корпоративного почтового сервера, на который будут передаваться SMTP-письма после анализа в Traffic Monitor.

   b. Укажите в файле `/etc/exim4/`**`update-exim4.conf.conf`** значение параметра `dc_relay_domains` (по умолчанию значение пустое):

```
dc_relay_domains='*'
```

Такая конфигурация позволяет использовать пограничный почтовый сервер для досылки писем, не нарушающих политику Traffic Monitor.

5. Сгенерируйте конфигурацию, выполнив команду-скрипт:

```
update-exim4.conf
```

6. Перезагрузите Exim, выполнив команду:

```
service exim4 restart
```

7. В конфигурационном файле **luaengined.conf** в секции TransportModes в свойстве Smtp укажите действительное FQDN-имя сервера Traffic Monitor с перехватчиком (например, tm-server1.local) и значение режима Normal (режим *Блокировка*):

```
"Smtp": [{"Server": "tm-server1.local", "Mode": "Normal"}]
```

> **Важно!**
>
> При распределенной установке режим определяется процессом **iw_luaengined**, расположенным локально или на другой ноде кластера. Поэтому на каждой ноде в файле /opt/iw/tm5/etc/luaengined.conf в секции TransportModes в свойстве Smtp укажите несколько пар значений действительных FQDN-имен серверов TM и нужных режимов. Например:
>
> ```
> "Smtp": [{"Server": "tm-server1.local", "Mode": "Copy"}, {"Server":"tm-server2.local.ru", "Mode": "Normal"}]
> ```
>
> Обратите внимание, что при этом файлы **iwssid.lua** и **luaengined.conf** должны быть одинаковыми на всех нодах.

8. Перезагрузите конфигурацию процесса **iw_luaengined**:

```
iwtm reload luaengined
```

Чтобы трафик передавался вне зависимости от вынесенного вердикта:

1. В коде, указанном выше в пункте 6, задайте значение режима " Transparent". Например:

```
"Smtp": [{"Server": "tm-server1.local", "Mode": "Transparent"}]
```

2. Сохраните файл.
3. Перезагрузите Систему:

```
iwtm restart
```

Досылка SMTP-писем с ошибками обработки, отправленных "в разрыв"

SMTP-письма, в процессе обработки которых произошли ошибки, помещаются в очереди ошибок: **queue/x2x-errors** и **queue/errors**. Досылка писем (в том числе с вердиктом *Карантин*) из очередей ошибок осуществляется посредством демона **iw_rammer**, после чего очереди очищаются. Адреса отправителей и получателей берутся (при наличии) из XML-файла. В случае их отсутствия письмо досылке не подлежит. При отправке письма Офицеру безопасности адреса отправителя и получателя указываются в конфигурационном файле /opt/iw/tm5/etc/**rammer.conf**. Во вложении к письму передаются XML- и DAT-файлы объекта. Досылка письма адресату, а также оповещения Офицеру безопасности осуществляется через почтовый сервер Exim (порт **2020**). Уведомления Офицеру безопасности со вложенным доставленным письмом приходят в виде "письма-события", отправитель которого берется из исходного письма. Данные для подключения (адрес и порт) задаются в конфигурационном файле **rammer.conf** (см. *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам. rammer.conf*).

SMTP-письмо будет досылаться при соблюдении одновременно всех условий:

1. Если оно еще не было доставлено штатным способом (демоном **iw_messed**).
2. Если во время обработки письма и попадания его в очередь ошибок установлен режим работы *Блокировка*.
3. Если у письма не проставлен вердикт *Заблокировано*.

Средством принудительной досылки писем служит утилита /opt/iw/tm5/bin/ **rammer_tool**. Для вызова списка возможных настроек наберите в командной строке:

```
/opt/iw/tm5/bin/rammer_tool --help
```

Автоматическая блокировка событий с вердиктом Карантин

Чтобы Система выставляла вердикт *Заблокировано* событиям с вердиктом *Карантин* по истечении заданного срока, в файле opt/iw/tm5/etc/**web.conf** в секции **autoForbid**, подсекции **quarantined** измените значение параметра **timeout** (в минутах). Значение по умолчанию – 0, т.е. автоматическая блокировка отключена.

При изменении срока ожидания блокировки также могут потребоваться настройки:

- параметр **batchSize** – количество обрабатываемых за раз событий. Значение по умолчанию – 5000. Для изменения перейдите в файл opt/iw/tm5/etc/**web.conf** в секцию **autoForbid**, подсекцию **quarantined**.
- расписание запуска задачи cron. Для изменения перейдите в файл etc/cron.d/**web_cron**. По умолчанию задача запускается раз в 4 часа и выглядит так:

  ```
  0 */4 * * * iwtm /opt/iw/tm5/www/backend/protected/yiic autoforbid quarantined
  ```

Примечание:

Посредством задачи cron Система присваивает вердикт *Заблокировано* заданному количеству событий с истекшим сроком ожидания. Например, если установлен срок ожидания 1 час, а периодичность запуска задачи cron – 4 часа, то у событий, которые находятся в карантине уже 1 час и больше, автоматическая смена вердикта произойдет в течение 4 часов.

Не рекомендуем устанавливать периодичность запуска задачи cron менее, чем 30 минут.

Слишком большое значение параметра **batchSize** может влиять на нагрузку системы.

Приостановка отправки письма до подтверждения сотрудником

В Системе реализован механизм, предотвращающий отправку конфиденциальной информации по ошибке. Система приостанавливает отправку письма до дополнительного подтверждения сотрудником, отправившим его.

При этом:

1. Система перехватывает письмо с конфиденциальной информацией и помещает его в карантин.
2. Сотрудник получает почтовое уведомление с информацией о приостановке отправки и ссылкой на страницу подтверждения.
3. Сотрудник переходит по ссылке и либо подтверждает отправку, либо окончательно блокирует ее:
    - в случае подтверждения Система досылает письмо получателю;
    - если отправка не была подтверждена в течение заданного срока ожидания, Система автоматически блокирует письмо.

Система также может отправлять почтовые уведомления о блокировке/разблокировке отправки.

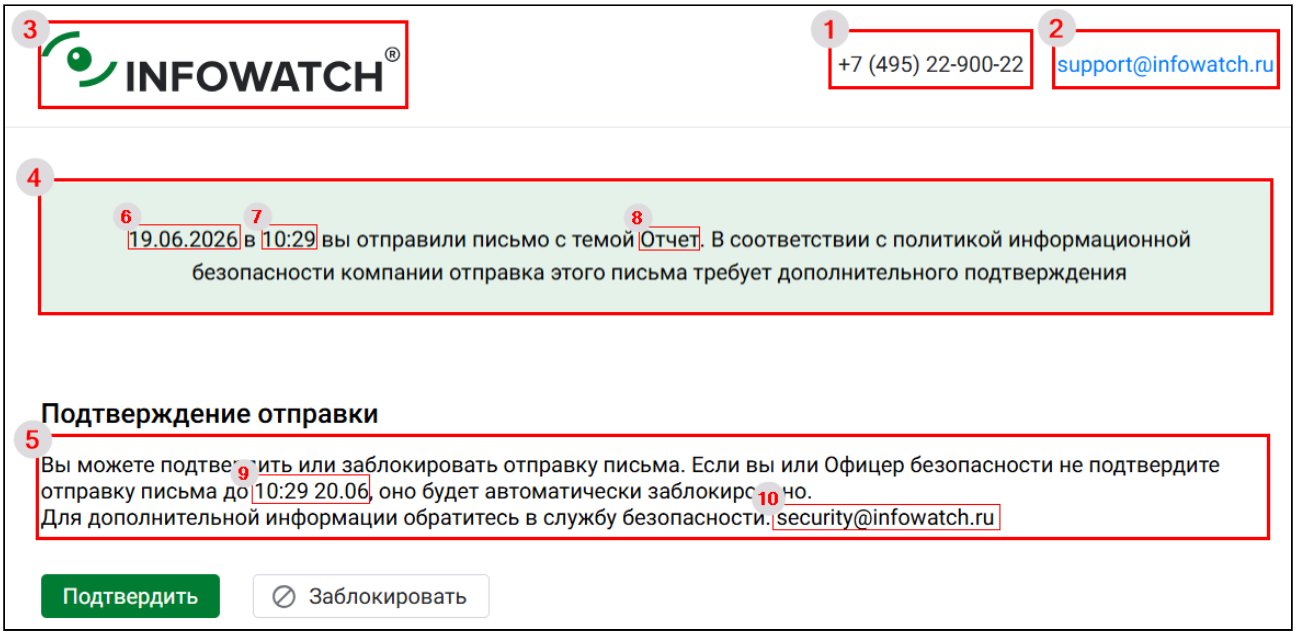
> **Примечание:**
>
> Заблокировать или подтвердить отправку может также пользователь Системы (Офицер безопасности) в Консоли управления Traffic Monitor. Если Офицер безопасности изменил вердикт раньше сотрудника, выбор действий на странице подтверждения становится недоступен.
>
> Срок ожидания по умолчанию – 24 часа. Об изменении срока см. ниже.

Вы можете настроить:

- шаблон почтового уведомления, см. *InfoWatch Traffic Monitor. Руководство пользователя. Настройка уведомлений.*
- внешний вид страницы подтверждения: текст, акцентный цвет, логотип, контактная информация, адрес страницы;
- срок ожидания подтверждения.

Настройка страницы подтверждения

По умолчанию форма подтверждения имеет следующий вид:



Чтобы настроить отображение страницы ввода пароля (изменить акцентный цвет, добавить логотип и контактную информацию):

1. В директории `/opt/iw/tm5/www/frontend/tmng/tmng/custom/` создайте файл `justify.json`.
2. Из файла `justify.json.example`, расположенного в этой же директории, скопируйте в `justify .json` блок с параметрами. Убедитесь, что вы не переносите в файл блок с комментарием.
3. Если нужно добавить логотип, поместите файл с изображением в директорию `/opt/iw/tm5/www/frontend/tmng/tmng/custom/`
4. В файле `justify.json` измените значения параметров согласно таблице. Любой параметр опционален и может быть удален.

Параметр	Описание
`accentColor`	Акцентный цвет страницы в формате HEX. Пример: `#3f51b5`

`phones`
`emails`
	Номера на снимке экрана: 1, 2
	Список телефонных номеров/электронных адресов для связи. Вы можете указать несколько значений в виде массива строк. В качестве разделителя используйте запятую.
	Примеры:
	`["+1 (234) 56-789-01", "+1 (234) 56-789-02"]`
	`["support@support.example", "support1@support.example"]`

Параметр	Описание
`securityContact`	Адрес службы безопасности, отображаемый в тексте подтверждения. Значение по умолчанию: `security@infowatch.ru`
`logo`	*Номер на снимке экрана: 3* Путь к файлу с логотипом, указывается относительно директории `/opt/iw/tm5/www/frontend/tmng/` . Поддерживаемые форматы файлов: SVG, PNG, JPEG, AVIF, WebP. Пример: `/tmng/custom/logo.svg`
`texts`	*Номера на снимке экрана: 4, 5* Настраиваемый текст страницы. См. описание ниже.

5. Сохраните изменения.

Настройка текста страницы подтверждения

Секция `texts` содержит подсекции `ru` и `en`, каждая из которых содержит параметры:

- `alert` – текст уведомления о том, что отправка письма требует подтверждения. Отображается в отдельном блоке под шапкой страницы;
- `description` – основной текст страницы подтверждения. Отображается под заголовком "Подтвердите отправку" и непосредственно над кнопками подтверждения/блокировки.

В текстах `alert` и `description` по умолчанию используются параметры:

Параметр	Описание
`date`	*Номер на снимке экрана: 6* Дата отправки письма. Задается автоматически на основе информации из события.
`time`	*Номер на снимке экрана: 7* Время отправки письма. Задается автоматически на основе информации из события.
`subject`	*Номер на снимке экрана: 8* Тема письма. Задается автоматически на основе информации из события.
`expiry`	*Номер на снимке экрана: 9* Дата и время истечения срока ожидания подтверждения. Задается автоматически на основе даты и времени отправки письма и срока ожидания.

Параметр	Описание
`contact`	*Номер на снимке экрана: 10* Контакт службы безопасности. Используется значение, заданное в переменной `securityContact`. Если переменная `securityContact` отсутствует, используется значение по умолчанию: `security@infowatch.ru`

Вы можете располагать параметры в текстах в любом порядке, а также удалять параметры, если в них нет необходимости.

Настройка адреса страницы подтверждения

Вы можете изменить адрес страницы подтверждения: вместо адреса Traffic Monitor будет отображаться адрес другого севера с установленным и настроенным Nginx.

Для этого:

1. На любом сервере с Nginx создайте файл `/etc/nginx/conf.d/confirmation_page.conf`.
2. Вставьте в файл следующее содержимое:

```
server {
    listen 80;

    # Домен, на котором будет доступна страница
    server_name <имя_домена>;

    # При использовании протокола HTTPS
    #listen 443 ssl;

    # Если требуется, укажите расположение SSL-ключа и сертификата
    #ssl_certificate     <расположение_сертификата>;
    #ssl_certificate_key <расположение_ключа>;

    charset utf-8;

    # Настройки проксирования
    proxy_http_version 1.1;
    proxy_ssl_server_name on;

    # Таймауты соединения с целевым сервером
    proxy_connect_timeout 10s;
    proxy_send_timeout 60s;
    proxy_read_timeout 60s;

    # Передача информации об исходном запросе
    proxy_set_header X-Real-IP         $remote_addr;
    proxy_set_header X-Forwarded-For   $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-Host  $host;
```

```
    # Передача служебных заголовков API
    proxy_set_header X-API-PERSONALHASH $http_x_api_personalhash;
    proxy_set_header X-API-VERSION      $http_x_api_version;

    # Проксирование API-запросов на основной сервер Traffic Monitor
    location ~ ^/(justify|xapi|)(/|$) {
        # Укажите доменное имя или IP-адрес сервера
        proxy_pass https://<сервер_Traffic_Monitor>
    }

    location ~* \.(?:css|js|png|jpg|jpeg|gif|svg|ico|woff2?|ttf|eot|json)$ {
        # Укажите доменное имя или IP-адрес сервера
        proxy_pass https://<сервер_Traffic_Monitor>
    }

    # Запрет всех остальных запросов
    location / {
        return 404;
    }
}
```

3. Заполните следующие параметры:
   - `server_name` – доменное имя или IP-адрес сервера с Nginx, отображаемый в качестве адреса страницы подтверждения;
   - `proxy_pass` (встречается дважды) – фактический адрес Traffic Monitor (доменное имя или IP-адрес).
4. Для работы по протоколу HTTPS раскомментируйте строки:
   - `listen 443 ssl;`
   - `ssl_certificate     <расположение_сертификата>;`
   - `ssl_certificate_key <расположение_ключа>;`

   В переменных `ssl_certificate` и `ssl_certificate_key` укажите расположение SSL-сертификата и ключа.
5. На сервере Traffic Monitor в конфигурационном файле `/opt/iw/tm5/etc/`**`web.conf`** в параметре **`justify_host`** укажите адрес сервера с Nginx.
   Например:

```
justify_host: "http://domainname.ru" или justify_host: "https://203.0.113.0"
```

Настройка срока ожидания подтверждения

Чтобы изменить время, в течение которого Система ожидает подтверждения сотрудника / Офицера безопасности до окончательной блокировки, в файле `opt/iw/tm5/etc/`**`web.conf`** в секции **`autoForbid`**, подсекции **`justify`** измените значение параметра **`timeout`** (в минутах). Значение по умолчанию – 1440 минут (24 часа).

При изменении срока ожидания также могут потребоваться настройки:

- параметр **`batchSize`** – количество обрабатываемых за раз событий. Значение по умолчанию – 5000. Для изменения перейдите в файл `opt/iw/tm5/etc/`**`web.conf`** в секцию **`autoForbid`**, подсекцию **`justify`**.

- расписание запуска задачи cron. Для изменения перейдите в файл `etc/cron.d/web_cron`. По умолчанию задача запускается раз в 4 часа и выглядит так:

```
*/* 4 * * * iwtm /opt/iw/tm5/www/backend/protected/yiic autoforbid justify
```

Примечание:

Посредством задачи cron Система присваивает вердикт *Заблокировано* заданному количеству событий с истекшим сроком ожидания.
Например, если установлен срок ожидания 1 час, а периодичность запуска задачи cron – 4 часа, то у событий, для которых уже прошел 1 час с момента отправки запроса подтверждения, автоматическая смена вердикта произойдет в течение 4 часов.

Не рекомендуем устанавливать периодичность запуска задачи cron менее, чем 30 минут. Слишком большое значение параметра `batchSize` может влиять на нагрузку системы.

Настройки почтовых серверов для перехвата SMTP-трафика

Раздел содержит информацию о настройке почтовых серверов для перехвата сервером Traffic Monitor:

- *Настройка пересылки скрытых копий Microsoft Exchange Server 2007 и 2010*
- *Настройка пересылки скрытых копий ZCS Zimbra*
- *Настройка пересылки скрытых копий MDaemon*
- *Настройка сервера Exim4 в системе Traffic Monitor*
- *Настройка пересылки скрытых копий Exim4*

Настройка пересылки скрытых копий Microsoft Exchange Server 2007 и 2010

Чтобы обеспечить отправку скрытых копий SMTP-сообщений, в Exchange Management Console нужно создать и настроить коннектор, который будет пересылать почту на сервер Traffic Monitor. Для этого выполните перечисленные ниже действия:

Создание SMTP-коннектора для пересылки копий почтовых сообщений на сервер Traffic Monitor

1. Выберите узел **Organization Configuration –> Hub Transport** и нажмите **New Send Connector**.
2. В открывшемся окне мастера создания коннектора введите имя создаваемого коннектора и из раскрывающегося списка выберите для него тип **Custom**. Нажмите **Next**.
3. На шаге **Address space** создайте новое адресное пространство для перенаправления трафика. Для этого нажмите **Add**. В открывшемся диалоговом окне укажите параметры адресного пространства и нажмите **OK**. Затем нажмите **Next**.
4. На шаге **Network Settings** выберите **Route mail through the following smart hosts** и нажмите **Add**. В открывшемся диалоговом окне укажите IP-адрес сервера TM, на который нужно перенаправлять почту, и нажмите **OK**. Затем нажмите **Next**.
5. На шаге **Configure smart host authentication settings** выберите **None** – по умолчанию Postfix на сервере Traffic Monitor не требует авторизации. Нажмите **Next**.
6. На шаге **SourceServer** выберите сервер, на котором будет работать созданный коннектор. Нажмите **Next**.

7. На шаге **New Connector** убедитесь, что параметры коннектора заданы верно, и нажмите **New**. Дождитесь окончания процесса создания и нажмите **Finish**.

Окно мастера создания коннектора будет закрыто.

Создание контакта, на который будут перенаправляться копии почтовых сообщений

1. Выберите узел **Recipient Configuration –> Mail Contact** и нажмите **New Mail Contact**.
2. В открывшемся окне мастера создания контакта выберите **MailContact** и нажмите **Next**.
3. На шаге **Configure smart host authentication settings** введите общую информацию о контакте. В строке **External mail address** нажмите **Edit**. В открывшемся диалоговом окне **SMTP Address** укажите почтовый адрес, на который будут перенаправляться копии почтовых сообщений.

> **Важно!**
>
> Домен почтового адреса контакта должен совпадать с доменом коннектора.

4. На шаге **New Mail Contact** убедитесь, что параметры коннектора заданы верно, и нажмите **New**. Дождитесь окончания процесса создания и нажмите **Finish**.

Окно мастера создания контакта будет закрыто.

> **Важно!**
>
> Для корректной работы Системы нужно, чтобы среди пользователей ОС Linux (на сервере InfoWatch Traffic Monitor) был пользователь с таким же доменным именем, как новый контакт. Например, если на данном шаге создается контакт *user@company.com*, то нужно, чтобы в число пользователей Linux входил пользователь *user*.
> Чтобы добавить пользователя на ОС Linux, от имени пользователя root выполните следующую команду:
> useradd <username>
>
> где <username> – требуемое имя пользователя. Для приведенного выше примера (пользователь *user*) нужно будет выполнить команду:
> useradd user

Создание транспортного правила для копирования писем

1. Выберите узел **Organization Configuration -> HubTransport** и нажмите **New Transport Rule**.
2. В открывшемся окне мастера создания транспортного правила введите имя создаваемого правила и установите флажок в поле **EnableRule**. Нажмите **Next**.
3. На шаге **Conditions** установите флажок для условия **from users inside or outside the organization**. В качестве параметра условия выберите **Inside**. Нажмите **Next**.
4. На шаге **Actions** установите флажок для действия **Blind carbon copy (Bcc) the message to address**. Нажмите на гиперссылку с параметром **address** и в открывшемся окне **Select Recipient** выберите ранее созданный контакт, а затем нажмите **OK**. В окне мастера создания транспортного правила нажмите **Next**.
5. При необходимости на шаге **Exceptions** вы можете настроить исключения из правила. Например, чтобы не выполнять копирование писем, отправляемых определенными

пользователями, установите флажок в поле **except when the message is from people** и в параметрах исключения выберите желаемых пользователей. Нажмите **Next**.

6. На шаге **Create Rule** убедитесь, что параметры правила заданы верно, и нажмите **New**. Дождитесь окончания процесса создания и нажмите **Finish**.

Блокирование отправки сообщений при недоступности сервера Traffic Monitor

1. Выберите узел **Organization Configuration -> Hub Transport** и нажмите  **New remote Domain**.
2. Укажите такое же имя, как у домена, использованного в п. 3 шага 2 данного раздела (при создании контакта, на который будет производиться перенаправление копий почтовых сообщений).
3. Выделите новый домен щелчком правой кнопки мыши и в контекстном меню выберите **Properties**.
4. В открывшемся окне перейдите на вкладку **Message Format**.
5. Снимите флажок в пункте **Allow non-delivery reports**.
6. Нажмите **OK**.

> **Важно!**
>
> Если в MS Exchange используется правило журналирования, для корректной обработки этих писем включите настройку в Traffic Monitor. Для этого в конфигурационном файле `messed.conf` укажите:
>
> `"ExchangeJournalReports": true,`
>
> Для применения изменений перезапустите службу **iw_messed**.

Настройка пересылки скрытых копий ZCS Zimbra

> **Важно!**
>
> Все команды должны выполняться от имени пользователя **zimbra**.

Настройка транспортной таблицы

Используйте конфигурационный блок для Zimbra 5.0.9 и выше со строкой вида:

```
zmlocalconfig -e postfix_transport_maps="hash:/opt/zimbra/postfix/conf/
transportfile proxy:ldap:/opt/zimbra/conf/ldap-transport.cf"
```

> **Важно!**
>
> Данная команда должна быть выполнена через **zmlocalconfig**. В этой ситуации редактирования **main.cf** будет недостаточно.

1. Проверьте существующую транспортную таблицу:
   `zmlocalconfig grep -i postfix_transport_maps`
   Получите вывод команды следующего вида:
   `postfix_transport_maps = proxy:ldap:/opt/zimbra/conf/ldap-transport.cf`

2. Создайте транспортный файл:
   `mcedit /opt/zimbra/postfix/conf/infowatch`
3. Добавьте в файл следующую строчку:
   `dlp.iw :[192.168.0.144]`
4. Проверьте права (владельцем и группой должны быть **zimbra**):
   `ll /opt/zimbra/postfix/conf/infowatch`
   `chown zimbra:zimbra /opt/zimbra/postfix/conf/infowatch`
5. Конвертируйте транспортный файл в БД:
   `postmap /opt/zimbra/postfix/conf/infowatch`
6. Добавьте транспортный файл перед файлом по умолчанию:
   `zmlocalconfig -e postfix_transport_maps="hash:/opt/zimbra/postfix/conf/infowatch proxy:ldap:/opt/zimbra/conf/ldap-transport.cf"`
7. Убедитесь, что в параметре `relay_domains` файла **main.cf** содержатся все домены, обрабатываемые сервером:
   `mcedit /opt/zimbra/postfix/conf/main.cf`
   Найдите или создайте строчку:
   `relay_domains = mydomain.com, mydomain.org, dlp.iw`

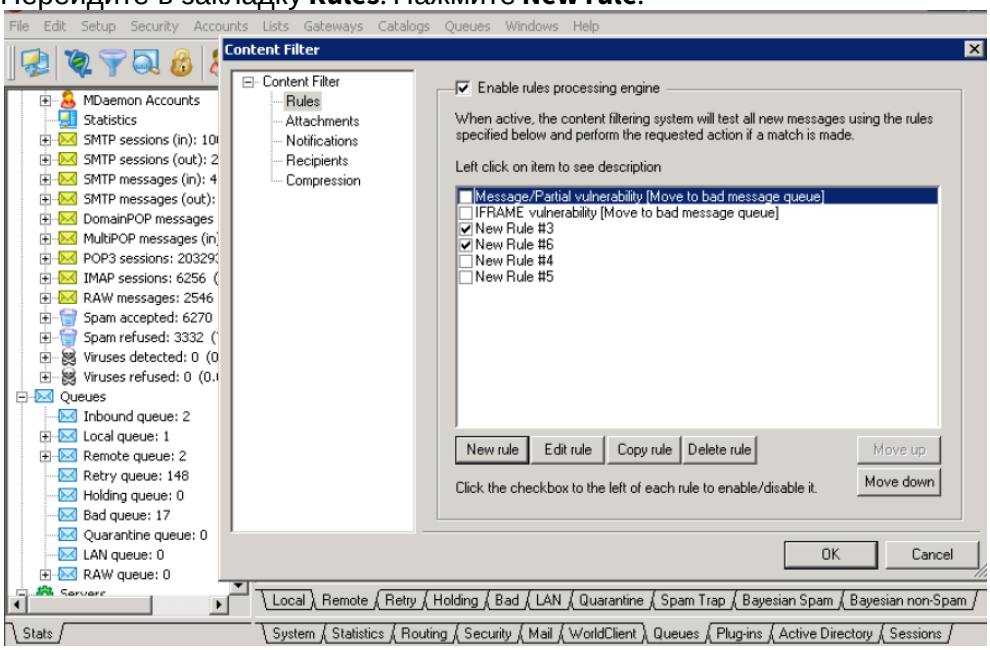
Настройка отправки BCC

1. В файл **/opt/zimbra/postfix/conf/main.cf** добавьте следующую строчку:
   `/opt/zimbra/postfix/conf/main.cf`
2. Перезагрузите Zimbra:
   `zmcontrol restart`

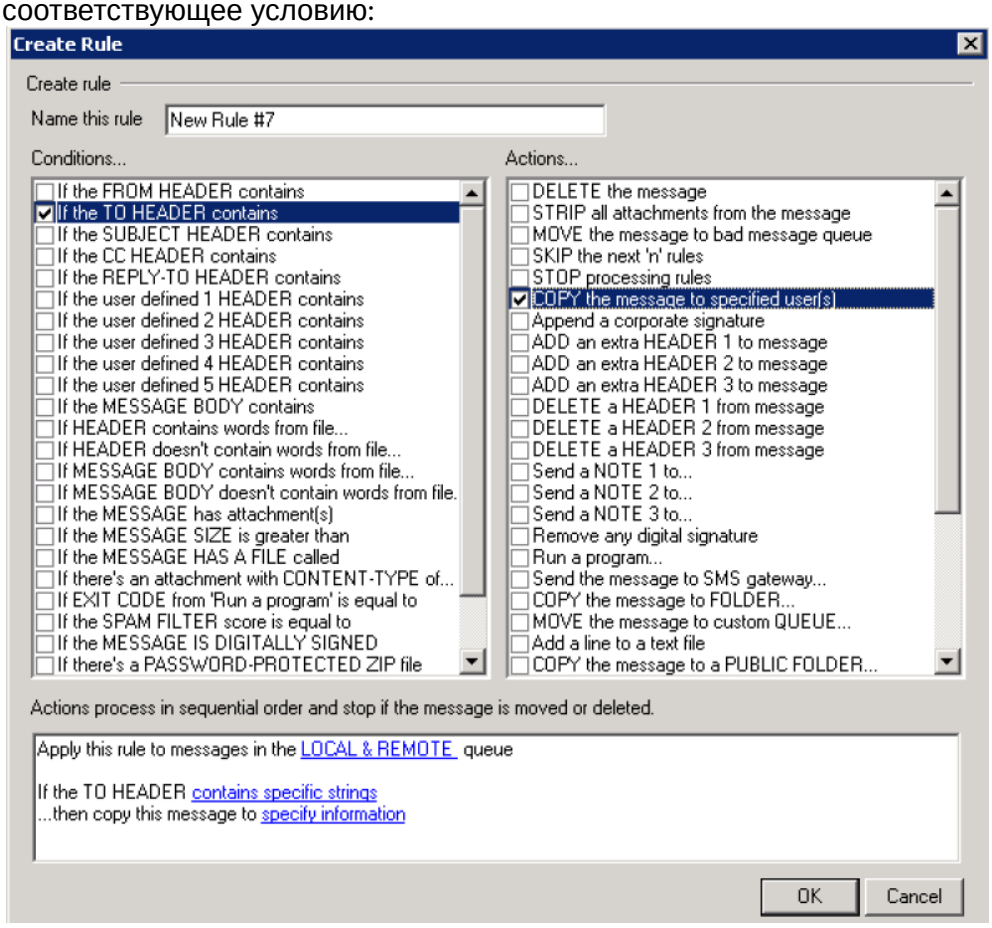
Настройка пересылки скрытых копий MDaemon

В почтовом клиенте MDaemon есть опция **Content Filter**, при помощи которой можно настроить фильтрацию входящей/исходящей почты, проходящей через сервер MDaemon.

1. Откройте MDaemon и зайдите во вкладку **Security > Content Filter**.
2. Перейдите в закладку **Rules**. Нажмите **New rule**:



3. В левой колонке выберите условие действия. В правой колонке выберите действие, соответствующее условию:



4. Выберите секцию, выделенную голубым, чтобы добавить значения правилам.
5. Нажмите **Add** и затем **OK**.

Настройка сервера Exim4 в системе Traffic Monitor

Чтобы настроить встроенный в Систему сервер Exim4 для пересылки принятых им скрытых копии в Traffic Monitor, выполните следующие шаги:

1. В файле конфигурации **/etc/exim4/exim4.conf.template** внесите правки:
   a. Строку

```
acl_smtp_rcpt = MAIN_ACL_CHECK_RCPT
```

   замените на

```
acl_smtp_rcpt = accept
```

   b. Строку

```
local_interfaces = MAIN_LOCAL_INTERFACES
```

   замените на

```
local_interfaces = 0.0.0.0
```

c. Строку

```
MAIN_HOST_LOOKUP = *
```

замените на

```
MAIN_HOST_LOOKUP =
```

d. Перед строкой

```
begin acl
```

добавьте строки

```
primary_hostname=<fqdn сервера>
recipients_max=100
message_size_limit=50M
MAIN_RELAY_NETS==127.0.0.0/8 ; 10.0.0.0/8 ; 192.168.0.0/16 ; 172.16.0.0/12
daemon_smtp_ports=25
```

e. После строки

```
begin routers
```

добавьте строки

```
forward_route:
  driver = manualroute
  domains = *
  self = send
  transport = remote_smtp_iwtm
  route_list = * 127.0.0.1::2025
  no_more
```

f. После строки

```
begin transports
```

добавьте строки

```
remote_smtp_iwtm:
  driver = smtp
  command_timeout = 10s
```

В качестве альтернативного варианта вы можете внести изменения в конфигурационный файл с помощью потокового текстового редактора **sed**, выполнив команды:

```
sed -i "s/acl_smtp_rcpt = MAIN_ACL_CHECK_RCPT/acl_smtp_rcpt = accept/g" /etc/exim4/
exim4.conf.template
sed -i "s/local_interfaces = MAIN_LOCAL_INTERFACES/local_interfaces = 0.0.0.0/g" /
etc/exim4/exim4.conf.template
sed -i "s/MAIN_HOST_LOOKUP = \*/MAIN_HOST_LOOKUP =/g" /etc/exim4/exim4.conf.template
sed -i "/begin acl/
iprimary_hostname=$HOSTNAME\nrecipients_max=100\nmessage_size_limit=50M\nMAIN_RELAY_
NETS==127.0.0.0/8 ; 10.0.0.0/8 ; 192.168.0.0/16 ;
172.16.0.0/12\ndaemon_smtp_ports=25" /etc/exim4/exim4.conf.template
sed -i "/begin routers/aforward_route:\n  driver = manualroute\n  domains = *\n
self = send\n  transport = remote_smtp_iwtm\n  route_list = * 127.0.0.1::2025\n
no_more" /etc/exim4/exim4.conf.template
sed -i "/begin transports/aremote_smtp_iwtm:\n  driver = smtp\n  command_timeout =
10s" /etc/exim4/exim4.conf.template
```

2. Перезапустите Exim4:

```
sudo systemctl restart exim4
```

3. Чтобы корректно принимать почту с различными мандатными метками:
   a. Директории `db`, `input` и `msglog`, расположенные в `/var/spool/exim4`, должны иметь следующие атрибуты:
   `drwxrwxrwxm-- 2 Debian-exim Debian-exim Уровень_3:Низкий:Нет:ccnr,ehole db`
   `drwxrwxrwxm-- 2 Debian-exim Debian-exim Уровень_3:Низкий:Нет:ccnr,ehole input`
   `drwxrwxrwxm-- 2 Debian-exim Debian-exim Уровень_3:Низкий:Нет:ccnr,ehole msglog`
   Для этого выполните команду:
   `sudo /usr/sbin/pdpl-file 3:::ccnr,ehole <имя директории>`
   b. В директории `db` создайте файлы со следующими привилегиями (или измените атрибуты существующих файлов):
   `-rw-r-----m-- 1 Debian-exim Debian-exim Уровень_3:Low:Нет:ehole retry.lockfile`
   `-rw-r-----m-- 1 Debian-exim Debian-exim Уровень_3:Low:Нет:ehole wait-remote_smtp`
   `-rw-r-----m-- 1 Debian-exim Debian-exim Уровень_3:Low:Нет:ehole wait-remote_smtp.lockfile`
   Для этого выполните команду:
   `sudo /usr/sbin/pdpl-file 3:::ehole <имя файла>`

Настройка пересылки скрытых копий Exim4

Для настройки пересылки скрытых копий создайте дополнительные файлы конфигурации:

1. Создайте файл конфигурации **/etc/exim4/conf.d/main/30_exim4-config_system_filter** со следующим содержимым:
```
# System wide filter:
    system_filter = /etc/exim4/conf.d/system.filter
    system_filter_user = Debian-exim
    system_filter_group = Debian-exim
    system_filter_reply_transport = bcc_transport
# System wide filter end.
```
2. Создайте файл фильтра **/etc/exim4/conf.d/system.filter**. В нем укажите домен почтового сервера, с которого нужно создавать скрытые копии, а также вспомогательный почтовый адрес со вспомогательным доменом:
```
# Exim filter
if first_delivery
 and ("$h_to:, $h_cc:, $h_bcc" contains "<почтовый_домен>")
 or ("$h_from:" contains "<почтовый_домен>")
then
 unseen deliver "bcc@<вспомогательный_домен>"
endif
```
3. Создайте маршрут для вспомогательного домена **/etc/exim4/conf.d/router/120_exim4-config_iwtm_route** со следующим содержимым:
```
iwtm_route:
  driver = manualroute
  domains = <вспомогательный_домен>
  transport = bcc_transport
  route_list = * <IP-адрес_сервера_Traffic_Monitor>::<порт>
```

> **Примечание:**
>
> Укажите значение порта **25** для отправки копий на сервер Exim4 в системе Traffic Monitor.
> Укажите значение порта **2025** для отправки копий в Traffic Monitor через SMTPD.

4. Создайте описание транспорта `bcc_transport`, используемого для доставки сообщений. Нужно создать файл **/etc/exim4/conf.d/transport/30_exim4-config_bcc_transport** со следующим содержимым:
```
bcc_transport:
  driver = smtp
  command_timeout = 10s
```
5. Для обновления и перезапуска Exim4 выполните команды:
```
sudo update-exim4.conf
sudo /etc/init.d/exim4 restart
```
6. Чтобы корректно пересылать почту с различными мандатными метками:
   a. Директории `db`, `input` и `msglog`, расположенные в `/var/spool/exim4`, должны иметь следующие атрибуты:
```
drwxrwxrwxm-- 2 Debian-exim Debian-exim
Уровень_3:Низкий:Нет:ccnr,ehole db
drwxrwxrwxm-- 2 Debian-exim Debian-exim
```

`Уровень_3:Низкий:Нет:ccnr,ehole input`
`drwxrwxrwxm-- 2 Debian-exim Debian-exim`
`Уровень_3:Низкий:Нет:ccnr,ehole msglog`
Для этого выполните команду:
`sudo /usr/sbin/pdpl-file 3:::ccnr,ehole <имя директории>`

b. В директории `db` создайте файлы со следующими привилегиями (или измените атрибуты существующих файлов):
`-rw-r-----m-- 1 Debian-exim Debian-exim Уровень_3:Низкий:Нет:ehole retry`
`-rw-r-----m-- 1 Debian-exim Debian-exim Уровень_3:Низкий:Нет:ehole retry.lockfile`
`-rw-r-----m-- 1 Debian-exim Debian-exim Уровень_3:Низкий:Нет:ehole wait-bcc_transport`
`-rw-r-----m-- 1 Debian-exim Debian-exim Уровень_3:Низкий:Нет:ehole wait-bcc_transport.lockfile`
Для этого выполните команду:
`sudo /usr/sbin/pdpl-file 3:::ehole <имя файла>`

4.5.2 Прием объектов, перехваченных InfoWatch Device Monitor

1. Установите и настройте серверную часть Traffic Monitor (см. *InfoWatch Traffic Monitor. Руководство по установке. Установка InfoWatch Traffic Monitor*).
2. Настройте передачу событий из Device Monitor на сервер Traffic Monitor (см. *InfoWatch Device Monitor (Windows). Руководство пользователя. Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor* или *InfoWatch Device Monitor (Linux). Руководство пользователя. Серверы DM*).
3. Настройте параметры анализа объектов (см. *InfoWatch Traffic Monitor. Руководство пользователя. Раздел "Технологии"*).

