

INFOWATCH

InfoWatch Traffic Monitor 7.0

Руководство администратора

11/06/2020

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Введение 5
1.1 Аудитория 5
1.2 Комплект документов 5
1.3 Техническая поддержка пользователей 5
2 Обзор Traffic Monitor 6
2.1 Функции InfoWatch Traffic Monitor 6
2.1.1 Схема перехвата SMTP-трафика 6
2.1.2 Каналы перехвата Device Monitor 7
2.1.3 Анализ информации на файловых ресурсах внутрикорпоративной сети 8
2.2 Состав InfoWatch Traffic Monitor (Astra Linux) 8
2.3 Лицензирование 10
3 Типы установки Системы 12
4 Настройка Системы после установки 13
4.1 Предварительные настройки 13
4.1.1 Настройка синхронизации времени 13
4.1.2 Конфигурирование работы Sphinx при распределенной установке 14
4.2 Настройка перехвата трафика 14
4.2.1 Настройка перехвата SMTP-трафика 15
4.2.1.1 Прием копий с почтового сервера 15
4.2.1.2 Настройки почтовых серверов для перехвата SMTP-трафика 17
4.2.2 Прием объектов, перехваченных InfoWatch Device Monitor 19
4.2.3 Проверка файлов, находящихся в корпоративной сети 19
4.3 Автозапуск процессов 20
4.3.1 Проверка автозапуска процессов 20
4.3.2 Включение и выключение автозапуска процессов 23
4.4 Модуль взаимодействия с удаленной базой данных 24
4.4.1 Настройка сбора данных в филиальной сети 24
4.4.2 Настройка клиентской части модуля взаимодействия с удаленной БД 24
4.4.3 Настройка серверной части модуля взаимодействия с удаленной БД 26
4.5 Настройка OCR-экстракторов 26
4.6 Настройка отправки уведомлений пользователям и сотрудникам 29
4.7 Ограничение количества найденных событий 29
4.8 Настройка Сервера InfoWatch Device Monitor 29
4.8.1 Раздел <applicationSettings> 31

4.8.2 Раздел <system.diagnostics> ... 36
4.8.3 Удаление временных файлов Device Monitor ... 38
4.9 Настройка межсервисного взаимодействия (служба Consul) ... 39
4.9.1 Запуск и остановка службы ... 39
4.9.2 Регистрация сервисов в Consul ... 40
4.9.3 Распределенная установка ... 42
4.9.4 Настройка сетевых правил доступа в Consul ... 44
4.9.5 Конфигурационный файл consul.json и unit-файл iwtm-consul.service ... 44
4.10 Изменение предустановленного пароля в Системе ... 47
5 Конфигурирование перехватчика Краулер ... 48
5.1 Настройка сетевых правил доступа ... 48
5.2 Конфигурационные файлы Краулер ... 50
5.2.1 Конфигурационный файл сервера Краулер ... 50
5.2.1.1 Изменение учетной записи, от имени которой запускается служба сервера Краулер ... 51
5.2.1.2 Скрипты сканирования SharePoint ... 51
5.2.2 Конфигурационный файл сканера Краулер ... 52
5.2.3 Выключение шифрования трафика между компонентами ... 53
5.3 Работа с журналами Краулер ... 54
5.4 Автоматическое удаление событий Краулер ... 55
6 Мониторинг ... 56
6.1 Настройки подсистемы мониторинга ... 56
6.1.1 Настройка подключения Device Monitor ... 56
6.1.2 Ручная настройка индикаторов ... 57
6.1.3 Настройка адреса сервера синхронизации времени для подсистемы мониторинга ... 57
6.1.4 Настройка порогов срабатывания для индикатора нагрузки ... 57
7 Администрирование базы данных ... 58
7.1 PostgreSQL ... 58
7.1.1 Проведение регламентных работ на сервере базы данных ... 58
7.1.2 Табличные пространства в базе данных InfoWatch Traffic Monitor ... 59
7.1.3 Управление ежедневными табличными пространствами ... 60
7.1.3.1 Архивирование ежедневных табличных пространств ... 60
7.1.3.2 Восстановление ежедневных табличных пространств ... 63
7.1.3.3 Настройка размещения файлов в файловой системе ... 64
7.1.3.4 Настройка режимов хранения файлов табличного пространства ... 65
7.1.3.5 Удаление ежедневных табличных пространств ... 67
7.1.4 Резервное копирование базы данных ... 69
7.1.4.1 Создание резервной копии базы данных ... 69
7.1.4.2 Восстановление базы данных из резервной копии ... 72

8 Администрирование серверной части InfoWatch Traffic Monitor 74
8.1 Процессы серверной части Traffic Monitor Server 74
8.1.1 Список процессов серверной части Traffic Monitor 74
8.1.2 Работа с процессами серверной части Traffic Monitor 82
8.2 Настройка конфигурационных файлов серверной части Traffic Monitor 83
8.3 Настройка использования OCR 84
8.3.1 Конфигурационный файл ocr_custom.xml 85
8.4 Настройка параметров обработки архивов вложений 87
8.4.1 Конфигурационный файл extractors.xml 87
8.5 Архивирование каталога очереди сообщений 90
8.6 Логирование работы Системы 90
8.7 Файловые очереди 91
8.8 Восстановление работоспособности системы в аварийных ситуациях 94
8.9 Управление языками с поддержкой морфологии 95
8.9.1 Добавление нового языка для поиска событий. Морфология и добавление терминов. 95
8.9.2 Обновление установленного языка 96
8.9.3 Удаление языка для поиска и терминов 97
8.10 Настройка передачи информации в SIEM 97
8.10.1 Настройки на стороне SIEM 98
8.10.1.1 Табличное представление событий TM 98
8.10.1.2 Табличное представление аудита пользователей 104
8.10.2 Настройки на стороне TM 110
8.10.2.1 Передача логов в SIEM 111
8.10.2.2 Управление пользователем siem 111
8.10.3 Типы логов, передаваемых в SIEM 113
8.11 Удаление временных файлов 113
9 Приложение A. Рекомендации по составлению имен и паролей .. 115
10 Приложение B. Индикаторы мониторинга 116

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.

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.

Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ.
Вы также можете посетить раздел технической поддержки на нашем сайте:
https://www.infowatch.ru/services/support
Перед обращением в службу технической поддержки рекомендуется посетить раздел База знаний на нашем сайте: https://kb.infowatch.com/. Возможно, там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

2 Обзор Traffic Monitor

В этой главе:

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

2.1 Функции InfoWatch Traffic Monitor

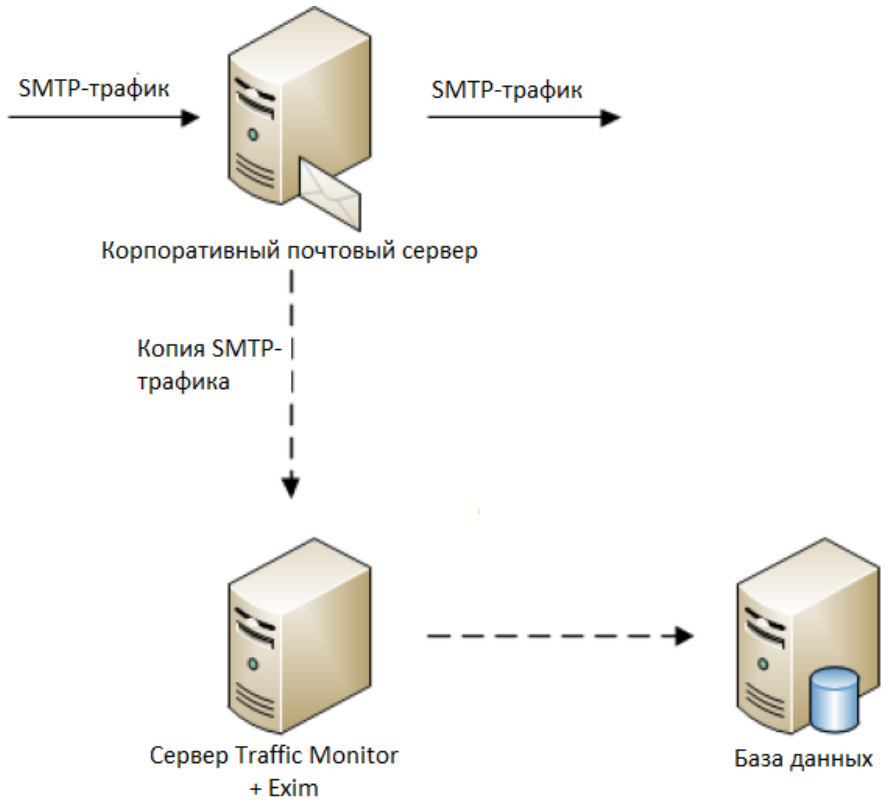
InfoWatch Traffic Monitor позволяет контролировать информационные потоки в корпоративной среде для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.

Основные функции InfoWatch Traffic Monitor:

- Перехват в потоке/на шлюзе трафика, передаваемого по протоколу SMTP, с учетом мандатных меток (начиная с Traffic Monitor версии 6.10.10);
- Перехват трафика на рабочих станциях агентами Device Monitor;
- Анализ информации на файловых ресурсах внутрикорпоративной сети;
- 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

На корпоративном почтовом сервере требуется 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.

2.1.2 Каналы перехвата Device Monitor



На клиентские ОС Microsoft Windows устанавливаются Агенты Device Monitor, которые осуществляют следующие действия:

- контроль отправки и получения электронной почты по протоколам SMTP, IMAP, POP3 и с помощью MAPI, включая зашифрованные сообщения по стандарту S/MIME (см. статью "Настройка правила для Mail Monitor");

- контроль трафика, передаваемого по протоколу HTTP и HTTPS (см. статью "Настройка правила для HTTP(S) Monitor");
- контроль доступа сотрудников к периферийным устройствам компьютерной системы;
- мониторинг печати на контролируемых компьютерах;
- контроль систем мгновенного обмена сообщениями: Skype (в том числе анализ голосового трафика), Telegram (версия для ПК), Facebook, VK (ВКонтакте), Jabber (протокол XMPP), протокол MMP;
- контроль трафика, передаваемого по протоколу FTP и FTPS;
- контроль передачи данных по сетевым соединениям вне корпоративной сети;
- контроль подключения с помощью Microsoft RDP или Citrix ICA;
- контроль файлов, копируемых с/на съемные устройства, сетевые ресурсы и ресурсы, подключенные через терминальную сессию;
- контроль облачных хранилищ файлов;
- контроль снимков экрана;
- контроль приложений.

На клиентские ОС Astra Linux устанавливаются Агенты Device Monitor, которые осуществляют следующие действия:

- контроль отправки и получения электронной почты по протоколам SMTP, IMAP, POP3;
- мониторинг печати на контролируемых компьютерах
- контроль файлов, копируемых с/на съемные устройства, сетевые ресурсы;
- контроль облачных хранилищ файлов;
- контроль трафика, передаваемого по протоколу FTP и FTPS;
- контроль систем мгновенного обмена сообщениями: Facebook, VK (ВКонтакте), Jabber (протокол XMPP);
- контроль трафика, передаваемого по протоколу HTTP и HTTPS.

Подробнее о настройке указанных действий смотрите документ "InfoWatch Traffic Monitor. Руководство пользователя", раздел "Правила (DM)".

Все перехваченные данные могут быть отправлены для анализа на сервер Traffic Monitor.

2.1.3 Анализ информации на файловых ресурсах внутрикорпоративной сети

Анализ содержания файловых серверов и сетевых ресурсов возможен после установки специального модуля на сервер под управлением ОС MS Windows Server.
О настройке данного функционала см. "Конфигурирование перехватчика Краулер".

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) осуществляется агентами подсистемы Device Monitor.

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 следующих технологий: • Категории и термины; • Текстовые объекты; • Эталонные документы; • Векторные изображения; • Бланки; • Печати;
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. 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 следующих модулей: • Модуль мониторинга; • Модуль контроля; • Модуль настройки.