4.6 Автозапуск процессов

В этом разделе описаны особенности автозапуска процессов Системы, а именно:

- *Проверка автозапуска процессов*
- *Включение и выключение автозапуска процессов*

Общая информация о работе с процессами изложена в разделе *Процессы серверной части Traffic Monitor*.

4.6.1 Проверка автозапуска процессов

Важно!

Отключите автозапуск нелицензированных процессов, отвечающих за перехват трафика. Это позволит уменьшить количество сообщений в журнале протоколирования.

Примечание:

О включении и выключении автозапуска процессов см. *Включение и выключение автозапуска процессов*.

При логическом выделении основного сервера, сервера перехвата, сервера с БД и сервера с веб-консолью убедитесь, что автозапуск процессов настроен в соответствии с указаниями в таблице.

Автозапуск должен быть включен только для процессов, которые необходимы данному экземпляру сервера Traffic Monitor для корректной работы:

Процесс	По умолчанию автозапуск включен
`iw_adlibitum`	Да **Примечание:** Процесс должен работать только на основном сервере.
`iw_agent`	Да
`iw_analysis`	Да
`iw_kicker`	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью.
`iw_blackboard`	Да
`iw_bookworm`	Да
`iw_capstack`	Нет
`iw_cas`	Да
`iw_configerator`	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью.
`iw_deliver`	Да **Примечание:** Процесс должен работать только на основном сервере.
`iw_icap`	Да
`iw_is`	Да **Примечание:** Процесс должен работать только на основном сервере.
`iw_indexer`	Да **Примечание:** Процесс должен работать только на основном сервере.

Процесс	По умолчанию автозапуск включен
`iw_image_autoling`	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью.
`iw_text_autoling`	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью.
`iw_licensed`	Да
`iw_luaengined`	Да
`iw_messed`	Да
`iw_pas`	Да

`iw_proxy_http`
`iw_proxy_icq`
`iw_proxy_smtp`
	Нет

`iw_qmover_client`	Нет
`iw_qmover_server`	Нет
`iw_sample_compiler`	Да
`consul`	Да
`iw_smtpd`	Да
`iw_system_check`	Да
`iw_tech_tools`	Да
`iw_updater`	Да
`iw_warpd`	Да
`iw_x2x`	Да
`iw_x2db`	Да

Процесс	По умолчанию автозапуск включен
`iw_xapi_xapi` `iw_xapi_puppy`	Да
`iw_space_manager`	Да **Примечание:** Процесс должен работать только на сервере с БД.
`iw_attributor`	Нет
`iw_rest2push`	Нет **Примечание:** нужно запустить процесс вручную. Подробнее см. *Включение и выключение автозапуска процессов*.

Чтобы проверить, для каких процессов включен автозапуск, используйте команду:

```
iwtm status
```

Команда выведет список всех процессов Traffic Monitor с их статусами. В поле `enabled state` указан статус автозапуска:

- `loaded (enabled)` – автозапуск процесса включен;
- `loaded (disabled)` – автозапуск процесса выключен;
- `loaded (static)` – статический режим, включение зависит от настроек процесса;
- `masked (masked)` или `masked (bad)` – сервис замаскирован, автозапуск выключен.

Чтобы проверить статус автозапуска для отдельного процесса, используйте команду:

```
iwtm status <имя_процесса>
```

Примечание:

Чтобы удалить с сервера все процессы `iw_kicker`, удалите пакет `iwtm-web-meta`:

```
rpm -e iwtm-web-meta
```

4.6.2 Включение и выключение автозапуска процессов

Чтобы включить/выключить автозапуск процесса, используйте команды:

- **Включение автозапуска процесса**

```
iwtm enable <имя_процесса>
```

- **Выключение автозапуска процесса**

```
iwtm disable <имя_процесса>
```

- **Включение автозапуска сразу нескольких процессов**

```
iwtm enable <имя_процесса1> <имя_процесса2> ... <имя_процессаN>
```

- **Выключение автозапуска сразу нескольких процессов**

```
iwtm disable <имя_процесса1> <имя_процесса2> ... <имя_процессаN>
```

- **Включение автозапуска сразу всех процессов**

```
iwtm enable all
```

- **Выключение автозапуска сразу всех процессов**

```
iwtm disable all
```

Пример включения/выключения службы `iw_proxy`:

Служба `iw_proxy` состоит из трех компонентов: `iw_proxy_http`, `iw_proxy_icq` и `iw_proxy_smtp`. Поэтому:

1. Для каждого процесса службы включите/выключите возможность автозапуска:
   - **Включение автозапуска**

```
iwtm enable iw_proxy_http iw_proxy_icq iw_proxy_smtp
```

   - **Выключение автозапуска**

```
iwtm disable iw_proxy_http iw_proxy_icq iw_proxy_smtp
```

2. Перезапустите процессы службы `iw_proxy`:

```
iwtm restart iw_proxy_http iw_proxy_icq iw_proxy_smtp
```

Все процессы Traffic Monitor со статусом `loaded ( enabled)` подлежат автозапуску, а процессы со статусом `masked (masked)` могут быть запущены только вручную.

Запуск процесса вручную

Чтобы запустить процесс вручную:

1. Смените статус процесса на `loaded ( enabled)` при помощи команды:

```
iwtm enable <имя_процесса>
```

2. Запустите процесс:

```
iwtm start <имя_процесса>
```

Чтобы настроить параметры автозапуска процесса:

1. Перейдите в директорию хранения unit-файлов `/usr/lib/systemd/system`.
2. Внесите изменения в unit-файл процесса и сохраните их. Подробнее см. *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*. *Описание конфигурационных и unit-файлов демонов Traffic Monitor*.
3. Перезагрузите конфигурацию при помощи команды:

```
systemctl daemon-reload
```

4. Добавьте настроенный процесс в автозапуск:

```
iwtm enable <имя_процесса>
```

5. Запустите процесс:

```
iwtm start <имя_процесса>
```

6. Проверьте, запустился ли процесс, одним из способов:
   - при помощи команды проверки статуса конкретного процесса:

     ```
     iwtm status <имя_процесса>
     ```

   - при помощи команды проверки статусов всех процессов:

     ```
     iwtm status
     ```

   В поле `Active` или в строке, относящейся к процессу, указан статус процесса:

   - `active (running)` – процесс запущен;
   - `inactive (dead)` – процесс не запущен.

4.7 Модуль взаимодействия с удаленной базой данных

Если схема развертывания Системы выбрана таким образом, что база данных, в которую передаются перехваченные объекты, находится на удаленном сервере, то нужно установить модуль взаимодействия с удаленной базой данных.

Удаленной считается база данных, установленная на отдельно стоящем сервере при помощи ключа установки **TME DB Server** или **TME All-in-one** (подробно о ключах установки см. *InfoWatch Traffic Monitor. Руководство по установке. Распределенная установка TM Enterprise*).

Стандартным процессом передачи данных в базу является **iw_x2db** (см. *Список процессов серверной части Traffic Monitor*). Использование модуля взаимодействия с удаленной базой данных дает дополнительную возможность регулировать:

- скорость передачи файлов в файловую очередь;
- расписание проходимости канала передачи файлов.

Настройка модуля взаимодействия с отдельно стоящей базой данных включает следующие задачи:

- *Настройка клиентской части модуля взаимодействия с удаленной БД*
- *Настройка серверной части модуля взаимодействия с удаленной БД*

4.7.1 Настройка сбора данных в филиальной сети

Если Система установлена в сети филиалов, то за отправку данных о перехваченных событиях и их получение на сервере Traffic Monitor отвечают службы:

- **iw_qmover_client** – пересылает данные из филиала;
- **iw_qmover_server** – принимает данные в головном отделении.

По умолчанию данные службы отключены и запускаются Офицером безопасности вручную из Консоли управления Traffic Monitor:

- **iw_qmover_server** – в первую очередь;
- **iw_qmover_client** – во вторую очередь.

Их конфигурация настраивается в соответствующих конфигурационных файлах директории `/opt/iw/tm5/etc`: **qmover_client.conf** и **qmover_server.conf** (подробнее см. *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам. qmover_client.conf и iw_qmover_client.service* и *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам. qmover_server.conf и iw_qmover_server.service*).

4.7.2 Настройка клиентской части модуля взаимодействия с удаленной БД

Настройка общих параметров

1. Настройте следующие параметры клиента в конфигурационном файле **qmover_client.conf**, расположенном в директории `/opt/iw/tm5/etc`:

Параметр	Описание
`ListenerIP`	IP-адрес сервера (служба **qmover_server**).
`Port`	Порт сервера (центральный офис).

`NookDir`	Рабочий каталог службы **qmover_server**.
`ChannelWidth`	Ширина полосы пропускания канала, скорость закачки данных в Traffic Monitor (Кб/с). Может быть неявно ограничена параметром `WindowSize`

2. Перезапустите Traffic Monitor:
   `iwtm restart`

Настройка автозапуска процессов

- Включите автозапуск для процесса **iw_qmover_client**.
- Отключите автозапуск для процессов **iw_x2db**, **iw_x2x**, **iw_deliverd** и **iw_adlibitum**.

Подробнее о включении и выключении автозапуска процессов см. *Включение и выключение автозапуска процессов*.

Изменение ширины полосы пропускания для канала передачи данных

По умолчанию полоса пропускания имеет ширину 256 Кб/с. Но вы можете настроить автоматическое изменение полосы пропускания в различные периоды времени. Для этого используется утилита **iw_qmover_channel_width_setter**.
Допускается изменение ширины полосы пропускания. Минимальная ширина – 10 Кб/с. Максимальная ширина не установлена, но рекомендуемое максимальное значение – 2 Мб/с.

Чтобы настроить ограничения на ширину полосы пропускания
Запустите утилиту с обязательными параметрами:
`iw_qmover_channel_width_setter <unix_socket_name> <полоса_пропускания>`, где:

- `unix_socket_name` – имя сокета (автоматически создается при запуске на время выполнения службы, при завершении службы автоматически удаляется). Значение по умолчанию – `/opt/iw/tm5/run/.channel_socket`;
- `полоса_пропускания` – ширина полосы пропускания, в Кб/с, которую нужно установить.

Пример
Есть канал с полосой пропускания 256 Кб/с. Нужно, чтобы в период с 9.00 до 18.00 канал был занят на 50%. А с 18.00 до 9.00 – на 100%.
Рассчитайте ширину полосы пропускания, исходя из загрузки вашего канала. В этом примере ширина полосы пропускания для разных интервалов времени составляет:

Интервал	**Ширина полосы пропускания**	
	Процент от ширины канала	В пересчете на Кб/с
С 9.00 до 18.00	50%	128
С 18.00 до 9.00	100%	256

Добавьте в /**etc/crontab** команды:

```
00 9 * * * iwtm /opt/iw/tm5/bin/iw_qmover_channel_width_setter /opt/iw/tm5/run/.channel_socket 128
 00 18 * * * iwtm /opt/iw/tm5/bin/iw_qmover_channel_width_setter /opt/iw/tm5/run/.channel_socket 256
```

4.7.3 Настройка серверной части модуля взаимодействия с удаленной БД

Настройка конфигурации

Настройте следующие параметры клиента в конфигурационном файле **/opt/iw/tm5/etc/qmover_server.conf**. Директория, в которой хранится очередь объектов – `/opt/iw/tm5/queue/db`. Для этого:

1. Укажите IP-адрес обслуживаемого агента (филиал) в параметре `IP`.
2. Укажите порт, на котором сервер прослушивает объекты, поступающие от агентов, в параметре `Port`.

> **Важно!**
>
> При изменении параметров филиалов (изменение количества филиалов или их IP-адресов) следует внести изменения в файл **qmover_server.conf**.

Настройка автозапуска

Включите автозапуск для процесса **iw_qmover_server** (подробнее о включении и выключении автозапуска процессов см. *Включение и выключение автозапуска процессов*).

4.8 Настройка OCR-экстракторов

Настройка OCR для различных перехватчиков производится в конфигурационных файлах:

- **чтобы включить OCR для анализа перехваченных изображений**, внесите изменения в файл `/opt/iw/tm5/etc/warpd.conf`. В секции `Warp` задайте параметру `EnableOCR` значение `true`.
- **чтобы включить OCR для анализа изображений, загружаемых в качестве эталонных документов**, внесите изменения в файл `/opt/iw/tm5/etc/sample_compiler.conf`. Задайте параметру `EnableOCR` значение `true`.

Чтобы настроить OCR для каналов перехвата, используйте файл `/opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml`. Уровни настроек перечислены от более низкого приоритета к более высокому:

- на уровне сервиса;
- на уровне типа события для конкретного сервиса;
- на уровне протокола для конкретного типа события.

Подробнее о настройках см. *Настройка использования OCR*.

После того, как вы внесли изменения в файлах, перезапустите сервисы Traffic Monitor:

```
iwtm restart
```

> **Примечание:**

В случае распределенной установки Traffic Monitor на несколько серверов задайте настройки включения OCR для каждого сервера отдельно.

Примечание:

Если с помощью SDK был зарегистрирован новый тип событий, то к нему применяются настройки для сервиса, к которому относится данный тип события. Если зарегистрирован новый протокол, для него действуют настройки типа события, к которому относится данный протокол.

Каналы перехвата

В таблице ниже перечислены каналы перехвата, для анализа событий из которых в Traffic Monitor может использоваться OCR.

Сервис	Тип события	Протокол
Почта	Электронная почта	POP3 SMTP IMAP
	Веб-почта	HTTP HTTPS
Интернет-активность	Веб-сообщение	HTTP HTTPS
Хранение	Data Discovery	-

4.8.1 Поддерживаемые OCR-экстракторы

При установке Traffic Monitor с помощью инсталлятора на серверную часть Системы устанавливаются оба OCR-экстрактора и для использования выбирается один из них:

- Content AI ContentReader Engine 12
- Tesseract 4.1.1

Если вы выбрали Content AI ContentReader Engine, нужно *добавить лицензию вручную.*

Различия в функциональности экстракторов приведены в таблице ниже:

Функциональность	Content AI ContentReader Engine	Tesseract
Распознавание углов поворота изображения	0(+/-20), 90(+/-20), 180(+/-20) и 270(+ /-20) градусов	-

Функциональность	Content AI ContentReader Engine	Tesseract
Распознавание цветного изображения	+	-
Коррекция изображения	+	-
Рекомендуемое разрешение изображения	300 DPI для текста с размером шрифта от 10pt 400–600 DPI для текста с размером шрифта 9pt и меньше	300 DPI для текста с размером шрифта от 10pt 400–600 DPI для текста с размером шрифта от 9pt и меньше

Примечание:

Чтобы избежать больших отклонений от рекомендуемого разрешения изображения, при работе экстрактора Content AI ContentReader Engine используется параметр `AutoOverwriteResolution` (со значением `true` по умолчанию). Он позволяет автоматически определять разрешение изображения.

Настройки Tesseract

Включение экстрактора

Чтобы включить использование экстрактора Tesseract:

1. Удалите символьную ссылку `/opt/iw/tm5/bin/iw_image2text`.
2. Создайте символьную ссылку:

```
ln -s /opt/iw/tm5/bin/iw_image2text_ts /opt/iw/tm5/bin/iw_image2text
```

Ограничение размера изображения

Чтобы изменить ограничение на размер пересылаемого изображения:

1. Перейдите в директорию `/opt/iw/tm5/etc/image2text_ts.conf`.
2. Отредактируйте параметры `MaxSizeInKb` (верхняя граница) и `MinSizeInKb` (нижняя граница). По умолчанию установлено 1536 КБ и 40 КБ соответственно.

Применение OCR только к событиям облачного хранилища

Чтобы включить OCR только для событий облачного хранилища:

1. Откройте справочник `/opt/iw/tm5/etc/config/bookworm/services.xml` и найдите соответствующие для облачного хранилища параметры `mnemo` и `key`.
   Например:

```
object_type mnemo="cloud_storage"

key="AA9DFB259F0DFEE040BADC95815E13A200000000"
```

2. Скопируйте значения параметров `key` и `mnemo` и вставьте в `/opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml`

Настройки Content AI ContentReader Engine

Настройка лицензии

Для того, чтобы настроить лицензию Content AI ContentReader Engine:

1. Введите полученные серийный номер и пароль в конфигурационный файл `image2text_fre.conf`, расположенный в директории `/opt/iw/tm5/etc`:
   - в поле `SerNum` введите серийный номер;
   - в поле `Pwd` введите пароль.
2. Скопируйте полученный файл с лицензией (формат `.LocalLicense`) в директорию `/var/lib/Content_AI/SDK/12/Licenses`.
3. Убедитесь, что у пользователя `iwtm` есть права на доступ к скачанному файлу.
4. Перезапустите сервис `iw_warpd`.

Включение экстрактора

Чтобы настроить на работу экстрактор Content AI ContentReader Engine:

1. Удалите символьную ссылку `/opt/iw/tm5/bin/iw_image2text`.
2. Создайте символьную ссылку:

```
ln -s /opt/iw/tm5/bin/iw_image2text_fre /opt/iw/tm5/bin/iw_image2text
```

Быстрый режим обработки документов

Экстрактор Content AI ContentReader Engine может работать в двух режимах:

- сбалансированный – предусматривает максимально качественную обработку изображений. Этот режим включен по умолчанию. Настройки его пользовательского профиля находятся в файле `/opt/iw/tm5/etc/ CRProfile.ini`;
- быстрый – позволяет максимально быстро обработать изображения. При синтезе документа одновременно загружается 64 страницы. Настройки пользовательского профиля находятся в файле `/opt/iw/tm5/etc/CRProfile_fast.ini`.
  При необходимости этот режим можно настроить вручную.
  В быстром режиме включены:
  - быстрый режим определения ориентации страниц (качество снижено);
  - стандартный анализ страницы, без подбора шаблонов;
  - игнорирование теней;
  - обнаружение таблиц во время анализа;
  - быстрое извлечение объектов (качество снижено).

  В быстром режиме выключены:

- балансировочный режим;
- обработка изображений, как фото;
- сжатие изображений;
- использование бинаризации изображений;
- детектирование параметров шрифта;
- удаление мусора с изображения;
- удаление шумов с временного изображения;
- детектирование "пористого" текста;
- распознавание всего текста на изображении, включая текст в самих изображениях;
- извлечение из изображения всего возможного текста;
- детектирование заголовков;
- детектирование сносок;
- детектирование оглавления;
- детектирование колонтитулов;
- детектирование страниц документа.

Чтобы активировать быстрый режим обработки документов, в конфигурационном файле **`image2text_fre.conf`**, расположенном в директории `/opt/iw/tm5/etc`, укажите путь до файла с настройками пользовательского профиля в параметре `"Profile":"etc/CRProfile_fast.ini"` и сохраните изменения.

> **Важно!**
>
> Оптимизация скорости обработки документов недоступна для скан-копий схем, карт местности и монохромных изображений.

Ограничение размера изображения

Чтобы изменить ограничение на размер пересылаемого изображения:

1. Перейдите в директорию `/opt/iw/tm5/etc/` **`image2text_fre.conf`**.
2. Отредактируйте параметры `MaxSizeInKb` (верхняя граница) и `MinSizeInKb` (нижняя граница). По умолчанию установлено 1536 КБ и 40 КБ соответственно.

Применение OCR только к событиям облачного хранилища

Чтобы включить OCR только для событий облачного хранилища:

1. Откройте справочник `/opt/iw/tm5/etc/config/bookworm/`**`services.xml`** и найдите соответствующие для облачного хранилища параметры `mnemo` и `key`. Например:

```
object_type mnemo="cloud_storage"

key="AA9DFB259F0DFEE040BADC95815E13A200000000"
```

2. Скопируйте значения параметров `key` и `mnemo` и вставьте в `/opt/iw/tm5/etc/config-perm/bookworm/`**`ocr_custom.xml`**

4.9 Настройка отправки уведомлений пользователям и сотрудникам

Пользователь Консоли управления может настроить отправку уведомлений из Системы пользователю или сотруднику. Чтобы Система могла отправлять уведомления, нужно:

- указать Системе электронный адрес, с которого будут отправляться уведомления – электронные сообщения пользователям или сотрудникам;
- настроить отправку писем через почтовый сервер Exim.

Уведомления отправляются в результате срабатывания тех или иных правил в политиках (подробнее см. *InfoWatch Traffic Monitor. Руководство пользователя*).

Чтобы проверить, отправляются ли письма через почтовый сервер
Выполните команду:
`sendmail -v <employee@company.com> < <sample.log>`
где:

- `<employee@company.com>` – почтовый адрес пользователя, которому будет отправлено уведомление;
- `<sample.log>` – текстовый файл, содержимое которого будет служить текстом письма (для проверки рекомендуем использовать простой текстовый файл размером до 1 МБ).

4.10 Ограничение количества найденных событий

Вы можете указать ограничение для количества событий, которые будут выведены в Консоли управления в результате применения фильтра. Для этого в таблице *SETTING* базы данных укажите требуемое значение для атрибута *query_stop_count*. По умолчанию задано ограничение 10 000.

4.11 Настройка межсервисного взаимодействия (служба Consul)

Для регистрации сервисов, мониторинга доступности и обнаружения компонентов Traffic Monitor используется децентрализованный отказоустойчивый discovery-сервис Consul. Агент Consul:

- устанавливается на каждый хост и является полноправным участником кластера;
- обнаруживает сервисы, собирает данные об их состоянии, реализуют интерфейсы DNS, API HTTP и RPC CLI;
- может быть запущен в одном из двух режимов: клиентском или серверном.

Consul используется во всех типах установки. Сведения о режимах установки Системы приведены в документе *InfoWatch Traffic Monitor. Руководство по установке. Схемы развертывания Системы и выбор типа установки*.

При схеме установки Системы All-in-one конфигурирование параметров подключения к службе Консул осуществляется автоматически при установке. Исключение составляет распределенная установка, когда компоненты Traffic Monitor и база данных установлены на разных серверах (Система установлена на более чем одну ноду и имеет более одного сетевого интерфейса). Информацию по настройке см. в статье *Конфигурирование Consul и создание кластера*.

Настройка работы службы осуществляется в конфигурационном файле по пути `/opt/iw/tm5/etc/consul/consul.json`. Полное описание параметров можно посмотреть на странице *Конфигурационный файл consul.json и unit-файл iwtm-consul.service*.

4.11.1 Запуск и остановка службы

Для запуска службы Consul используется любая из команд:

- ```
  service iwtm-consul start
  ```
- ```
  systemctl start iwtm-consul.service
  ```

Для остановки службы Consul используются команды:

- ```
  service iwtm-consul stop
  ```
- ```
  systemctl stop iwtm-consul.service
  ```

Ручной запуск агента Consul при необходимости может быть осуществлен следующим способом:

```
consul agent -data-dir=<path> -bind=<bind_addr> -bootstrap -server -ui
```

где:

- `<path>` – путь до директории со служебными данными (например: `/opt/iw/tm5/var/consul`);
- `<bind>` – адрес сетевого интерфейса.

Если в Системе больше одного сетевого интерфейса, укажите один параметр (на выбор):

- `-bind=<ip-адрес>`;
- `-config-file` или `-config-dir` – путь к конфигурационному файлу (например: `/opt/iw/tm5/etc/consul`).

При загрузке нескольких конфигурационных файлов их опции будут объединены.

4.11.2 Регистрация сервисов в Consul

Сервис можно зарегистрировать в Consul двумя способами:

- использовать HTTP API или конфигурационный файл агента, если сервис может общаться с Consul самостоятельно;
- зарегистрировать сервис как внешний компонент.

Сервисы с обязательной регистрацией в Consul	Сервисы, установленные на нодах с присутствием Consul Server или Consul Client
iw_adlibitum iw_agent	iw_adlibitum iw_agent

Сервисы с обязательной регистрацией в Consul	Сервисы, установленные на нодах с присутствием Consul Server или Consul Client
iw_analysis	iw_analysis
iw_blackboard	iw_bookworm
iw_bookworm	iw_capstack
iw_capstack	iw_cas
iw_cas	iw_configerator
iw_icap	iw_icap
iw_deliver	iw_indexer
iw_indexer	iw_licensed
iw_licensed	iw_kicker
iw_luaengined	iw_luaengined
iw_messed	iw_messed
iw_pas	iw_pas
iw_proxy_http	iw_proxy_http
iw_proxy_icq	iw_proxy_icq
iw_proxy_smtp	iw_proxy_smtp
iw_qmover_server	iw_qmover_server
iw_sample_compiler	iw_sample_compiler
iw_system_check	iw_system_check
iw_smtpd	iw_smpd
iw_tech_tools	iw_tech_tools
iw_updater	iw_updater
iw_warpd	iw_warpd
iw_xapi_xapi	iw_xapi_xapi
iw_xapi_puppy	iw_xapi_puppy
iw_x2x	iw_x2x
iw_x2db	iw_x2db
	Web GUI

После регистрации взаимодействие между сервисами Traffic Monitor и Consul осуществляется по сценарию:

- регистрация при помощи клиента Consul;
- установление TCP-соединения или возврат HTTP-кода;
- дерегистрация.

Клиент Consul получает от сервера список доступных для подключения компонентов Traffic Monitor.

4.11.3 Распределенная установка

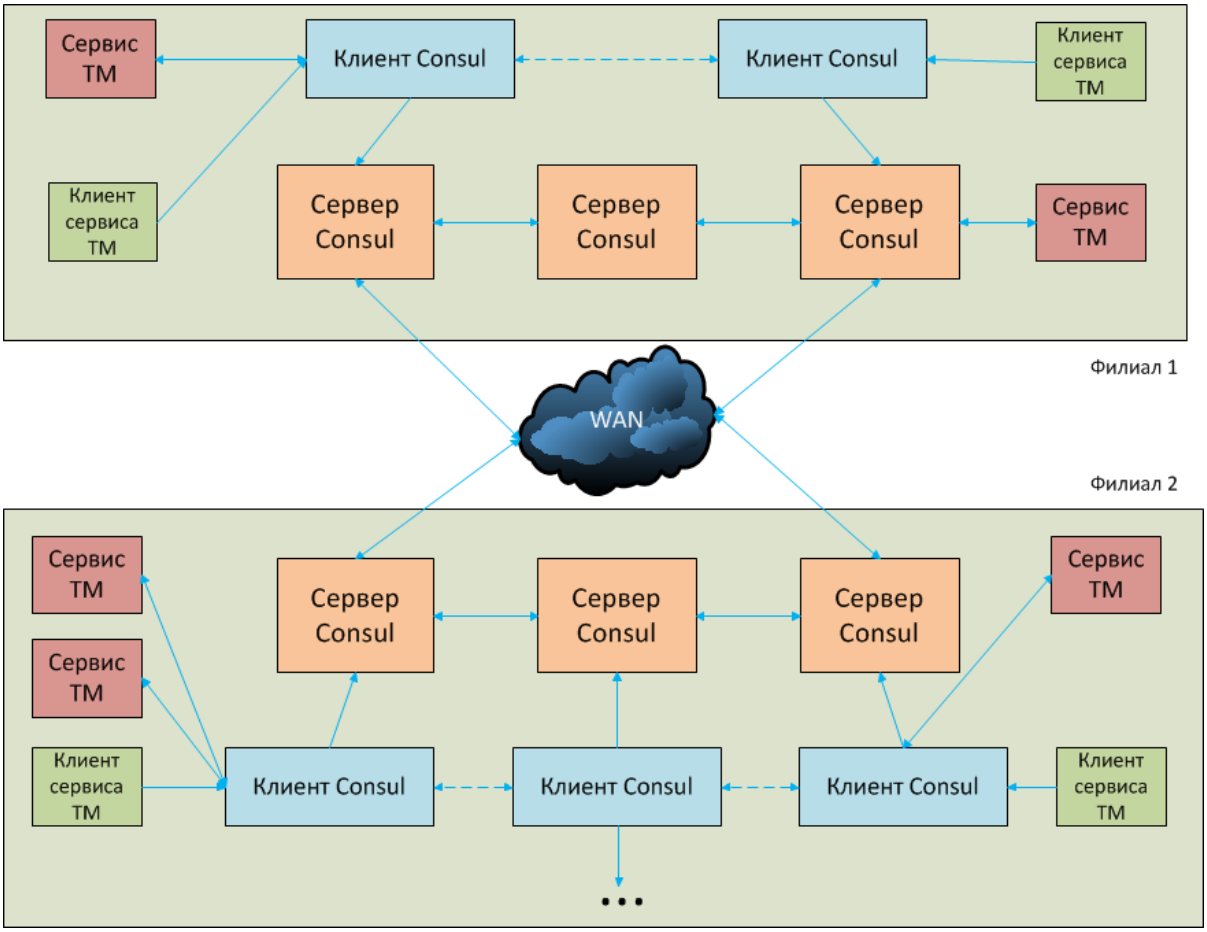
> **Важно!**
>
> Для использования Consul нужно реализация full-mesh топологии сети (соединение "каждый с каждым") всех агентов внутри кластера, а также серверов при объединении их в WAN.

Кластеризация

Агент собирает данные об узле и сервисе и отсылает их серверу. Компоненты Системы в поиске сервисов обращаются с запросом к агенту, запущенному на локальном компьютере, который пересылает его доступному серверу. Если сервер не в состоянии ответить на запрос, он может направить его в другой дата-центр (филиал) и вернуть полученный ответ.

Серверы образуют кластер и самостоятельно назначают сервер-Лидер, отвечающий за координацию элементов в кластере. Первый/единственный сервер обычно запускается в bootstrap-режиме (назначается лидером вручную). При старте агента для присоединения к кластеру достаточно указать один сервер этого кластера. При его конфигурировании в опции `retry_join` рекомендуем указывать все серверы кластера. Кворум для проведения операций и обеспечения согласованности требуется в каждом дата-центре. При наличии нескольких дата-центров в каждом создается отдельный кластер. Дата-центры не изолированы друг от друга в рамках задачи обнаружения сервисов. Агент в одном дата-центре может получить информацию из другого дата-центра.

Сеть Consul может использовать один сервер, но мы рекомендуем использовать от трех до семи серверов в дата-центре, чтобы избежать потери данных.



Пример:

Кластер из трех узлов (серверов) сохраняет свою работоспособность при выходе из строя одного сервера.

Примеры использования интерфейса командной строки:

Команда	Описание
`consul members`	Вывод списка членов кластера.
`consul catalog services -node <имя_ноды>`	Вывод списка сервисов кластера на конкретном компьютере.
`consul operator raft list-peers -stale=true`	Вывод списка всех серверов даже в случае развала кластера.

Присоединение к кластеру

Регистрация дополнительных нод на кластере возможна любым из указанных способов:

- введите команду:

```
consul join <ip-адрес>
```

  При этом убедитесь, что в конфигурационном файле `consul.json` у всех серверов и клиентов Consul совпадают параметры `datacenter` и `encrypt` (см. *Конфигурационный файл consul.json и unit-файл iwtm-consul.service*)
- в конфигурационном файле `consul.json` в параметре `retry_join` укажите список всех серверов, к которым нужно присоединиться.

4.11.4 Настройка сетевых правил доступа в Consul

Для установки сетевого обмена нужно, чтобы следующие порты между всеми агентами Consul (серверами и клиентами) были открыты.

Порт по умолчанию	Интерфейс	Поддерживаемые протоколы	Описание
8300	Server RPC	TCP	Используется серверами для обработки входящих запросов от других агентов.
8301	Serf LAN	TCP, UDP	Используется агентами для обработки потоков данных в локальной сети.
8302	Serf WAN	TCP, UDP	Используется серверами для обмена данными по WAN с другими серверами.
8400	CLI RPC	TCP	Используется всеми агентами для обработки RPC из CLI.
8500	HTTP API	TCP	Используется клиентами для взаимодействия с интерфейсом HTTP API.
8600	DNS	TCP, UDP	Используется для разрешения DNS-запросов.

4.11.5 Конфигурационный файл consul.json и unit-файл iwtm-consul.service

Конфигурационный файл **`consul.json`**

Содержимое	Описание
`{`	

Содержимое	Описание
`"bootstrap_expect": 1,`	Количество ожидаемых серверов в кластере (только для режима сервера).
`"server": true,`	Запуск агента в режиме сервера (`false` – в режиме клиента).
`"datacenter": "iwtm",`	Название дата-центра.
`"data_dir": "/opt/iw/tm5/var/consul",`	Директория для служебных данных Consul.
`"encrypt": "4RTZ5ttYY6RwIYX28XWNPw==",`	Секретный ключ, разделяемый между агентами кластера.
`"log_level": "WARN",`	Уровень логирования.
`"enable_syslog": true,`	Разрешить логирование в `syslog`.
`"disable_update_check": true,`	Запрет проверки на наличие обновлений Consul.
`"leave_on_terminate": false,`	Если `true`, то при получении SIGTERM рассылает прощальное сообщение и покидает кластер в штатном порядке. По умолчанию: для сервера – `false`, для клиента – `true`.
`"skip_leave_on_interrupt": true,`	Если `false`, то при получении сигнала прерывания (например, SIGINT) покидает кластер в штатном порядке. По умолчанию: для сервера – `true`, для клиента – `false`.
`"rejoin_after_leave": true,`	Если `true`, то присоединяется к кластеру при старте.
`"limits": {`	Секция ограничений.
`"http_maxconns_per_client": 500`	Максимально возможное число HTTP(S)-соединений от одного клиента.
`},`	
`"retry_join": "0.0.0.0",`	В случае распределенной установки содержит список серверов, к которым надо присоединиться.
`"ui_config": {`	Секция настроек веб-интерфейса.

Содержимое	Описание
`  "enabled": false`	Доступ к веб-интерфейсу (по умолчанию запрещен).
`  },`	
`  "client_addr": "0.0.0.0"`	IP клиента, к которому открыт доступ по веб-интерфейсу.
`}`	

Unit-файл **`iwtm-consul.service`**

Код	Описание
`[Unit]`	Раздел для определения метаданных демона и настройки его взаимодействия с другими демонами.
`Description=Consul Service discovery agent`	Название демона.
`Requires=network-online.target`	Сервисы не могут работать без `network-online.target`.
`After=network-online.service`	Демоны, которые будут запущены до запуска текущего демона.
`[Service]`	Раздел настройки запуска демона.
`StandartOutput=syslog`	Перенаправление стандартного вывода в `syslog`.
`StandartError=syslog`	Перенаправление стандартного вывода ошибок в `syslog`.
`Type=simple`	Тип запуска демона. `simple` – демон запускается и переходит в режим ожидания на консоли.
`User=iwtm`	Имя пользователя, от которого осуществляется запуск демона.
`Group=iwtm`	Имя группы пользователя.

Код	Описание
`SyslogIdentifier=iwtm-consul`	Устанавливает имя процесса для префиксных строк журнала, отправленных в систему ведения журнала или в буфер журнала ядра.
`PermissionsStartOnly=true`	Запуск команд из `ExecStartPre` от имени пользователя **`root`**.
`ExecStartPre=/opt/iw/tm5/bin/consul validate /opt/iw/tm5/etc/consul`	Полный путь и аргументы команды, которые должны быть выполнены до запуска основного процесса.
`ExecStart=/opt/iw/tm5/bin/consul agent $OPTIONS -config -dir= /opt/iw/tm5/etc/consul`	Полный путь и аргументы команды, которая должна быть выполнена для запуска демона. Запускается от имени пользователя, указанного в `User`.
`ExecReload=/bin/kill -s SIGHUP $MAINPID`	Команда для перезагрузки конфигурации демона, если она доступна. Запускается от имени пользователя, указанного в `User`.
`KillSignal=SIGINT`	Команда, по которой можно принудительно завершить работу демона.
`TimeoutStopSec=5`	Время, в течение которого система будет ждать остановки демона, прежде чем пометить его как недоступный или завершенный принудительно.
`[Install]`	Определение поведения демона, если он включен или отключен.
`WantedBy=multi-user.target`	Запускать этот демон, когда система грузится в `multi-user` режиме.

4.12 Рекомендации по настройке безопасного окружения

Компоненты Traffic Monitor используют различные сетевые порты на серверах Системы.

> **Примечание:**
>
> Подробнее о наборах компонентов и шаблонах на серверах Системы см. *InfoWatch Traffic Monitor. Руководство по установке. Схемы развертывания Системы и выбор типа установки*.

О процессах на серверах Traffic Monitor см. *Процессы серверной части Traffic Monitor*.

Чтобы предотвратить несанкционированный доступ к компонентам, рекомендуется настроить сетевой экран. Должны быть разрешены только те соединения, которые нужны для работы компонентов.

4.12.1 Порты компонентов

Порт	Взаимодействие между компонентами		Назначение порта
	Источник	Получатель	
Уникальные порты, необходимые для работы Traffic Monitor			
TCP 9100	Сервер Device Monitor	Сервер Traffic Monitor	Передача теневых копий на анализ из Device Monitor.
	Сервер Data Discovery	Сервер Traffic Monitor	Передача объектов на анализ из Data Discovery.
TCP 40731	Сервер Traffic Monitor с компонентом "Перехватчики"	Сервер Data Storage	Передача данных для хранения в Data Storage.
	Сервер Traffic Monitor с компонентом "Веб-консоль"	Сервер Data Storage	Получение данных от Data Storage для доступа к ним в веб-интерфейсе.
TCP 30050	Сервер Traffic Monitor	Сервер Data Analysis Service	Протокластеризация текстовых данных с помощью сервиса Data Analysis Service.
TCP 9101	Сервер со специализированным коннектором	Сервер Traffic Monitor	Передача объектов на анализ с помощью Push API. Специализированный коннектор с использованием программного интерфейса Push API может быть создан для передачи объектов с серверов, работающих по неподдерживаемым протоколам обмена, например разработанным заказчиком.
	Адаптер Lotus Domino	Сервер Traffic Monitor	Передача объектов на анализ с помощью адаптера Lotus Domino.