2.3 Лицензирование

уже После установки Системы необходимо также установить лицензию.
Для этого запросите файл лицензионного ключа (см. документ "InfoWatch Traffic Monitor. Руководство пользователя", раздел "Запрос лицензии").
Лицензия определяет срок действия, количество пользователей, набор модулей перехвата и модулей 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 требуется 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 рекомендуется сохранить файл лицензионного ключа на каком-либо носителе информации.

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

Ниже приведены списки модулей, которые используются в продукте.

Модули перехвата		
Подсистема	**Типы событий**	**Протокол**
TM	Email	SMTP
	Краулер	-
DM	Web-сообщение	HTTP HTTPS
	Email	POP3 SMTP
	Печать	-

Съемные устройства	-
Сетевые ресурсы	-
Облачное хранилище	HTTPS
XMPP	XMPP
FTP	FTP
Vkontakte	HTTPS
Facebook	HTTPS

Модули анализа:

1. Лингвистический анализ;
2. Детектор эталонных документов;
3. Детектор векторных изображений;
4. Детектор текстовых объектов;
5. Детектор форм;
6. Детектор печатей.

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. документ "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Схемы развертывания Системы и выбор типа установки"):

- *"Все-в-одном" Enterprise* - тип установки Системы с расширенными возможностями, включая: использование СУБД PostgreSQL, настройку масштабируемости, тонкий контроль за рабочими станциями. Подробнее см. документ "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Установка TM Enterprise и TM Standard в режиме "Все-в-одном";
- *Распределенная установка TM Enterprise (База данных + Сервер Traffic Monitor)* - тип установки Системы для функционирования под большой нагрузкой и работой с большим объемом данных. Подробнее см. документ "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Распределенная установка TM Enterprise".

Важно!

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

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

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

- Crawler - предназначен для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных, а также для контроля файловых ресурсов компании (подробнее см. документ "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Установка подсистемы Краулер").
- InfoWatch Device Monitor - предназначен для настройки схем безопасности, системы мониторинга компьютеров, контроля доступа к компьютерам компании и др. (подробнее см. документ "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Установка InfoWatch Device Monitor").
- 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;
- 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 (подробнее см. документ «*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;
- 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.

Также рекомендуется изменить предустановленные в Системе пароли, следуя требованиям информационной безопасности (подробнее в статье Изменение предустановленных паролей в Системе).

4.1 Предварительные настройки

После установки системы необходимо выполнить следующие настройки:

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

4.1.1 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 ntp:
   ```
   systemctl stop ntp
   ```
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 ntpdate -q <IP> (где IP - адрес проверяемого сервера), например:
   ```
   root@atl-iw:~# ntpdate -q 10.10.0.98
   server 10.10.0.98, stratum 3, offset 9.196765, delay 0.04437
   11 Sep 13:09:02 ntpdate[13819]: step time server 10.10.0.98 offset 9.196765
   sec
   root@atl-iw:~#
   ```
6. Настройте синхронизацию, указав сервер NTP-синхронизации в файле **/etc/ntp.conf**.
   Для этого добавьте запись вида (укажите IP-адрес вашего NTP-сервера):
   ```
   server 10.10.0.98
   ```
7. Запустите службу ntp:
   ```
   systemctl start ntp
   ```
8. Проверьте текущее состояние службы ntp с помощью команды:
   ```
   systemctl status ntp
   ```
9. Включите автоматическую синхронизацию времени:
   ```
   chkconfig --level 345 ntpd on
   ```

4.1.2 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 **TME DB server** (Сведения о режимах установки Системы приведены в Руководстве по установке, статья "Установка Системы").

Распределенной установкой считается схема установки, когда Traffic Monitor и база данных установлены на разных серверах с ключами **TME Node server** и **TME DB server** соответственно.

> **Примечание:**
>
> При наличии нескольких серверов укажите IP-адрес сервера, на котором запущена служба **sphinx** (сервер с базой данных) в параметре `hostname` секции `search` конфигурационного файла **web.conf** сервера **TME Node server** .

4.2 Настройка перехвата трафика

В Системе доступен перехват данных, передаваемых по протоколу SMTP (с Traffic Monitor версии 6.10.10).

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

В ОС Astra Linux 1.6 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, начиная с версии 6.10.10, 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;
- Проверка файлов, находящихся в корпоративной сети.

> **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".

> **Важно!**
>
> После настройки перехвата трафика необходимо настроить параметры анализа объектов (см. документ "InfoWatch Traffic Monitor. Руководство пользователя").

> **Важно!**
>
> На агентах DM, работающих под ОС Astra Linux, перехват почтового трафика осуществляется только по каналам SMTP, POP3 и IMAP.

4.2.1 Настройка перехвата SMTP-трафика

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

- Прием копий с почтового сервера;
- 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 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 необходимо, 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 конфигурационном файле **system.lua**, расположенном в директории `/opt/iw/tm5/etc/scripts`, раскомментирован фрагмент кода:

```
function try_set_transport_mode(processing, mode, warning)
if not get_child(processing, 'transport_mode') then
processing:add_child('transport_mode'):set_text(mode);
return true;
elseif warning then
Log(LogSeverityLevel.warning, 'transport_mode is already set ');
end;
```

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.

Настройки почтовых серверов для перехвата SMTP-трафика

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

- Настройка пересылки скрытых копий Exim4;
- Настройка сервера Exim4 в системе Traffic Monitor.

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 необходимо создавать скрытые копии, а также вспомогательный адрес e-mail с 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. Необходимо 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>
   ```

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. Создайте файл etc/exim4/exim4.conf
2. Внесите в него следующую информацию и сохраните изменения:

```
primary_hostname = <Ваш хостнейм>
recipients_max=100
message_size_limit=50M
hostlist relay_from_hosts = MAIN_RELAY_NETS
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
#no policy checks
acl_smtp_rcpt = accept
#Routers: standard DNS routing and local users
begin routers
forward_route:
driver = manualroute
domains = *
self = send
transport = remote_smtp
route_list = * 127.0.0.1::2025
no_more
```

```
#Transports: SMTP and local mailboxes
begin transports
remote_smtp:
driver = smtp
command_timeout = 10s
```

3. Перезапустите Exim:
   ```
   sudo service exim4 restart
   ```
4. 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>
      ```

4.2.2 Прием объектов, перехваченных InfoWatch Device Monitor

1. Установите и настройте серверную часть Traffic Monitor (см. документ "InfoWatch Traffic Monitor. Руководство по установке", статья "Установка Сервера Traffic Monitor (TME Node server)").
2. Настройте передачу событий из Device Monitor на сервер Traffic Monitor (см. в базе знаний статью "Интеграция Device Monitor с различными версиями Traffic Monitor").
3. Настройте параметры анализа объектов (см. документ "InfoWatch Traffic Monitor. Руководство пользователя", статья "Технологии").

4.2.3 Проверка файлов, находящихся в корпоративной сети

Описание данного способа перехвата трафика см. в статье "Анализ информации на файловых ресурсах внутрикорпоративной сети".
Анализ содержания файловых серверов и сетевых ресурсов возможен после установки специального модуля на сервер под управление MS Windows Server ОС.

1. Установите и настройте сервер Traffic Monitor (см. документ "InfoWatch Traffic Monitor. Руководство по установке", статья "Установка Сервера Traffic Monitor (TME Node server)").
2. Установите и настройте Краулер (см. документ "InfoWatch Traffic Monitor. Руководство по установке", статья "Установка подсистемы Краулер").

3. Настройте общие параметры работы сканера Краулер (см. документ "InfoWatch Traffic Monitor. Руководство администратора", статья "Конфигурирование перехватчика Краулер").
4. Настройте параметры анализа объектов (см. документ "InfoWatch Traffic Monitor. Руководство пользователя").

4.3 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 Server".

4.3.1 Проверка автозапуска процессов

Важно!

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

При логическом выделении основного сервера, сервера перехвата 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 Процесс объединяет сервисы: • `selection` • `iw_blackboard` • `iw_systemcheck` • `iw_agent` • `xapisamplecompiler` • `export` • `iw_sample_compiler` • `report` • `import` • `notifier` • `crawler` Чтобы включить сервис, выставьте сервису значение `1` в секции `kickers` конфигурационного файла **web.conf**. Чтобы выключить сервис, выставьте сервису значение `0` в секции `kickers` конфигурационного файла **web.conf**. **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
iw_icap	Да
iw_icap_buf	Да
iw_is	Да
iw_indexer	Да **Примечание:** Процесс должен работать только на основном сервере
iw_image_autoling	Да

iw_text_autoling	Да
iw_licensed	Да **Примечание:** Процесс должен работать только на основном сервере
iw_luaengined	Да **Примечание:** Процесс должен работать только на основном сервере кластера
iw_messed	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_sniffer	Нет
iw_system_check	Да
iw_updater	Да
iw_warpd	Да
iw_x2x	Да
iw_x2db	Да
iw_xapi_xapi iw_xapi_puppy	Да

Примечание:

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

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

Подробнее о включении автозапуска процессов см. "Включение и выключение автозапуска процессов".

4.3.2 Включение и выключение автозапуска процессов

Чтобы включить/отключить автозапуск процесса (пример приведен для iw_proxy):

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

1. Для возможности автозапуска процесса (например, **iw_proxy_http**) необходимо установить ему статус `enable`, выполнив команду:
   `iwtm enable iw_proxy_http`
   Чтобы отключить возможность автозапуска процесса, установите статус `disable`:
   `iwtm disable iw_proxy_http`
2. Перезапустите службу **iw_proxy**:
   `iwtm restart iw_proxy`

Все процессы Traffic Monitor со статусом `enable` подлежат автозапуску, а процессы со статусом `disable` могут быть запущены только вручную.

Чтобы настроить автозапуск процесса:

1. Директория хранения unit-файлов: **/usr/lib/systemd/system.** Внесите изменения в unit-файл нужного процесса, (см. "Описание конфигурационных и unit-файлов демонов Traffic Monitor") и сохраните его.
2. Выполните перезагрузку конфигурации:
   `systemctl daemon-reload`
3. Добавьте настроенный процесс в автозапуск:
   `iwtm enable <имя_демона>`
4. Запустите процесс:
   `iwtm start <имя_демона>`
5. Проверить, запустился ли сервис, можно любой из команд:
   `systemctl status <имя_демона>`
   `iwtm status`

Чтобы включить автозапуск сразу нескольких процессов, введите:

```
iwtm enable <имя_демона1> <имя_демона2> ... <имя_демонаN>
```

Чтобы выключить автозапуск сразу нескольких процессов, введите:

```
iwtm disable <имя_демона1> <имя_демона2> ... <имя_демонаN>
```

Чтобы включить автозапуск всех процессов в Системе, введите:

```
iwtm enable all
```

Чтобы выключить автозапуск всех процессов в Системе, введите:

```
iwtm disable all
```

4.4 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 необходимо установить модуль взаимодействия с удаленной базой данных.

Удаленной считается база данных, установленная на отдельностоящем сервере при помощи ключа установки **TME DB Server** или **TME All-in-one** (подробно о ключах установки см. "InfoWatch Traffic Monitor. Руководство по установке", статья "Установка из дистрибутива TME").

Стандартным процессом передачи данных в базу является **iw_x2db** (см. "Список модулей Traffic Monitor Server"). 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 отдельностоящей базой данных включает следующие задачи:

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

4.4.1 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. документ "Справочник по конфигурационным файлам", статьи "qmover_client.conf" и "qmover_server.conf").

4.4.2 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 (Кбит/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 Кбит/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 Кбит/с.
Максимальная ширина не установлена, но рекомендуемое максимальное значение – 2 Мбит/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 удаляется автоматически); значение по умолчанию - `/opt/iw/tm5/run/.channel_socket`;
- `полоса_пропускания` – ширина полосы пропускания, в кбит/с, которую нужно установить.

Пример
Имеется канал с полосой пропускания 256 кбит/с. Необходимо, 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 величины канала	В пересчете на кбит/с
9.00 до 18.00	50%	128
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
```

4.4.3 Настройка серверной части модуля взаимодействия с удаленной БД

Настройка конфигурации

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

Параметр	Описание
IP (секция `Clients`)	IP-адрес обслуживаемого агента (филиал)
Queue (секция `Clients`)	Директория, в которой хранится очередь объектов, по умолчанию – `queue/db`
Port	Порт, на котором сервер прослушивает объекты, поступающие от агентов

> **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".