Порт	Взаимодействие между компонентами		Назначение порта
	Источник	Получатель	
	Адаптер MS Lync	Сервер Traffic Monitor	Передача объектов на анализ с помощью адаптера MS Lync.
	Адаптер Smart Logger	Сервер Traffic Monitor	Передача объектов на анализ с помощью адаптера Smart Logger.
	Адаптер MS ActiveSync	Сервер Traffic Monitor	Передача объектов на анализ с помощью адаптера ActiveSync.
Порты, необходимые для работы Traffic Monitor при распределенной установке			
TCP 5433	Сервер Traffic Monitor	БД сервера Traffic Monitor	Соединение с СУБД PostgreSQL Traffic Monitor.
TCP 8300	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Consul (RPC).
TCP 8301	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Consul (Serf LAN).
UDP 8301	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Consul (Serf LAN).
TCP 8302	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Consul (Serf WAN).
UDP 8302	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Consul (Serf WAN).
TCP 8400	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Consul (CLI RPC).
TCP 8500	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Consul (HTTP API).
TCP 8600	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Consul (DNS-интерфейс).
TCP 9997	Сервер Traffic Monitor	Сервер Traffic Monitor	Соединение службы Consul с ICAP.

Порт	Взаимодействие между компонентами		Назначение порта
	Источник	Получатель	
TCP 9998	Сервер Traffic Monitor	Сервер Traffic Monitor	Соединение службы Consul с Analysis.
TCP 9999	Сервер Traffic Monitor	Сервер Traffic Monitor	Соединение службы Consul с Messed.
TCP 9090	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Bookworm.
TCP 9091	Консоль управления Traffic Monitor	Сервер Traffic Monitor	Служба Sample Compiler.
TCP 9093	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Blackboard.
TCP 9095	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Licensed.
TCP 9096	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Adlibitum.
TCP 9097	Консоль управления Traffic Monitor	Сервер Traffic Monitor	Служба System Check.
TCP 9099	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Agent.
TCP 9102	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Tech Tools.
TCP 9250	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба X2X.
TCP 9306	Консоль управления Traffic Monitor	БД сервера Traffic Monitor	Соединение с БД индексации.
TCP 9310	Консоль управления Traffic Monitor	БД сервера Traffic Monitor	Соединение с БД индексации.

Порт	Взаимодействие между компонентами		Назначение порта
	Источник	Получатель	
TCP 9987	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба CAS.
TCP 9988	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Luaengined.
TCP 9989	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба PAS.
TCP 16888	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Qmover.
TCP 9103	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Image_autoling.
TCP 9104	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Text_autoling.
TCP 1111	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Prometheus (мониторинг).
TCP 1112	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Node-exporter (мониторинг).
TCP 1113	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Consul-exporter (мониторинг).
TCP 1114	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Postgres-exporter (мониторинг).
TCP 1115	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Alert-manager (мониторинг).
TCP 1116	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Statsd-exporter (мониторинг).
TCP 1117	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Gearman-exporter (мониторинг).
TCP 1118	Сервер Traffic Monitor	Сервер Traffic Monitor	Служба Process-exporter (мониторинг).

Порт	Взаимодействие между компонентами		Назначение порта
	Источник	Получатель	
Стандартные порты для взаимодействия продуктов InfoWatch			
TCP 443	Device Monitor Server	БД сервера Traffic Monitor	Получение политик Traffic Monitor.
	Vision Server	БД сервера Traffic Monitor	Соединение с DataExport API Traffic Monitor.
	Activity Monitor Server	БД сервера Traffic Monitor	
	Prediction Server	БД сервера Traffic Monitor	
	Data Explorer Server	БД сервера Traffic Monitor	
TCP 5433	Сервер Traffic Monitor	Сервер удаленной БД	Удаленная БД Traffic Monitor в случае ее использования.
Порты интеграции со сторонними сервисами			
TCP 2025/587	Почтовый сервер	Сервер Traffic Monitor	Simple Mail Transfer Protocol (SMTP).
	Сервер Traffic Monitor	Почтовый сервер	
UDP 53	Сервер Traffic Monitor	Сервер DNS	Domain Name System (DNS).
UDP 123	Сервер Traffic Monitor	Сервер NTP	Network Time Protocol (NTP).
TCP 389	Сервер Traffic Monitor	Сервер AD	Lightweight Directory Access Protocol (LDAP).
	Сервер Device Monitor	Сервер AD	
TCP 636	Сервер Traffic Monitor	Сервер AD	Lightweight Directory Access Protocol Secure (LDAPS).

Порт	Взаимодействие между компонентами		Назначение порта
	Источник	Получатель	
TCP 3268	Сервер Traffic Monitor	Сервер AD	Microsoft Global Catalog.
TCP 3269	Сервер Traffic Monitor	Сервер AD	Microsoft Global Catalog (LDAPS).
UDP 514	Сервер Traffic Monitor	Сервер SIEM	Интеграция с SIEM по протоколу syslog.
TCP 5433	Сервер SIEM	БД сервера Traffic Monitor	Интеграция с SIEM (PostgreSQL БД Traffic Monitor).
TCP 1344	Proxy-сервер	Сервер Traffic Monitor	Internet Content Adaptation Protocol (ICAP).
Удаленное управление и администрирование			
TCP 22	Автоматизированное рабочее место	Сервер Traffic Monitor	Конфигурирование сервера по SSH-протоколу.
TCP 443	Автоматизированное рабочее место	Консоль управления Traffic Monitor	Подключение к Консоли управления Traffic Monitor.
TCP 3000	Автоматизированное рабочее место	Сервер Traffic Monitor	Подключение к консоли Grafana (система мониторинга).

4.13 Настройка управления вердиктом

По умолчанию для правил копирования в политиках защиты данных управление вердиктом недоступно, и в блоке **Действия при срабатывании правила** полю **Назначить событию вердикт** присвоено значение *Разрешить*.

Если вы хотите, чтобы Система при срабатывании правила присваивала событию вердикт *Запретить* или *Поместить на карантин*, включите управление вердиктом:

1. Подключитесь к базе данных, которую использует сервер Traffic Monitor.
2. Откройте таблицу `setting` базы данных.
3. Смените значение параметра `allow_change_verdict_copy` с `0` на `1`.

В Консоли управления в правиле копирования, для которого нужно настроить вердикт, станет доступен выбор значения в поле **Назначить событию вердикт**: *Разрешить, Заблокировать* или *Поместить на карантин*.

Чтобы снова запретить управление вердиктом, укажите значение `0` для параметра `allow_change_verdict_copy`.

> **Примечание:**
>
> Если вы назначите вердикт, а затем в таблице `setting` отключите управление вердиктом, то в правиле копирования останется назначенный вами вердикт без возможности изменения.

5 Настройки автоматического удаления событий Data Discovery

Traffic Monitor применяет к событиям Data Discovery специальный antigarbage-фильтр. **По умолчанию** фильтр удаляет события Data Discovery, на которые не сработали политики Traffic Monitor или в которых не найдены объекты защиты.

Удаление событий Data Discovery можно настроить в конфигурационном файле `/opt/iw/tm5/etc/luaengined.conf`.

Режимы работы antigarbage-фильтра определяются параметром `DeleteDDEventsWithoutPolicy`:

- `true` – сохранять в базе данных Traffic Monitor только события, на которые сработали политики;
- `false` (значение по умолчанию) – сохранять события, которые содержат объект защиты или на которые сработали политики.

Чтобы antigarbage-фильтр не удалял события Data Discovery, укажите в параметре `DisableDeleteDDEventsForServers` серверы Data Discovery, для которых нужно сделать исключение.

Чтобы применить изменения:

1. Сохраните файл.
2. Перезапустите службу `iw_luaengined`: `iwtm restart luaengined`

Пример:
Вы хотите, чтобы antigarbage-фильтр не применялся к событиям с серверов MainDD и DDcompany, а для остальных серверов нужно сохранять только события, в которых сработали политики.

Значения параметров для конфигурационного файла luaengined.conf примера:

```
"DeleteDDEventsWithoutPolicy": true,
"DisableDeleteDDEventsForServers": ["MainDD", "DDcompany"],
```

6 Мониторинг

Подсистема мониторинга выполняет следующие функции:

- мониторинг работы всех серверов, входящих в состав Traffic Monitor (как физических, так и виртуальных);
- мониторинг всех программных компонентов, входящих в состав решения (ОС, СУБД, БД, процессы и т. д.);
- контроль значений индикаторов для каждого сервера и компонента. Под контролем подразумевается периодическое получение значения индикатора и его сравнение с пороговым значением;
- возможность включения и отключения мониторинга отдельных индикаторов и отдельных серверов;
- отправка на почту уведомлений о выходе значений индикаторов из нормальных пределов.

Подсистема мониторинга автоматически устанавливается при установке серверных компонентов Traffic Monitor с помощью инсталлятора. О порядке установки см. *InfoWatch Traffic Monitor. Руководство по установке*.

Если Система развернута на нескольких серверах с использованием инсталлятора и шаблонов установки, диагностика серверов будет настроена автоматически, а состав датчиков будет соответствовать шаблонам.

Также доступна *Ручная настройка индикаторов*.

6.1 Настройки подсистемы мониторинга

> **Важно!**
>
> Если Система развернута на нескольких серверах с использованием инсталлятора и шаблонов установки, диагностика серверов будет настроена автоматически, а состав датчиков будет соответствовать шаблонам.

Настройка подсистемы мониторинга включает следующие задачи:

- *Настройка подключения Device Monitor*
- *Ручная настройка индикаторов*
- *Настройка адреса сервера синхронизации времени для подсистемы мониторинга*

6.1.1 Настройка подключения Device Monitor

Чтобы настроить мониторинг для сервера Device Monitor:

1. Отредактируйте файл `/opt/iw/tm5/etc/nagios/iwmon/iwmon-hosts-dm.cfg`:

- раскомментируйте секции `host` и `hostgroup`;
- в параметре `address` секции `host` определите имя хоста или IP-адрес сервера Device Monitor.

- В файле / `opt/iw/tm5` `/etc/nagios/iwmon/iwmon-services-dm.cfg` раскомментируйте секцию `service`.

- В файле `/opt/iw/tm5/etc/nagios/iwmon/iwmon-commands.cfg` раскомментируйте секцию `Check Dm server`.
- Перезапустите процесс nagios:
  `systemctl restart iwtm-nagios`

6.1.2 Ручная настройка индикаторов

Включение и выключение индикаторов производится в конфигурационных файлах директории `/opt/iw/tm5/etc/nagios/iwmon`:

- `iwmon-services-db-psql.cfg` – настройка индикаторов для базы данных PostgreSQL;
- `iwmon-services-dm.cfg` – настройка индикаторов для Device Monitor;
- `iwmon-services-loadavg.cfg` – настройка параметров нагрузки на серверы (индикатор "Общая нагрузка системы");
- `iwmon-services.cfg` – настройка основных индикаторов;
- `iwmon-services-queue.cfg` – настройка индикаторов очередей.

Параметр `service_description` отображает назначение каждого индикатора.

Чтобы включить индикатор, измените значение параметра `register` на `1.`

Чтобы выключить индикатор, измените значение параметра `register` на `0`.

Чтобы применить изменения, перезапустите процесс nagios:

`systemctl restart iwtm-nagios`

6.1.3 Настройка адреса сервера синхронизации времени для подсистемы мониторинга

Для корректной синхронизации времени на всех серверах Системы нужно указать IP-адрес NTP-сервера. Вы можете использовать любую службу точного времени, работающую по протоколу NTP и доступную из вашей сети: как сетевое оборудование, так и контроллеры домена Windows.
Чтобы настроить синхронизацию времени на сервере:

1. Откройте на редактирование файл `/opt/iw/tm5/etc/nagios/iwmon/iwmon-services-ntp.cfg`.
2. В значении параметра `check command` замените IP-адрес, заданный по умолчанию, на актуальный IP-адрес NTP-сервера (сервера синхронизации времени).

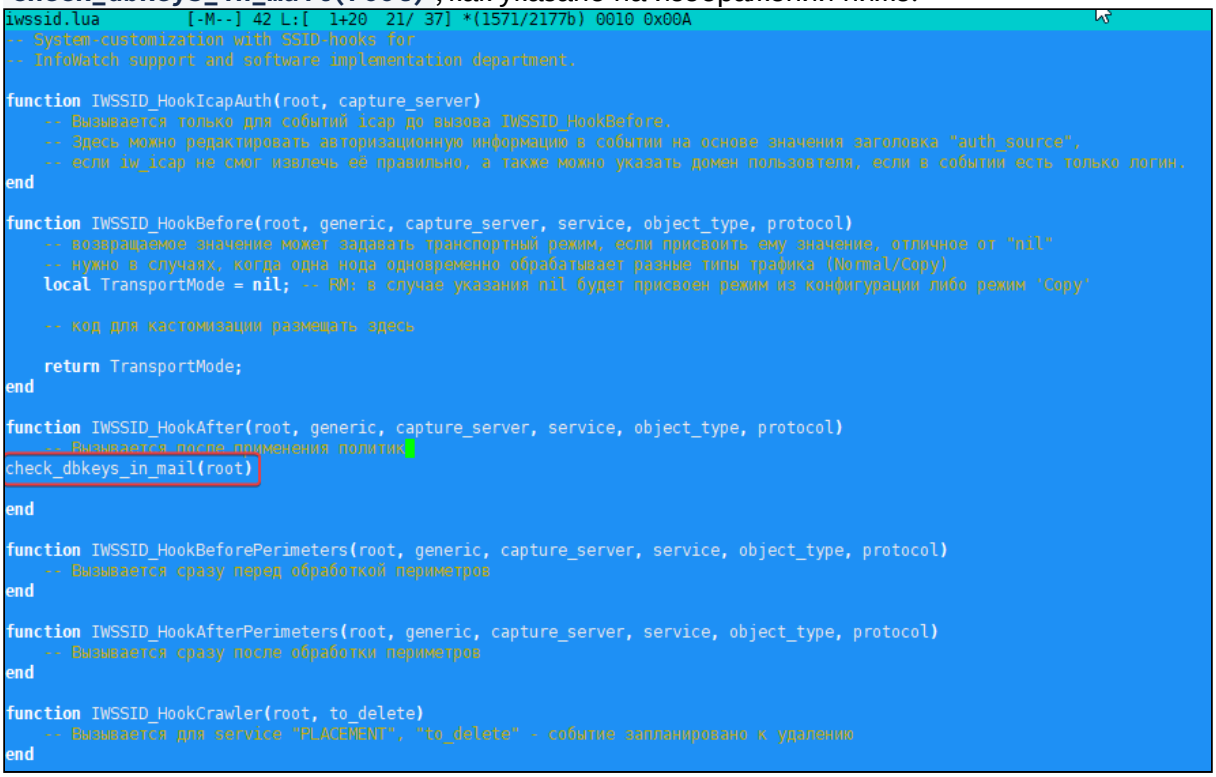
7 Автоматическая проверка допустимого получателя с помощью выгрузки из базы данных

С помощью выгрузки из базы данных Traffic Monitor может контролировать отправку данных по электронной почте. Выгрузка из базы данных должна соответствовать требованиям (см. *InfoWatch Traffic Monitor. Руководство пользователя. Рекомендации по подготовке выгрузки*), в том числе содержать в последнем столбце каждой строки адрес электронной почты, на который разрешено отправлять данные этой строки. Поля последнего столбца считаются ключами и по ним выгрузка не индексируется. Это решение позволяет защитить большой объем данных без ручного создания множества объектов защиты и политик. В транспортном режиме Блокировка (работа "в разрыв") Traffic Monitor позволит блокировать отправку писем с защищаемыми данными или отправлять их в карантин.

По умолчанию после установки Traffic Monitor функциональность отключена.

Чтобы включить возможность использовать выгрузку из базы данных для проверки получателей:

1. В файле `/opt/iw/tm5/etc/scripts/iwssid.lua` добавьте команду вызова функции `check_dbkeys_in_mail(root)`, как указано на изображении ниже.



2. После сохранения изменений проверьте права доступа с помощью команды:

```
ls -la /opt/iw/tm5/etc/scripts/iwssid.lua
```

Пример вывода с корректными правами доступа:

```
-rw-r--r--. 1 iwtm iwtm 2181 июл 24 09:43 /opt/iw/tm5/etc/scripts/iwssid.lua
```

3. Если права были изменены и не соответствуют примеру, для изменения прав доступа выполните команду:

```
chown -R iwtm:iwtm /opt/iw/tm5/etc/scripts/iwssid.lua
```

4. Перезапустите сервисы Traffic Monitor с помощью команды:

```
iwtm restart
```

Важно!

Учитывайте, что на работу с выгрузками из базы данных влияют параметры конфигурационного файла `/opt/iw/tm5/etc/cas.conf`:

- `MinWords` (значение по умолчанию – `10`). При такой настройке Система создаст событие с нарушением, если письмо с недопустимым получателем содержит в анализируемом элементе события не менее 10 слов, включая слова, соответствующие условиям обнаружения выгрузки. В противном случае объект защиты не будет детектироваться и будет создано событие без нарушения;
- `MaxCheckLimit` (значение по умолчанию – `0`). При значении больше нуля Система продолжает поиск до тех пор, пока не найдет указанное максимальное количество строк с уникальными ключами (или количество уникальных строк, если выгрузка без ключей). Параметр доступен только при использовании типа поиска *Следующие друг за другом все слова из ячейки без учета порядка* и при выключенной оптимизации (`"StopOnLimitExceed": false`).

Подробнее о параметрах см. *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*.

Чтобы отключить функциональность:

1. В файле `/opt/iw/tm5/etc/scripts/iwssid.lua` удалите команду вызова функции `check_dbkeys_in_mail(root)`.
2. Перезапустите сервисы Traffic Monitor с помощью команды:

```
iwtm restart
```

8 Администрирование базы данных

Этот раздел содержит информацию по администрированию:

- *PostgreSQL*

Информацию по сбору статистики базы данных можно посмотреть в статье базы знаний *Сбор статистики БД*.

8.1 PostgreSQL

Чтобы подключиться к серверу БД (базы данных) из терминала сервера Traffic Monitor, от имени пользователя `root` выполните команду:

```
psql postgres iwtm
```

Для подключения к БД с рабочих станций под управлением Windows используйте программу pgAdmin.

Информация для подключения содержится в конфигурационном файле **/opt/iw/tm5/csw/postgres/database.conf**

Раздел содержит инструкции по администрированию PostgreSQL:

- *Табличные пространства в базе данных InfoWatch Traffic Monitor;*
- *Управление ежедневными табличными пространствами;*
- *Статистика загруженности ежедневных табличных пространств;*
- *Резервное копирование базы данных;*
- *Проведение регламентных работ на сервере базы данных;*
- *Логирование базы данных.*

> **Примечание:**
>
> Чтобы изменить пароль пользователя БД, см. статью *Изменение предустановленного пароля*.

8.1.1 Табличные пространства в базе данных InfoWatch Traffic Monitor

Общая информация

Данные InfoWatch Traffic Monitor хранятся в БД в виде табличных пространств (ТП). Существует два типа ТП Traffic Monitor:

Тип ТП	Назначение
Основное	Хранение настроек, которые нужны для анализа и обработки объектов (конфигурация, теги, цвета и пр.). Управление системой через Консоль управления (роли, учетные записи пользователей и пр.).

Тип ТП	Назначение
Ежеднев ное	Хранение объектов, перехваченных в течение суток. Хранение информации о результатах анализа и обработки объектов (разобранные объекты, категории, термины и пр.).

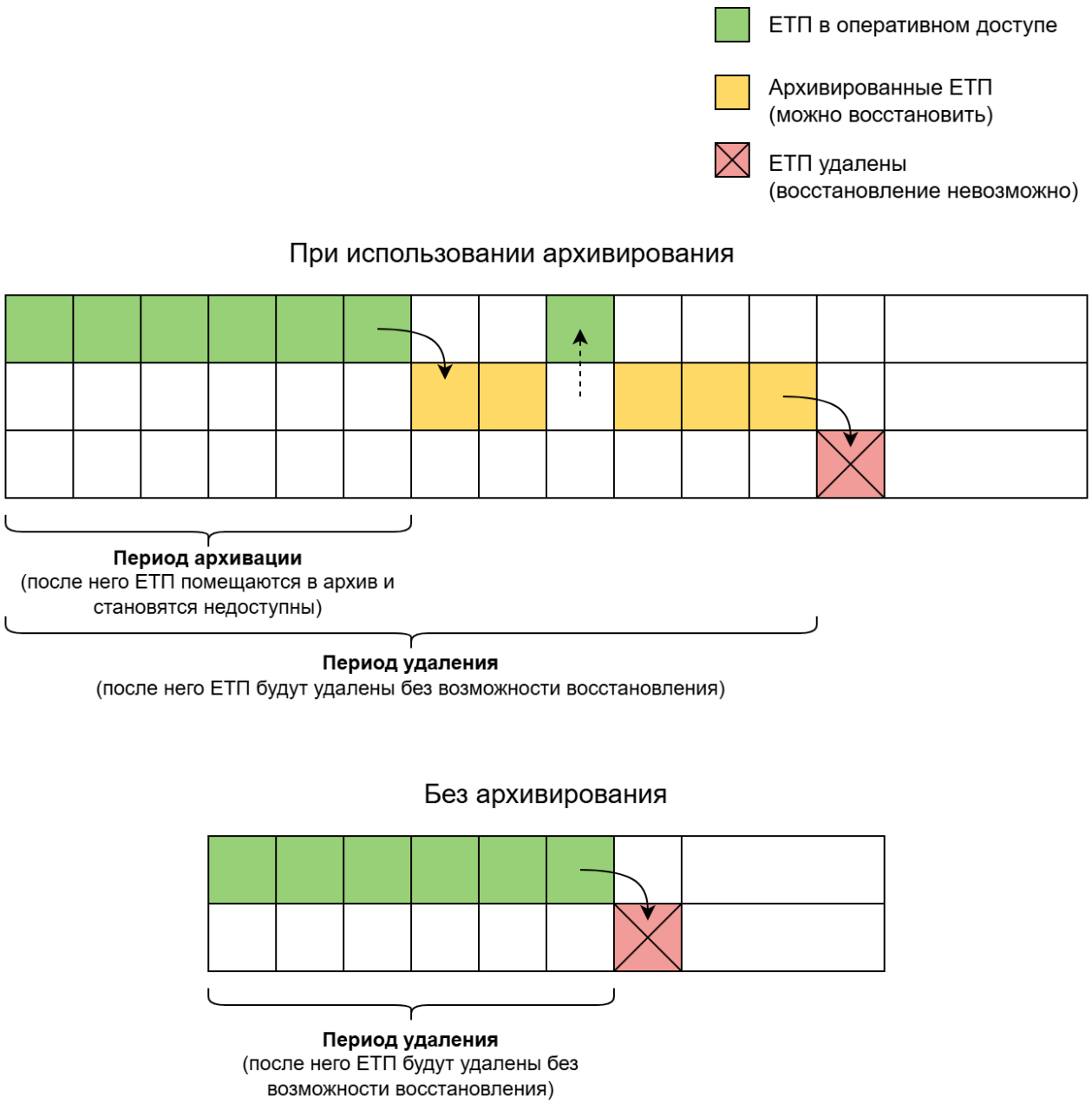
Данные об объектах, перехваченных в течение суток (по UTC+0), хранятся в трех ежедневных табличных пространствах (ETП) следующих типов:

- События без нарушений
- События с нарушениями
- Другой (снимки экрана)

ETП создаются каждый день с таким расчетом, чтобы в БД всегда были ETП для работы в ближайшие шесть суток, не включая текущие. Всем ETП автоматически присваивается имя *IWTM_YYYYMMDD_X,* где *X* – номер ETП (значение TBS_ID из таблицы TBS_LIST). Тип ETП определяется значением TBS_TYPE: 0 – Нет нарушения, 1 – Нарушение, 2 – Другой (снимки экрана).

Жизненный цикл ETП можно разбить на 3 этапа:

1. **Обычное хранение**
   Изначально ETП хранятся в БД и находятся в оперативном доступе. Если вы используете Data Storage, то контенты из событий этого ETП, например вложения, снимки экрана, звуковые файлы и т.д., хранятся там.
2. **Хранение в архиве** (опционально)
   Если вам нужно хранить события длительное время, но не нужен оперативный доступ к ним, перед удалением их можно архивировать.
   Для этого включите автоматическое архивирование ETП. По истечении **периода архивации** они попадут в архив и перестанут быть доступны. При необходимости их можно будет восстановить (пунктирная стрелка на диаграмме).
3. **Удаление**
   Чтобы избежать переполнения диска, вы можете удалить те ETП, которые уже не нужно хранить.
   Для этого включите автоматическое удаление ETП. По истечении **периода удаления** они будут удалены без возможности восстановления.



По умолчанию автоматическое архивирование и удаление ETП выключены. Их можно включить во время установки или после нее. Также при этом нужно задать **период архивации** и/или **период удаления** ETП. Подробнее см. статьи по архивированию и удалению.
Настраивайте **период архивации** и **период удаления** так, чтобы на дисках, где хранятся ETП, всегда было достаточно свободного места и они не переполнились.

Если нужно архивировать/восстановить/удалить единичные ETП, вы можете сделать это вручную в веб-интерфейсе Traffic Monitor. См. *InfoWatch Traffic Monitor. Руководство пользователя. Управление табличными пространствами*.
Если веб-интерфейс недоступен, используйте для этого утилиту сервиса **iw_space_manager** (см. *Управление ежедневными табличными пространствами с помощью консольной утилиты*). В последнюю очередь выполняйте действия с ETП вручную через БД.

Хранение

Основное ТП по умолчанию хранится в каталоге `/u02/pgdata`
Ежедневные табличные пространства по умолчанию хранятся в каталоге `/u02/pgdata1`
Подробнее о размещении ЕТП см. *Настройка размещения файлов в файловой системе*.

О режимах хранения ЕТП см. *Настройка режимов хранения файлов табличного пространства*.

Архивирование

Процесс архивирования включает в себя:

- отключение ЕТП от БД;
- перемещение ЕТП в заданный каталог (по умолчанию `/u02/arch`).

Данный каталог следует размещать на отдельном носителе, чтобы освободить пространство на диске с оперативными данными и избежать его переполнения.
При использовании Data Storage бинарные данные архивированного ЕТП будут перемещены на медленный диск Data Storage.

При архивации данные не сжимаются. Поэтому на выделенном диске они будут занимать примерно столько же места. Размер диска для хранения архивированных ЕТП можно оценить, исходя из того, сколько места занимают ЕТП в оперативном доступе в их директориях хранения (по умолчанию `/u02/pgdata1` в БД и `/opt /dsdata/_seaweedfs` в Data Storage).

Подробнее архивирование описано в разделе *Архивирование ежедневных табличных пространств*.

Для доступа к данным архивированного ЕТП нужно восстановить его. См. *Восстановление ежедневных табличных пространств*.

Удаление

При включенном автоматическом удалении Система ежедневно удаляет ЕТП старше периода удаления. Его значение настраивается отдельно для каждого типа ЕТП: События с нарушениями, События без нарушений, Другой (снимки экрана).

Подробнее о способах удаления см. *Удаление ежедневных табличных пространств*.

8.1.2 Управление ежедневными табличными пространствами

В этом разделе:

- *Настройка размещения файлов на файловой системе*
- *Настройка режимов хранения файлов табличного пространства*
- *Архивирование ежедневных табличных пространств*
- *Восстановление ежедневных табличных пространств*
- *Удаление ежедневных табличных пространств*
- *Управление ежедневными табличными пространствами с помощью консольной утилиты*

Настройка размещения файлов в файловой системе

При установке Системы (см. *InfoWatch Traffic Monitor. Руководство по установке*) задается использование одной директории ежедневных табличных пространств (ЕТП), расположенной в `/u02/pgdata1`

Примечание.

Для архивирования табличных пространств используется директория `/u02/arch`

Однако при больших нагрузках рекомендуем размещать ЕТП распределенно, на разных файловых системах (LUN-ах, физических дисках) для их поочередного использования. Например, если задано 3 файловых системы, то данные будут размещаться следующим образом:

Первый день – ЕТП создается в файловой системе 1.
Второй день – ЕТП создается в файловой системе 2.
Третий день – ЕТП создается в файловой системе 3.
Четвертый день – ЕТП создается в файловой системе 1.
…

Распределение файлов ЕТП (количество и расположение) можно изменять с помощью следующих сценариев.

Пример сценария, изменяющего количество отдельных мест хранения ЕТП:

```
begin;
select pkg_part_set_df_path_cnt('4');
commit;
```

Важно!

Изменив количество мест хранения ЕТП, обязательно откорректируйте (добавьте/удалите) пути их расположения.

Пример сценария, изменяющего пути для расположения ЕТП:

```
begin;
select pkg_part_set_df_path('/test1/', 1);
select pkg_part_set_df_path('/test2/', 2);
select pkg_part_set_df_path('/test3/', 3);
select pkg_part_set_df_path('/test4/', 4);
commit;
```

Примечание:

Рекомендуем при указании пути в конце указывать символ "/".

Пример сценария просмотра содержимого ЕТП:

```
select a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) ||
 '-' ||
power(10, trunc(log(10, a.binary_size + a.text_size)) + 1) size_range,
count(1) cnt, sum(a.binary_size) binary_size, sum(a.text_size) text_size
```

```
from
(
select date_trunc('day', o.capture_date) d, s.display_name code, o.object_id,
coalesce(length(os.source),0)+coalesce(length(os.context),0)+
coalesce(length(o.gui_xml),0)+coalesce(length(o.preview_data),0) binary_size,
coalesce(length(o.text), 0) text_size
from object o
inner join service s on o.service_code = s.service_id and s.language = 'eng'
inner join object_source os on os.object_id = o.object_id
where o.capture_date between to_date('05.05.2014', 'dd.mm.yyyy') and
to_date('14.05.2014', 'dd.mm.yyyy')
) a
group by a.d, a.code, power(10, trunc(log(10, a.binary_size + a.text_size))) ||
'-' ||
  power(10, trunc(log(10, a.binary_size + a.text_size)) + 1)
order by 1, 2, 3;
```

Примечание:

Чтобы получить результат анализа размеров перехваченных объектов в ТП вместе со служебной информацией БД, рекомендуем использовать pgAdmin.

Настройка режимов хранения файлов табличного пространства

Существует три режима хранения данных в БД (базе данных):

- **Normal** – переключение на следующий раздел, если он указан, происходит при переполнении предыдущего.
- **Fast/Slow disks** – разделение пулов на быстрый и медленный. Новые данные сохраняются в быстром разделе и через указанное количество дней Система перемещает их на медленные разделы. Медленный пул работает при этом в режиме Normal.
- **Rotate** – переход к следующему разделу происходит ежедневно или при переполнении предыдущего.

Режим хранения вы выбираете при установке Traffic Monitor. По умолчанию инсталлятор предлагает режим **Normal** (обычный). В процессе эксплуатации режим хранения может быть изменен.

По умолчанию ЕТП (ежедневные табличные пространства) хранятся в директории `/u02/pgdata1`

Примечание:

Описываемые в этой статье режимы относятся только к данным, хранящимся в БД. Изменение режима не влияет на данные, хранящиеся в Data Storage.

Режим Fast/Slow disks

Система переносит данные с быстрого диска на медленный каждую ночь. Если вы переходите с режима **Normal** на режим **Fast/Slow**, на вашем старом разделе хранится большой объем ЕТП и вы указываете старый раздел в качестве быстрого диска, то перенос данных может занять продолжительное время.
Если вы будете использовать старый диск в качестве быстрого, перед переключением режима убедитесь, что выполнены следующие условия:

- размер нового раздела не меньше, чем размер старого. То есть там достаточно места для переноса всех ЕТП со старого раздела;
- в старом разделе есть свободное место в размере не меньше самого объемного ЕТП, которое будет перенесено на медленный диск.

Система создает ЕТП каждую ночь так, чтобы в БД всегда были ЕТП для работы в ближайшие шесть суток, не включая текущие. Поэтому если при переходе с режима **Normal** на режим **Fast/Slow** в качестве быстрого диска указать новый раздел, то первые семь суток Система будет сохранять события в уже созданные ЕТП на медленном диске. При этом новые ЕТП будут создаваться на быстром диске.

Для настройки режима **Fast/Slow** мы будем использовать новый раздел `/u03/pgdata/` в качестве медленного диска, а старый раздел `/u02/pgdata1/` – в качестве быстрого.

Чтобы настроить режим хранения Fast/Slow (быстрые и медленные диски):

1. Отредактируйте файл `/etc/fstab`, чтобы новый раздел автоматически монтировался в `/u03`:
   `/dev/sdd1 /u03/ ext4 defaults 1 2`
2. Создайте папку `pgdata`:
   `mkdir /u03/pgdata`
3. Смените пользователя:
   `chown -R postgres:postgres /u03`
4. Зайдите в БД:
   `su - iwtm`
   `psql -p 5433 -h <IP-адрес_сервера_БД> postgres iwtm`
   `psql -p 5433 -h 127.0.0.1 postgres iwtm` – для подключения к локальной БД
5. Укажите период хранения на быстрых дисках (по умолчанию – `7`):
   `select pkg_part_set_fast_days(7);`
6. Укажите путь к быстрому диску:
   `select pkg_part_set_fast_path('/u02/pgdata1/',1);`
7. Укажите путь к медленному диску:
   `select pkg_part_set_df_path('/u03/pgdata/',1);`
8. При необходимости можно использовать несколько медленных дисков. Данные будут записываться на следующий медленный диск при заполнении предыдущего. Для добавления дополнительных медленных дисков укажите новый путь:
   `select pkg_part_set_df_path('/u03/pgdata2/',2);`
9. Укажите общее количество медленных дисков (до 10):
   `select pkg_part_set_df_path_cnt('2');`
10. Поменяйте режим на быстрые-медленные диски:
    `select pkg_part_set_filesys_type('fast/slow');`
    Данные будут перенесены с быстрых дисков на медленные с помощью ночного задания.
11. Чтобы запустить перенос файлов вручную, выполните:
    `select iwtm.pkg_part_move_fast_tablespaces_to_slow();`

Примечание:

В Системе можно использовать нескольких медленных дисков.

Примечание:

При режиме **Fast/Slow** ТП снимков экрана хранятся только в медленных разделах.

Чтобы перейти обратно в режим хранения Normal:

1. Проверьте содержимое директории быстрых дисков `/u02/pgdata1/`:
   `ls /u02/pgdata1/`
2. Проверьте содержимое директории медленных дисков `/u03/pgdata/`:
   `ls /u03/pgdata/`
3. Зайдите в БД:
   `su - iwtm`
   `psql -p 5433 -h <IP-адрес_сервера_БД> postgres iwtm`
   `psql -p 5433 -h 127.0.0.1 postgres iwtm` – для подключения к локальной БД
4. Измените период хранения на быстрых дисках:
   `select pkg_part_set_fast_days(-1);`
   Значение `-1` указывается для переноса ЕТП за сегодняшний день
5. Запустите задачу переноса ЕТП с быстрых дисков на медленные:
   `select iwtm.pkg_part_move_fast_tablespaces_to_slow();`
6. Проверьте содержимое директории быстрых дисков. На них должны остаться ЕТП, которые создаются на будущие даты. Такие ЕТП нужно удалить вручную с помощью сервиса **iw_space_manager**:
   `iw_space_manager tbs:delete <tbs_id>`
   или с помощью команды в БД (если вы не используете Data Storage):
   `select pkg_part_delete_tablespace(<tbs_id>);`
7. Запустите задание (cron) сервиса **iw_space_manager** для немедленного создания ЕТП:
   `iw_space_manager cron`
   или задание в БД (если не используете Data Storage):
   `/opt/iw/tm5/bin/dbtools/dbconf-jobs-postgres.sh start iwtm_add_parts`
8. Проверьте, что все ЕТП перенесены с быстрых дисков:
   `ls /u02/pgdata1/`
9. Проверьте, что на медленных дисках созданы ЕТП на будущие даты:
   `ls -alt /u03/pgdata/`
10. Включите режим **Normal**:
    `select pkg_part_set_filesys_type('normal');`

Режим Rotate

Чтобы настроить режим хранения Rotate (ежедневное переключение):

1. Монтируйте новый раздел и убедитесь, что он может монтироваться автоматически при перезагрузке.
2. Создайте папку `pgdata`:
   `mkdir /u03/pgdata`
3. Смените пользователя:
   `chown -R postgres:postgres /u03`

4. Зайдите в БД:
   `su - iwtm`
   `psql -p 5433 -h <IP-адрес_сервера_БД> postgres iwtm`
   `psql -p 5433 -h 127.0.0.1 postgres iwtm` – для подключения к локальной БД
5. Добавьте путь второго раздела:
   `select pkg_part_set_df_path('/u03/pgdata/',2);`
6. Укажите новое количество путей:
   `select pkg_part_set_df_path_cnt(2);`
7. Переключитесь на режим **rotate**:
   `select pkg_part_set_filesys_type('rotate');`

```
postgres=# select * from setting where setting like 'df_%';
setting | value | editable
-------------+---------------+----------
df_path1 | /u02/pgdata1/ | 1
df_path2 | /u03/pgdata/ | 1
df_path_cnt | 2 | 1
df_filesys_type | rotate | 1
```

> **Примечание:**
>
> Параметры режимов хранятся в таблице `setting` БД. Их особенности описаны в статье *Настройка режима хранения данных в ТП. Хранение данных на разных дисках*.

Архивирование ежедневных табличных пространств

Процесс архивирования состоит из отключения ежедневных табличных пространств (ЕТП) от базы данных (БД) и их перемещения в заданный каталог (по умолчанию `/u02/arch`). Данный каталог следует размещать на отдельном носителе, чтобы освободить пространство на диске с оперативными данными и избежать его переполнения. При необходимости архивированные ЕТП могут быть восстановлены.

В Системе есть следующие способы архивирования ЕТП:

- автоматическое архивирование после истечения указанного периода (см. *Автоматическое архивирование ежедневных табличных пространств*);
- ручное архивирование единичных ЕТП:
  - в веб-интерфейсе Traffic Monitor. См. *InfoWatch Traffic Monitor. Руководство пользователя. Управление табличными пространствами*;
  - с помощью консольной утилиты сервиса **iw_space_manager** (см. *Управление ежедневными табличными пространствами с помощью консольной утилиты*);
  - через БД (см. *Архивирование ежедневных табличных пространств вручную в базе данных*).

Если вам нужно архивировать единичное ЕТП, рекомендуем делать это в веб-интерфейсе Traffic Monitor. Если веб-интерфейс недоступен, используйте утилиту сервиса **iw_space_manager**. В последнюю очередь используйте архивирование ЕТП вручную через БД.

Архивирование при использовании Data Storage

Если вы используете Data Storage, то при архивировании ЕТП бинарные данные будут перемещены на медленный диск Data Storage.
Если медленный диск не подключен, то в веб-интерфейсе Traffic Monitor при архивировании ЕТП будет указан статус "Архивировано". Но при этом бинарные данные ЕТП будут храниться на быстром диске сервера Data Storage, внутри директории для размещения бинарных данных, указанной при установке хранилища (по умолчанию `/opt/dsdata/_seaweedfs`).

Путь к медленному диску указывается при установке Data Storage. Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Установка Платформы*.
Чтобы добавить путь к медленному диску Data Storage после установки хранилища:

1. Создайте директорию и смонтируйте в нее медленный диск:

   ```
   mkdir -p /mnt/slowdisk
   mount /dev/<your_slowdisk> /mnt/slowdisk
   ```

2. Назначьте пользователя и права доступа для директории, в которую смонтировали медленный диск:

   ```
   chown 1000 /mnt/slowdisk
   chmod 700 /mnt/slowdisk
   ```

3. Откройте деплоймент Data Storage для редактирования с помощью команды:

   ```
   kubectl -n infowatch edit deployment datastorage-<node_label>
   ```

   где `<node_label>` – здесь и далее это лейбл ноды, на которой установлено хранилище. Для центральной ноды кластера или, если хранилище установлено не в кластере платформенных продуктов, используйте лейбл `central`. Для офисной ноды лейбл задается при установке, по умолчанию: `office`.
4. В секцию `containers` -> `volumeMounts` добавьте следующие строки:

   ```
   - mountPath: /var/lib/dataslow
     name: datastorage-dataslow-host-volume-<node_label>
   ```

5. В секцию `volumes` добавьте следующие строки:

   ```
   - hostPath:
       path: /mnt/slowdisk
       type: ""
     name: datastorage-dataslow-host-volume-<node_label>
   ```

6. Сохраните изменения и выйдите из редактора.

Автоматическое архивирование ежедневных табличных пространств

По умолчанию автоматическое архивирование ЕТП (ежедневных табличных пространств) выключено. Чтобы Система архивировала ЕТП по расписанию, включите эту функцию и задайте время, по истечении которого нужно архивировать ЕТП. Подробнее см. далее.

Ежедневно, в 00:00 по времени сервера, процедура сервиса **iw_space_manager** будет архивировать ЕТП, которые удовлетворяют следующему условию:

Дата табличного пространства меньше или равна разнице между текущей датой и заданным интервалом времени для архивирования табличного пространства.

Таким образом, будут архивироваться все ЕТП старше заданного значения.

> **Важно!**
>
> Если в качестве интервала времени используются месяцы или годы, то рекомендуем использовать максимальное значение интервала в расчете. Для месяца – 31 день. Для года – 366 дней. Например, чтобы архивировать ЕТП старше 4 лет, указывайте интервал 366*4=1464 дня.

Перед тем, как включить автоматическое архивирование, проверьте, что каталог архивирования задан верно:

```
select value
from setting
where setting = 'archive_path';
```

Пользователь `postgres` должен быть владельцем каталога.

Если каталог установлен неправильно, установите его, выполнив следующую команду:

```
begin;
select sp_setting_set('archive_path', '/test/archive/');
commit;
```

Для автоматического архивирования ТП (по умолчанию функция выключена) вы можете использовать сценарии (запускаются от имени владельца схемы данных):

- для ЕТП, хранящего объекты со статусом *Нарушение*:

  ```
  begin;
  select sp_setting_set('violation_archive_enabled', '1');
  select sp_setting_set('violation_archive_period', 'D');
  commit;
  ```

- для ЕТП, хранящего объекты со статусом *Нет нарушений*:

  ```
  begin;
  select sp_setting_set('noviolation_archive_enabled', '1');
  select sp_setting_set('noviolation_archive_period', 'D');
  commit;
  ```

- для ЕТП, хранящего *снимки экрана (скриншоты)*:

```
begin;
select sp_setting_set('other_archive_enabled', '1');
select sp_setting_set('other_archive_period', 'D');
commit;
```

где:
1 – показатель того, что автоматическое архивирование включено (чтобы выключить, вместо 1 используйте значение 0);
D – количество дней, по истечении которого ЕТП будет архивировано Системой. Это число должно быть меньше устанавливаемого количества дней до удаления ЕТП (см. *Удаление ежедневных табличных пространств*).

Архивирование ежедневных табличных пространств вручную в базе данных

Рекомендуем архивировать единичные ЕТП (ежедневные табличные пространства) через веб-интерфейс или с помощью утилиты **iw_space_manager**.

Архивирование ЕТП вручную в базе данных производится в порядке, представленном ниже.

Важно!

При этом способе архивирования данные, хранящиеся в Data Storage, не архивируются.

Выборка ЕТП и файлов данных

Список отключаемых ТП можно получить, выполнив запросы к базе данных от имени владельца схемы базы данных. Запросы составляются в соответствии со стратегией архивирования, принятой в вашей организации.

Пример:

Для выборки ЕТП с указанием основных атрибутов (название, идентификатор, путь, тип, дата создания, размер) можно применить следующий запрос:

```
SELECT t.tbs_name, t.tbs_id, t.tbs_type, t.part_date, pg_tablespace_location(oid),
pg_size_pretty(pg_tablespace_size(spcname)), t.status, t.note
FROM  pg_tablespace, iwtm.tbs_list t
WHERE t.tbs_name = pg_tablespace.spcname AND t.status IN (0, 3);
```

```
tbs_name  | tbs_id | tbs_type | part_date  | pg_tablespace_location | pg_size_pretty | status |       note
----------+--------+----------+------------+------------------------+----------------+--------
+--------------------
   iwtm_2 |      2 |        1 | 2017-03-30 |     /u02/pgdata/iwtm_2 |         692 kB |      0 | Partitions
created
   iwtm_3 |      3 |        2 | 2017-03-30 |     /u02/pgdata/iwtm_3 |         692 kB |      0 | Partitions
created
   iwtm_4 |      4 |        0 | 2017-03-31 |     /u02/pgdata/iwtm_4 |          25 MB |      0 | Partitions
created
   iwtm_5 |      5 |        1 | 2017-03-31 |     /u02/pgdata/iwtm_5 |         692 kB |      0 | Partitions
created
   iwtm_6 |      6 |        2 | 2017-03-31 |     /u02/pgdata/iwtm_6 |         692 kB |      0 | Partitions
created
```

```
   iwtm_7 |      7 |        0 | 2017-04-01 |     /u02/pgdata/iwtm_7 |         692 kB |      0 | Partitions
created
   iwtm_8 |      8 |        1 | 2017-04-01 |     /u02/pgdata/iwtm_8 |         692 kB |      0 | Partitions
created
   iwtm_9 |      9 |        2 | 2017-04-01 |     /u02/pgdata/iwtm_9 |         692 kB |      0 | Partitions
created
```

Важно!

Настоятельно рекомендуем использовать запрос для получения списка файлов. Его пример описывается далее в этом разделе. Это связано с тем, что список файлов данных, полученный другими способами, может оказаться неполным.

Отключение ЕТП от базы данных

Важно!

Не отключайте ЕТП во время работы заданий `iwtm_iwtm_add_parts`, `iwtm_iwtm_delete_tablespaces`, `iwtm_iwtm_archive_tablespaces` так как это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:

   ```
   select pkg_part_archive_tablespace(N);
   ```

   где `N` – это значение атрибута `tbs_id` целевого ТП из таблицы `tbs_list`.
   После выполнения этого сценария статус ЕТП изменится на *Отключено от базы данных*.
2. Повторите вызов процедуры для каждого ЕТП, которое нужно отключить.

Перенос файлов данных

Перенесите каталоги с заархивированными ТП, принадлежащие отключенным ЕТП, на другой носитель информации.

Для получения списка отключенных ТП используйте команду:

```
select * from tbs_list where status = 10;
```

Файлы данных хранятся в каталоге:

```
select value from setting where setting = 'archive_path';
```

Восстановление ежедневных табличных пространств

Важно!

Табличное пространство (ТП) можно восстанавливать только в той схеме базы данных, в которой оно было отключено (даже если эта схема была обновлена). Восстановить ТП после полной переустановки схемы базы данных невозможно.

В Системе есть следующие способы восстановления ежедневных табличных пространств (ЕТП):

- в веб-интерфейсе Traffic Monitor. См. *InfoWatch Traffic Monitor. Руководство пользователя. Управление табличными пространствами*;
- с помощью консольной утилиты сервиса **iw_space_manager**. См. *Управление ежедневными табличными пространствами с помощью консольной утилиты*;
- через базу данных (БД) – этот способ описан далее. Рекомендуем использовать его в последнюю очередь.

Перемещение файлов данных

Для восстановления ЕТП нужно переместить файлы данных этого ТП с внешнего носителя в каталог, путь к которому можно получить с помощью запроса:

```
select value from setting where setting = 'archive_path';
```

Важно!

Убедитесь, что пользователь *postgres* имеет права на чтение и запись в том каталоге, куда будут перемещаться файлы данных.

Подключение ЕТП

Важно!

Не подключайте ЕТП во время работы заданий `iwtm_iwtm_add_parts, iwtm _iwtm_delete_tablespaces` и `iwtm_iwtm_archive_tablespaces`. Это может привести к повреждению данных.

1. От имени владельца схемы БД вызовите процедуру:

   ```
   select pkg_part_restore_tablespace(N);
   ```

   где `N` – ID табличного пространства (указывается в `tbs_list`).
   После выполнения процедуры статус ЕТП изменится на *Восстановлено*.
2. Повторите вызов процедуры для каждого ЕТП, которое нужно подключить.

Удаление ежедневных табличных пространств

В Системе есть следующие способы удаления ежедневных табличных пространств (ЕТП):

- автоматическое по расписанию. Описано ниже;
- ручное удаление единичных ЕТП:
  - в веб-интерфейсе Traffic Monitor. См. *InfoWatch Traffic Monitor. Руководство пользователя. Управление табличными пространствами*;

- с помощью консольной утилиты сервиса **iw_space_manager**. См. *Управление ежедневными табличными пространствами с помощью консольной утилиты*;
- через базу данных (БД). Описано ниже.

Рекомендуем использовать автоматическое удаление. В противном случае может переполниться диск, либо накопится большое количество данных для удаления. Это приведет к значительным временным затратам на выполнение этой процедуры в будущем и, как следствие, к увеличению времени простоя сервера Traffic Monitor.

Важно!

Удаление ТП – необратимая операция. После ее выполнения вы не сможете восстановить удаленные данные.
Система удаляет как данные ЕТП из директории хранения (по умолчанию `/u02/pgdata1` или `/u02/arch` для архивированных), так и информацию о ЕТП из БД. При использовании Data Storage также удаляются данные из хранилища.

Во время удаления ТП доступ к соответствующим таблицам закрыт. По этой причине в лог-файлах процессов **iw_deliver**, **iw_x2db**, **iw_updater** могут отображаться ошибки доступа к БД. После удаления ТП эти процессы восстанавливают доступ к БД автоматически.

Автоматическое удаление

По умолчанию автоматическое удаление ЕТП выключено. Чтобы Система удаляла ЕТП по расписанию, включите эту функцию и задайте время, по истечении которого нужно удалять ЕТП. Подробнее см. далее.
Ежедневно, в 00:00 по времени сервера, процедура сервиса **iw_space_manager** будет удалять ЕТП, которые удовлетворяют следующему условию:

Дата табличного пространства меньше или равна разнице между текущей датой и заданным интервалом времени для удаления табличного пространства.

Таким образом, будут удаляться все ЕТП старше заданного значения.

Важно!

Если в качестве интервала времени используются месяцы или годы, то рекомендуем в расчете использовать максимальное значение интервала. Для месяца – 31 день. Для года – 366 дней. Например, чтобы удалять ЕТП старше четырех лет указывайте интервал 366*4=1464 дня.

Включение автоматического удаления

Автоматическое удаление по расписанию настраивается отдельно для каждого типа ЕТП.
Чтобы включить его, установите флаг удаления `delete_enabled` и задайте срок хранения ЕТП `delete_period`. Для этого от имени владельца схемы данных выполните следующие сценарии:

- для ЕТП, хранящих объекты со статусом *Нарушение*:

```
begin;
select sp_setting_set('violation_delete_enabled', '1');
select sp_setting_set('violation_delete_period', 'D');
commit;
```

- для ЕТП, хранящих объекты со статусом *Нет нарушений*:

```
begin;
select sp_setting_set('noviolation_delete_enabled', '1');
select sp_setting_set('noviolation_delete_period', 'D');
commit;
```

- для ЕТП, хранящих *снимки экрана (скриншоты)*:

```
begin;
select sp_setting_set('other_delete_enabled', '1');
select sp_setting_set('other_delete_period', 'D');
commit;
```

где:
`1` – показатель того, что автоматическое удаление включено (чтобы выключить, вместо 1 задайте значение 0);
`D` – количество дней, по прошествии которых ЕТП будут удалены. Это число должно быть больше устанавливаемого количества дней до архивирования ЕТП (см. *Автоматическое архивирование ежедневных табличных пространств*).

Настройка автоматического удаления с помощью скрипта

Также вы можете настроить автоматическое удаление ЕТП, используя скрипт `/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh` или `/opt/iw/tm5/bin/dbtools/dbconf-jobs-postgres.sh`. Возможные команды:

Цель	Команда
Задать период для удаления	`/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh set violation|noviolation|other <days> [-v]`
Включить автоудаление	`/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh enable violation|noviolation|other [-v]`
Выключить автоудаление	`/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh disable violation|noviolation|other [-v]`
Просмотреть статус настроек	`/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh show [-v]`
Удалить все ЕТП	`/opt/iw/tm5/bin/dbtools/dbconf-jobs-postgres.sh start iwtm_delete_tablespace`

Пример

Чтобы включить автоматическое удаление тех ЕТП, которые хранят объекты со статусом *Нет нарушения* и старше 15 суток, выполните команды:

```
/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh set noviolation 15 [-v]
/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh enable noviolation [-v]
```

Удаление вручную

Если вам нужно немедленно запустить процедуру автоматического удаления ЕТП (например, из-за нехватки места в файловой системе был изменен интервал удаления, но следующий запуск задания произойдет нескоро), от имени владельца схемы БД выполните сценарий:

```
select pkg_part_delete_tablespaces();
```

В результате будут удалены ЕТП, для которых включено удаление по расписанию и определен срок хранения.

Приведенная выше команда влияет только на данные в БД. Если вы используете Data Storage, запустите процедуру автоматического удаления ЕТП с помощью сервиса **iw_space_manager**:

```
iw_space_manager cron
```

Чтобы удалить одно ЕТП по его идентификатору (ID), выполните следующую команду:

```
select pkg_part_delete_tablespace(<ID>);
```

Данная команда влияет только на данные в БД. Если вы используете Data Storage, удаляйте ЕТП с помощью сервиса **iw_space_manager**:

```
iw_space_manager tbs:delete <tbs_id>
```

Управление ежедневными табличными пространствами с помощью консольной утилиты

Управление ежедневными табличными пространствами (ЕТП) средствами командной строки осуществляется с помощью консольной утилиты, вызывающей сервис **iw_space_manager**. Сервис доступен пользователю **iwtm** и включен по умолчанию.

При использовании Data Storage сервис **iw_space_manager** архивирует/восстанавливает/удаляет также и бинарные данные из хранилища.

Команды и параметры сервиса:

Команды	Описание
`tbs:archive [options] [--] <id>`	Запуск архивации ЕТП с указанием его ID. Пример архивации ЕТП с ID=123: `iw_space_manager tbs:archive 123`
`tbs:create <type> <capture>`	Создание ЕТП с указанием его: • типа: 0 – без нарушений, 1 – с нарушениями, 2 – снимки экрана; • даты создания в формате YYYY-MM-DD. Пример создания нового ЕТП с нарушениями за 1 сентября 2023 года: `iw_space_manager tbs:create 1 2023-09-01`
`tbs:delete [options] [--] <id>`	Удаление ЕТП с указанием его ID.
`tbs:get [options]`	Получение списка существующих ЕТП. Дополнительные параметры: • `--limit=LIMIT` – максимальное количество позиций списка для вывода на экран; • `--offset=OFFSET` – не показывать первые N позиций списка (по умолчанию N=0); • `--order=ORDER` – сортировать список ЕТП по имени и дате создания: ASC – по возрастанию, DESC – по убыванию. Пример вывода списка из 20 ЕТП, отсортированных по имени и убыванию даты создания: `iw_space_manager tbs:get -- limit=20 --order="TBS_NAME:ASC,PART_DATE:DESC"`
`tbs:restore [options] [--] <id>`	Восстановление архивированного ЕТП с указанием его ID. Пример восстановления из архива ЕТП с ID=123: `iw_space_manager tbs:restore 123`
	Возможно выполнение с общими для всех указанных команд параметрами: • `-f, --force` – запуск без проверки валидации в случае аварийных ситуаций с базой данных. Позволяет совершать операции над ТП, в которых дата перехвата объектов совпадает с сегодняшней датой; • `--used-configs` – запуск с параметрами из конфигурационного файла; • `-p, --configpath [=CONFIGPATH]` – расположение конфигурационного файла. По умолчанию: `opt/iw/tm5/etc`;

Команды	Описание
	• `--force-config-load` – принудительно загружать файл конфигурации, даже если указаны параметры запроса.
`tbs:clearLostBuckets`	Удаление устаревших, потерянных и неиспользуемых корзин ТП (доступно, начиная с версии Traffic Monitor 7.10.1)

Для получения логов и отладочных сообщений запустите сервис с параметрами:

- `-v` – обычный вывод логов;
- `-vv` – вывод логов с расширенной детализацией;
- `-vvv` – вывод логов с полной детализацией.

Чтобы получить список возможных команд, выполните: `iw_space_manager list`

8.1.3 Статистика загруженности ежедневных табличных пространств

Для анализа загруженности ежедневных табличных пространств (ЕТП) вы можете использовать скрипт `/opt/iw/tm5/bin/dbtools/tablespace_stat_postgres/tablespace_stat_postgres.sh`. С его помощью вы можете получить статистику по содержимому ТП за выбранный период. Скрипт выполняет один из шести сценариев, и в каждом собирается различная информация. Подробнее сценарии описаны *ниже*.

Чтобы вывести информацию об использовании скрипта:

1. Перейдите в директорию, где располагается скрипт, с помощью команды:
   `cd /opt/iw/tm5/bin/dbtools/tablespace_stat_postgres/`
2. Запустите скрипт без указания параметров, выполнив команду:
   `./tablespace_stat_postgres.sh`

В результате будет выведена справочная информация:

```
tablespace_stat.sh: usage: [ report_number ] [ -e ]

report_number:
1 - Period stats
2 - Period stats with count of objects
3 - Statistics on a given tbs id by event type
4 - Period stats by event type
5 - Period stats by person
6 - Statistics on a given person id

-e, --export : for export to csv
```

Чтобы использовать скрипт:

1. Перейдите в директорию, где располагается скрипт, выполнив команду:
   `cd /opt/iw/tm5/bin/dbtools/tablespace_stat_postgres/`
2. Запустите скрипт с помощью команды:
   `./tablespace_stat_postgres.sh <номер_сценария> <-e>`
   где номер сценария задается цифрой от 1 до 6;
   `-e` или `--export` – это ключ, который вы можете указать, чтобы выгрузить результаты работы скрипта в формате CSV.
   Пример команды запуска скрипта:
   `./tablespace_stat_postgres.sh 1`

3. Укажите параметры в зависимости от сценария:
    - для сценариев 1, 2, 4, 5, 6 – период, за который нужно вывести статистику:
        a. Введите нижнюю границу периода в формате dd.mm.yyyy и нажмите **Enter**.
        b. Введите верхнюю границу и нажмите **Enter**.

> **Примечание:**
>
> Если не вводить значения для границ периода и нажать **Enter** дважды, то по умолчанию будет выведена статистика за последние две недели.
> Если задать только нижнюю границу, то будет выведена информация за период с указанной даты до текущей.

    - для сценария 3 – ID табличного пространства;
    - для сценария 6 – ID сотрудника.

В случае выгрузки результатов выполнения скрипта файл будет сохранен в директории, где находится скрипт, и будет иметь имя:
`report <название сценария>_<дата>.csv`
где `<название сценария>` имеет значение в зависимости от номера сценария:

Номер сценария	Название сценария	Краткое описание
1	tbs_stat_period	Статистика за период времени.
2	tbs_stat_period_count	Статистика за период времени с указанием количества событий в ТП.
3	tbs_stat_by_tbs_id	Статистика по конкретному ТП.
4	tbs_stat_by_event_type	Статистика по типам событий за период.
5	tbs_stat_by_persons	Статистика по топ-10 сотрудников.
6	tbs_stat_by_person_id	Статистика по конкретной персоне.

`<дата>` – дата выполнения скрипта. Имеет формат `<год-месяц-день часы-минуты-секунды>`.
Пример имени файла выгрузки: `report_tbs_stat_period_count_2024-12-17_18-20-39.csv`

Сценарии работы скрипта

Сценарий 1

В результате выполнения сценария 1 будет выведена статистика по месту, занимаемому табличными пространствами, за указанный период времени.

```
Period tablespace stats

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date: 18.07.2026
Enter value for end_date: 19.07.2026
 tbs_id | tbs_type | part_date  | tbs_db_size | tbs_content_size |   | avg_tbs_size_by_all_tbs | avg_tbs_content_size_by_all_tbs
--------+----------+------------+-------------+------------------+---+-------------------------+---------------------------------
    168 |        2 | 19.07.2026 | 804 kB      | 0 bytes          |   | 1285 kB                 | 51 kB
    167 |        1 | 19.07.2026 | 1420 kB     | 53 kB            |   |                         |
    166 |        0 | 19.07.2026 | 1460 kB     | 53 kB            |   |                         |
    108 |        2 | 18.07.2026 | 1076 kB     | 90 kB            |   |                         |
    107 |        1 | 18.07.2026 | 1468 kB     | 54 kB            |   |                         |
    106 |        0 | 18.07.2026 | 1484 kB     | 53 kB            |   |                         |
(6 rows)
```

В столбцах будет указана следующая информация:

tbs_id	Идентификационный номер (ID) ТП
tbs_type	Тип ТП: 0 – Без нарушения 1 – Нарушение 2 – Другой (снимки экрана)
part_date	Дата создания ТП
tbs_db_size	Размер ТП в базе данных без учета бинарных данных
tbs_content_size	Размер бинарных данных ТП. Если вы используете Data Storage, эти данные хранятся там
avg_tbs_size_by_all_tbs	Средний размер одного ТП в БД без учета бинарных данных за указанный период времени
avg_tbs_content_size_by_all_tbs	Средний размер бинарных данных одного ТП за указанный период времени

Сценарий 2

В результате выполнения сценария 2 будет выведена статистика с количеством объектов по ТП за указанный период.

```
Period tablespace stats with count of objects

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date: 18.07.2026
Enter value for end_date: 19.07.2026

 tbs_id | part_date  | tbs_type | tbs_status | count_objects | tbs_db_size | tbs_content_size | avg_tbs_size_by_all_tbs | avg_tbs_content_size_by_all_tbs
--------+------------+----------+------------+---------------+-------------+------------------+-------------------------+---------------------------------
    168 | 19.07.2026 |        2 | 0 - online |             0 | 804 kB      | 0 bytes          | 1285 kB                 | 51 kB
    167 | 19.07.2026 |        1 | 0 - online |            16 | 1420 kB     | 53 kB            |                         |
    166 | 19.07.2026 |        0 | 0 - online |            26 | 1460 kB     | 53 kB            |                         |
    108 | 18.07.2026 |        2 | 0 - online |             3 | 1076 kB     | 90 kB            |                         |
    107 | 18.07.2026 |        1 | 0 - online |            17 | 1468 kB     | 54 kB            |                         |
    106 | 18.07.2026 |        0 | 0 - online |            27 | 1484 kB     | 53 kB            |                         |
(6 rows)
```

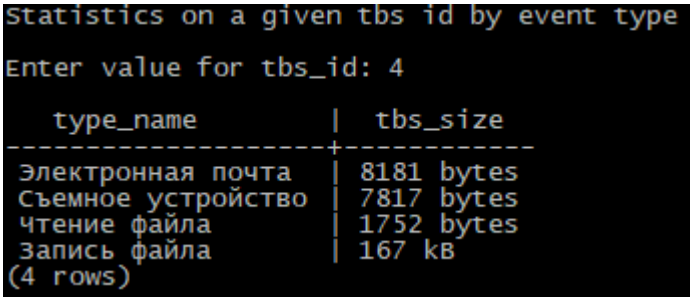
В столбцах будет указана следующая информация:

tbs_id	Идентификационный номер (ID) ТП
part_date	Дата создания ТП

tbs_type	Тип ТП: 0 – Без нарушения 1 – Нарушение 2 – Другой (снимки экрана)
tbs_status	Статус ТП: 0 – online (подключено, в нормальном состоянии) 3 – read only (только для чтения) 5 – before exchange (перед отключением для архивации) 7 – prepared offline (подготовлено к отключению для архивации) 9 – disconnected (отключено перед перемещением в архив) 10 – offline (архивировано и отключено) 11 – plugged (подключено перед восстановлением) 13 – before update (перед обновлением для восстановления) 15 – after update (после обновления для восстановления) 17 – before revert (перед восстановлением из архива) 20 – restored (восстановлено из архива)
count_objects	Количество событий в ТП
tbs_db_size	Размер ТП в базе данных без учета бинарных данных
tbs_content_size	Размер бинарных данных ТП. Если вы используете Data Storage, эти данные хранятся там
avg_tbs_size_by_all_tbs	Средний размер одного ТП в БД без учета бинарных данных за указанный период времени
avg_tbs_content_size_by_all_tbs	Средний размер бинарных данных одного ТП за указанный период времени

Сценарий 3

В результате выполнения сценария 3 будет выведена статистика по конкретному ТП.



В столбцах будет указана следующая информация:

type_name	Тип событий
tbs_size	Общий размер событий указанного типа в ТП

Сценарий 4

В результате выполнения сценария 4 будет выведена статистика по типам событий за указанный период.

```
Period stats by event type

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date:
Enter value for end_date:

  object_type       | objects_size | count_objects | max_objects_in_hour
--------------------+--------------+---------------+---------------------
 Электронная почта  | 167 kB       |             5 |                   4
 Съемное устройство | 8181 bytes   |             1 |                   1
 Чтение файла       | 7817 bytes   |             1 |                   1
 Запись файла       | 1752 bytes   |             1 |                   1
(4 rows)
```

В столбцах будет указана следующая информация:

object_type	Тип событий
objects_size	Общий размер событий указанного типа
count_objects	Количество событий указанного типа
max_objects_in_hour	Максимальное количество событий в час в течение дня

Сценарий 5

В результате выполнения сценария 5 будет выведена статистика по топ-10 сотрудников, события с участием которых занимают наибольшее место в БД, за указанный период времени.

```
Period stats by persons

Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date:
Enter value for end_date:

               person_id                 |  display_name  | object_count | objects_size
-----------------------------------------+----------------+--------------+--------------
 B37174C262444412B7AC8ECDCA544BD200000000 | Ivanov Ivan    |            3 | 109 kB
 099914C8CFD6416CB734C7721A2CF37600000000 | Petrov Petr    |            2 | 62 kB
 554BEE71D78B49CE80DA30301022AC9400000000 | Margaret Smith |            1 | 47 kB
(3 rows)
```

В столбцах будет указана следующая информация:

person_id	Идентификационный номер (ID) сотрудника

display_name	Отображаемое имя (ФИО) сотрудника
object_count	Количество событий
objects_size	Общий размер событий с участием сотрудника

Сценарий 6

В результате выполнения сценария 6 будет выведена статистика по конкретному сотруднику за указанный период времени.

```
Statistics on a given person id

Enter value for person_id: B37174C262444412B7AC8ECDCA544BD200000000
Date format: dd.mm.yyyy (empty - no filter. Default - 14 days)
Enter value for start_date:
Enter value for end_date:

'Ivanov Ivan'
 object_type        | object_count | objects_size
--------------------+--------------+--------------
 Электронная почта  |            3 | 109 kB
(1 row)
```

В столбцах будет указана следующая информация:

object_type	Тип событий
object_count	Количество событий
objects_size	Общий размер событий с участием сотрудника

8.1.4 Резервное копирование базы данных

Чтобы снизить риски потери данных, рекомендуем ежемесячно создавать резервную копию (бэкап) базы данных (БД). Для хранения бэкапов рекомендуется использовать специально выделенные системы хранения.

Для специалистов, не являющихся администраторами PostgreSQL, то есть не располагающих стандартными методами создания резервной копии БД, рекомендуем описанную ниже процедуру "холодного бэкапа", выполняемую на остановленной БД. Данная процедура также может применяться для переноса БД с одного сервера на другой.

Если в дополнение к БД вы используете хранилище бинарных данных Data Storage, вместе с резервной копией БД создавайте бэкап хранилища. Данная процедура описана вместе с созданием бэкапа БД.

Далее в разделе:

- *Создание резервной копии базы данных*
- *Восстановление базы данных из резервной копии*

Создание резервной копии базы данных

Процедура создания резервной копии (выполнения "холодного" бэкапа) осуществляется в следующем порядке:

- *Определение размера резервной копии*
- *Проверка хранилища резервной копии*
- *Создание каталогов для резервной копии*
- *Остановка системы*
- *Остановка PostgreSQL*
- *Копирование файлов БД в хранилище резервных копий*
- *Создание резервной копии Data Storage*

Определение размера резервной копии

Чтобы рассчитать размер будущего архива, нужно узнать суммарный размер следующих каталогов:

- каталог с базой PostgreSQL;
- каталог основного табличного пространства;
- каталоги ежедневных табличных пространств;
- каталог хранения данных Data Storage `/opt/dsdata/_seaweedfs`, если вы используете хранилище.

Для этого:

1. На сервере базы данных войдите в систему от имени пользователя **root**.
2. Получите суммарный размер каталогов:
   ```
   du -sx -BM /u01/postgres/ /u02/pgdata  /u02/pgdata1  /u02/arch
   ```
3. На сервере Data Storage аналогичным образом определите размер каталога `/opt/dsdata/_seaweedfs`.

Если используется другой режим хранения, то данные могут находиться в других директориях (подробнее см. *Настройка режимов хранения файлов табличного пространства*).

Проверка хранилища резервной копии

Чтобы проверить приемлемость выбранного хранилища резервной копии:

1. Смонтируйте внешнее хранилище на сервере базы данных (БД). Оно должно соответствовать следующим требованиям:
   - размещаться на компьютере, отличном от того, где работает БД или Data Storage;
   - быть доступно с компьютеров, где работают серверы и БД, подлежащие резервному копированию;
   - иметь больше свободного места на жестком диске, чем размер резервной копии.
2. Определите количество свободного места на жестком диске:
   a. Выполните следующую команду от имени **root**:
      ```
      OS>df -h
      ```
   b. Убедитесь, что свободного места в смонтированном разделе больше, чем размер резервной копии.

Создание каталогов для резервной копии

> **Внимание!**
>
> Директории файлов резервной копии должны находиться на компьютере, отличном от того, где расположены базы данных или Data Storage.

Чтобы создать структуру каталогов для бэкапа:

1. Войдите в систему от имени пользователя **root**.
2. Создайте директорию для хранения файлов резервной копии:
   `mkdir /opt/IWTM_Backup_Files`
3. Создайте следующие поддиректории:
   ```
   mkdir /opt/IWTM_Backup_Files/postgres
   mkdir /opt/IWTM_Backup_Files/pgdata
   mkdir /opt/IWTM_Backup_Files/pgdata1
   mkdir /opt/IWTM_Backup_Files/arch
   ```

Остановка системы

Остановка системы является необязательным шагом, но рекомендуется, особенно если на сервере мало свободного места.

Чтобы остановить систему:

1. На каждом компьютере, где запущены процессы серверной части Traffic Monitor, зайдите в систему от имени пользователя **root**.
2. Остановите все запущенные процессы:
   `iwtm stop`
   По окончании процедуры резервного копирования сервисы можно запустить с помощью следующих команд:
   `iwtm start`

Остановка PostgreSQL

> **Важно!**
>
> Перед началом резервного копирования файлов базы данных (БД) нужно остановить БД PostgreSQL.

Чтобы остановить БД PostgreSQL:

1. На компьютере, где работает БД, зайдите в систему от имени пользователя **root**.
2. В командной строке введите:
   ```
   systemctl stop pgagent
   systemctl stop postgresql
   ```
   По окончании процедуры резервного копирования сервисы можно запустить с помощью следующей команды:
   ```
   systemctl start pgagent
   systemctl start postgresql
   ```

Копирование файлов БД в хранилище резервных копий

Чтобы скопировать файлы базы данных (БД):

1. Остановите все сервисы PostgreSQL (см. *Остановка PostgreSQL*). Чтобы убедиться в остановке, выполните команду:
   `ps aux | grep postgre`
   Если сервисы PostgreSQL не остановлены, файлы резервной копии могут быть повреждены и оказаться непригодными для восстановления.

2. На компьютере, где установлена БД, скопируйте данные из директорий БД в созданные ранее директории. Копировать нужно все содержимое директорий, включая ссылки. Если система была установлена с помощью инсталлятора и были оставлены параметры по умолчанию, то:
    - скопируйте содержимое директории **/u01/postgres/** в директорию **/opt/IWTM_Backup_Files/postgres**
    - скопируйте содержимое директории **/u02/pgdata/** в директорию **/opt/IWTM_Backup_Files/pgdata**
    - скопируйте содержимое директории **/u02/pgdata1/** в директорию **/opt/IWTM_Backup_Files/pgdata1**
    - скопируйте содержимое директории **/u02/arch/** в директорию **/opt/IWTM_Backup_Files/arch**

Важно!

В качестве хранилища файлов используйте только следующие устройства:

- внешний диск с файловыми системами Ext4, XFS;
- удаленное блочное устройство, подключенное по протоколам iSCSI, NFS;
- локально подключенное блочное устройство с файловыми системами Ext4, XFS.

Создание резервной копии Data Storage

Данные Traffic Monitor хранятся в Data Storage в корзинах (bucket). Чтобы создать резервную копию хранилища бинарных данных, нужно создать копии этих корзин. Эта процедура состоит из следующих шагов:

1. *Включение возможности резервного копирования*
2. *Получение токена для работы с сервисом Data Storage*
3. *Получение списка корзин для бэкапа*
4. *Создание задачи резервного копирования*
5. *Проверка успешного завершения копирования*

В процессе создания копии Data Storage потребуется выполнять запросы с помощью утилиты **curl**. При их выполнении в качестве адреса сервера `<ADDRESS>` вы можете указывать:

- **localhost:40731**, если запросы будут выполняться на сервере, где установлено хранилище.
- **<IP_адрес_сервера>:40732**, если запросы отправляются с другого сервера.

Включение возможности резервного копирования

Чтобы можно было создать резервную копию Data Storage, нужно задать директорию для нее.

Рекомендуем делать это при установке хранилища, указывая при запуске инсталлятора параметр `--dsbackupspath` с директорией сохранения бэкапов.
Пример: `./setup.py install --dsbackupspath=/opt/dsbackups`

Чтобы задать директорию уже после установки, добавьте ее в деплоймент Data Storage. Для этого:

1. На сервере Data Storage создайте директорию для хранения резервной копии хранилища:

```
mkdir /opt/dsbackups
```

2. Смонтируйте в эту директорию внешнее хранилище резервных копий. Требования к хранилищу бэкапов описаны в статье *Проверка хранилища резервной копии*.
3. Назначьте пользователя и права доступа для созданной директории:

```
chown 1000 /opt/dsbackups
chmod 700 /opt/dsbackups
```

4. Откройте деплоймент Data Storage для редактирования с помощью команды:

```
kubectl -n infowatch edit deployment datastorage-<node_label>
```

   где `<node_label>` – здесь и далее лейбл ноды, на которой установлено хранилище. Для центральной ноды кластера или, если хранилище установлено не в кластере платформенных продуктов, используйте лейбл `central`. Для офисной ноды лейбл задается при установке, по умолчанию: `office`.
   Следующие действия зависят от того, какой вы используете текстовый редактор. В нашем примере мы используем **vi**. Чтобы войти в режим ввода, нажмите клавишу **i**.
5. В секцию `containers` -> `volumeMounts` добавьте следующие строки:

```
- name: datastorage-databackups-host-volume-<node_label>
  mountPath: /var/lib/databackups
  mountPropagation: HostToContainer
```

   В этом и следующем шаге делайте отступы с помощью пробела и не используйте табуляцию.
6. В секцию `volumes` добавьте следующие строки:

```
- name: datastorage-databackups-host-volume-<node_label>
  hostPath:
    path: /opt/dsbackups
```

7. Сохраните изменения и выйдите из редактора.
   Например, если вы используете редактор **vi**, нажмите **Esc** и введите `:wq`.