4.5 Настройка OCR-экстракторов

Настройка OCR для различных перехватчиков производится в следующих конфигурационных файлах:

- **warpd.conf** – чтобы включить OCR для анализа перехваченных изображений, в секции `Warp` укажите параметру `EnableOCR` значение `true`;
- **sample_compiler.conf** – чтобы включить OCR для анализа изображений, загружаемых в качестве эталонных документов, укажите параметру `EnableOCR` значение `true`.

В файле **/opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml** вы можете настроить OCR для каналов перехвата:

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

Подробнее о настройках см. "Настройка использования OCR"

Примечание.

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

Важно!

Настройка на уровне протокола имеет более высокий приоритет, чем настройка на уровне типа события. Настройка на уровне типа события имеет более высокий приоритет, чем настройка на уровне сервиса.

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.

После того, как вы внесли изменения в файлах, выполните команду:

```
iwtm restart
```

В таблице ниже перечислены каналы перехвата, для которых может использоваться OCR.

Сервис	Тип события	Протокол
Почта	Email	POP3 SMTP IMAP
	Web-почта	HTTP HTTPS
Интернет-активность	Web-сообщение	HTTP HTTPS
Хранение	Краулер	-

При установке с помощью программы-инсталлятора (**kickstart**) на серверную часть Системы устанавливаются оба OCR-экстрактора. По умолчанию на работу настроен ABBYY FineReader Engine 11. Распознавание текста из извлеченных изображений производится с использованием одного из двух OCR-экстракторов: ABBYY FineReader Engine 11 и Tesseract 3.0.
Функциональные ограничения экстракторов приведены в таблице ниже:

Функциональность	ABBYY FineReader Engine 11	Tesseract 3.0
Распознавание углов поворота изображения	0(+/-20) , 90(+/-20), 180(+/-20) и 270(+ /-20) градусов	-

Распознавание цветного изображения	+	-
Коррекция изображения	+	-
Рекомендуемое разрешение изображения	300dpi для текста с размером шрифта от 10pt 400-600dpi для текста с размером шрифта 9pt и меньше	300dpi для текста с размером шрифта от 10pt 400-600dpi для текста с размером шрифта от 9pt и меньше

Примечание:

Чтобы избежать больших отклонений от рекомендуемого разрешения изображения, при работе экстрактора ABBYY FineReader Engine 11 используется параметр `AutoOverwriteResolution` (со значением `true` по умолчанию), позволяющий автоматически определять разрешение изображения.

Чтобы настроить на работу экстрактор ABBYY FineReader Engine 11:

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
   ```

Чтобы заменить используемый экстрактор ABBYY FineReader Engine 11 на Tesseract 3.0:

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
   ```

Чтобы изменить ограничение на размер пересылаемого изображения:

1. Перейдите в директорию **/opt/iw/tm5/etc/image2text_fre.conf** (для FineReader Engine 11) или /**opt/iw/tm5/etc/image2text_ts.conf** (для Tesseract).
2. Отредактируйте параметры `MaxSizeInKb` (верхняя граница) и `MinSizeInKb` (нижняя граница). По умолчанию установлено 1536 КБ и 200 КБ соответственно.

Чтобы включить OCR только для событий облачного хранилища:

1. Откройте справочник `/opt/iw/tm5/etc/config/bookworm/services.xml` и найдите соответсвующие для облачного хранилища `mnemo` и `key`.
   Например,
   ```
   object_type mnemo="cloud_storage"
   key="AA9DFB259F0DFEE040BADC95815E13A200000000"
   ```
2. Скопируйте данные key и `mnemo` и вставьте в `/opt/iw/tm5/etc/config-perm/bookworm/ocr_custom.xml`

Если в качестве OCR-экстрактора используется ABBYY FineReader Engine 11, необходимо настроить лицензию ABBYY. Для этого:

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/ABBYY/SDK/11/Licenses**.
3. Убедитесь, что у пользователя **iwtm** есть права на доступ к скачанному файлу.
4. Перезапустите сервис **iw_warpd**.

4.6 Настройка отправки уведомлений пользователям и сотрудникам

Пользователь Консоли управления имеет возможность настроить отправку уведомлений из Системы пользователю или сотруднику. Чтобы Система имела возможность отправлять уведомления, требуется:

- 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. документ "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>` - email-адрес пользователя, которому будет отправлено уведомление
- `<sample.log>` - текстовый файл, содержимое которого будет служить текстом письма (для проверки рекомендуется использовать простой текстовый файл размером до 1 МБ).

4.7 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.

4.8 Настройка Сервера InfoWatch Device Monitor

В настоящем разделе описана низкоуровневая настройка Сервера InfoWatch Device Monitor. Выполнять описанные ниже действия без помощи инженеров InfoWatch не рекомендуется.

Для корректной работы InfoWatch Device Monitor на компьютерах, на которых установлены его компоненты, должны быть открыты следующие порты:

Порт по умолчанию	Поддерживаемые протоколы	Компоненты InfoWatch Device Monitor		Описание
		Источник	Получатель	
15003	TCP	Консоль	Сервер	Подключение Консоли InfoWatch Device Monitor к Серверу
15004	TCP	Агент	Сервер	Шифрованные соединения с Агентами InfoWatch Device Monitor
15100	UDP	Сервер	Агент	Уведомления Агентов InfoWatch Device Monitor (например, об изменениях схемы безопасности, настроек сервера)
15101	TCP	Агент	Сервер	Отправка Агентам InfoWatch Device Monitor сведений о возможностях Сервера
15505	TCP	Сервер	Агент	Распространение, обновление и удаление Агентов InfoWatch Device Monitor
15506	TCP	Сервер	Агент	Сбор логов, включение и отключение диагностического режима
локальный порт, генерируется динамически	TCP	Агент		Модуль Агента в сессии пользователя, процесс `DM.Client.exe`

Настройка Сервера осуществляется с помощью конфигурационного XML-файла `InfoWatch.DeviceMonitor.Server.exe.config`. Конфигурационный файл размещается в том же каталоге, что и исполняемый файл Сервера `InfoWatch.DeviceMonitor.Server.exe`.