Получение токена для работы с сервисом Data Storage

Для работы с сервисом Data Storage нужно получить Bearer-токен для HTTP-авторизации. В запросах к Data Storage его нужно указывать в заголовке Authorization.
Значение токена может устаревать, и тогда в ответ на запрос сервис возвращает HTTP-код 440. В таком случае получите токен повторно.

Чтобы получить токен, отправьте в Data Storage запрос следующего вида:

```
curl -X GET -I --silent "http://<ADDRESS>/v2/logon?extAPIToken=<DS_user_token>" 2>&1 | grep
'^Authorization'
```

где `<ADDRESS>` – адрес сервера. Подробнее см. *выше*.
`<DS_user_token>` – токен авторизации Data Storage. Значение по умолчанию: `1exwo92iwpczl1hy6jxy`. Подробнее см. *Настройка соединения с Data Storage*.

В результате будет выведен заголовок Authorization в следующем формате:
`Authorization: Bearer <token_value>`

Получение списка корзин для бэкапа

Чтобы получить список идентификаторов корзин Data Storage, в которых хранятся данные Traffic Monitor, подключитесь к базе данных (БД) Traffic Monitor и выполните запрос:

```
select distinct(storage_bucket_id) from iwtm.tbs_list;
```

Если вам нужно узнать список всех существующих корзин Data Storage (их идентификаторы bucketID), выполните следующий запрос к сервису хранилища:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets?filter=*" 2>&1
```

где `<AUTH_HEADER>` – это заголовок Authorization, полученный на предыдущем шаге;
`<ADDRESS>` – адрес сервера.

Результат в формате JSON может иметь следующий вид:


```
{
  "data": [
    {
      "backendType": "seaweedfs",
      "id": "barbucket",
      "isDumped": false,
      "isInaccurate": false,
      "isSlowDrive": false,
      "size": 27632
    },
    {
      "backendType": "seaweedfs",
      "id": "bazbucket",
      "isDumped": false,
      "isInaccurate": false,
      "isSlowDrive": false,
      "size": 27633
    },
    {
      "backendType": "file",
      "id": "oldbucket",
      "isDumped": false,
      "isInaccurate": false,
      "isSlowDrive": false,
      "size": 27634
    }
  ]
}
```

Также вы можете отфильтровать список корзин с помощью регулярного выражения, используя утилиту **jq**. Например, следующий запрос найдет все корзины, у которых значение bucketID начинается на подстроку `bar`:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets?filter=*" 2>&1 | jq --raw-output
'.data.[] | select(.backendType=="seaweedfs") | select(.id|test("^bar")).id'
```

Создание задачи резервного копирования

Чтобы создать задачу на бэкап корзины, выполните следующий запрос:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?bucketID=<BUCKET_ID>"
```

где `<AUTH_HEADER>` – заголовок Authorization;
`<ADDRESS>` – адрес сервера. Подробнее см. *выше*;
`<BUCKET_ID>` – идентификатор корзины.

В ответ будет выведен идентификатор созданной задачи:

```
{
  "taskID": "fe8163f2-a0fb-4990-8bb7-87aee5c425bc"
}
```

Также вы можете создать задачу на бэкап корзины и получить идентификатор этой задачи, используя утилиту **jq**:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?bucketID=<BUCKET_ID>" |
jq --raw-output '.taskID'
```

Далее по идентификатору задачи можно проверить успешность выполнения резервного копирования корзины.

Проверка успешного завершения копирования

Чтобы убедиться в том, что копирование успешно завершено, проверьте статус задачи. Для этого выполните запрос:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?taskID=<TASK_ID>"
```

где `<AUTH_HEADER>` – это заголовок Authorization;
`<ADDRESS>` – адрес сервера. Подробнее см. *выше*;
`<TASK_ID>` – идентификатор задачи.

В случае успеха будут выведены имена созданных файлов данных и индекса в директории бэкапа:

```
{
  "bucketID": "foobucket",
  "dataFilename": "foobucket_0.tar.gz",
  "indexFilename": "foobucket_extindex.tar.gz",
  "taskStatus": "Success"
```

```
}
```

У случае неудачи будет выведено описание ошибки:

```
{
  "bucketID": "foobucket",
  "error": "permission denied: cannot extract data tarball",
  "taskStatus": "Success"
}
```

Убедитесь в том, что задача завершена и имеет один из следующих статусов: Success, Canceled, Failed.

Также вы можете получить статус задачи, используя утилиту **jq**:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/backups?taskID=<TASK_ID>" | jq
--raw-output '.taskStatus'
```

Восстановление базы данных из резервной копии

Чтобы восстановить базу данных (БД) и/или Data Storage:

1. Выберите способ восстановления БД, если это нужно:
   - если БД была повреждена вследствие сбоя системы или ошибки пользователя, восстановите старую БД. Например, если случайно был удален важный файл, вы можете восстановить БД до состояния, когда этот файл еще существовал (см. *Восстановление на той же базе данных*).
   - если старая БД не может больше использоваться, создайте новую и восстановите данные на ней (см. *Восстановление на новой базе данных*).
2. Следуйте одному из сценариев ниже. Инструкции можно найти в статьях *Остановка системы*, *Остановка PostgreSQL* и *Восстановление Data Storage*.

Если вы используете Data Storage и оно не повреждено, то при восстановлении БД действия с хранилищем не требуются. Data Storage не взаимодействует с БД напрямую.

Чтобы восстановить только БД:

1. Остановите службы Traffic Monitor.
2. Восстановите БД выбранным способом.
3. Запустите службы Traffic Monitor.

Чтобы восстановить только Data Storage:

1. Остановите службы Traffic Monitor.
2. Остановите БД.
3. Восстановите Data Storage.
4. Запустите БД.
5. Запустите службы Traffic Monitor.
6. Убедитесь, что соединение между Traffic Monitor и Data Storage установлено. При необходимости настройте его. Подробнее см. *Настройка соединения с Data Storage*.

Чтобы восстановить и БД, и Data Storage:

1. Остановите службы Traffic Monitor.
2. Восстановите Data Storage.

3. Восстановите БД.
4. Запустите службы Traffic Monitor.
5. Убедитесь, что соединение между Traffic Monitor и Data Storage установлено. При необходимости настройте его.

> **Важно!**
>
> Не допускается обновлять Traffic Monitor на другую версию до или в процессе восстановления БД и Data Storage.

Восстановление на той же базе данных

Ниже описана процедура восстановления на базе данных (БД), имеющей ту же структуру каталогов, что и та, с которой была создана резервная копия.

Чтобы восстановить БД без установки новой:

1. Убедитесь в работоспособности БД. Проверьте существующую схему БД, сервер БД, где размещена эта схема, и компьютер, на котором работает сервер БД;
2. Остановите сервисы PostgreSQL:
   ```
   systemctl stop postgresql
   systemctl stop pgagent
   ```
3. Выполните следующие шаги:
   a. Удалите все содержимое каталогов **/u01/postgres/**, **/u02/pgdata/**, **/u02/pgdata1/**, **/u02/arch/**
   b. Скопируйте содержимое директории **/opt/IWTM_Backup_Files/postgres** в директорию **/u01/postgres/**
   c. Скопируйте содержимое директории **/opt/IWTM_Backup_Files/pgdata/** в директорию **/u02/pgdata/**
   d. Скопируйте содержимое директории **/opt/IWTM_Backup_Files/pgdata1/** в директорию **/u02/pgdata1/**
   e. Скопируйте содержимое директории **/opt/IWTM_Backup_Files/arch/** в директорию **/u02/arch/**
4. Проверьте права. При необходимости измените их:
   ```
   chown -R postgres /u01/postgres/
   chown -R postgres /u02/pgdata/
   chown -R postgres /u02/pgdata1/
   chown -R postgres /u02/arch/
   ```
5. Запустите БД:
   ```
   systemctl start postgresql
   systemctl start pgagent
   ```

Восстановление на новой базе данных

Чтобы восстановить базу данных (БД) с помощью создания новой:

1. Установите новую БД и настройте ее согласно статье *InfoWatch Traffic Monitor. Руководство по установке. Настройка удаленной базы данных*.

> **Примечание:**
>
> Если вы установили БД на том же сервере, то во время настройки переустановите дополнительные пакеты `pgagent` и `postgresql-contrib`, используя в команде параметр `--reinstall`.

2. Скопируйте содержимое каталогов резервной копии, проверьте права и запустите сервисы БД аналогично *Восстановлению на той же базе данных*.
   Файлы БД нужно копировать в те же каталоги, в которых они хранились в старой БД.

Восстановление Data Storage

Восстановление данных хранилища бинарных данных заключается в восстановлении корзин из их резервных копий. Эта процедура состоит из следующих шагов:

1. *Получение токена для работы с сервисом Data Storage*
2. *Создание задачи восстановления корзины*
3. *Проверка успешного завершения задачи*

При выполнении **curl**-запросов к Data Storage в качестве адреса сервера `<ADDRESS>` вы можете указывать:

- **localhost:40731**, если запросы будут выполняться на сервере, где установлено хранилище;
- **<IP_адрес_сервера>:40732**, если запросы отправляются с другого сервера.

Получение токена для работы с сервисом Data Storage

Для работы с сервисом Data Storage нужно получить Bearer-токен для HTTP-авторизации. В запросах к Data Storage его нужно указывать в заголовке Authorization.
Значение токена может устаревать, тогда в ответ на запрос сервис возвращает HTTP-код 440. В таком случае получите токен повторно.

Чтобы получить токен, отправьте в Data Storage запрос следующего вида:

```
curl -X GET -I --silent "http://<ADDRESS>/v2/logon?extAPIToken=<DS_user_token>" 2>&1 | grep
'^Authorization'
```

где `<ADDRESS>` – адрес сервера.
`<DS_user_token>` – токен авторизации Data Storage. Значение по умолчанию: `1exwo92iwpczl1hy6jxy`. Подробнее см. *Настройка соединения с Data Storage*.

В результате будет выведен заголовок Authorization в формате `Authorization: Bearer <token_value>`.

Создание задачи восстановления корзины

Чтобы создать задачу на восстановление корзины, выполните следующий запрос:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?bucketID=<BUCKET_ID>"
```

где `<AUTH_HEADER>` – заголовок Authorization;
`<ADDRESS>` – адрес сервера;
`<BUCKET_ID>` – идентификатор корзины.

В ответ будет выведен идентификатор созданной задачи:

```
{
  "taskID": "fe8163f2-a0fb-4990-8bb7-87aee5c425bc"
}
```

Также вы можете создать задачу на восстановление корзины и получить идентификатор этой задачи, используя утилиту **jq**:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?bucketID=<BUCKET_ID>"
 | jq --raw-output '.taskID'
```

Далее по идентификатору задачи можно проверить успешность восстановления корзины.

> **Важно!**
>
> Вы можете восстановить корзину, только если корзины с таким же идентификатором нет в Data Storage.

Проверка успешного завершения задачи

Чтобы убедиться в том, что восстановление успешно завершено, проверьте статус задачи. Для этого выполните запрос:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?taskID=<TASK_ID>"
```

где `<AUTH_HEADER>` – это заголовок Authorization;
`<ADDRESS>` – адрес сервера;
`<TASK_ID>` – идентификатор задачи.

В случае успеха вы увидите следующий ответ:

```
{
  "bucketID": "foobucket",
  "taskStatus": "Success"
}
```

Убедитесь в том, что задача завершена и имеет один из следующих статусов: `Success, Canceled, Failed`.

Также вы можете получить статус задачи, используя утилиту **jq**:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?taskID=<TASK_ID>" | jq
--raw-output '.taskStatus'
```

8.1.5 Проведение регламентных работ на сервере базы данных

> **Важно!**
>
> Категорически не рекомендуем выключать сервер базы данных (БД) кнопкой питания. В некоторых случаях это может привести к повреждению БД.

При выполнении регламентных работ на сервере БД придерживайтесь такого порядка:

1. Закройте все окна браузера, отображающие Консоль управления. Убедитесь, что отсутствуют соединения со схемой БД Traffic Monitor из других программ. Если такие соединения есть, отключите их.
2. На сервере Traffic Monitor остановите процессы Traffic Monitor:
   ```
   iwtm stop
   service iwtm-php-fpm stop
   service nginx stop
   ```
3. На сервере БД получите список заданий, запускающихся по расписанию. Для этого в `psql` от имени владельца схемы выполните запрос:
   ```
   select jobname,  case when jobagentid is null then 'scheduled' else 'running' end state
   from pgagent.pga_job
   where jobenabled= true;
   ```
4. Выключите задания, выполнив сценарий:
   ```
   select iwtm.pkg_utility_disable_job('JOB_1');
   ...
   select iwtm.pkg.utility_disable_job('JOB_N');
   commit;
   ```
   где `JOB_1… JOB_N` – имена выключаемых заданий.
5. Убедитесь, что ни одно задание не выполняется. Для этого выполните запрос:
   ```
   select pga_job.jobname
   from pgagent.pga_job
   where pga_job.jobagentid is not null;
   ```
   Текущее задание невозможно остановить из PostgreSQL – это следует сделать посредством остановки агента из Linux с помощью команды:
   `systemctl stop pgagent` (остановка всех задач при помощи единой команды).
6. Выполните работы с БД.
7. По окончании работ с сервера Traffic Monitor проверьте соединение с сервером БД:
   ```
   psql postgres iwtm
   ```
   Если проверка пройдена успешно, тогда в ответ на выполнение команды будет выведено приглашение `psql`:
   `postgre=#` или `postgres=>`
8. Запустите процессы Traffic Monitor Server:
   ```
   iwtm start
   service iwtm-php-fpm start
   service nginx start
   ```
9. Проверьте системный журнал на наличие ошибок. Путь к файлу журнала:
   `/var/log/messages`

10. Если в системном журнале содержится информация об ошибках, то обратитесь в службу технической поддержки.
11. Включите выполнение ранее отключенных заданий:
```
BEGIN
select iwtm.pkg_utility_enable_job('JOB_1');
...
select iwtm.pkg_utility_enable_job('JOB_N');
commit;
end;
/
```
где `JOB_1… JOB_N` – имена ранее остановленных заданий.

8.1.6 Логирование базы данных

Traffic Monitor записывает лог базы данных PostgreSQL в файл `/u01/postgres/pg_log/postgresql.log`. Кроме того, Система формирует логи о заданиях, выполняемых с помощью pgAgent, и сохраняет их в файл `/u01/postgres/pg_log/pgagent-15.log`

Логированием заданий СУБД PostgreSQL в Traffic Monitor управляет скрипт `/opt/iw/tm5/csw/postgres/scripts/sys_log/sys_log.sh`, который позволяет устанавливать уровень логирования и выгружать данные лога в CSV-файл. При работе скрипта используются настройки текущего конфигурационного файла `/opt/iw/tm5/csw/database.conf`

Скрипт поддерживает следующие команды:

- чтобы установить уровень логирования, выполните команду:
  `/opt/iw/tm5/csw/postgres/scripts/sys_log/sys_log.sh level <уровень>`
  где `<уровень>` может принимать значения: `debug`, `info`, `warning` или `error`.
  Если выполнить команду без указания уровня, то отобразится текущий уровень логирования;
- чтобы выгрузить архив лога, выполните команду:
  `/opt/iw/tm5/csw/postgres/scripts/sys_log/sys_log.sh export`
  При этом, если требуется, можно задать количество выгружаемых строк:
  `/opt/iw/tm5/csw/postgres/scripts/sys_log/sys_log.sh export <количество строк>`
  При экспорте файл с логами сохраняется с именем вида `iwtm_sys_log_<гггг-мм-дд_чч-мм-сс>.csv.gz` в текущей директории.

О хранении логов на диске см. *Ротация логов базы данных*.

Ротация логов базы данных

Ротация логов базы данных (БД) – это процесс архивирования, хранения и удаления старых данных в журналах, нужный для экономии и освобождения свободного дискового пространства. В Traffic Monitor ротация настроена на лог БД в текстовом формате: `/u01/postrges/pg_log/*.log`. Он ротируется службой **logrotate** по 100 МБ и удаляется после превышения количества в 100 файлов.

Настройки службы **logrotate** находятся в `/etc/logrotate.d/iwtm-pg-conf`

8.2 Восстановление Data Storage

Восстановление хранилища бинарных данных заключается в восстановлении корзин из их резервных копий. Эта процедура состоит из следующих шагов:

1. *Получение токена для работы с сервисом Data Storage*
2. *Создание задачи восстановления корзины*
3. *Проверка успешного завершения задачи*

При выполнении **curl**-запросов к Data Storage в качестве адреса сервера `<ADDRESS>` вы можете указывать:

- **localhost:40731**, если запросы будут выполняться на сервере, где установлено хранилище;
- **<IP_адрес_сервера>:40732**, если запросы отправляются с другого сервера.

8.2.1 Получение токена для работы с сервисом Data Storage

Для работы с сервисом Data Storage нужно получить Bearer-токен для HTTP-авторизации. В запросах к Data Storage его нужно указывать в заголовке Authorization.
Значение токена может устаревать, тогда в ответ на запрос сервис возвращает HTTP-код 440. В таком случае получите токен повторно.

Чтобы получить токен, отправьте в Data Storage запрос следующего вида:

```
curl -X GET -I --silent "http://<ADDRESS>/v2/logon?extAPIToken=<DS_user_token>" 2>&1 | grep
'^Authorization'
```

где `<ADDRESS>` – адрес сервера.
`<DS_user_token>` – токен авторизации Data Storage. Значение по умолчанию: `1exwo92iwpczl1hy6jxy`. Подробнее см. *Настройка соединения с Data Storage*.

В результате будет выведен заголовок Authorization в формате `Authorization: Bearer <token_value>`.

8.2.2 Создание задачи восстановления корзины

Чтобы создать задачу на восстановление корзины, выполните следующий запрос:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?bucketID=<BUCKET_ID>"
```

где `<AUTH_HEADER>` – заголовок Authorization;
`<ADDRESS>` – адрес сервера;
`<BUCKET_ID>` – идентификатор корзины.

В ответ будет выведен идентификатор созданной задачи:

```
{
  "taskID": "fe8163f2-a0fb-4990-8bb7-87aee5c425bc"
}
```

Также вы можете создать задачу на восстановление корзины и получить идентификатор этой задачи, используя утилиту **jq**:

```
curl -X POST --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?bucketID=<BUCKET_ID>"
 | jq --raw-output '.taskID'
```

Далее по идентификатору задачи можно проверить успешность восстановления корзины.

> **Важно!**
>
> Вы можете восстановить корзину, только если корзины с таким же идентификатором нет в Data Storage.

8.2.3 Проверка успешного завершения задачи

Чтобы убедиться в том, что восстановление успешно завершено, проверьте статус задачи. Для этого выполните запрос:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?taskID=<TASK_ID>"
```

где `<AUTH HEADER>` – это заголовок Authorization;
`<ADDRESS>` – адрес сервера;
`<TASK_ID>` – идентификатор задачи.

В случае успеха вы увидите следующий ответ:

```
{
  "bucketID": "foobucket",
  "taskStatus": "Success"
}
```

Убедитесь в том, что задача завершена и имеет один из следующих статусов: Success, Canceled, Failed.

Также вы можете получить статус задачи, используя утилиту **jq**:

```
curl -X GET --header "<AUTH_HEADER>" --silent "http://<ADDRESS>/v3/buckets/restores?taskID=<TASK_ID>" | jq
--raw-output '.taskStatus'
```

9 Администрирование серверной части InfoWatch Traffic Monitor

В этой главе описаны компоненты серверной части Traffic Monitor, настройки и методы их использования:

- *Процессы серверной части Traffic Monitor*
- *Настройка использования OCR*
- *Настройка параметров обработки архивов вложений*
- *Настройка параметров поиска с использованием групповых символов*
- *Настройка интеграции с Data Analysis Service*
- *Настройка соединения с Data Storage*
- *Настройка отправки событий в Платформу*
- *Логирование работы Системы*
- *Файловые очереди*
- *Восстановление работоспособности системы в аварийных ситуациях*
- *Управление языками с поддержкой морфологии*
- *Настройка передачи информации в SIEM*
- *Удаление временных файлов*

9.1 Процессы серверной части Traffic Monitor

В этом разделе:

- *Список процессов серверной части Traffic Monitor*
- *Настройка конфигурационных файлов серверной части Traffic Monitor*
- *Работа с процессами серверной части Traffic Monitor*

9.1.1 Список процессов серверной части Traffic Monitor

Работа Системы осуществляется посредством процессов. Один и тот же процесс может быть запущен единовременно в нескольких экземплярах.

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
Сбор данных	`iw_icap`	Обрабатывает HTTP-трафик. Принимает HTTP-запросы от ICAP-клиента. Извлекает данные из HTTP-запросов. Затем извлеченные данные добавляются в XML-контекст. Готовый XML-контекст передается подсистеме анализа и принятия решения для проверки. По окончании анализа передает ICAP-клиенту ответ с разрешением/запретом на доставку HTTP-запроса. Посредством файловой очереди HTTP-запрос передается	`/opt/iw/tm5/etc/icap.conf`

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
		процессу **iw_x2x**, а затем – процессу **iw_x2db**.	
	iw_icap_buf	Сохраняет части большого по объему файла в своем хранилище. Далее сформированный объект в виде полного файла отправляет одним запросом в **iw_icap** для анализа.	/opt/iw/tm5/etc/icap_buf.conf
	iw_proxy	Принимает копию трафика и передает ее модулю iw_messed, разбив на HTTP-, ICQ- и SMTP-трафик. Включает следующие процессы: • iw_proxy_http – процесс, принимающий копию HTTP-трафика. Принимает HTTP-запрос, формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа и принятия решения **iw_analysis**. • iw_proxy_icq – процесс, принимающий копию ICQ-трафика. Принимает ICQ-сообщение, формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа и принятия решения **iw_analysis**. • iw_proxy_smtp – процесс, принимающий копию SMTP-трафика. Принимает SMTP-письмо, формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа **iw_messed**.	/opt/iw/tm5/etc/proxy.conf

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
		По окончании анализа объект передается процессу **`iw_x2x`**, а затем – процессу **`iw_x2db`**.	
	`iw_smtpd`	Принимает SMTP-письма. В случае интеграции с почтовым сервером Postfix принимает входящие сообщения от Postfix. Если интеграции с Postfix нет, сообщения принимаются от корпоративного почтового сервера или от почтового клиента (в зависимости от настроек вашей почтовой системы). Принимает входящие сообщения в формате SMTP, преобразует в XML-контекст данные SMTP-конверта. Затем передает SMTP-письмо и XML-контекст процессу **`iw_messed`**.	`/opt/iw/tm5/etc/smtpd.conf`
	`iw_capstack`	Выполняет обработку трафика, передаваемого по протоколам POP3, IMAP, NRPC.	`/opt/iw/tm5/etc/capstack.conf`
	`iw_messed`	Обрабатывает SMTP-письма. Извлекает данные из SMTP-, POP3- и IMAP-объектов. Затем извлеченные данные добавляются в полученный XML-контекст. Готовый XML-контекст, содержащий данные конверта и письма, передается подсистеме анализа и принятия решения для проверки. По окончании анализа **`iw_messed`** передает SMTP-письма, доставка которых разрешена, компоненту почтовой системы, ответственному за доставку почты (только в нормальном и прозрачном транспортном режиме). В случае интеграции с почтовым сервером Postfix таким компонентом является Postfix. Если интеграции с Postfix нет, то, в зависимости от настроек вашей почтовой системы, таким компонентом может быть корпоративный почтовый сервер или почтовый клиент. Проверенное SMTP-	`/opt/iw/tm5/etc/messed.conf`

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
		письмо посредством файловой очереди передается процессу **iw_x2x**, а затем – процессу **iw_x2db**.	
	iw_xapi	Включает в себя две службы: **iw_xapi_xapi** и **iw_xapi_puppy**. Получает объекты от InfoWatch Device Monitor и внешних систем (через адаптеры) по Thrift-интерфейсу, передает их в файловую очередь. Далее отправляет объекты процессу **iw_analysis**. При получении EML-объектов передает их процессу **iw_messed**.	/opt/iw/tm5/etc/xapi.conf
	iw_analysis	Принимает объекты из файловой очереди, в которую их передает **iw_xapi_xapi** / **iw_xapi_puppy**, **iw_proxy_icq**, **iw_proxy_http**. Посредством файловой очереди отправляет на обработку процессам **iw_warpd**, **iw_cas**, **iw_pas**, **iw_luaengined**. Далее объекты передаются в файловую очередь для отправки процессу **iw_x2x**, а затем – процессу **iw_x2db**.	/opt/iw/tm5/etc/analysis.conf /opt/iw/tm5/etc/analysis_client.conf – клиентский конфигурационный файл для соединения с iw_cas и iw_pas
	iw_rest2push	Позволяет принимать объекты от внешних систем по протоколу HTTP/HTTPS. Подключается к службе iw_xapi_puppy, передает события по Thrift-протоколу.	/opt/iw/tm5/etc/rest2push.conf
Обработка данных	iw_warpd	Управляет процессами извлечения данных из контейнеров, вложенных в перехваченные объекты.	/opt/iw/tm5/etc/warpd.conf
	iw_image2text_fre	Осуществляет распознавание текста в изображениях при помощи OCR Content AI ContentReader Engine.	/opt/iw/tm5/etc/image2text_fre.conf

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
	`iw_image2text_ts`	Осуществляет распознавание текста на изображениях при помощи OCR Tesseract.	`/opt/iw/tm5/etc/image2text_ts.conf`
	`iw_cas`	Выполняет роль сервера контентного анализа. Процесс **`iw_cas`** принимает от подсистем перехвата текстовые запросы в формате plain-text для проведения контентного анализа. По окончании контентного анализа возвращает результат запроса подсистеме анализа и принятия решения.	`/opt/iw/tm5/etc/cas.conf`
	`iw_image_autoling`	Выполняет автоматическую классификацию графических объектов.	`/opt/iw/tm5/etc/iw_image_autoling.conf`
	`iw_text_autoling`	Выполняет автоматическую классификацию текстовых объектов.	`/opt/iw/tm5/etc/iw_text_autoling.conf`
	`iw_pas`	Получает результаты анализа **`iw_cas`**. Определяет наличие объекта защиты и добавляет объекту соответствующие атрибуты.	`/opt/iw/tm5/etc/pas.conf`
	`iw_luaengined`	Обеспечивает выполнение LUA-скрипта согласно действующей политике.	`/opt/iw/tm5/etc/luaengined.conf` `/opt/iw/tm5/etc/lua.conf` – клиентский конфигурационный файл для соединения с `iw_luaengined`
	`iw_x2x`	Получает данные с XML+DAT-файлами посредством файловой очереди. Полученные файлы модифицируются и отправляются процессу **`iw_x2db`**.	`/opt/iw/tm5/etc/x2x.conf`
	`iw_tech_tools`	Верифицирует условия для выгрузок из БД и регулярные выражения, позволяет нормализовать текст в	`/opt/iw/tm5/etc/tech_tools.conf`

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
		соответствии с регулярными выражениями.	
Загрузка в БД	`iw_qmover_client`	Работает на сервере Traffic Monitor, установленном в филиале. Отправляет перехваченные объекты в БД центрального офиса.	`/opt/iw/tm5/etc/qmover_client.conf`
	`iw_qmover_server`	Работает на сервере Traffic Monitor, установленном в центральном офисе. Принимает объекты, полученные от Агента, установленного в филиале. Передает через **`iw_x2x`** объекты процессу **`iw_x2db`** для сохранения в БД.	`/opt/iw/tm5/etc/qmover_server.conf`
	`iw_x2db`	Загружает в БД объекты, проверенные подсистемой анализа и принятия решения, из выходной файловой очереди процесса **`iw_x2x`**.	`/opt/iw/tm5/etc/x2db.conf`
Инфраструктура	`iw_adlibitum`	Управляет процессами получения актуальных данных с сервера Active Directory, Domino Directory, Samba DC, Альт Домен, Astra Linux Directory, Astra Linux Directory Pro и FreeIPA.	`/opt/iw/tm5/etc/adlibitum.conf`
	`iw_agent`	Нужен для управления конфигурацией Системы.	`/opt/iw/tm5/etc/agent.conf`
	`iw_attributor`	Осуществляет взаимодействие с Data Analysis Service: передает данные для анализа и загружает принятые данные в БД.	`/opt/iw/tm5/etc/attributor.conf`
	`iw_blackboard`	Предоставляет Thrift-интерфейс для вычитки файловой очереди команд и передает их выполнение другим службам. Команды включают в себя добавление статусов и контактов персонам, обновление метаинформации о контакте, добавление статусов рабочим станциям, отправку уведомлений	`/opt/iw/tm5/etc/blackboard.conf`

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
		о событиях, добавление приложений в список.	
	`iw_bookworm`	Выполняет роль справочника в Системе.	`/opt/iw/tm5/etc/bookworm.conf` `/opt/iw/tm5/etc/bookworm_client.conf` – клиентский конфигурационный файл для соединения с `iw_bookworm`.
	`iw_cas_config_compiler`	Переводит конфигурационный файл сервера контентного анализа в бинарный вид для возможности использования конфигурации в контентном анализе.	`/opt/iw/tm5/etc/cas_config_compiler.conf`
	`iw_configerator`	Формирует конфигурацию, которая отправляется в Device Monitor.	`/opt/iw/tm5/etc/configerator.conf`
	`iw_deliver`	Выполняет доставку писем. Отправляет SMTP-письма получателям в случае, если доставка письма разрешена из Консоли управления (только в нормальном и прозрачном транспортных режимах). Также этот процесс доставляет SMTP-письма, которые по той или иной причине (например, ввиду отсутствия связи с почтовым relay-сервером или почтовым клиентом) не смог доставить процесс **`iw_messed`**.	`/opt/iw/tm5/etc/deliver.conf`
	`iw_metainfo_fetcher`	Осуществляет выборку данных из БД, содержащих метаинформацию о всех контактах, в том числе о контактах, участвующих в событиях (для индексации). Отправляет их процессу **`iw_is`**.	–
	`iw_audit_fetcher`	Осуществляет выборку из БД данных событий расширенного	–

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
		аудита для индексации. Отправляет их процессу **iw_is**.	
	iw_is	Управляет процессом индексирования данных и работой поисковых серверов для полнотекстового поиска. Подготавливает файлы с описанием данных, которые через файловые очереди доходят до индексатора, и запускает его.	/opt/iw/tm5/etc/is.conf
	iw_indexer	Индексирует текст в событиях из БД. Получает доступ к БД для ее индексации и складывает индексы в файловое хранилище. При выполнении поискового запроса **sphinx** получает ID объектов из файлового хранилища индексов.	/opt/iw/tm5/etc/indexer.conf
	iw_kicker	Служит для корректной работы WebGUI, осуществляет запуск сервисов: agent, blackboard, export, import, report, notifier, selection, systemcheck, xapisamplecompiler, samplecompiler, querytracker, reporttracker	/opt/iw/tm5/etc/kicker.conf
	iw_licensed	Подсистема лицензирования. Производит мониторинг и обработку установленных в Системе лицензий.	/opt/iw/tm5/etc/licensed.conf /opt/iw/tm5/etc/license.conf – клиентский конфигурационный файл для соединения с iw_licensed
	iw_rammer	Выполняет досылку писем с ошибками обработки при работе "в разрыв".	/opt/iw/tm5/etc/rammer.conf
	iw sample_compiler	Создает цифровые отпечатки из загруженных эталонных файлов.	/opt/iw/tm5/etc/sample_compiler.conf

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
	`consul`	Производит обнаружение, регистрацию и мониторинг доступности сервисов, взаимодействующих с интерфейсом пользователя.	`/opt/iw/tm5/etc/consul/consul.json`
	`iw_system_check`	Собирает данные от службы Nagios и предоставляет их для отображения в Консоли управления.	`/opt/iw/tm5/etc/system_check.conf`
	`iw_updater`	Загружает конфигурацию из БД на сервер Traffic Monitor.	`/opt/iw/tm5/etc/updater.conf`
	`iw_space_manager`	Управляет табличными пространствами в разделе **Табличные пространства** Консоли управления.	`/opt/iw/tm5/etc/space_manager.conf`

Внимание!

В данной версии Traffic Monitor перехват для Astra Linux осуществляется на стороне Device Monitor и перехватчиками **`iw_smtpd`** и **`iw_icap`** на стороне Traffic Monitor. Поэтому следующие сервисы Traffic Monitor должны быть установлены, но отключены по умолчанию до принудительного запуска:

- `iw_proxy`
- `iw_capstack`

9.1.2 Настройка конфигурационных файлов серверной части Traffic Monitor

Полный перечень конфигурационных файлов Системы и описание настроек, которые вы можете изменять для отражения специфики работы Системы в вашей инфраструктуре, находятся в документе *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*. Не рекомендуем изменять файлы, не описанные в данном документе.

Расположение конфигурационных файлов: `/opt/iw/tm5/etc`

Конфигурационные файлы Системы имеют формат JSON. Названия конфигурационных файлов соответствуют названиям тех компонентов, для настройки которых они используются. Например, для конфигурирования компонента **iw_x2x** используется конфигурационный файл **x2x.conf**.

Различают общие настраиваемые секции параметров и параметры, специфичные для каждого из конфигурационных файлов.

См. документ *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*:

- описание общих секций:
  - *Общая секция Bookworm*
  - *Общая секция Discovery*
  - *Общая секция Logging*
  - *Общая секция Statistics*
  - *Общая секция Statistic*
  - *Общая секция ThriftServers*
  - *Общая секция ThriftClients*
- описание отдельных файлов.

9.1.3 Работа с процессами серверной части Traffic Monitor

Список процессов Traffic Monitor представлен в главе *Список процессов серверной части Traffic Monitor*.

Все процессы Traffic Monitor Server запускаются от имени пользователя `iwtm`, который создается в процессе установки Traffic Monitor Server автоматически (подробнее о учетных записях см. документ *InfoWatch Traffic Monitor. Руководство по установке*).

> **Примечание:**
>
> Имя пользователя прописывается в unit-файлах процессов в параметре `User`. Для стабильной работы Системы рекомендуется оставить значение этого параметра без изменений.

Во время работы состояние процессов Traffic Monitor Server проверяется сценарием `pguard`, который создается в директории `/opt/iw/tm5/bin` в ходе установки. Если по какой-либо причине один или несколько процессов Traffic Monitor Server были остановлены, сценарий `pguard` перезапускает эти процессы.
Управление работой процессов Traffic Monitor Server выполняется при помощи bash-скрипта `/opt/iw/tm5/bin/iwtm`, который является сценарием автозапуска для уровней запуска (runlevel) 2, 3, 4, 5.

> **Примечание:**
>
> - Процессы `iw_qmover_server`, `iw_qmover_client` доступны, но для них по умолчанию выключен автозапуск. Каждый процесс запускается на соответствующей стороне (в филиалах `iw_qmover_client`, в центральном офисе `iw_qmover_server`).
> - Процесс `iw_rammer` не установлен по умолчанию. После ручной установки он становится доступен в списке процессов.
> - Если нужно остановить процессы на серверах распределенного кластера Traffic Monitor, в первую очередь остановите процессы на сервере, установленном при помощи шаблона *Перехватчики*, в последнюю – на сервере *База данных*. Запуск процессов необходимо начинать с сервера, установленного при помощи шаблона *База данных*, и заканчивать сервером *Перехватчики*.
> - Остановка и запуск процессов при использовании сервером Traffic Monitor внешнего хранилища Data Storage проводятся также, как и без него.

Ключи запуска для сценария `iwtm`:

Ключ запуска	Назначение
`start`	Запуск процессов
`stop`	Безопасная остановка процессов
`status`	Вывод на экран информации о состоянии процессов (запущен/не запущен/доступен/не доступен)
`restart`	Перезапуск процессов (последовательное выполнение `start` и `stop`)
`reload`	Перезагрузка конфигурации процесса
`kill`	Передача процессу сигнала для его немедленного завершения (SIGKILL)
`test`	Вывод на экран всех доступных демонов `iwtm`
`enable`	Назначение демону статуса "доступен" – автозапуск демона разрешен
`disable`	Назначение демону статуса "недоступен" – автозапуск демона запрещен
`services_state`	Вывод на экран всех доступных демонов `iwtm` с побитовыми масками

Примеры команд

Команда	Описание
`iwtm status`	Проверить состояние процессов Traffic Monitor Server

Любая команда на выбор:
`service iw_cas start` (если требуется просмотр логов)
`iwtm start cas`
`iwtm start iw_cas`
`iwtm start iw_cas.service`
	Запустить сервер контентного анализа (CAS)

Команда	Описание
`systemctl start iw_cas` (без возможности просмотра логов) `systemctl start iw_cas.service`	

Важно!

В каталоге `/opt/iw/tm5/run` хранятся PID-файлы. При аварийном завершении работы необходимо перед запуском процессов стереть все PID-файлы.

Изменение параметров автозапуска процессов

Информация о необходимости включения и отключения автозапуска процессов изложена в статье *Проверка автозапуска процессов*.

Для каждого процесса, управляемого bash-скриптом `iwtm`, можно задать возможность автозапуска в командной строке. Эта настройка описана в статье *Включение и выключение автозапуска процессов*. Подробнее о командах systemd в статье *Команды для работы с systemd*.

9.1.4 Шифрование SSL Thrift

Чтобы использовать шифрование:

1. Подготовьте ключ и сертификаты.
2. Остановите сервисы на ноде Traffic Monitor с помощью команды:

   ```
   iwtm stop
   ```

3. Настройте секции `ThriftServers` и `ThriftClients` в конфигурационных файлах сервисов, для которых необходимо использовать соединение SSL Thrift.
4. В файле `/opt/iw/tm5/etc/web.conf` укажите, для каких сервисов необходимо использовать соединение SSL Thrift. Для этого в секции `ssl` установите значение `true` для сервисов, которые будут использовать шифрование.
   Например:

   ```
   "ssl": {
       "iw_xapi_puppy": true,
       "iw_adlibitum": false,
       "iw_blackboard": false,
       "iw_bookworm": false,
       "iw_agent": false,
       "iw_licensed": true,
       "iw_sample_compiler": false,
       "iw_image_autoling": true,
       "iw_text_autoling": true,
       "iw_system_check": false,
   ```

```
    "iw_tech_tools": false
},
```

5. Запустите сервисы:

```
iwtm start
```

Важно!