По умолчанию после установки Сервер расположен в каталоге

```
C:\Program Files\InfoWatch\Device Monitor\Server
```

Конфигурационный файл можно просматривать при помощи любого текстового или XML-редактора. Кодировка файла UTF-8.

Корневым элементом конфигурационного файла является элемент `<configuration>`. Корневой элемент включает в себя дочерние элементы (конфигурационные разделы). Структура конфигурационного файла с описанием разделов приведена в следующей таблице. По ссылкам в названиях разделов содержится подробная информация об их настройке.

Важно!

Редактирование конфигурационного файла без помощи инженеров InfoWatch настоятельно не рекомендуется.

По завершении редактирования необходимо перезапустить сервер Device Monitor.

Конфигурационный раздел	Описание
<configSections>	Служебный раздел. Содержит описание всех остальных разделов. Редактирование этого раздела не разрешается.
<runtime>	Содержит настройки для среды выполнения Microsoft .NET Framework. Эти настройки необходимы для корректной работы Сервера. В разделе `<runtime>` определен элемент `gcServer`, предназначенный для настройки сборщика мусора. Элемент имеет атрибут `enabled`, принимающий значение `true` (включен параллельный сбор мусора) или `false` (выключен параллельный сбор мусора). Изменение этого раздела крайне не рекомендуется.
<applicationSettings>	Содержит настройки отдельных модулей Сервера, таких как порты, размеры буферов, таймауты и пр.
<system.diagnostics>	Содержит настройки протоколирования. Протоколирование может быть полезно при диагностике работы компонентов Сервера.

Если в процессе работы потребуется удалить временные файлы, генерируемые Device Monitor, вы можете это сделать с помощью специальной утилиты: подробнее см. "Удаление временных файлов".

4.8.1 Раздел <applicationSettings>

Раздел `<applicationSettings>` предназначен для настройки отдельных модулей Сервера. Всего таких модулей шесть. Все разделы имеют одинаковую структуру: в состав любого из этих разделов входит набор элементов, предназначенных для настройки параметров модуля. Каждый элемент `<setting>` имеет следующие атрибуты:

- `name` — имя настройки.
- `serializeAs` — способ сериализации данных. Данные всегда сериализуются в виде строки (используется тип данных string).

Настройки параметров модуля определяется дочерним элементом `<value>`. Например:

```
<setting name="RemotingPort" serializeAs="String">
<value>15003</value>
</setting>
```

Описание параметров для каждого модуля приводится в следующей таблице.

Параметр	Описание
<InfoWatch.DeviceMonitor.Server.Core.Properties.Settings> Настройки ядра Сервера	
RemotingPort	Порт TCP, обслуживающий подключения Консоли управления. Значение по умолчанию 15003 (крайне не рекомендуется изменять это значение)
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: ▪ ru-RU ▪ en-US
MachineName	IP-адрес сетевого интерфейса, посредством которого Сервер принимает соединения с Консолью управления. Значение по умолчанию 127.0.0.1. Изменять это значение нужно, только если Сервер имеет 2 или более сетевых интерфейсов. В этом случае для корректной работы необходимо явно задать адрес интерфейса, посредством которого сервер принимает входящие соединения от различных экземпляров Консоли управления
CheckServerSettingsInterval	При наличии кластеризации – период (в секундах) синхронизации с базой данных. По истечении этого времени Сервер запрашивает базу данных об изменениях в схеме безопасности, произведенных с помощью основного Сервера, использующего ту же базу данных. Значение по умолчанию 10.
<InfoWatch.DeviceMonitor.Server.Database.Properties.Settings> Настройки модуля, взаимодействующего с базой данных	
DatabaseType	Тип базы данных. Возможные значения: • Oracle • Microsoft • PostgreSql
ConnectionString	Строка соединения с базой данных. Должна соответствовать правилам, установленным для строк соединения ADO.NET. Например: Data Source=isis\s2005;Initial Catalog=g1228_9;Integrated Security=True
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: ▪ ru-RU ▪ en-US

`ConnectionPoolSize`	Количество соединений к БД, которые будут открыты и которые будет использовать сервер в своей работе. Значение по умолчанию `20`.
`CommunicationPort`	Номер порта, используемого при соединении сервера с Агентом распространения при установке Агента через механизм задач. Не рекомендуется менять в процессе работы. Значение по умолчанию `15505`.
`UpdateStatusTimeOut`	Интервал времени, через который необходимо обновлять статус выполнения задачи на удаленном компьютере. С данным интервалом сервер опрашивает удаленные компьютеры, где разворачивается Агент, о статусе установки продукта, для отображения информации на сервере. Значение по умолчанию `60`.
`<InfoWatch.DeviceMonitor.Server.Gui.Properties.Settings>` Настройки модуля, предоставляющего интерфейс для Консоли управления	
`CultureName`	Язык диагностических и других сообщений модуля. Возможные значения: ▪ `ru-RU` ▪ `en-US`
`InitialLeaseTime`	Время (в минутах), в течение которого сеанс соединения с Консолью управления считается действительным
`RenewOnCallTime`	Время (в минутах), на которое продлевается время жизни сеанса соединения Консоли с сервером.
`<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings>` Настройки модуля, обслуживающего клиентские подключения (контролируемые компьютеры)	
`Backlog`	Длина очереди клиентских соединений, ожидающих подключения. Значение по умолчанию `64`.
`CultureName`	Язык диагностических и других сообщений модуля. Возможные значения: • `ru-RU` • `en-US`
`ShadowCopyTempDir`	Полный путь к каталогу, в котором хранятся временные теневые копии, ожидающие отправки в InfoWatch Traffic Monitor. Значение по умолчанию: `C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir`

DmpV1Adress	Список IP-адресов (разделитель в перечислении – «;»), на которых сервер должен прослушивать порты. Возможны следующие значения: • AllAny – порты на всех IP адресах, которые имеются на компьютере (значение по умолчанию); • AllIp4 – порты на всех IP адресах версии 4;
Dmpv1TraceLevel	Уровень трассировки протокола взаимодействия клиента и сервера. Возможны следующие значения: ▪ 1 – выключить трассировку; ▪ 2 – выполнять трассировку только для информации о пакете (значение по умолчанию); ▪ 3 – полная трассировка. **Примечание:** Трассировка будет выведена в приемник диагностических сообщений (по умолчанию Журнал приложений Windows) только в случае значения параметра 3 и уровня протоколирования для фильтра модуля - Verbose (см. " Раздел ").
Dmpv1TraceClients	Список IP-адресов Агентов (разделитель в перечислении – «;»), взаимодействие с которыми необходимо трассировать. При значении All выполняется трассировка для всех Агентов.
Dmpv1ConnectionsLimit	Количество одновременно обрабатываемых соединений по протоколу TCP/IP с клиентами. Значение по умолчанию 200.
Dmpv1ConnectionsQueueLimit	Максимальное количество соединений, ожидающих обработку. Если значение превышено, то соединения "урезаются" до значения, указанного в параметре Dmpv1ConnectionsQueueLengthAfterCut. Значение по умолчанию 500.
Dmpv1ConnectionsQueueLengthAfterCut	Количество соединений после урезания очереди при превышении очередью максимального размера. Значение по умолчанию 250.
TimeoutPeriodSeconds	Величина таймаута, по истечении которого зависшее соединение между Агентом и Сервером будет закрыто, частично созданные теневые копии будут удалены (отправка теневых копий будет повторяться при следующем установленном соединении). Значение по умолчанию 120.
SSLPort	Номер порта для шифрованных соединений. Значение по умолчанию 15004.

<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings> Базовые настройки коннектора Traffic Monitor Server	
DBPollTime	Период (в миллисекундах) опроса базы данных, в процессе которого проверяется наличие событий в базе данных
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: • ru-RU • en-US
NumberOfConnections	Количество соединений с InfoWatch Traffic Monitor. Значение по умолчанию 4. Максимальное значение 32.
QueueSendLimit	Максимальное количество событий, которые могут быть переданы из базы данных в InfoWatch Traffic Monitor за одну транзакцию. Значение по умолчанию 200.
ShadowCopyTrasferBlockSize	Размер блока данных теневой копии, пересылаемой на сервер Traffic Monitor, в МБ. Значение по умолчанию 16.
<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings> Настройки низкоуровневого драйвера базы данных	
CultureName	Язык диагностических и других сообщений модуля. Возможные значения: • ru-RU • en-US
MaxConnectionWaitingTime	Время ожидания свободного соединения из пула в секундах. Значение по умолчанию - 300
CommandTimeoutSeconds	Время выполнения операции или запроса в секундах. Значение по умолчанию - 30. **Примечание:** Данный параметр не работает для СУБД Oracle.

LongCommandTimeoutSeconds	Время выполнения длительной операции или запроса в секундах. Применяется, когда время выполнения составляет значительный промежуток. Значение по умолчанию - 0 (бесконечность). **Примечание:** Данный параметр не работает для СУБД Oracle.

4.8.2 Раздел <system.diagnostics>

Раздел предназначен для диагностики работы Сервера. Включает в себя следующие элементы:

- <trace>. Общие настройки модуля диагностики.
- <sources>. Настройки, необходимые для диагностики отдельных компонентов Сервера.
- <switches>. Управление уровнем детализации диагностической системы в целом. Включает в себя определения детализаторов. Как правило, существует один детализатор. Если для разных модулей требуются разные настройки детализации, то необходимо использовать фильтры. При этом общий детализатор, должен иметь значение, соответствующее максимальной детализации одного из модулей.

Элемент *<trace>*

Используется для описания глобальных настроек модуля диагностики. В данном элементе можно задавать величину отступов в сообщениях, параметры сохранения данных из потока диагностики на жесткий диск.

Элемент *<sources>*

Используется для настройки отдельных модулей приложения. Включает в себя дочерние элементы <source> – по одному на каждый модуль приложения (список модулей Сервера см. "Раздел ").

Также в списке модулей присутствуют вспомогательные, которые необходимы для вывода отладочной информации для основных компонентов:

- InfoWatch.DeviceMonitor.Server.FileIdentification.Core - модуль который описывает объектную модель сигнатур;
- InfoWatch.DeploymentSubSystem - модуль подсистемы отвечающей за развертывание на компьютеры;
- InfoWatch.DeviceMonitor.EventPostProcessorManager - модуль пост-обработки событий печати;
- InfoWatch.DeviceMonitor.ScreenShotStorage - модуль для сохранения скриншотов в файловую систему;
- InfoWatch.DeviceMonitor.Server.Remote.Install - модуль для запуска удаленной установки\обновления\удаления агента на компьютер.

Элемент <source> имеет следующие атрибуты:

- name. Имя модуля сервера.
- switchName. Имя модуля, определяющего детализацию диагностики (детализатора).
- switchType. Тип модуля, определяющего детализацию диагностики. Всегда имеет значение System.Diagnostics.SourceSwitch.

В каждом элементе <source> также содержится определение приемника диагностических сообщений (<listeners>). Приемником диагностических сообщений может быть:

- журнал приложений Windows (Application log);

- системный отладочный вывод (можно просматривать с помощью специальных инструментов, например, DebugView);
- текстовый файл.

Элемент <source> имеет дочерний элемент <listeners>. В данном элементе содержатся параметры приемника диагностических сообщений. Элемент <listeners> может включать в себя следующие дочерние элементы:

- <add>. Добавление нового приемника диагностических сообщений.
- <remove>. Удаление приемника диагностических сообщений. Применяется только для удаления приемника сообщений по умолчанию (таковым является журнал приложений Windows). С этой целью нужно установить имя элемента равным Default:
  <remove name="Default" />

Элемент *<add>*

Данный элемент добавляет приемник диагностических сообщений к модулю Сервера. Элемент содержит следующие атрибуты:

- name. Имя приемника диагностических сообщений.
- type. Тип приемника диагностических сообщений.
- initializeData. Идентификатор модуля Сервера. Как правило, это значение совпадает с именем соответствующего модуля Сервера. Если в качестве приемника используется журнал приложений Windows, то это информация, которая заносится в столбец source.