Если до обновления Traffic Monitor на версию 7.15 было включено шифрование, перед запуском сервисов проверьте, что конфигурационные файлы содержат добавленные вами настройки.

Подготовка ключа и сертификатов

Для шифрования требуются:

- доверенный корневой сертификат (CA). После установки Traffic Monitor расположен в `/opt/iw/tm5/etc/cert/trusted_certificates`;
- сертификат, подписанный корневым сертификатом (CA). После установки Traffic Monitor расположен в `/opt/iw/tm5/etc/cert/server.pem`;
- приватный ключ. После установки Traffic Monitor расположен в `/opt/iw/tm5/etc/cert/private_key.pem`.

Вы можете:

- использовать сертификаты и ключ, поставляемые с продуктом. Их расположение указано выше;
- сгенерировать и использовать собственные сертификаты и ключ.

Для подготовки собственных сертификатов и ключа выполните следующие действия:

1. Создайте резервные копии предустановленных сертификатов, расположенных в папке `/opt/iw/tm5/etc/cert`.

   Примечание:

   В инструкции для новых сертификатов используются названия предустановленных.

2. Создайте приватный ключ с помощью команды:

```
openssl genrsa -out ca.key 4096
```

3. Создайте самоподписанный корневой сертификат (CA) с помощью команды:

```
openssl req -x509 -new -key ca.key -out trusted_certificates -days 3650 -subj "/C=RU/
ST=Moscow/L=Moscow/O=MyOrg/CN=My Internal CA"
```

   где:

- `C` – код страны;
- `ST` – регион;
- `L` – город;
- `O` – название организации;
- `CN` – название продукта/сервиса.

4. Создайте приватный ключ для сервера с помощью команды:

```
openssl genrsa -out private_key.pem 2048
```

5. Создайте запрос на подпись (CSR – Certificate Signing Request) с помощью команды:

```
openssl req -new -key private_key.pem -out server.csr -subj "/C=RU/ST=Moscow/O=MyOrg/
OU=Department/CN=XAPI"
```

где:

- `C` – код страны;
- `ST` – регион;
- `L` – город;
- `O` – название организации;
- `OU` – название подразделения;
- `CN` – название продукта/сервиса.

6. Подпишите запрос своим корневым сертификатом (CA) с помощью команды:

```
openssl x509 -req -in server.csr -CA trusted_certificates -CAkey ca.key -CAcreateserial
-out server.pem -days 365
```

> **Важно!**
>
> Если для разных нод или сервисов вы будете использовать разные сертификаты, создайте и подпишите каждый серверный сертификат корневым (CA).
>
> Для всех нод и сервисов используйте один корневой сертификат (CA).

7. На каждой ноде Traffic Monitor:
   a. Скопируйте корневой сертификат (CA) по пути `/opt/iw/tm5/etc/cert/trusted_certificates`.
   Использование другой папки не поддерживается.
   b. Скопируйте сертификат сервера по пути `/opt/iw/tm5/etc/cert/server.pem`.
   c. Скопируйте приватный ключ по пути `/opt/iw/tm5/etc/cert/private_key.pem`.
8. Поменяйте владельца всех файлов в папке `/opt/iw/tm5/etc/cert` с помощью команды:

```
chown -R iwtm:iwtm /opt/iw/tm5/etc/cert
```

Настройки конфигурационных файлов

Вы можете настроить Thrift-соединение в конфигурационных файлах:

- `/opt/iw/tm5/etc/image_autoling.conf`
- `/opt/iw/tm5/etc/cas.conf`
- `/opt/iw/tm5/etc/agent.conf`
- `/opt/iw/tm5/etc/system_check.conf`
- `/opt/iw/tm5/etc/pas.conf`
- `/opt/iw/tm5/etc/luaengined.conf`
- `/opt/iw/tm5/etc/blackboard.conf`
- `/opt/iw/tm5/etc/sample_compiler.conf`
- `/opt/iw/tm5/etc/licensed.conf`
- `/opt/iw/tm5/etc/adlibitum.conf`
- `/opt/iw/tm5/etc/bookworm.conf`
- `/opt/iw/tm5/etc/text_autoling.conf`
- `/opt/iw/tm5/etc/xapi.conf`
- `/opt/iw/tm5/etc/tech_tools.conf`
- `/opt/iw/tm5/etc/messed.conf`

Настройки производятся в следующих секциях:

- **`ThriftServers`** – сервисы, к которым подключаются клиенты;
- **`ThriftClients`** – сервисы, которые подключаются к серверам.

По умолчанию шифрование в конфигурационных файлах выключено. Чтобы включить шифрование, в обоих секциях:

- в параметре `TransportType` укажите значение `ssl`;
- в параметрах `CertificatePath`, `PrivateKeyPath` и `TrustedCertificatesPath` укажите пути до сертификата клиента, подписанного корневым сертификатом, приватного ключа и корневого сертификата;
- если требуется включить аутентификацию, в параметре `AuthenticateClient` укажите значение `true`;
- если требуется установить для SSL-сокетов версию шифрования протокола не ниже TLS 1.2 и исключить из доступных алгоритмов шифрования все алгоритмы из групп 3DES и RC4, в параметре `UseLegacySSL` укажите значение `false`.

Также в секции `Thrift Servers` в параметре `Port` укажите порт входящих соединений, в зависимости от сервиса:

- `adlibitum` – 9096
- `agent` – 9099
- `blackboard` – 9093
- `bookworm` – 9090
- `cas` – 9987
- `image_autoling` – 9103
- `text_autoling` – 9104
- `licserv` – 9095
- `luaengined` – 9988
- `pas` – 9989
- `sample_compiler` – 9091
- `system_check` – 9097
- `tech_tools` – 9102
- `puppy` – 9101
- `xapi` – 9100

Подробнее о параметрах секций см. *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*.

Важно!

Для успешного соединения ключи и сертификаты клиентов (`ThriftClients`) и сервера (`ThriftServers`) должны быть подписаны одним корневым сертификатом.

9.2 Настройка использования OCR

Технология OCR предназначена для перевода изображений рукописного, машинописного или печатного текста в текстовые данные. По умолчанию технология отключена для всех сервисов, типов событий и связанных с ними протоколов. OCR используется для:

- анализа перехваченных изображений;
- анализа изображений, загруженных как эталонные документы.

Для работы технологии используются процессы:

- **`iw_warpd`** – для извлечения данных из контейнеров, вложенных в перехваченные объекты;
- **`iw_sample_compiler`** – для создания цифровых отпечатков из загруженных эталонных файлов.

Включение и настройка технологии OCR осуществляется в конфигурационных файлах этих процессов. Подробнее см. *Настройка OCR-экстракторов*.

При необходимости использование OCR для анализа перехваченных изображений можно настроить следующими способами:

Уровень перехвата	События, к содержимому которых применяется настройка	Приоритет выполнения настройки
Сервис	Полученные по протоколам типов событий этого сервиса (если для данных типов событий или протоколов не задана своя настройка OCR)	Низкий
Тип события для конкретного сервиса	Полученные по протоколам этого типа события (если для этих протоколов не задана своя настройка OCR)	Средний
Протокол для конкретного типа события	Полученные по выбранному протоколу для указанного типа события	Высокий

Настройки OCR задаются в справочнике демона **`iw_bookworm`** в каталоге `/opt/iw/tm5/etc/config-perm/`**`bookworm`** :

- `ocr.xml` – предустановленные настройки, используемые по умолчанию;
- `ocr_custom.xml` – пользовательские настройки для конкретного типа внедрения.

Важно!

При обновлении Системы на текущую версию параметры OCR будут сброшены на предустановленные. В случае добавления или изменения функциональных возможностей OCR новые настройки будут доступны в файле `ocr.xml`. Пользовательские настройки останутся в файле `ocr_custom.xml` без изменений.

9.2.1 Включение использования технологии OCR при внедрении

Для включения использования технологии OCR при внедрении нужно внести изменения в файле `ocr_custom.xml` (подробнее см. *Конфигурационный файл ocr_custom.xml*), а именно:

1. Выбрать конкретные объекты: сервисы, протоколы и типы событий[1].
2. Задать идентификаторы объектов справочника сервисов и типов событий (файлы с описанием находятся в каталоге `/opt/iw/tm5/etc/config/bookworm/`).
3. Включить использование OCR (`ocr_enabled="true"`).

Примечание:

[1] Новые типы событий, зарегистрированные через плагин, автоматически добавляются в `/opt/iw/tm5/etc/config/bookworm/services.xml` и становятся доступными для обработки и переноса в файл `ocr_custom.xml`.

9.2.2 Настройка OCR для нескольких нод

При необходимости настройки OCR для нескольких нод (распределенная установка) требуется задать правила для каждой из нод. Для этого нужно:

1. Создать новый XML-файл для описания ноды в каталоге `/opt/iw/tm5/etc/config-perm/bookworm`
2. Указать созданный XML-файл в секции `CustomNodeXMLPath` конфигурационного файла `/opt/iw/tm5/etc/bookworm.conf`
3. Указать в параметре `<ocr_option node>` название ноды из файла `/opt/iw/tm5/node_name`
4. Описать переопределяемые правила для ноды, как описано выше.

Примечание:

В этом случае будет установлен следующий приоритет настроек (по убыванию):

- справочник с настройками для ноды;
- справочник с пользовательскими настройками;
- справочник с предустановленными настройками.

9.2.3 Конфигурационный файл ocr_custom.xml

С помощью конфигурационного файла `/opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml` вы можете включить OCR:

- для отдельных сервисов и протоколов;

- сразу на всех доступных уровнях.

Рекомендуем включать только нужные правила.

В начале конфигурационного файла представлен закомментированный символами `<!-- -->` блок с примерами правил включения OCR, где:

- `object_type` – тип события;
- `service` – сервисы;
- `protocol` – протоколы;
- `key` – ключи;
- `mnemo` – идентификаторы объектов справочника типов событий, сервисов и протоколов.

Конфигурационный файл ocr_custom.xml по умолчанию:

```
<?xml version="1.0" encoding="UTF-8"?>
<!---Примеры правил включения OCR представлены ниже.
<ocr_options node="*" ocr_enabled="false">
  <service key="CE6D8E0E27DA11E2962FC1DB6088709B00000000" mnemo="email" ocr_enabled="false">
    <object_type key="D2B5132E27DA11E28444C2DB6088709B00000000" mnemo="email" ocr_enabled="false">
      <protocol key="501A9868F3460E2E5AAF0C6AB21F8D6F63C09109" mnemo="pop3" ocr_enabled="false"/>
      <protocol key="2ECB2A264E31677895BC5D8845D33BC26F637CDF" mnemo="imap" ocr_enabled="false"/>
      <protocol key="A324CCB227DA11E2A8D99FDB6088709B00000000" mnemo="smtp" ocr_enabled="false"/>
      <protocol key="5F7E60DB3E86EFF90FDA87E72209EA1B0E017F16" mnemo="mapi" ocr_enabled="false"/>
      <protocol key="93B79EB44EE1A45522C08319EC47B499294776D7" mnemo="nrpc" ocr_enabled="false"/>
    </object_type>
    <object_type key="D8333C9027DA11E29E34CADB6088709B00000000" mnemo="email_web" ocr_enabled="false">
      <protocol key="A779DB3627DA11E2ADDCA0DB6088709B00000000" mnemo="http" ocr_enabled="false"/>
      <protocol key="7ED97C84BDBDD99C1C21AC0A6D6191F6A891C440" mnemo="https" ocr_enabled="false"/>
    </object_type>
  </service>

  <service key="DD6ECB5227DA11E2B507CBDB6088709B00000000" mnemo="im" ocr_enabled="false">
    <object_type key="E266719627DA11E2A83ECCDB6088709B00000000" mnemo="im_icq" ocr_enabled="false">
      <protocol key="ABA5D02027DA11E2B78FA1DB6088709B00000000" mnemo="oscar" ocr_enabled="false"/>
    </object_type>
    <object_type key="EEC2D87627DA11E29EA6D2DB6088709B00000000" mnemo="im_mail_ru" ocr_enabled="false">
      <protocol key="B8C7FC6A27DA11E2A080B7DB6088709B00000000" mnemo="mmp" ocr_enabled="false"/>
    </object_type>
    <object_type key="F249A80827DA11E29BA2D3DB6088709B00000000" mnemo="im_skype" ocr_enabled="false">
      <protocol key="DD3D593857521DE2E9618C26FD3E1B914F8A16F9" mnemo="skype" ocr_enabled="false"/>
    </object_type>
    <object_type key="E7C3A26C27DA11E296D3CDDB6088709B00000000" mnemo="im_xmpp" ocr_enabled="false">
      <protocol key="AF69EA3427DA11E2BE09A2DB6088709B00000000" mnemo="xmpp" ocr_enabled="false"/>
    </object_type>
  </service>

  <service key="0794BBB227DB11E2BD81E9DB6088709B00000000" mnemo="web" ocr_enabled="false">
    <object_type key="0CAFCC9027DB11E2AD27EDDB6088709B00000000" mnemo="web_common" ocr_enabled="false">
      <protocol key="A779DB3627DA11E2ADDCA0DB6088709B00000000" mnemo="http" ocr_enabled="false"/>
      <protocol key="7ED97C84BDBDD99C1C21AC0A6D6191F6A891C440" mnemo="https" ocr_enabled="false"/>
    </object_type>
  </service>

  <service key="111CBA0427DB11E2AB82EEDB6088709B00000000" mnemo="file" ocr_enabled="false">
    <object_type key="1515A7B027DB11E2BBB2EFDB6088709B00000000" mnemo="file_exchange" ocr_enabled="false">
```

```
      <protocol key="BEFB1A7C27DA11E2AB10B8DB6088709B00000000" mnemo="ftp" ocr_enabled="false"/>
    </object_type>
    <object_type key="190D004827DB11E287B1F0DB6088709B00000000" mnemo="file_copy_out" ocr_enabled="false"/>
  </service>

  <service key="1DA8A90427DB11E289E8F5DB6088709B00000000" mnemo="print" ocr_enabled="false">
    <object_type key="225BD8F427DB11E2926DF9DB6088709B00000000" mnemo="print_common" ocr_enabled="false"/>
  </service>

  <service key="7843FC5BEA024E9B274E26DB43B7E680D8BC9356" mnemo="placement" ocr_enabled="false">
    <object_type key="602A224D9335579214E3188D1D2745DB9F85D500" mnemo="crawler" ocr_enabled="false"/>
  </service>
</ocr_options>
-->

<ocr_options node="*" ocr_enabled="false">
</ocr_options>
```

Система учитывает только незакомментированный блок.

Чтобы включить OCR на всех уровнях сразу, на уровне сервиса, типа события и на уровне протокола, укажите в конце файла значение `<ocr_options node="*" ocr_enabled="true">`.

Пример с включением на всех уровнях:

```
<ocr_options node="*" ocr_enabled="true">
</ocr_options>
```

Чтобы включить OCR только для конкретных сервисов и протоколов, добавьте в блок в конце файла правила со значением `true`.

Пример с включением конкретных правил:

```
<ocr_options node="*" ocr_enabled="false">
   <service key="CE6D8E0E27DA11E2962FC1DB6088709B00000000" mnemo="email" ocr_enabled="true">
    <object_type key="D2B5132E27DA11E28444C2DB6088709B00000000" mnemo="email" ocr_enabled="true">
      <protocol key="501A9868F3460E2E5AAF0C6AB21F8D6F63C09109" mnemo="pop3" ocr_enabled="true"/>
      <protocol key="2ECB2A264E31677895BC5D8845D33BC26F637CDF" mnemo="imap" ocr_enabled="true"/>
      <protocol key="A324CCB227DA11E2A8D99FDB6088709B00000000" mnemo="smtp" ocr_enabled="true"/>
      <protocol key="5F7E60DB3E86EFF90FDA87E72209EA1B0E017F16" mnemo="mapi" ocr_enabled="true"/>
      <protocol key="93B79EB44EE1A45522C08319EC47B499294776D7" mnemo="nrpc" ocr_enabled="true"/>
    </object_type>
    <object_type key="D8333C9027DA11E29E34CADB6088709B00000000" mnemo="email_web" ocr_enabled="true">
      <protocol key="A779DB3627DA11E2ADDCA0DB6088709B00000000" mnemo="http" ocr_enabled="true"/>
      <protocol key="7ED97C84BDBDD99C1C21AC0A6D6191F6A891C440" mnemo="https" ocr_enabled="true"/>
    </object_type>
  </service>
</ocr_options>
```

9.3 Настройка параметров обработки архивов вложений

Обработка вложений настраивается в конфигурационных файлах:

- файл `/opt/iw/tm5/etc/extractors.conf` (см. документ *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам. extractors.conf*);

- файл `/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml` (см. *Конфигурационный файл extractors.xml*);
- файл `/opt/iw/tm5/etc/config-perm/bookworm/extractors_customization.xml` (см. *Конфигурационный файл extractors_customization.xml*).

Важно!

Если в MS Exchange используется правило журналирования, для корректной обработки этих писем включите соответствующую опцию в Traffic Monitor. Для этого в конфигурационном файле `messed.conf` укажите:

```
"ExchangeJournalReports": true,
```

Чтобы опция стала активной, повторно загрузите конфигурацию или перезапустите службу.

9.3.1 Конфигурационный файл extractors.xml

Файл `/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml` содержит настройки справочника и базу сигнатур, с помощью которых определяется тип файлов при распаковке архивов и вложений.

Параметр	Описание и примеры настройки
`FilenameCharsets`	Если кодировка имени файла отличается от стандартной (ANSI, UTF), то файл будет обрабатываться как соответствующий кодировкам, указанным в данном параметре. Несколько значений перечисляются через запятую; Система будет последовательно пытаться обработать файл в перечисленных кодировках, пока не найдет похожую. Значения по умолчанию – `UTF-8`, `cp1251`, `cp866`
`MinFileSizeInBytes`	Минимальный размер файла (в байтах), подлежащего распаковке. Это ограничение позволяет увеличить производительность Системы за счет отказа от распаковки небольших файлов. Значение по умолчанию – `10` **Примечание:** • настройка также распространяется на тип событий *Буфер обмена*, т. е. Система не анализирует текст из буфера обмена, если его объем менее указанного значения; • настройка не распространяется на тип событий *Ввод с клавиатуры*. • для XML-экстрактора значение по умолчанию – `76`
`MaxTextPlainSizeInKb`	Верхняя граница размера файла, сигнатура которого не определена. При превышении порогового значения файл автоматически считается бинарным и не отправляется на анализ в `iw_cas`. Значение по умолчанию – `25600`

`SpeedInKBs`	Предположительная скорость работы экстрактора в расчете на 1 ГГц частоты процессора (в Кб/с). Может принимать целочисленные значения от 1 и выше. Значение по умолчанию – `100`
`TimeoutInSec`	Время ожидания до завершения обработки файла (в секундах). Значение по умолчанию – `0`
`UseLog`	Логирование экстрактора. Значение по умолчанию – `false`

Если общие значения параметров, указанные в секции `<extractor_defaults>`, не подходят для каких-либо типов файлов, включите эти параметры в секции для нужных типов файлов с другими значениями.

Пример:

Время работы экстрактора можно вычислить по формуле:

Время работы экстрактора = Размер файла в КБ / 1024 / (`SpeedInKBs` * Тактовая_частота процессора в МГц / 1000)

Остальные секции содержат сигнатуры, при помощи которых детектируются типы файлов, находящиеся во вложениях и архивах. Секции имеют следующий набор параметров:

Параметр	Описание и примеры настройки
`Extension`	Расширение файла архива. Необязательный параметр, нужен для корректной работы некоторых архиваторов, которые требуют наличия правильного расширения входных файлов. **Пример:** `Ext = arj`
`Name`	Имя формата. Используется для точного определения имени формата при распаковке файла. Для определения/уточнения формата может включать также список имен: `"defaultname, name1(code1), name2(code2)"` В этом случае формат определяется на основании кода (`codeN`), присвоенного файлу при распаковке. Например, если распаковка завершается с кодом `code1`, то считается, что файл имеет формат `name1`. Список имен может также включать имя по умолчанию (`defaultname`), которое будет присваиваться в случаях, когда код не присвоен: • **Пример 1** (одно имя формата): `text/xml` • **Пример 2** (список имен формата): `"application/arj, UNKNOWN(9), text/encrypted(4)"` По умолчанию формат файла определяется как `application/arj`. Если формат архива не удается определить, ему присваивается

	имя `UNKNOWN`. Для зашифрованного архива используется имя формата `text/encrypted`.
`Signature`	Сигнатура формата, которая представляет собой "образцовую" последовательность значений (байтов) с начальным смещением и масками. Эта последовательность нужна для однозначного определения формата файлов по их содержимому. Сигнатура может включать до 16 триад вида `[OFFSET]:BYTE_VALUE/[MASK]` Допускается также и строковая сигнатура, например "`BZh`" для BZIP2. Эта сигнатура означает указанную последовательность байтов от смещения 0. Поиск строковых сигнатур выполняется без учета регистра символов. Параметр `OFFSET` является необязательным. Для первого байта этот параметр по умолчанию равен `0`, для всех последующих – увеличивается на единицу. Смещение можно задать с символом "`?`" – поиск образца в первых `N` байтах файла. Например, для поиска образца в первых 500 байтах файла, нужно задать смещение "`500?`". Параметр `MASK` также является необязательным и равен `0xFF` по умолчанию. **Пример** (сигнатура заголовка WAV-формата): `Sign = "'RIFF', 0x8: 'WAVEfmt'"` Начиная от смещения 0, расположена последовательность '`R`','`I`','`F`','`F`', далее от смещения 8 должно следовать '`W`','`A`','`V`','`E`','`f`','`m`','`t`'
`Comment`	Комментарий с пояснениями. **Пример** (указание используемой версии архиватора): `Comment = "bzip2 v. 1.0.x"`
`Command`	Строка команды для извлечения файлов. **Пример:** `Extract = "/usr/bin/bzip2 -f -dc ${SRC} > ${OUTDIR}/${SRC}"` где `${OUTDIR}` – каталог, в который будет распакован архив, а `${SRC}` – имя файла, который нужно распаковать.
`ExcludeFromContext`	Если параметр включен (`true`), то распаковка объекта выполняется, но информация об архиваторе не добавляется в XML-контекст объекта. Это позволяет не отображать в контексте объекта фиктивные контейнеры типа MS-TNEF. По умолчанию параметр включен.
`CaseInsensitive`	Учет регистра символов при обработке файла. Значение по умолчанию – `false`

`CreateTags`	Извлечение метаинформации из файла. Значение по умолчанию – `true`
`Archive`	Регламентирует вид извлеченной информации: • `true` – файлы; • `false` – данные.
`PIRegexp`	Содержит описание сигнатуры PIRE для детектирования формата файла. Может быть указан несколько раз в пределах одного `Extractor`. Имеет атрибуты: • `assurance` – достоверность определения формата файла этой сигнатурой; • `offset` – смещение, на котором нужно начинать поиск этой сигнатуры; • `max_length` – длина проверяемого участка; • `case_sensitive` – включение значимости регистра букв в описании сигнатуры.
`DetectableByRegexp`	Может использоваться для отключения детектирования формата с помощью PIRE (для него будут использоваться сигнатуры из `Signature`).
`OpenFifoRetryTimeout`	Таймаут между попытками открыть FIFO-очередь.
`OpenFifoRetryCount`	Количество попыток открыть FIFO-очередь.
`ResultCharset`	Указывает кодировку извлеченного экстрактором текста.
`NeedProcess`	Требуется ли отправлять на анализ файлы с указанным MIME-типом.

Примечание:

Некоторые перехваченные файлы формата XML могут содержать чувствительные данные, которые указаны внутри XML-тэгов разметки файла. По умолчанию Система не извлекает текст из них. Чтобы настроить извлечение текста из XML-тэгов:

1. Откройте на редактирование файл **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml**
2. Найдите элемент со следующим содержанием:

```
<Command>bin/text-extractor -t xml -i ${OUTDIR}</Command>
```

3. Замените параметр `-t xml` на `-t xmltxt`
4. Сохраните изменения и закройте файл.
5. Обновите конфигурацию процесса `iw_bookworm`, выполнив команду:

```
iwtm reload bookworm
```

6. Перезапустите процессы:

```
iwtm restart analysis
iwtm restart messed
iwtm restart icap
```

В результате в извлеченном тексте будут видны XML-тэги и прочая служебная информация, которая не сохраняется при стандартном способе извлечения текста из XML.

9.3.2 Конфигурационный файл extractors_customization.xml

В конфигурационном файле `/opt/iw/tm5/etc/config-perm/bookworm/extractors_customization.xml` вы можете дополнить или изменить настройки экстракторов, заданные в `/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml`.

Параметр	Описание	Примеры настройки
`<Signature>`	Сигнатура формата, которая представляет собой "образцовую" последовательность значений (байтов) с начальным смещением и масками. Эта последовательность необходима для однозначного определения формата файлов по их содержимому. Сигнатура может включать до 16 триад вида `[OFFSET]:BYTE_VALUE/[MASK]` Допускается также и строковая сигнатура, например "`BZh`" для BZIP2. Эта сигнатура означает указанную последовательность байтов от смещения 0. Поиск строковых сигнатур выполняется без учета регистра символов. Необязательные параметры: • `OFFSET` Смещение можно задать с символом "`?`" – поиск образца в первых `N` байтах файла. Например, для поиска образца в первых 500 байтах файла нужно задать смещение "`500?`" • `MASK`	Пример сигнатуры заголовка WAV-формата: `Sign = "'RIFF', 0x8: 'WAVEfmt'"` Начиная от смещения 0, расположена последовательность '`R`', '`I`','`F`','`F`', далее от смещения 8 должно следовать '`W`','`A`','`V`', '`E`','`f`','`m`','`t`'
`<FilenameCharsets>`	Если кодировка имени файла отличается от стандартной (ANSI, UTF), то файл будет обрабатываться как соответствующий кодировкам, указанным в данном параметре. Несколько значений перечисляются через запятую; Система	`UTF-8`, `cp1251`, `cp866`

	будет последовательно пытаться обработать файл в перечисленных кодировках, пока не найдет похожую.	
`<SpeedInKBs>`	Предположительная скорость работы экстрактора в расчете на 1 ГГц частоты процессора (в Кб/с). Может принимать целочисленные значения от 1 и выше.	`100`
`<UseLog>`	Логирование экстрактора.	• `true` – использовать • `false` – не использовать
`<TimeoutInSec>`	Время ожидания до завершения обработки файла (в секундах).	`1000`
`<MinFileSizeInBytes>`	Минимальный размер файла (в байтах), подлежащего распаковке. Это ограничение позволяет увеличить производительность Системы за счет отказа от распаковки небольших файлов. **Примечание:** • обработка файлов размером меньше 10 байт не поддерживается. Данное ограничение также распространяется на тип событий *Буфер обмена*. • для XML-экстрактора значение по умолчанию – `76`	`1024`
`<MaxTextPlainSizeInKb>`	Верхняя граница размера файла, сигнатура которого не определена. При превышении порогового значения файл автоматически считается бинарным и не отправляется на анализ в `iw_cas`.	`25600`
`<PreCommand>`	Команда, которую нужно выполнить перед извлечением данных или после него.	`bin/dwg-extractor -i ${SRC} -t ${OUTDIR}/out.txt -u ${OUTDIR}/out.vectxt`
`<PostCommand>`		

Примечание:

Некоторые перехваченные файлы формата JPEG могут быть склеены с архивами, потенциально содержащими чувствительные данные. По умолчанию Система не извлекает текст из таких файлов. Чтобы настроить извлечение текста из склеенных JPEG-файлов:

1. Откройте на редактирование файл **extractors_customization.xml**:

2. Внутри элемента `<extractors>` вставьте элемент со следующим содержанием:

```
<extractor profile_name="jpg" key="dY5k14hWa0nivGOvSP4BUe0vTJdME5IY4xjNsqKl">
        <PostCommand>bin/7zz x -y -p{} ${SRC} -o${OUTDIR}</PostCommand>
</extractor>
```

3. Сохраните изменения и закройте файл.
4. Перезапустите процессы Traffic Monitor:

```
iwtm restart
```

9.4 Настройка параметров поиска с использованием групповых символов

При создании запроса в разделе **События** Консоли управления Traffic Monitor вы можете указать отправителей и получателей. Чтобы указать значения их контактов или метаданных контактов, вы можете использовать групповые символы в конце строки. Для поиска с использованием групповых символов Система рассматривает контакты и их метаданные как ключевые слова, и индексирует все возможные префиксы ключевых слов. Префикс – это начальная часть слова. Если искать в индексе определенный префикс, найдутся все ключевые слова, содержащие этот префикс.

Индексация происходит, начиная с минимальной заданной длины префикса, которая определяется параметром `min_prefix_len` в файле `is.conf` . По умолчанию значение `min_prefix_len` равно 3.

Пример:

Существуют пользователи с логинами *ex_user*, *exact_user* и *example_user*. Значение `min_prefix_len` равно 3.

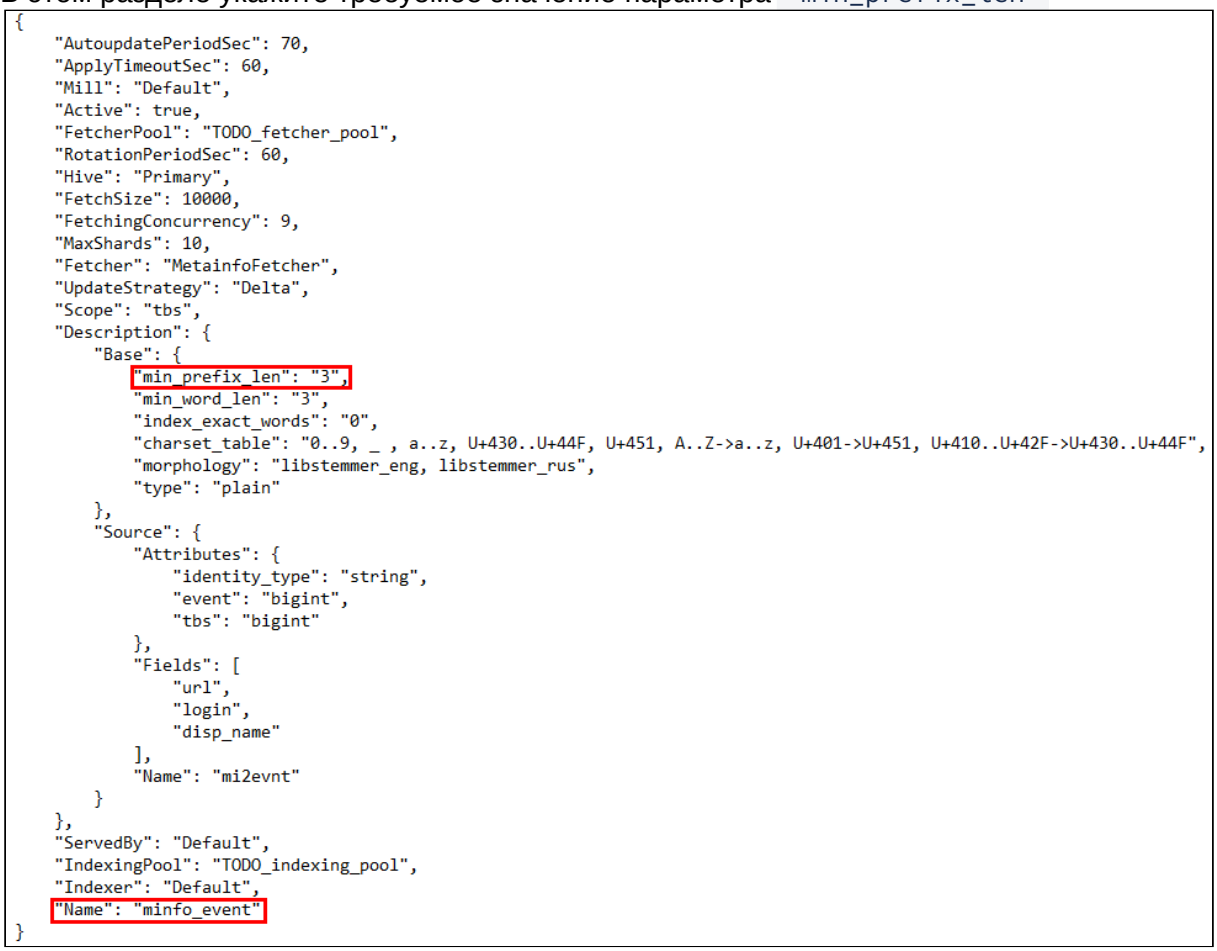
Если создать запрос с маской `"exa*"` , то в результате будут найдены события с участием пользователей *exact_user* и *example_user*. При этом запрос с маской `"ex*"` не вернет никаких результатов.

Если изменить значение `min_prefix_len` на 2, то в результатах поиска по маске `"ex*"` будут события для всех трех пользователей *ex_user*, *exact_user* и *example_user*.

Чтобы изменить минимальную длину префикса:

1. На сервере Traffic Monitor перейдите в директорию `/opt/iw/tm5/etc/`
2. Откройте файл `is.conf`
3. В корневом поле `"Indices"` найдите раздел с параметром `"Name": "minfo_event"`

4. В этом разделе укажите требуемое значение параметра `"min_prefix_len"`



```
{
    "AutoupdatePeriodSec": 70,
    "ApplyTimeoutSec": 60,
    "Mill": "Default",
    "Active": true,
    "FetcherPool": "TODO_fetcher_pool",
    "RotationPeriodSec": 60,
    "Hive": "Primary",
    "FetchSize": 10000,
    "FetchingConcurrency": 9,
    "MaxShards": 10,
    "Fetcher": "MetainfoFetcher",
    "UpdateStrategy": "Delta",
    "Scope": "tbs",
    "Description": {
        "Base": {
            "min_prefix_len": "3",
            "min_word_len": "3",
            "index_exact_words": "0",
            "charset_table": "0..9, _ , a..z, U+430..U+44F, U+451, A..Z->a..z, U+401->U+451, U+410..U+42F->U+430..U+44F",
            "morphology": "libstemmer_eng, libstemmer_rus",
            "type": "plain"
        },
        "Source": {
            "Attributes": {
                "identity_type": "string",
                "event": "bigint",
                "tbs": "bigint"
            },
            "Fields": [
                "url",
                "login",
                "disp_name"
            ],
            "Name": "mi2evnt"
        }
    },
    "ServedBy": "Default",
    "IndexingPool": "TODO_indexing_pool",
    "Indexer": "Default",
    "Name": "minfo_event"
}
```

5. Сохраните файл.
6. Осуществите переиндексацию. Для этого:
    a. Остановите процесс **iw_is**.
    b. Удалите директорию `/var/lib/sphinx/indices/minfo_event`
    c. Запустите процесс **iw_is**.
    Процесс переиндексации может занять некоторое время в зависимости от количества событий в Traffic Monitor. В течение этого времени при выполнении команды `iwtm status iw_is` будет возвращаться ошибка выполнения запроса.

9.5 Настройка интеграции с Data Analysis Service

В Traffic Monitor для событий с вложениями вы можете выполнить *Поиск аналогов* (подробнее. см. *InfoWatch Traffic Monitor. Руководство пользователя. Поиск аналогов*).

Чтобы включить Поиск аналогов, настройте интеграцию Traffic Monitor с Data Analysis Service:

1. Установите Data Analysis Service. Подробнее см. *InfoWatch Data Analysis Service. Руководство по установке, конфигурированию и администрированию. Установка Data Analysis Service*.

> **Важно!**

Для взаимодействия **Traffic Monitor версий 7.16.0 и 7.16.1** с **Data Analysis Service версии 1.6.x, начиная с 1.6.4, и версии 1.7.x, начиная с 1.7.1**, после установки/обновления Сервиса необходимо выполнить следующую команду для каждого его экземпляра:

```
kubectl set env deploy -n infowatch das-adapter-<node_label> AUTH_REQUIRED=False
```

где `<node_label>` – это лейбл ноды платформенного кластера, на которую установлен экземпляр Data Analysis Service. Для центральной ноды используйте лейбл `central`. Для офисной ноды лейбл задается при установке, по умолчанию: `office`.

2. Настройте соединение с Data Analysis Service с помощью утилиты **platform_conf_ctl**. Для этого:
   a. На сервере Traffic Monitor перейдите в директорию `/opt/iw/tm5/bin/`, где находится утилита.
   b. Выполните команду:
   ```
   ./platform_conf_ctl --das-set-uri <host_DAS>:30050
                       --das-set-token <token_value>
                       --das-set-enabled
                    1
   ```
   где `<host_DAS>` – это имя хоста или IP-адрес сервера Data Analysis Service, `<token_value>` – это значение токена для соединения с Data Analysis Service. По умолчанию используйте значение токена `2exwo92iwpczl1hy6jxy`.
   Узнать актуальное значение токена можно:
   - на центральной ноде кластера, в котором расположен сервер Data Analysis Service, с помощью командной строки:
     i. Перейдите в директорию `<distr>/platform`, где `<distr>` – это директория, куда был распакован дистрибутив Data Analysis Service или какого-либо платформенного продукта;
     ii. Выполните команду:
     `./setup.py tokens list`
     В результате будет выведен список токенов для подключения к Платформе. Актуальный токен авторизации Data Analysis Service будет указан напротив сущности *DMServer*.
   - в консоли управления продукта Платформы, в разделе **Основные настройки** в поле **Токен для Device Monitor Server**.
     Доступно, если в кластере установлен платформенный продукт с веб-интерфейсом и в нем есть данная настройка.
3. В конфигурационном файле `/opt/iw/tm5/etc/attributor.conf` в строке `"tmhost": "set_tmhost_here"` вместо `set_tmhost_here` укажите IP-адрес сервера Traffic Monitor. Сохраните изменения.

> **Примечание:**
>
> Здесь вы также можете изменить:
>
> - уровень логирования процесса **iw_attributor**. Для этого в секции "`Logger`" установите нужное значение для параметра "`level`". Подробнее см. *Логирование работы Системы*;

- минимальный размер контентов, отправляемых на обработку в Data Analysis Service. Подробнее см. *ниже;*
- максимальное количество контентов, отправляемых на обработку в Data Analysis Service в одном запросе. Подробнее см. *ниже*.

4. Включите файловую очередь в базе данных (БД). Для этого подключитесь к серверу БД (подробнее см. раздел *Администрирование базы данных*) и выполните следующую команду:
```
UPDATE object_queue
SET enabled = 1
WHERE object_queue_id = 5;
```
5. Демаскируйте процесс **iw_attributor**. Для этого на сервере Traffic Monitor выполните команду:
```
systemctl unmask iw_attributor
```
6. Запустите процесс **iw_attributor**:
```
iwtm start iw_attributor
```
7. Убедитесь, что процесс **iw_attributor** запущен и имеет статус *active*.
```
Service iw_attributor.service is active (running); enabled state: loaded (enabled)
```
Для этого выполните команду:
```
iwtm status iw_attributor
```
8. Включите автозапуск процесса **iw_attributor**:
```
iwtm enable iw_attributor
```

> **Примечание:**
>
> Data Analysis Service обрабатывает события, произошедшие после данной настройки. Для событий, произошедших до настройки, функция *Поиск аналогов* будет недоступна, и они не будут учтены при поиске аналогов других событий.

Чтобы выключить Поиск аналогов:

1. Остановите процесс **iw_attributor**. Для этого на сервере Traffic Monitor выполните команду:
```
iwtm stop iw_attributor
```
2. Выключите автозапуск процесса **iw_attributor**:
```
iwtm disable iw_attributor
```
3. Выключите файловую очередь в БД. Для этого подключитесь к серверу БД и выполните следующую команду:
```
UPDATE object_queue
SET enabled = 0
WHERE object_queue_id = 5;
```

Настройка минимального размера контентов, отправляемых на обработку в Data Analysis Service

Чтобы отфильтровать поток контентов, отправляемых на обработку в Data Analysis Service, вы можете задать их минимальный размер для отправки. Это позволит отсеять малоинформативные контенты

небольшого размера, например тексты, извлеченные с изображений и содержащие менее 50 кириллических символов. Чтобы задать минимальный размер:

1. На сервере Traffic Monitor откройте для редактирования конфигурационный файл `/opt/iw/tm5/etc/attributor.conf`
2. В поле `"TextSizeMinimumInBytes"` укажите минимальный размер в байтах.
3. Сохраните изменения в файле.

По умолчанию поле `"TextSizeMinimumInBytes"` имеет значение 500 байтов.

> **Примечание:**
>
> Данный параметр ограничивает отправку данных только по объему текстового контента. Если вложение содержит изображения или другие виды контейнеров, учитывается только размер извлеченного из них текста.
>
> Если вложение представляет собой архив, то каждый элемент его содержимого будет проходить фильтрацию отдельно.

Настройка количества контентов, отправляемых в Data Analysis Service в одном запросе

Если в Data Analysis Service отправляется слишком много контентов в одном запросе, то время, в течение которого Traffic Monitor ожидает ответ от Сервиса, может быть превышено. В таком случае запрос может быть не обработан. Во избежание этого максимально допустимое количество контентов в одном запросе ограничено параметром `contentAmountPerRequest`.

Traffic Monitor объединяет в один запрос группы контентов, извлеченные из разных файлов, если суммарное количество этих контентов не превышает заданного в параметре.
Если количество контентов из одного файла превышает значение параметра `contentAmountPerRequest`, то они все равно будут отправлены одним запросом.

Чтобы изменить максимально допустимое количество контентов, отправляемых в одном запросе:

1. На сервере Traffic Monitor откройте для редактирования конфигурационный файл `/opt/iw/tm5/etc/attributor.conf`
2. В поле `"contentAmountPerRequest"` укажите количество контентов.
3. Сохраните изменения в файле.

По умолчанию поле `"contentAmountPerRequest"` имеет значение 1000.

9.6 Настройка соединения с Data Storage

Для оптимизации хранения данных и увеличения производительности СУБД может быть установлено внешнее хранилище бинарных данных Data Storage. Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Схемы развертывания Системы и выбор типа установки* и *Установка Data Storage*.

Чтобы настроить соединение между Traffic Monitor и Data Storage:

1. Установите уровень протоколирования `debug` для процесса `iw_x2db`. Это позволит убедиться в успешности соединения после того, как оно будет настроено. Подробнее см. *Логирование работы Системы*.
2. На сервере Traffic Monitor выполните команду:
   `platform_conf_ctl --ds-set-enabled <bool> --ds-set-uri <platform-uri> --ds-set-token <token>`
   где укажите следующие параметры:

Параметр	Описание	Примеры
`--ds-set-enabled <bool>`	Использование Data Storage. Чтобы хранить бинарные данные событий в Data Storage, укажите значение `1`. Если указать значение `0`, то Data Storage не будет использоваться для хранения бинарных данных новых событий.	`--ds-set-enabled 1`
`--ds-set-uri <platform-uri>`	Имя хоста или IP-адрес сервера Data Storage. По умолчанию используются протокол `http` и порт `40731`.	`--ds-set-uri my.platform.com` `--ds-set-uri http://my.platform.com:40731`
`--ds-set-token <token>`	Токен авторизации Data Storage. Значение токена по умолчанию: `1exwo92iwpczl1hy6jxy` **Важно!** В целях повышения безопасности не рекомендуем использовать значение токена по умолчанию. Узнать актуальное значение токена можно: • на сервере Data Storage с помощью командной строки. Для этого: a. Перейдите в директорию, куда был распакован дистрибутив Платформы. b. Выполните команду: `./setup.py tokens list` В результате будет выведен список токенов для подключения к Платформе. Актуальный токен авторизации Data Storage будет указан напротив сущности `DataStorageUser`. Обновить токен авторизации Data Storage можно, выполнив команду: `./setup.py tokens refresh DataStorageUser` • в консоли управления продукта Платформы, в разделе **Основные настройки** в поле **Токен для Data Storage User**. Доступно, если на сервере с Data Storage установлен платформенный продукт с	`--ds-set-token default` `--ds-set-token 1exwo92iwpczl1hy6jxy`

Параметр	Описание	Примеры
	веб-интерфейсом и в нем есть данная настройка. В этом случае токен можно обновить, нажав .	

При успешном соединении в логе `/var/log/infowatch/x2db.log` появится сообщение вида:

```
[DEBUG  ] : <DataStorage> platform request headers: GET /v2/logon?extAPIToken=1exwo92iwpczl1hy6jxy HTTP/1.1
Host: my.platform.com
User-Agent: tmOperator
Accept: application/json
X-IW-ACTIVEPRODUCT: TM

[DEBUG  ] : <DataStorage> platform response: HTTP/1.1 200 OK
```

После окончания настройки вы можете установить тот уровень протоколирования процесса `iw_x2db`, который был до настройки.

Чтобы просмотреть текущие настройки соединения с Data Storage:

На сервере Traffic Monitor выполните команду:
`platform_conf_ctl`

Чтобы разорвать соединение с Data Storage:

На сервере Traffic Monitor выполните команду:
`platform_conf_ctl --ds-remove`
Данные хранилища перестанут быть доступны.

Если вы хотите перестать сохранять бинарные данные событий в Data Storage, но иметь доступ к уже хранящимся там данным, выполните команду:
`platform_conf_ctl --ds-set-enabled 0`
Новые события будут целиком сохраняться в БД Traffic Monitor, начиная со следующего ежедневного табличного пространства, т. е. со следующего дня по UTC+0.

9.7 Настройка отправки событий в Платформу

Начиная с версии 7.14, Traffic Monitor может отправлять события в Платформу двумя способами:

- согласно настройкам синхронизации в Центре расследований;
- в реальном времени.

Отправка событий в реальном времени позволяет уменьшить нагрузку на Traffic Monitor.

> **Важно!**
>
> Убедитесь, что в Traffic Monitor и Центре расследований выбран один и тот же способ отправки событий.
>
> Платформа может получать события в реальном времени начиная с версии 2.5.

9.7.1 Переключение способа отправки событий

Чтобы переключить способ отправки событий в настройках Traffic Monitor, на сервере Traffic Monitor запустите утилиту `platform_conf_ctl` при помощи команды:

```
platform_conf_ctl --fl-set-enabled <bool> --fl-set-uri <uri> --fl-set-token <token> --fl-set-integration-id
<id>
```

Укажите в ней следующие параметры соединения с платформенным сервисом **FactsLoader**:

Параметр	Описание
`--fl-set-enabled`	Включение/отключение отправки событий в реальном времени: • `true` (по умолчанию) – включение отправки событий в реальном времени; • `false` – отключение отправки событий в реальном времени; отправка согласно настройкам синхронизации в Центре расследований.
`--fl-set-uri`	URI-идентификатор хоста Платформы в формате **`http://`**`<host>:<port>`, где `<host>` – имя хоста или IP-адрес сервера Платформы, `<port>` – порт сервера Платформы. По умолчанию используется порт `10104`. **Важно!** В этом параметре должен быть указан адрес той же ноды Платформы, что выбрана в поле "Филиал" интеграции с Traffic Monitor в Центре Расследований. Подробнее см. *Руководство администратора* используемого платформенного продукта, статья *Интеграция с InfoWatch Traffic Monitor.*
`--fl-set-token`	Значение токена для соединения с Платформой. Вы можете получить его в Центре Расследований,  **Настройки** → **Настройки системы** → **Основные настройки**, в поле **Токен для Data Storage User**. Подробнее см. *Руководство администратора* используемого платформенного продукта, статья *Основные настройки*. Вы можете задать значение токена по умолчанию, если не обновляли его. Для этого укажите `--fl-set-token default`. В целях безопасности рекомендуется не использовать значение токена по умолчанию.
`--fl-set-integration-id`	Уникальный идентификатор интеграции Платформы с Traffic Monitor. Вы можете скопировать ID интеграции в разделе  **Настройки** → **Настройки системы** → **Интеграции**. На плитке интеграции нажмите  и выберите **Скопировать ID**. Подробнее см. *Руководство администратора* используемого платформенного продукта, статья *Интеграция с InfoWatch Traffic Monitor.*

Если Traffic Monitor использует Data Storage для хранения собственных данных, то в параметре `--fl-set-uri` указывайте адрес сервера Data Storage или любого другого сервера Платформы, находящегося в одном кластере с Data Storage. Бинарные данные продолжат храниться в том же Data

Storage, что и раньше. Текстовые данные – в базе данных Traffic Monitor. При этом сервис **FactsLoader** будет загружать текстовые контенты на свой сервер и хранить там для отображения событий в Центре Расследований.
О настройке соединения с хранилищем см. *Настройка соединения с Data Storage*.

Если Traffic Monitor не использует Data Storage для хранения собственных данных, то после настройки соединения с сервисом **FactsLoader** все данные будут храниться в БД Traffic Monitor, как и раньше. Но при этом их копии также будут храниться на сервере Платформы, указанном в параметре `--fl-set-uri`.

> **Примечание:**
>
> В случае распределенной установки утилиту нужно запускать на сервере, установленном при помощи шаблона *Перехватчики*.

Пример команды включения отправки в реальном времени:

```
platform_conf_ctl --fl-set-enabled true --fl-set-uri http://10.60.23.249:10104  --fl-set-token default --fl-set-integration-id e06bd150-513b-4eb6-975a-533cf96e50ab
```

Команда отключения отправки в реальном времени и перехода на отправку по расписанию:

```
platform_conf_ctl --fl-set-enabled false
```

9.7.2 Настройка отправки событий в реальном времени

Чтобы настроить отправку в реальном времени:

1. В Центре расследований скопируйте ID интеграции.
2. На сервере Traffic Monitor используйте утилиту, чтобы переключить способ отправки событий.
3. Перезапустите службу `iw_x2db`:

   ```
   systemctl restart iw_x2db
   ```

4. Перейдите в Центр расследований. Чтобы отображались события с момента последней синхронизации до переключения на режим отправки в реальном времени, запустите синхронизацию вручную.
5. Переключите способ отправки в Центре расследований и сохраните изменения.

9.7.3 Настройка отправки событий по расписанию

Если ранее Центр расследований не синхронизировался с Traffic Monitor, то достаточно настроить интеграцию в Центре расследований.

Если ранее была настроена отправка событий в реальном времени:

1. На сервере Traffic Monitor используйте утилиту, чтобы переключить способ отправки событий:

```
platform_conf_ctl --fl-set-enabled false
```

2. Перезапустите службу `iw_x2db`:

```
systemctl restart iw_x2db
```

3. Перейдите в Центр расследований и в интеграции с Traffic Monitor отключите загрузку событий в реальном времени.
4. При необходимости измените расписание автоматической синхронизации и сохраните изменения.

Подробнее о настройках интеграции в Центре расследований см. *Руководство администратора* используемого платформенного продукта, статья *Интеграция с InfoWatch Traffic Monitor.*

9.8 Логирование работы Системы

Для удобства отслеживания работы процессов подсистема протоколирования имеет шесть уровней:

Название уровня	Описание
`fatal`	Показывает ошибки, которые препятствуют дальнейшей работе процесса.
`error`	Показывает сообщения об ошибках, которые не являются критическими для работоспособности процесса.
`warning`	Выводит сведения о потенциально опасных ситуациях.
`info`	Общая полезная информация о процессе (старт/стоп, применение конфигураций и т. д.).
`debug`	Выводит информацию, которая чаще всего используется для диагностики работы сервиса (IT, системные администраторы и т. д.).
`trace`	Чаще всего используется для отслеживания кода разработчиками.

Настройка уровней протоколирования

> **Важно!**
>
> Следует учитывать, что изменение уровня протоколирования на более подробный может значительно снизить производительность Системы.

Конфигурационные файлы хранятся в директории `/opt/iw/tm5/etc`. По умолчанию все процессы имеют уровень протоколирования `warning`.

Чтобы изменить уровень протоколирования для процессов Traffic Monitor Server:

1. В конфигурационном файле нужного процесса в секции `Logging` установите для параметра `GlobalLevel` нужное значение.
2. Сохраните измененный файл.
3. После внесения изменений в системный журнал перезапустите процесс:
   `iwtm restart <имя_службы>`

Все логи процессов по умолчанию хранятся в каталоге `/var/log/infowatch`

Для экстракторов, у которых нет отдельного конфигурационного файла, настройте уровень протоколирования в конфигурационном файле **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml**:

1. Откройте конфигурационный файл.
2. Для параметра `text-extractor` добавьте значение `-l <level>`, где <level> – уровень протоколирования. Например:
   `< Command> bin/text-extractor -l error -t ooxml -i ${OUTDIR}" < Command>`
3. После внесения изменений перезапустите процессы:
   `iwtm restart bookworm`
   `iwtm restart warpd`

> **Примечание:**
>
> Данный тип настройки протоколирования доступен для экстракторов следующих форматов: DOCX, HTML, MSOFFICE_XML, MSOLE, ODP, ODT, PPTX, XLSX, XML.

9.9 Файловые очереди

Чтобы обеспечить загрузку имеющихся очередей объектов:

1. Остановите службы `iw_icap`, `iw_deliver`, `iw_luaengined`, `iw_is`, `iw_smtpd`, `iw_xapi_xapi`, `iw_xapi_puppy`, `iw_analysis`, `iw_messed`, `iw_proxy_http`, `iw_proxy_icq`, `iw_proxy_smtp`, `iw_capstack`.
2. Переместите объекты из очереди ошибок в нужную очередь.
3. Дождитесь, пока будут обработаны все объекты в файловой очереди.
4. Запустите службы `iw_icap`, `iw_deliver`, `iw_luaengined`, `iw_is`, `iw_smtpd`, `iw_xapi_xapi`, `iw_xapi_puppy`, `iw_analysis`, `iw_messed`, `iw_proxy_http`, `iw_proxy_icq`, `iw_proxy_smtp`, `iw_capstack`.

Чтобы запустить все службы, выполните команду:

```
iwtm start
```

По окончании процесса убедитесь, что службы запущены:

```
iwtm status
```

Варианты команд для запуска/остановки отдельных служб:

Запуск службы	Остановка службы
`iwtm start icap`	`iwtm stop icap`
`iwtm start deliver`	`iwtm stop deliver`
`iwtm start luaengined`	`iwtm stop luaengined`
`iwtm start is`	`iwtm stop is`
`iwtm start smtpd`	`iwtm stop smtpd`
`iwtm start xapi_xapi`	`iwtm stop xapi_xapi`
`iwtm start xapi_puppy`	`iwtm stop xapi_puppy`
`iwtm start analysis`	`iwtm stop analysis`
`iwtm start messed`	`iwtm stop messed`
`iwtm start proxy_http`	`iwtm stop proxy_http`
`iwtm start proxy_icq`	`iwtm stop proxy_icq`
`iwtm start proxy_smtp`	`iwtm stop proxy_smtp`
`iwtm start capstack`	`iwtm stop capstack`

Объекты в Системе перемещаются посредством файловых очередей:

Путь к директории очереди	Формат файлов в очереди
`queue/analysis`	`.xml & .dat`
`queue/smtp`	`.xml & .dat`
`queue/db`	`.xml & .dat`
`queue/blackboard`	`.dat`
`queue/blackboard_errors`	`.dat`
`queue/is`	`.xml & .dat`
`queue/x2x`	`.xml & .dat`

Путь к директории очереди	Формат файлов в очереди
`queue/errors`	`.xml & .dat`
`queue/x2x-errors`	`.xml & .dat`
`queue/x2db-errors`	`.xml & .dat`
`queue/final-errors`	`.xml & .dat`

Каждая из очередей содержит дополнительные технические очереди для отслеживания процесса обработки объектов: `.db`, `.in`, `.out`.

Пример:

Для очереди `queue/smtp` процесс обработки разделен на следующие этапы:

1. `queue/smtp/.in` – файл формируется в данной очереди в процессе получения объектов от Postfix службой `iw_smtpd`. Если объект по какой-то причине задерживается в этой очереди, нужно проверить службы `iw_smtpd` или `iw_proxy_smtp`.
2. `queue/smtp/.db` – по окончании обработки файл перемещается из очереди `.in` в очередь `.db`. В эту очередь попадают почтовые EML-объекты от `iw_xapi`.
3. `queue/smtp/.out` – в эту очередь объект перемещается следующей службой в цепочке – `iw_messed`.

Особенность:

Очереди, обслуживающие службу `iw_is`, дополнительно разделяются на:

- `queue/is/cmd/` – файловая очередь команд `iw_is`;
- `queue/is/fetching/` – очередь команд на загрузку;
- `queue/is/indexing/` – очередь команд на индексацию;
- `queue/is/errors/` – очередь ошибок.

Очередь	Службы, которые помещают события в очередь	Служба, которая забирает события из очереди
`queue/analysis`	`iw_xapi_xapi`, `iw_xapi_puppy`	`iw_analysis`
`queue/smtp`	`iw_xapi_xapi`, `iw_xapi_puppy`, `iw_smtpd`, `iw_proxy_smtp`, `iw_capstack`	`iw_messed`
`queue/db`	`iw_messed`, `iw_analysis`, `iw_icap`, `iw_proxy_icq`, `iw_proxy_http`	`iw_x2x`
`queue/blackboard`	`iw_x2db`, `iw_deliver`	`iw_blackboard`

Очередь	Службы, которые помещают события в очередь	Служба, которая забирает события из очереди
`queue/blackboard_errors`	ошибка при обработке `iw_blackboard`	-
`queue/x2x`	`iw_x2x`	`iw_x2db`
`queue/is`	`iw_metainfo_fetcher`	`iw_is`
`queue/errors`	все службы, если произошла ошибка обработки	`iw_rammer`
`queue/x2x-errors`	ошибки обработки `iw_x2x`	
`queue/x2db-errors`	ошибки обработки `iw_x2db`	
`queue/final-errors`	`iw_rammer`	-

Сбор статистики по файловым очередям включается в конфигурационном файле службы в директории `/opt/iw/tm5/etc`. Установите значение `true` в параметре `Enabled` секции `Statistic`.

9.10 Восстановление работоспособности системы в аварийных ситуациях

При серьезных сбоях в работе серверов или сети восстановить работоспособность Системы можно, выполнив следующие действия:

1. Остановите процессы Traffic Monitor, выполнив команду:
   ```
   iwtm stop
   ```
2. Переместите объекты из очереди ошибок `queue/x2db-errors` в очередь `queue/x2x`. Процедура выполняется при помощи утилиты **iw_qtool** (см. статью *Как переместить объекты между очередями при помощи утилиты iw_qtool*).
3. Если Traffic Monitor Server работает с установленной СУБД PostgreSQL, то для проверки соединения выполните команды:
   `su - iwtm`
   `psql -p 5433 -h <IP-адрес_сервера_БД> postgres iwtm`
   `psql -p 5433 -h 127.0.0.1 postgres iwtm` - для подключения к локальной БД
   Если проверка пройдена успешно, то в ответ на выполнение указанной команды будет выведено приглашение psql:
   `postgres=#`
4. Запустите процессы Traffic Monitor, выполнив команду:
   ```
   iwtm start
   ```

Если после запуска Traffic Monitor работоспособность Системы не восстановлена:

1. Соберите диагностическую информацию, т. е. логи.
   Подробнее о логировании см. *Логирование базы данных PostgreSQL*, *Логирование работы Системы*.
2. Проверьте системный журнал на наличие ошибок. Путь к файлу журнала: `/var/log/messages`
3. Проанализируйте собранную информацию. Типовые ошибки и методы их устранения описаны в статье *Ошибки в базе данных PostgreSQL*. При необходимости обратитесь к администратору базы данных или в службу технической поддержки.

9.11 Управление языками с поддержкой морфологии

Языки с поддержкой морфологии в Traffic Monitor настраиваются посредством изменения конфигурационного файла и установки пакета со словарем языка.

В зависимости от настроек, заданных при установке, в Системе могут быть установлены два и более языков (см. *InfoWatch Traffic Monitor. Руководство по установке*). Обязательно устанавливаются русский и английский словари морфологии – даже в том случае, если это явно не указывалось при установке.

Сведения по доступным действиям приведены в статьях:

- *Добавление нового языка для поиска событий. Морфология и добавление терминов*
- *Обновление установленного языка*
- *Удаление языка для поиска и терминов*

9.11.1 Добавление нового языка для поиска событий. Морфология и добавление терминов.

Чтобы добавить в Систему новый язык для поиска событий:

1. Остановите процессы **iw_indexer** и **iw_is**:
   ```
   iwtm stop indexer
   iwtm stop is
   ```
2. Перейдите в локальный репозиторий, где находятся все пакеты, загруженные при установке:
   ```
   cd /opt/iw/distr
   ```
3. Перейдите в директорию, соответствующую текущей версии Traffic Monitor.
4. Выберите нужный пакет и выполните его установку с помощью команды:
   ```
   rpm -i <название пакета>
   ```
   Например, для установки пакета со словарем французского языка нужно ввести команду:
   ```
   rpm -i iwtm-sphinx-dict-fra-7.0.0-792.x86-64.rpm
   ```
5. Запустите процессы:
   ```
   iwtm start indexer
   iwtm start is
   ```

> **Примечание:**
>
> При установке нового словаря происходит полная переиндексация базы данных (БД), что занимает некоторое время.

Чтобы включить морфологию языка для поиска событий:

1. Остановите процессы **iw_indexer** и **iw_is**:
   `iwtm stop indexer`

   `iwtm stop is`
2. Откройте файл **sphinx_options.ini** с помощью команды:
   `mcedit /opt/iw/tm5/etc/sphinx_options.ini`
   и добавьте ключ нужного языка в параметр `sphinx_language`.
   Например, чтобы включить морфологию русского и турецкого языков в Системе, укажите следующие значения параметра:
   ```
   sphinx_languages = 'rus tur'
   ```

   > **Примечание:**
   >
   > Чтобы выставить приоритет языка, установите параметр с языком последним в списке значений `sphinx_languages` файла **sphinx_options.ini**.

3. Для добавления терминов откройте файл **database.conf** используемой СУБД PostgreSQL:
   `mcedit /opt/iw/tm5/csw/postgres/database.conf`
4. Добавьте в данный файл ключ языка с поддержкой морфологии из параметра `cfdb_language`, например:
   ```
   \set cfdb_language 'rus'
   ```

   > **Примечание:**
   >
   > Полный список ключей для морфологии разных языков приведен в статье *Список языков с поддержкой морфологии*.

5. Запустите процессы **iw_indexer** и **iw_is**:
   `iwtm start indexer`
   `iwtm start is`

9.11.2 Обновление установленного языка

Чтобы обновить существующий в Системе словарь:

1. Перейдите в каталог с пакетами словарей:
   `cd /opt/iw/disrt/7.0.0/`
2. Выполните установку пакета:
   `rpm -i <название пакета>`
   Например:
   `rpm -i iwtm-sphinx_dict-deu-7.0.0.792.x86_64.rpm`

> **Примечание:**
>
> При обновлении словаря повторная индексация базы данных производиться не будет: новые языки с поддержкой морфологии будут использоваться только для новых событий.

9.11.3 Удаление языка для поиска и терминов

Чтобы удалить словарь из Системы:

1. Остановите процессы **iw_indexer** и **iw_is**:
   ```
   iwtm stop indexer
   iwtm stop is
   ```
2. Откройте файл **database.conf** используемой СУБД PostgreSQL:
   ```
   mcedit /opt/iw/tm5/csw/postgresql/database.conf
   ```
3. Удалите код языка с поддержкой морфологии из параметра `define cfdb_language`.
4. Удалите файлы индексации из директории `/var/lib/sphinx/`
5. Запустите процессы:
   ```
   iwtm start indexer
   iwtm stop is
   ```

После удаления словаря будет произведена полная переиндексация базы данных.

> **Примечание:**
>
> Чтобы сохранить язык БКФ, добавьте код языка с поддержкой морфологии в параметр `cfdb_language` конфигурационного файла **database.conf** непосредственно перед обновлением Системы. При этом язык с поддержкой морфологии также будет восстановлен.
>
> Чтобы удалить язык с поддержкой морфологии после обновления Системы, повторно пройдите шаги, указанные в данном разделе.

9.12 Настройка передачи информации в SIEM

Traffic Monitor может интегрироваться с SIEM-системами (Kaspersky Unified Monitoring and Analysis и др.). Под интеграцией подразумевается поступление в SIEM-систему консолидированной информации со всех установленных в компании компонентов системы Traffic Monitor.

Для интеграции используется скрипт **/opt/iw/tm5/bin/config/iwtm-siem.conf.py**, доступный на сервере Traffic Monitor.

Информация из Traffic Monitor доступна для SIEM системы:

1. Посредством табличного представления:
   - события, зарегистрированные в Traffic Monitor;
   - аудит сессий пользователей консоли Traffic Monitor.
2. Посредством rsyslog:
   - вход/выход пользователей Linux-сервера Traffic Monitor;
   - события, зафиксированные в системном журнале Linux-сервера Traffic Monitor, включая информацию о входе/выходе пользователей Базы Данных PostgreSQL;
   - состояние служб Linux-сервера Traffic Monitor или группы серверов.

В этом разделе:

- *Настройки на стороне SIEM*

- *Настройки на стороне ТМ*
- *Типы логов, передаваемых в SIEM*

9.12.1 Настройки на стороне SIEM

Чтобы подготовить SIEM к получению данных от Traffic Monitor:

1. В SIEM укажите таблицы, из которых нужно забирать информацию:
   - `IWTM.ARC_VIEW_OBJECTS2` – события Traffic Monitor;
   - `IWTM.ARC_VIEW_AUDIT_LOG` – аудит пользователей Traffic Monitor.
   - Создайте учетную запись SIEM для доступа к таблицам базы данных.
   - Настройте обработку данных, извлеченных из базы данных Traffic Monitor.

Информацию о табличных представлениях (иногда нужны для анализа) см. в статьях:

- *Табличное представление событий ТМ*
- *Табличное представление аудита пользователей*

> **Важно!**
>
> При настройке интеграции могут понадобиться дополнительные модули от производителя SIEM-системы, позволяющие ей работать с табличными представлениями. Например, для интеграции с HP ArcSight нужен модуль HP Flex Connector.

Табличное представление событий ТМ

При подключении к базе данных (БД) Traffic Monitor используйте созданного пользователя **siem** (см. *Создание пользователя siem*). Искомые данные содержатся в таблице `IWTM.ARC_VIEW_OBJECTS2`.

> **Примечание:**
>
> Если для импорта в SIEM нужно отфильтровать данные, вы можете сделать это по полю `capture_date` или `insert_date`. Мы рекомендуем выполнять фильтрацию по полю `insert_date`. Фильтрация по полю `object_id` не поддерживается.

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`object_id`	number(20)	Атрибут события *Идентификатор события.*	ID события в БД ТМ. Всегда присутствует.	`110`

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`monitorcode`	varchar2(4000)	Атрибут события *Тип события.*	Тип события определяет способ передачи данных. Может принимать одно из следующих значений: • Съемные устройства • Печать • ICQ • Skype • XMPP • Mail.Ru Агент • Telegram • VK (ВКонтакте) • Facebook • WhatsApp • MS Lync • FTP • Почта • Веб-почта • Веб-сообщение • Буфер обмена • Облачные хранилища • Ввод с клавиатуры • Терминальная сессия • Сетевые ресурсы • Чтение файла • Запись файла	`Email`
`protocol`		Атрибут события *Протокол.*	Протокол может принимать одно из следующих значений: • OSCAR • Skype • XMPP • MMP	

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
			• SIP • FTP • POP3 • IMAP • MAPI • SMTP • HTTP • HTTPS • NRPC • WhatsApp • Отсутствует	
`verdict`	varchar2(12)	Атрибут события *Вердикт.*	Возможны значения: • *Quarantined* (*Карантин*) • *Forbidden* (*Заблокировано*) • *Allowed* (*Пропущено*)	`Forbidden`
`date_of_capture`	varchar2(50)	Атрибут события *Дата перехвата* в ISO 8601 с указанием часового пояса даты перехвата.		`2014-06-19T18:56:26+04:00`
`capture_data`	timestamp	Дата перехвата события (в UTC, без указания часового пояса) в формате `timestamp`. В СУБД PostgreSQL атрибут имеет		timestamp

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
		повышенную точность – до миллисекунд. Используется для быстрой фильтрации данных.		
`insert_date`	timestamp	Дата вставки события (в UTC, без указания часового пояса) в формате `timestamp`		timestamp
`device`	varchar2(256)	Атрибут события *Имя устройства.*	Наименование устройства, с которого или на которое происходило копирование. Либо наименование принтера, на который был отправлен на печать документ из перехваченного события. Может быть не заполнено.	`Kingston USB Drive 5.0`
`websource`	varchar2(256)	Атрибут события *Ресурс.*	Адрес посещенного веб-ресурса или адрес облачного хранилища. Может быть не заполнено.	`Yahoo.com`
`recipientscontacts`	clob	Атрибут события *Получатели.*	Список контактов получателей через запятую. Контакты указаны в формате `<тип`	`email:ivanov@infowatch.ru`, `email:petr.p`

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
			`контакта>:<значение контакта>`. Может быть не заполнено.	`etrov@infowatch.ru`
`recipientsfullname`	clob	Атрибут события *Получатели.*	Список полных имен получателей через запятую. Указаны в том же порядке, что и в `recipients`. Указаны только в том случае, если получателей удалось идентифицировать. Поле может быть не заполнено.	`Ivanov Ivan Ivanovich`, `Petrov Petr Petrovich`
`recipientsdomainaccountname`	clob	Атрибут события *Получатели.*	Список ключей идентификации типа `auth` всех получателей через запятую. Указаны в том же порядке, что и в `recipients`. Может быть не заполнено.	`Ivanov@iw`, `Petrov@iw`
`senderdomainaccountname`	clob	Атрибут события *Отправители.*	Ключ идентификации типа `auth` отправителя. Поле может быть не заполнено.	`Petrov@iw`
`senderfullname`	clob	Атрибут события *Отправители.*	Полное имя отправителя. Поле может быть не заполнено.	`Petrov Petr Petrovich`

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`sendercontacts`	clob	Атрибут события *Отправители.*	Контакт отправителя, указанный в формате `<тип контакта>:<значение контакта>`. Может быть не заполнено.	`email:petr.petrov@infowatch.ru`
`sendermachinedomainname`	clob	Атрибут события *Рабочая станция.*	Доменное имя `dnshostname` рабочей станции отправителя. Может быть не заполнено.	`XP-PETROV`
`sendermachineip`	clob	Атрибут события *Рабочая станция.*	IP-адрес рабочей станции отправителя. Может быть не заполнено.	`192.0.2.0`
`perimetersin`	clob	Наименование периметра, в который вошло событие.	Список наименований периметров, в которые вошло событие. Периметры в списке указаны через запятую. Может быть не заполнено.	Периметр компании
`perimetersout`	clob	Наименование периметра, из которого ушло событие.	Список наименований периметров, из которых ушло событие. Периметры в списке указаны через запятую. Может быть не заполнено.	Периметр компании

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`tags`	clob	Атрибут события *Тег.*	Список тегов через запятую. Может быть не заполнено.	`New`
`categories`	clob	Атрибут события *Категория.*	Список категорий через запятую. Может быть не заполнено.	`Confidentially`
`text_objects`	clob	Атрибут события *Текстовый объект.*	Список текстовых объектов, обнаруженных в перехваченном событии. Текстовые объекты в списке указаны через запятую. Может быть не заполнено.	`special control`
`fingerprints`	clob	Атрибуты события *Бланк*, *Эталонный документ*, *Печать*, *Выгрузка из БД.*	Список названий форм, эталонных документов, печатей и выгрузок из БД, обнаруженных в перехваченном объекте. Элементы в списке указаны через запятую. Может быть не заполнено.	`Бланк заявки.doc`
`protecteddocuments`	clob	Атрибут события *Объект защиты.*	Список объектов защиты, обнаруженных в перехваченном объекте. Объекты защиты в списке указаны через запятую. Может быть не заполнено.	`Договор аренды`

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`policies`	clob	Атрибут события *Политика.*	Список названий политик, сработавших на перехваченном объекте. Политики в списке указаны через запятую. Может быть не заполнено.	`Политика контроля новых сотрудников`
`violationtype`	varchar2(40)	Атрибут события *Группа правил.*	Может принимать следующие значения: • *Copy* (*Нарушение копирования*) • *Placement* (*Нарушение хранения*) • *Transfer* (*Нарушение передачи*) Может быть не заполнено.	`Copy`
`violation_level`	Список	Атрибут события *Уровень нарушения.*	Может принимать следующие значения: • *High* (*Высокий*) • *Medium* (*Средний*) • *Low* (*Низкий*) • *No violation* (*Отсутствует*) Может быть не заполнено.	`Medium`
`userdecision`	varchar2(27)	Атрибут события *Решение*	Решение пользователя консоли.	`Violation`

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
		пользователя.	Может принимать следующие значения: • *Violation* (*Нарушение*) • *NoViolation* (*Нет нарушения*) • *NotProcessed* (*Решение не принято*) • *AdditionalProcessingNeeded* (*Требует дополнительной обработки*) Может быть не заполнено.	
`filepath`	clob	Атрибут события *Путь к файлу.*	Список путей к файлам. Пути в списке указаны через запятую. Может быть не заполнено.	`\\xp-petrov\C$\example.txt`
`attachments`	clob	Атрибут события *Имя файла вложения.*	Имена файлов вложений, указанные через запятую.	`example.txt`, `Petrov.doc`, `3.jpg`
`url`	varchar2(4000)	Атрибут события *URL.*	Полный адрес, с которого осуществлялась передача данных. Может быть не заполнено.	`192.0.2.0/3.jpg`
`capture_server_ip`	varchar2(256)	Атрибут события *Сервер перехвата IP.*	IP-адрес сервера, на котором были перехвачены данные. Может быть не заполнено.	`192.0.2.0`

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`capture_server_hostname`	varchar2(256)	Атрибут события *Имя сервера перехвата.*	Имя сервера, на котором были перехвачены данные. Может быть не заполнено.	`iwtm.infowatch.ru`

Важно!

Количество выводимых элементов в одной ячейке одной записи ограничено 1000 штук. Например: максимум 1000 получателей или извлеченных файлов в событии.

Табличное представление аудита пользователей

При подключении к БД (базе данных) Traffic Monitor используйте созданного пользователя **siem** (см. *Создание пользователя siem*). Искомые данные содержатся в таблице `IWTM.ARC_VIEW_AUDIT_LOG`.

Атрибут	Тип данных	Описание	Пример заполнения
`audit_log_id`	Number(20)	ID записи в аудите сессий пользователей консоли Traffic Monitor.	12345
`change_date`	Varchar2(50)	Дата и время зарегистрированного действия пользователя.	05.08.2015 09:35:10.641446000
`user_login`	varchar2(256)	Логин пользователя, совершившего действие.	Admin
`user_fullname`	varchar2(256)	Полное имя пользователя, совершившего действие.	Petrov Petr Petrovich
`user_email`	varchar2(256)	Почта пользователя, совершившего действие.	petr.petrov@infowatch.ru
`operation`	varchar2(40)	Тип действия, которое было произведено пользователем.	Edit

Атрибут	Тип данных	Описание	Пример заполнения
		Возможны значения: • restart (перезапуск) • delete_hash (удаление хэша) • sync (синхронизироват ь) • add_tag (добавить тег) • remove_tag (удалить тег) • run (выполнение запроса) • start (запуск) • stop (остановка) • view (просмотр) • create (создание) • update (редактирование) • delete (удаление) • login_failure (неуспешная попытка входа) • login (успешный вход) • logout (выход) • change_password (изменение пароля) • decision_update (изменение пользовательског о решения) • remove_tag (изменение тегов события) • delete_ref (удаление ссылки) • copy (копирование) • move (перемещение) • commit (применение изменений в	

Атрибут	Тип данных	Описание	Пример заполнения
		конфигурации системы) • rollback (откат изменений в конфигурации системы) • draft (сохранение изменений в конфигурации системы) • add (добавление) • import (импорт) • export (экспорт)	
`entity_type`	varchar2(40)	Тип объекта, над которым осуществлялось действие. Возможны значения: • AgentJob (диагностические данные) • Adlibitum (адлибитум) • Agent (служба) • Classifier (классификатор) • NetworkSettings (сетевые параметры) • NotificationSettings (состояние системы) • ObjectReport (выгрузка событий) • Query (запуск поиска событий) • QueryReportRun (агрегация отчета) • Setting (настройки) • UpdateSystem (обновление системы)	Dashboard

Атрибут	Тип данных	Описание	Пример заполнения
		• Category (категория) • Dashboard (дашборд) • DashboardWidget (виджет) • EtForm (эталонные формы) • EtStamp (эталонные печати) • EtTable (эталонные выгрузки) • Fingerprint (эталонные документы) • LdapContact (LDAP-контакт) • LdapGroup (LDAP-группа) • LdapPerson (LDAP-персона) • LdapStatus (LDAP-статус персоны) • LdapWorkstation (LDAP-рабочая станция) • Perimeter (периметр) • Policy (политика) • ProtectedDocuments (объект защиты) • Report (отчет) • Role (роль) • Selection (запрос) • ServiceLog (лог сервиса) • SystemList (список тематик ресурсов) • SystemListItem (список ресурсов заданной тематики) • Tag (тег)	

Атрибут	Тип данных	Описание	Пример заполнения
		• Term (термин) • TextObject (текстовый объект) • User (пользователь) • VisibilityArea (область видимости) • Config (конфигурация) • License (лицензия) • Object (событие) • ProtectedCatalog (каталог объекта защиты)	
`entity_display_name`	varchar2(4000)	Наименование объекта, над которым осуществлялось действие.	Statistics1
`property_changes`	clob	Описание произошедших изменений в формате JSON. Данное поле заполняется только в случае событий управления пользователями, ролями, областями видимости и при осуществлении входа в консоль управления. Возможны три формата заполнения поля.	
	-	**Формат №1.** Актуален только для событий управления ролями и областями видимости.	

		`{`
		`“old”: {`
		`“<ТИП ОБЪЕКТА>”:{`
		`{`
		`“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,`
		`“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”`
		`}`
			`{`
			`"old":{`
			`"visibilityareas":{`
			`}`
			`},`
			`"new":{`
			`"visibilityareas":[`
			`{`

Атрибут	Тип данных	Описание	Пример заполнения

		}
		}
		{
		“new”: {
		“<ТИП ОБЪЕКТА>”:{
		{
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”
		}
		}
		}
		}
		}
			"VISIBILITY_AREA_ID":"F00207A1E7E7743EE0433D003C0A5DD400000000",
			"DISPLAY_NAME":"<idclip>",
			"NOTE":"<idclip>",
			"VISIBILITY_AREA_CONDITION":"{"data":{"link_operator":"and","children":[]}}",
			"IS_SYSTEM":1
			}
			}
			}

	-	**Формат №2.** Актуален только для событий управления пользователями.	

		{
		“old”:{
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”
		}
		“new”:{
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”
		}
		}
			{
			"old":{
			"EMAIL":"asdasd@asdasd.ru",
			"CHANGE_DATE":"01-07-2014 09:46:29.000000"
			},
			"new":{
			"EMAIL":"asdasd11@asdasd.ru",
			"CHANGE_DATE":"01-07-2014 09:46:44.000000"
			}
			}

Атрибут	Тип данных	Описание	Пример заполнения
	-	**Формат №3.** Актуален только для событий входа пользователя в систему. -	
		`{ "request":{ "hostname": “<ИМЯ ХОСТА>”, "ip":"<IP-АДРЕС>", "login":"<ЛОГИН ПОЛЬЗОВАТЕЛЯ>" } }`	`{ "request":{ "hostname":null, "ip":"127.0.0.1", "login":"officer" } }`

9.12.2 Настройки на стороне TM

Чтобы настроить передачу консолидированной информации из Traffic Monitor (TM):

1. Создайте учетную запись базы данных (БД) для SIEM (см. *Создание пользователя siem*).
2. Настройте передачу информации из TM в SIEM (см. *Передача логов в SIEM*).
3. При необходимости измените настройки логирования аудита сессий пользователей БД TM (см. *Управление логированием сессий пользователей БД TM*).

> **Примечание:**
>
> Для взаимодействия с настройками SIEM используется менеджер настроек SIEM integration, запускаемый скриптом `iwtm-setuptool.py` в командной строке. Навигация в менеджере осуществляется с помощью стрелок клавиатуры и клавиши **Enter** или с помощью мыши. Возврат на предыдущее окно менеджера осуществляется с помощью стрелки клавиатуры влево. Выход из менеджера осуществляется нажатием клавиш **Ctrl+C**. Подробнее о работе в менеджере настроек см. статьи, указанные выше.

Управление пользователем siem

В данном разделе описывается создание, удаление и смена пароля для пользователя **siem**, от имени которого SIEM взаимодействует с TM:

- Создание пользователя siem;
- Смена пароля пользователя siem;
- Удаление пользователя siem.

Создание пользователя siem

Чтобы создать пользователя siem:

1. Запустите скрипт при помощи команды:
   `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. В появившемся меню менеджера настроек SIEM integration выберите опцию **DB siem user**.
3. Выберите опцию **Create DB siem user**.
4. Задайте параметры:

Параметр	Описание
`DB admin login`	Логин для учетной записи администратора PostgreSQL. **Примечание:** используется логин `postgres`
`DB admin password`	Пароль для учетной записи администратора PostgreSQL.
`DB siem user password`	Пароль для новой учетной записи siem.

5. Нажмите **Create**.

Смена пароля пользователя siem

Чтобы сменить пароль пользователю siem:

1. Запустите скрипт при помощи команды:
   `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. В появившемся меню менеджера настроек SIEM integration выберите опцию **DB siem user**.
3. Выберите опцию **Change password for DB siem user**.
4. Задайте параметры:

Параметр	Описание
`DB admin login`	Логин для учетной записи администратора PostgreSQL. **Примечание:** используется логин `postgres`
`DB admin password`	Пароль для учетной записи администратора PostgreSQL.
`New siem user password`	Новый пароль для учетной записи siem.

5. Нажмите **Change password**.

Удаление пользователя siem

Чтобы удалить пользователя siem:

1. Запустите скрипт при помощи команды: `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. В появившемся меню менеджера настроек SIEM integration выберите опцию **DB siem user**.
3. Выберите опцию **Delete DB siem user**.
4. Задайте параметры:

Параметр	Значение
`DB admin login`	Логин для учетной записи администратора PostgreSQL.
`DB admin password`	Пароль для учетной записи администратора PostgreSQL.

5. Нажмите **Delete**.

Передача логов в SIEM

Чтобы настроить передачу записей из лог-файлов Linux-сервера Traffic Monitor в SIEM:

1. Запустите скрипт при помощи команды: `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. В появившемся меню менеджера настроек SIEM integration выберите опцию **Log messages forwarding configuration**.
3. Задайте параметры передачи логов:

Параметр	Описание
`Enable forwarding`	Включение/выключение пересылки логов в SIEM. Возможные значения: `Yes/No`
`Forwarding server`	IP-адрес или DNS-имя сервера SIEM.
`Forwarding server port`	Порт сервера SIEM, на котором работает служба syslog.
`Forwarding protocol`	Протокол передачи данных в SIEM. Возможные значения: `TCP/UDP`
`Log messages severity`	Минимальный уровень лог-сообщений, пересылаемых на сервер SIEM. Возможные значения: `Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug`
`Size (MB)`	Допустимый размер очереди сообщений, требующих отправку в SIEM. Значение по умолчанию: `500`

4. Нажмите **OK**.

> **Важно!**
>
> Отключение пользователей с правами администратора от базы данных не логируется, поэтому в SIEM данная информация не попадает.

Управление логированием сессий пользователей БД TM

Включение и выключение логирования сессий пользователей базы данных (БД) Traffic Monitor в системном журнале ОС осуществляется через службу rsyslog.

Чтобы включить логирование сессий пользователей БД Traffic Monitor:

1. Запустите скрипт при помощи команды:
   `/opt/iw/tm5/bin/config/iwtm-setuptool.py`
2. В появившемся меню менеджера настроек SIEM integration выберите опцию **DB audit logging management**.
3. Введите учетные данные администратора БД:
   - **DB admin login** – логин для учетной записи администратора PostgreSQL;
   - **DB admin password** – логин для учетной записи администратора PostgreSQL.
4. Нажмите **Check logging status**.
5. Если:
   - **Logging status: disabled** – нажмите **Change logging status**, чтобы включить логирование;
   - **Logging status: enabled** – нажмите **Change logging status**, чтобы выключить логирование.

9.12.3 Типы логов, передаваемых в SIEM

Rsyslog формирует общий системный журнал и является протоколом, по которому логи передаются в SIEM.

Существует четыре основных типа логов, которые передаются в SIEM:

1. Логи от процессов **iw_***. Например:
   ```
   Mar 11 14:32:30 iw-VMware-4224da3ab iw_xapi: 5 (18485:0x00007f53001b97e0) [INFO   ] : <Root> Runtime environment initialized. Starting...
   ```
2. Логи от скрипта **pguard**, который отслеживает состояние сервисов и перезапускает их при необходимости:
   ```
   Mar 11 14:32:26 iw-VMware-4224da3ab pguard: 148 (18256:0) [INFO] : xapi Terminating pid 18257 (signal 15)
   ```
3. Логи входа и выхода **пользователей Linux**:
   ```
   Mar 11 14:32:02 iw-VMware-4224da3ab runuser: pam_unix(runuser:session): session opened for user iwtm by root(uid=0)
   ```
4. Логи **Nagios**:
   ```
   Feb 10 20:05:39 iw-VMware-4224289a4 nagios: SERVICE ALERT: IWTM;TM_DAEMONS_STATE;CRITICAL;SOFT;1;CRITICAL - updater(3)
   ```

9.13 Удаление временных файлов

Возможность удаления временных файлов реализована в продукте в виде сценария **clean_temporary_files.sh**.

Сценарий удаляет следующую информацию:

1. Файлы из директории временных файлов операционной системы (директория `/opt/iw/tm5/tmp/`).
2. Данные из директорий файловых очередей Traffic Monitor (директория `/opt/iw/tm5/queue/`).

> **Примечание:**
>
> Во время удаления временных файлов обработка поступающих в Систему событий будет остановлена. Данные обо всех необработанных на момент начала удаления событиях будут удалены.

Чтобы удалить временные файлы:

1. Запустите сценарий **clean_temporary_files.sh**:
   `/opt/iw/tm5/bin/clean_temporary_files.sh`
2. Согласитесь на удаление временных файлов:
   `yes`

10 Работа в Traffic Monitor в веб-интерфейсе Центра администрирования (Платформа)

Чтобы пользователю было удобно работать одновременно и с Traffic Monitor, и с продуктами на базе Платформы, реализована возможность работы в Traffic Monitor в веб-интерфейсе Центра администрирования (Платформа). Это позволит пользователям при работе не переключаться между продуктами, а работать в одном веб-интерфейсе.

Чтобы работать в Traffic Monitor в веб-интерфейсе Платформе, выполните следующие шаги:

1. Добавьте в Центре расследований интеграцию с Traffic Monitor. Если вы уже добавили интеграцию ранее, пропустите этот шаг.
   Чтобы добавить интеграцию:
   a. В веб-интерфейсе Центра расследований перейдите в раздел **Настройки** → **Настройки системы** → **Интеграции**.
   b. Нажмите:
      - **+ Добавить интеграцию** в центре окна, если еще не было настроено ни одной интеграции;
      - **+ Добавить** в правом верхнем углу, если ранее была настроена другая синхронизация.
   c. Выберите **InfoWatch Traffic Monitor** и введите параметры интеграции. Подробнее об интеграции и параметрах см. в *Руководстве администратора* используемого вами продукта на базе Платформы, в статье *Интеграция с InfoWatch Traffic Monitor*.
   d. Нажмите **Проверить соединение**, чтобы проверить полноту и корректность введенных параметров, и дождитесь сообщения **Соединение успешно установлено**.
      Также возможно появление следующих статусов:
      - **Задан некорректный токен**;
      - **Не удалось установить соединение** – был введен неверный адрес или сервер недоступен;
      - **Превышено время ожидания ответа от сервиса** – высокая нагрузка на Traffic Monitor, проблемы в сети или иные проблемы (при этом Traffic Monitor может быть доступен и синхронизация выполнится);
      - **Доступ к данным не разрешен** – в Traffic Monitor отсутствует лицензия на экспорт данных в Центр расследований или истек срок ее действия.
   e. Нажмите **Сохранить и синхронизировать**, чтобы запустить процесс синхронизации.
2. Чтобы включить отображение интерфейса Traffic Monitor в Платформе:
   a. Подключитесь к центральной ноде Платформы.
   b. Выполните команду:

      ```
      kubectl exec -it -n infowatch $(kubectl get pods -n infowatch | grep postgresql-central |  awk '//{print $1;}') -- psql -U postgres -d configstorage -c "UPDATE key_values SET obj = jsonb_set(obj, '{Obj}', 'true'::jsonb) WHERE id = 'FT_TMFrame'"
      ```

   c. Для применения изменений в веб-интерфейсе Платформы перезагрузите страницу браузера.
3. Для безопасного входа в продукт рекомендуем на компьютер, с которого вы будете авторизоваться в продукты, установить ssl/tls-сертификат, подписанный доверенным

сертификатом или сертификатом, выданным удостоверяющим центром.

> **Примечание:**
>
> Если сертификат не установлен, для доступа к Traffic Monitor вы можете открыть его в отдельной вкладке браузера и подтвердить небезопасный переход на сайт. После этого обновите вкладку с веб-интерфейсом Платформы, в Центре администрирования станет доступно окно авторизации Traffic Monitor.

4. Чтобы открыть интерфейс Traffic Monitor в Платформе:
   a. Для перехода в Центр администрирования в левом нижнем углу нажмите .
   b. Слева вверху раскройте пункт Traffic Monitor и выберите сервер, к которому хотите подключиться.
   c. В открывшемся окне авторизации введите логин и пароль вашей учетной записи Traffic Monitor.

Вы также можете настроить сквозную аутентификацию между продуктами Центра расследования и Traffic Monitor, подробнее см. *Настройка сквозной аутентификации между продуктами InfoWatch*.

> **Примечание:**
>
> В интерфейсе Traffic Monitor в Центре администрирования недоступны разделы Сводка, События и Отчеты и строка поиска событий по ID. Работать с событиями и отчетами вы можете в разделах Центра расследований.
>
> При работе в веб-интерфейсе Платформы недоступен выход из Traffic Monitor. После авторизации сессия пользователя завершится только по таймауту.

11 Настройка сквозной аутентификации между продуктами InfoWatch

Сквозная аутентификация позволяет вам переходить между Traffic Monitor и Центром расследований InfoWatch без повторного ввода логина и пароля. Технология единого входа возможна только при явном переходе из одного продукта в другой и только для пользователей, созданных на основании одинаковой учетной записи в Active Directory.

Чтобы настроить сквозную аутентификацию:

1. На главном сервере Центра расследований (центральная нода Платформы) введите команду в командной строке:

   ```
   kubectl get secret guardkeys-central -n infowatch --output='go-template={{index .data
   "ec256-public.pem"}}' | base64 -d
   ```

   Отобразится публичный ключ в PEM-формате. Пример ключа:

   ```
   -----BEGIN PUBLIC KEY-----
   MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEIlNdAukpfJjZspZHWV2uu6U9D9/H
   IDCRYBmIRApbE4J2aiS3DGQICAJ3QShiFZtRYVATtJSPsyWGX4CP46Dbxg==
   -----END PUBLIC KEY-----
   ```

2. Скопируйте и сохраните ключ.
3. На сервере Traffic Monitor подключитесь к базе данных:

   ```
   psql postgres iwtm
   ```

4. Укажите список доверенных систем, которые могут авторизоваться в Traffic Monitor, используя свои учетные записи. Для каждой доверенной системы задайте название и открытый ключ. Например, выполните команду:

   ```
   insert into trusted_system(system_name, public_key)
   values('my system','-----BEGIN PUBLIC KEY-----
   MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEIlNdAukpfJjZspZHWV2uu6U9D9/H
   IDCRYBmIRApbE4J2aiS3DGQICAJ3QShiFZtRYVATtJSPsyWGX4CP46Dbxg==
    -----END PUBLIC KEY-----');
   commit;
   ```

5. Выйдите из интерфейса базы данных:

   ```
   exit
   ```

6. В Консоли управления Traffic Monitor настройте и запустите синхронизацию с Active Directory для импорта пользователя, который будет работать в обеих системах. Дождитесь успешного завершения синхронизации.
7. В разделе **Управление доступом** добавьте нового пользователя из LDAP, назначьте ему роль на просмотр событий и область видимости.
8. Выйдите из учетной записи пользователя.
9. В веб-интерфейсе Центра расследований настройте и запустите ту же синхронизацию с Active Directory для импорта того же пользователя. Дождитесь успешного завершения синхронизации.

10. На вкладке **Пользователи** добавьте нового пользователя из LDAP и назначьте ему роль.
11. Выйдите из учетной записи пользователя и выполните вход от имени нового созданного пользователя LDAP.
12. Перейдите в раздел **События**, щелчком мыши выберите в списке одно или несколько событий и нажмите **Просмотр события**.

Откроется раздел **События** в Консоли управления Traffic Monitor, и Система автоматически авторизует вас. Кроме того, в журнале аудита будет зарегистрирован вход пользователя из внешней системы.

12 Взаимодействие с внешними системами

Обмен данными между Traffic Monitor и внешними системами осуществляется посредством API. Подробнее см. *InfoWatch Traffic Monitor. Введение в API*.

Также взаимодействие Traffic Monitor с другими внешними системами поддерживается посредством адаптеров, разработанных компанией InfoWatch. Подробнее о поддерживаемых интеграциях InfoWatch см. в разделе *Интеграционные решения IW Traffic Monitor*.

13 Приложение A. Рекомендации по составлению имен и паролей

Требования к именам пользователей

- Длина имени пользователя должна составлять от 1 до 20 символов.
- Имя пользователя должно состоять из букв латинского алфавита, цифр и символа подчеркивания «_».
- Имя пользователя должно начинаться с буквы.

Требования к паролям пользователей

- Длина пароля может составлять от 8 до 128 символов.
- Пароль пользователя должен состоять только из букв латинского алфавита, цифр и символов: «#», «$», «!» или «%».
- Пароль чувствителен к регистру символов.

Рекомендации по составлению надежных паролей

- Рекомендуемая длина пароля: от 10 до 30 символов.
- Рекомендуемый пароль должен представлять собой смешанный набор букв, цифр и символов.
- Не рекомендуется:
    - включать в состав пароля слова и словосочетания;
    - включать в состав пароля несколько идущих подряд одинаковых символов;
    - начинать и заканчивать пароль одним и тем же символом;
    - создавать новый пароль путем добавления символов к текущему паролю.

14 Приложение B. Индикаторы мониторинга

В приведенной ниже таблице перечислены все индикаторы, используемые подсистемой мониторинга для проверки состояния компонентов, установленных и работающих на серверах Системы в режиме установки "Все-в-одном". Под проверкой подразумевается периодическое получение значения индикатора и сравнение значения индикатора с пороговым значением. Если все индикаторы показывают критические значения, это может свидетельствовать о физической недоступности проверяемых серверов. Следует проверить их работоспособность.

Важно!

Если производились изменения конфигурационных файлов, то пороговые значения и период проверки могут отличаться от указанных.

Важно!

Если действия, рекомендованные в таблице, не привели к решению проблемы, обратитесь в службу технической поддержки InfoWatch по адресу *support@infowatch.com*.

Название индикатора	**Что проверяется и где проверяется**	**Периодичность опроса**	**Значения индикатора**	Подробности и рекомендации
Общая нагрузка системы	Загрузка серверов Linux-серверы, TMcap-серверы, серверы БД за последние 15, 5, 1 минуту	30 мин.	🔴 – хотя бы одна цифра превышает соответствующее значение 20.0,16.0,12.0 за 15, 5, 1 🟡 – хотя бы одна цифра превышает соответствующее значение 10.0,8.0,6.0 за 15, 5, 1 🟢 – ни одна цифра не превышает соответствующее значение 10.0,8.0,6.0 за 15, 5, 1	Проверьте загруженность серверов перехвата и анализа, серверов БД: 1. Выполните: `top` 2. Отсортируйте результаты: a. Shift+m - по загрузке ОЗУ; b. Shift+p - по загрузке ЦП.

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
Состояние компонентов Системы	Статусы служб системы	30 мин.	🔴 – хотя бы один сервис не запущен 🟢 – все сервисы запущены	Состав и количество служб Системы в режиме установки "Все-в-одном" известен и постоянен. Чтобы вывести на экран подробности о состоянии служб, введите: `iwtm status`
Состояние службы syslog	Запущен или нет сервис syslog	30 мин.	🔴 – не запущен 🟢 – запущен	Проверьте запуск службы rsyslog: `systemctl status rsyslog`
Количество активных пользователей	Количество пользователей (Офицеров безопасности), зарегистрированных в Системе (Linux-серверы)	30 мин.	🔴 – > 50 пользователей 🟡 – от 20 до 50 🟢 – < 20 пользователей	Необходимо уменьшить количество ОБ до 50 человек
Ошибки в журнале предупреждений БД	Наличие ошибок в журнале предупреждений БД (Серверы БД)	5 мин.	🔴 – есть ошибки 🟢 – нет ошибок	Необходимо снизить количество ошибок с SEVERITY=HIGH. **Поиск в pg_log должен осуществляться по наличию слов:** • FATAL • PANIC • ERROR
Доступность сервера	Время ответа на посылаемые пакеты и количество потерянных пакетов (Linux-серверы)	5 мин.	🔴 – > 500 мс 🟡 – от 100 до 500 мс 🟢 – < 100 мс	Пинг заданных серверов с параметрами `100.0,20%! 500.0,60%` означает, что ответ на посылаемые пакеты составляет больше 100 миллисекунд и теряется больше чем 20% пакетов, более

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
				500 миллисекунд и теряется 60% пакетов.
Доступность встроенного агента передачи почты	Доступность сервера Exim	30 мин.	🔴 – не доступен 🟢 – доступен	1. Проверьте состояние сервера Exim: `systemctl status exim4` 2. Запустите проверку конфигурационного файла */etc/exim4/exim4.conf* на правильность: `exim4 check`
Доступность сервера по SSH	Время ответа на запрос	10 мин.	🔴 – >= 10 с 🟢 – < 10 с	Проверьте состояние демона sshd: `systemctl status sshd`
Доступность сервера Device Monitor	Ответа на запрос	30 мин.	🔴 – нет соединения 🟢 – есть соединение	Должно отображаться, если в Системе установлена активная лицензия на Device Monitor. Проверьте наличие лицензии в разделе **Управление->Лицензии** в консоли управления Traffic Monitor
Использование файла подкачки	Количество свободного места в swap (виртуальная память). (Linux-серверы)	5 мин.	🔴 – свободно < 10% 🟡 – свободно от 50% до 10% 🟢 – свободно > 50%	Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Рекомендации по разбиению дискового пространства*

Название индикатора	**Что проверяется и где проверяется**	**Периодичность опроса**	**Значения индикатора**	Подробности и рекомендации
Свободное место в корневой партиции	Количество свободного места в корневой файловой системе. (Linux-серверы)	30 мин.	🔴 – < 10 000 Мб 🟡 – от 10 000 МБ до 20 000 Мб 🟢 – > 20 000 Мб	
Свободное место в партиции /var	Количество свободного места в файловой системе `/var.(` Linux-серверы)	30 мин.	🔴 – < 10 000 Мб 🟡 – от 10 000 Мб до 20 000 Мб 🟢 – > 20 000 Мб	
Состояние службы синхронизации времени	Статус сервиса ntpd. (NTPD)	30 мин.	🔴 – NTP сервер не доступен 🟢 – NTP сервер доступен	Проверьте состояние демона ntpd: `systemctl status ntpd`
Отклонение системного времени	Лаг времени на серверах Системы и сервере NTP. (Linux-серверы)	360 мин.	🔴 – > 40 с 🟡 – от 20 до 40 с 🟢 – < 20 с	Данная ошибка возникает, если Системе не удалось установить соединение с NTP-серверами или в конфигурации Системы не указано ни одного NTP-сервера. В этом случае появится сообщение об ошибке "*Can't create socket connection*". Убедитесь, что в конфигурационных файлах *ntp.conf* и *iwmon-services-ntp.cfg* указан один и тот же корректный NTP-сервер.
Наличие дампов памяти	Проверяется работоспособность сервисов, отсутствие падений, учитывается	30 мин.	🔴 – есть 5 или более дампов 🟡 – есть от 1 до 4 дампов	Обратитесь в службу технической поддержки InfoWatch по адресу *support@infowatch.com*

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
	количество файлов в каталоге /opt/iw/tm5 вида: • core_<....> • <...>.core (Linux-серверы)		🟢 – нет дампов	

Очередь ошибок обработки событий	Количество объектов в очереди **queue/final-errors** (iw_rammer)	1 мин.	🔴 – > 1
			🟢 – 0
				Вариант 1: Очистите очереди, используя команды:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/final-errors`
				`exit`
				Вариант 2:
				1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`
				2. Уменьшите период очистки файлов в папках файловой очереди в штатном задании cron (значение по умолчанию - 30 дней).
				3. Сохраните изменения и закройте файл.
				Для получения дополнительной информации см. *Блокировка "в разрыв"*

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
Состояние базы данных	Статус базы данных (в зависимости от используемой в системе СУБД)	10 мин.	🔴 – <> ok 🟢 – ok	Проверьте, доступна ли БД: 1. Зайдите в БД: `sqlplus iwtm@iwtm` 2. Введите пароль: xxXX1234 3. Наблюдайте: `SQL>`
Свободное место в основном каталоге БД	Свободное место на партиции хранения основной информации (По умолчанию: `/u01`)	30 мин.	🔴 – < 10 000 Мб 🟡 – от 10000 до 20 000 Мб 🟢 – > 20 000 Мб	Выделите больше места на диске для `/u01` (подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Рекомендации по разбиению дискового пространства*)
Свободное место в каталогах событий БД	Свободное место на партициях хранения событий (По умолчанию: `/u02`)	30 мин.	🔴 – < 7% 🟡 – от 7 до 15% (если для хранения ежедневных ТП используются несколько разделов, то при значении < 7% хотя бы в одном разделе) 🟢 – > 15%	Если для хранения ежедневных табличных пространств используется несколько дисковых разделов, то свободное место рассчитывается как сумма всех разделов, выделенных под ежедневные ТП на этапе установки Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Рекомендации по разбиению дискового пространства*
Свободное место в каталоге ежедневных	Свободное место в партиции	30 мин.	🔴 – < 7% 🟡 – от 7 до 15%	Индикатор добавляется, если при установке был

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
табличных пространств на быстром диске	хранения ежедневных табличных пространств на быстром диске.		🟢 – > 15%	выбран режим хранения данных *Быстрые и медленные диски* Подробнее см. *InfoWatch Traffic Monitor. Руководство по установке. Рекомендации по разбиению дискового пространства*
Размер журнала предупреждений БД	Размер журнала предупреждений для СУБД PostgreSQL: System Log	5 мин.	🔴 – > 3 Гб 🟡 – от 1 Гб до 3 Гб 🟢 – < 1 Гб	Обратитесь в службу технической поддержки InfoWatch по адресу *support@infowatch.com*
Наличие ошибок в журнале базы данных	Наличие ошибок	30 мин.	🔴 – > 1 🟡 – 1 🟢 – нет ошибок	Необходимо снизить количество ошибок с SEVERITY=Error
Очередь обработки почтового трафика	Количество объектов в очереди **queue/smtp** (iw_messed)	30 мин.	🔴 – > 10000 объектов 🟡 – от 1000 до 10000 объектов 🟢 – < 1000 объектов	1. Проверьте статус службы: `systemctl status iw_messed` 2. Просмотрите логи службы в `opt/iw/tm5/log/messed_app.log` 3. Проверьте нагрузку на оперативную память и swap: a. для краткого вывода выполните: `free -m` b. для расширенного вывода выполните:

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
				`cat /proc/meminfo`
Очередь на контентный анализ для xAPI/pushAPI-объектов	Количество объектов в очереди **queue/analysis** (iw_analysis)	30 мин.	🔴 – > 10000 объектов 🟡 – от 1000 до 10000 объектов 🟢 – < 1000 объектов	1. Проверьте статус службы: `systemctl status iw_analysis` 2. Просмотрите логи службы в `opt/iw/tm5/log/analysis.log` 3. Проверьте нагрузку на оперативную память и swap: a. для краткого вывода выполните: `free -m` b. для расширенного вывода выполните: `cat /proc/meminfo`
Очередь загрузки объектов от перехватчиков в сервис **iw_x2x**	Количество объектов от перехватчиков для **iw_x2x** в очереди **queue/db** (iw_x2x)	30 мин.	🔴 – > 10000 объектов 🟡 – от 1000 до 10000 объектов 🟢 – < 1000 объектов	1. Проверьте статус службы: `systemctl status iw_x2x` 2. Просмотрите логи службы в `opt/iw/tm5/log/x2x.log` 3. Проверьте нагрузку на оперативную память и swap: a. для краткого вывода выполните: `free -m`

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
				b. для расширенного вывода выполните: `cat /proc/meminfo`
Очередь загрузки в хранилище	Количество объектов в очереди **queue/x2x** на загрузку в хранилище сервисом **iw_x2db** (TMcap-серверы)	30 мин.	🔴 – > 10000 объектов 🟡 – от 1000 до 10000 объектов 🟢 – < 1000 объектов	1. Проверьте статус службы: `systemctl status iw_x2db` 2. Просмотрите логи службы в `opt/iw/tm5/log/x2db.log` 3. Проверьте нагрузку на оперативную память и swap: a. для краткого вывода выполните: `free -m` b. для расширенного вывода выполните: `cat /proc/meminfo`
Очередь обработки действий от примененных политик	Количество объектов в очереди **queue/blackboard** (Linux-серверы)	30 мин.	🔴 – > 1000 объектов 🟡 – от 200 до 1000 объектов 🟢 – < 200 объектов	1. Проверьте статус службы: `systemctl status iw_analysis` 2. Просмотрите логи службы в `opt/iw/tm5/log/analysis.log` 3. Проверьте нагрузку на оперативную память и swap:

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
				a. для краткого вывода выполните: `free -m` b. для расширенного вывода выполните: `cat /proc/meminfo`
Очередь объектов на индексацию в Sphinx для полнотекстового поиска	Количество объектов в очереди на индексацию в Sphinx для полнотекстового поиска	30 мин.	🔴 – > 10000 объектов 🟡 – от 1000 до 10000 объектов 🟢 – < 1000 объектов	1. Проверьте статус службы: `searchd --status -c /etc/infowatch/sphinx.conf` 2. Просмотрите логи службы в `opt/iw/tm5/log/sphinx/` 3. Проверьте нагрузку на оперативную память и swap: a. для краткого вывода выполните: `free -m` b. для расширенного вывода выполните: `cat /proc/meminfo` 4. Вычислите количество запущенных экземпляров `searchd`: a. если на ноде запущен `iw_is, то: 1`

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
				(сам iw_is)+ 4 (grep max_children /opt/iw/tm5/ etc/ is.conf)=5 b. если на ноде запущен iw_indexer, то: 1 (сам iw_ndexer)+ 8 (grep max_children /opt/iw/tm5/ etc/ sphinx.conf)=9 c. Итого: a+b=14 экземпляров searchd. Чем больше процессов, тем меньше вероятность длительного выполнения поискового запроса пользователя.
Очередь объектов на индексацию в Sphinx для поиска по метаинформации	Количество объектов в очереди на индексацию в Sphinx для поиска по метаинформации	30 мин.	🔴 – > 10000 объектов 🟡 – от 1000 до 10000 объектов 🟢 – < 1000 объектов	1. Проверьте статус службы: `searchd --status -c /etc/infowatch/sphinx.conf` 2. Просмотрите логи службы в `opt/iw/tm5/log/sphinx/` 3. Проверьте нагрузку на

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
				оперативную память и swap: a. для краткого вывода выполните: `free -m` b. для расширенного вывода выполните: `cat /proc/meminfo`
Количество ошибок индексации событий службой **iw_indexer**	Количество ошибок индексации (iw_indexer)	30 мин.	🔴 – > 100 ошибок 🟡 – от 10 до 100 🟢 – 10	1. Проверьте статус службы: `systemctl status iw_indexer` 2. Просмотрите логи службы в `opt/iw/tm5/log/indexer.log` 3. Проверьте нагрузку на оперативную память и swap: a. для краткого вывода выполните: `free -m` b. для расширенного вывода выполните: `cat /proc/meminfo`
Количество ошибок индексации метаинформации службой **iw_is**	Количество ошибок индексации метаинформации службой **iw_is**	30 мин.	🔴 – > 100 ошибок 🟡 – от 10 до 100 ошибок 🟢 – 10 ошибок	1. Проверьте статус службы: `systemctl status iw_is` 2. Просмотрите логи службы в

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
Очередь команд **iw_is**	Количество команд в очереди службы **iw_is**	30 мин.	🔴 – > 100 команд 🟡 – от 50 до 100 команд 🟢 – < 50 команд	`opt/iw/tm5/log/is.log` 3. Проверьте нагрузку на оперативную память и swap: a. для краткого вывода выполните: `free -m` b. для расширенного вывода выполните: `cat /proc/meminfo`
Очереди выборки данных	Количество объектов в очереди службы **iw_is**	30 мин.	🔴 – > 100 объектов 🟡 – от 50 до 100 объектов 🟢 – < 50 объектов	
Очередь индексации **iw_is**	Количество объектов в очереди службы **iw_is**	30 мин.	🔴 – > 100 объектов 🟡 – от 50 до 100 объектов 🟢 – < 50 объектов	
Очередь ошибок **iw_is**	Наличие ошибок сервиса **iw_is**	5 мин.	🔴 – > 500 🟡 от 50 до 500 🟢 – < 50	
Очередь команд для табличного пространства текста	Количество команд в очереди табличного пространства текста	30 мин.	🔴 – > 50 команд 🟡 – от 20 до 50 команд 🟢 – < 20 команд	1. Включите логирование работы службы **iw_indexer** на `debug` (см. *Логирование работы Системы*) 2. Просмотрите лог-файл **iw_indexer** на ошибки в `opt/iw/tm5/log/indexer.log` 3. Обратитесь в службу технической

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
Очередь команд для табличного пространства метаинформации	Количество команд в очереди табличного пространства метаинформации	30 мин.	🔴 – > 50 команд 🟡 – от 20 до 50 команд 🟢 – < 20 команд	поддержки InfoWatch

Очередь ошибок обработки событий	Количество объектов в очереди ошибок **queue/errors** (Extractors Framework, TMcap-серверы: iw_luaengined, iw_warpd, iw_cas)	30 мин.	🔴 – > 500 объектов
			🟡 – от 50 до 500 объектов
			🟢 – < 50 объектов
				Вариант 1: Очистите очередь, используя команды:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/errors`
				`exit`
				Вариант 2:
				1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`
				2. Уменьшите период очистки файлов в папках файловой очереди в штатном задании cron (значение по умолчанию - 30 дней).
				3. Сохраните изменения и закройте файл.

Очередь ошибок обработки событий сервисом **iw_x2x**	Количество объектов в очереди **queue/x2x-errors** (iw_x2x)	30 мин.	🔴 – > 500 объектов
			🟡 – от 50 до 500 объектов
			🟢 – 50
				Вариант 1: Очистите очередь, используя команды:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /`

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации

				`opt/iw/tm5/queue/x2x-errors`
				`exit`
				Вариант 2:
				1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`
				2. Уменьшите период очистки файлов в папках файловой очереди в штатном задании cron (значение по умолчанию - 30 дней).
				3. Сохраните изменения и закройте файл.

Очередь ошибок обработки событий сервисом **iw_x2db**	Количество объектов в очереди **queue/x2db-errors** (iw_x2db)	30 мин.	🔴 – > 500 объектов
			🟡 – от 50 до 500 объектов
			🟢 – 50
				Вариант 1: Очистите очередь, используя команды:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/x2db-errors`
				`exit`
				Вариант 2:
				1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`
				2. Уменьшите период очистки файлов в папках файловой очереди в штатном

Название индикатора	Что проверяется и где проверяется	Периодичность опроса	Значения индикатора	Подробности и рекомендации
				задании cron (значение по умолчанию - 30 дней). 3. Сохраните изменения и закройте файл.

Очередь ошибок обработки действий примененных политик	Количество объектов в очереди **queue/blackboard_errors** (Linux-серверы)	30 мин.	🔴 – > 500 объектов
			🟡 – от 50 до 500 объектов
			🟢 – 50
				Вариант 1: Очистите очередь, используя команды:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/blackboard-errors`
				`exit`
				Вариант 2:
				1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`
				2. Уменьшите период очистки файлов в папках файловой очереди в штатном задании cron (значение по умолчанию - 30 дней).
				3. Сохраните изменения и закройте файл.