Тип приемника — это полное имя типа приемника из библиотеки классов .NET Framework или собственного типа, реализующего требуемый интерфейс приемника диагностических сообщений.

В библиотеке классов .NET Framework определены следующие типы приемников диагностических сообщений:

- System.Diagnostics.EventLogTraceListener. Журнал приложений Windows (Application log).
- System.Diagnostics.ConsoleTraceListener. Вывод сообщений в консольном приложении.
- System.Diagnostics.TextWriterTraceListener. Вывод в текстовый файл.
- System.Diagnostics.DefaultTraceListener. Отладочный вывод Windows (по умолчанию включен).

Также элемент <add> содержит фильтр диагностических сообщений. Данный фильтр выводит только те сообщения, которым назначен уровень детализации, превышающий уровень, заданный в настройках фильтра. Определены следующие уровни детализации (приводятся в порядке убывания важности уровня):

- Verbose. Отладочный уровень. В журнале регистрируются все события. Этот уровень нужно применять только для отладки Device Monitor. Не разрешается устанавливать данный уровень, если Device Monitor работает в нормальном режиме, так как это приводит к значительному снижению производительности.
- Information. Информационный уровень. Регистрируются события не связанные с ошибками, такие как, например, информация об изменении параметров Сервера.
- Warning. Уровень предупреждения. Регистрируются некритичные ошибки в работе Device Monitor, такие как неожиданное прекращение соединения с Сервером, истекший таймаут соединения и пр.
- Error. Уровень ошибок. Регистрируются ошибки, мешающие корректной работе Device Monitor (т.е. ошибки, требующие исправления).

- `Critical`. Критический уровень. Регистрируются серьезные нарушения в работе, которые могут привести к неработоспособности Device Monitor.

Пример 1

Для детализатора установлен уровень протоколирования *Verbose*, а для фильтра какого-либо модуля – *Warning*. Тогда детализатор пропускает события с уровнем *Warning*, *Error* и *Critical*, но отфильтровывает события с уровнем *Information* и *Verbose*.

Пример 2

Для детализатора установлен уровень протоколирования *Error*, а для фильтра какого-либо модуля – *Warning*. В этом случае детализатор пропускает события с уровнем *Error* и *Critical*, но отфильтровывает события с уровнем *Warning*, *Information* и *Verbose*. Это происходит потому, что общий уровень детализации - *Error*, т.е. вне зависимости от того, как настроены фильтры, регистрируются только сообщения с уровнем *Error* и выше.

Элемент *<remove>*

Удаление приемника сообщений. Как правило, применяется для удаления приемника по умолчанию, выводящего диагностические сообщения в отладочный вывод Windows:

```
<remove name="Default" />
```

Элемент *<switches>*

Определяет детализаторы Сервера. Как правило, определен только один детализатор, который устанавливает глобальный (для всего Сервера) уровень детализации диагностической системы. Если отдельным модулям Сервера требуется более низкий уровень детализации, то в этом случае можно воспользоваться фильтрами.

По умолчанию элемент `<switches>` содержит только один дочерний элемент:

```
<add name="applicationLogger" value="Information"/>
```

Уровень детализации задается как значение атрибута `value`.

4.8.3 Удаление временных файлов Device Monitor

InfoWatch Device Monitor предоставляет возможность удалять временные файлы, генерируемые Device Monitor, а именно:

- все файлы из директории временных файлов операционной системы (%Temp%);
- данные из файловой очереди обработки событий Device Monitor (по умолчанию - `C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir`; о настройке см. "Раздел ").

Удаление производится с помощью утилиты `RemShadowCopyFiles`, расположенной в папке установки сервера (по умолчанию - `C:\Program Files\InfoWatch\DeviceMonitor\Server`).

Запуск утилиты должен производиться от имени учетной записи администратора, имеющего права на чтение и запись в директориях с удаляемыми файлами.

> **Важно!**
>
> На время выполнения процедуры обработка событий, поступающих в Device Monitor, будет приостановлена.
>
> Данные обо всех событиях, не обработанных на момент начала удаления, будут удалены.

Чтобы удалить временные файлы:

1. Авторизуйтесь на том сервере InfoWatch Device Monitor, где требуется произвести удаление временных файлов.
2. Запустите утилиту `RemShadowCopyFiles`.
3. Подтвердите удаление временных файлов, нажав **Y**.

Утилита выполнит остановку служб Device Monitor, выполнит удаление временных файлов, а затем вновь запустит службы Device Monitor.

> **Важно!**
>
> При удалении временных файлов из системной папки `%Temp%` может возникать отказ в доступе: некоторые файлы могут быть созданы и использоваться другими процессами, не относящимися к Device Monitor.

4.9 Настройка межсервисного взаимодействия (служба Consul)

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

- 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.

Консул устанавливается в режиме **All-in-one**, **TME DB server** и **TME Node server** (Сведения о режимах установки Системы приведены в Руководстве по установке, статья "Установка Системы").

При схеме установки Системы **All-in-one (TME/TMS)** конфигурирование параметров подключения к службе Консул осуществляется автоматически при установке. Исключение составляет распределенная установка, когда Traffic Monitor и База данных установлены на разных серверах с ключами **TME Node server** и **TME DB server** соответственно, когда Система установлена на более, чем одну ноду (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".

4.9.1 Запуск и остановка службы

Для запуска службы Консул используются любая из команд:

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

Для остановки службы Консул используются команды:

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

Ручной запуск агента Консул 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, то нужно указать 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.

4.9.2 Регистрация сервисов в Consul

Сервис можно зарегистрировать в Consul двумя способами:

- использовать HTTP API или конфигурационный файл агента, в случае 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_adlibitum
iw_agent	iw_agent
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
Crawler	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.

4.9.3 Распределенная установка

Важно!

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

Важно!

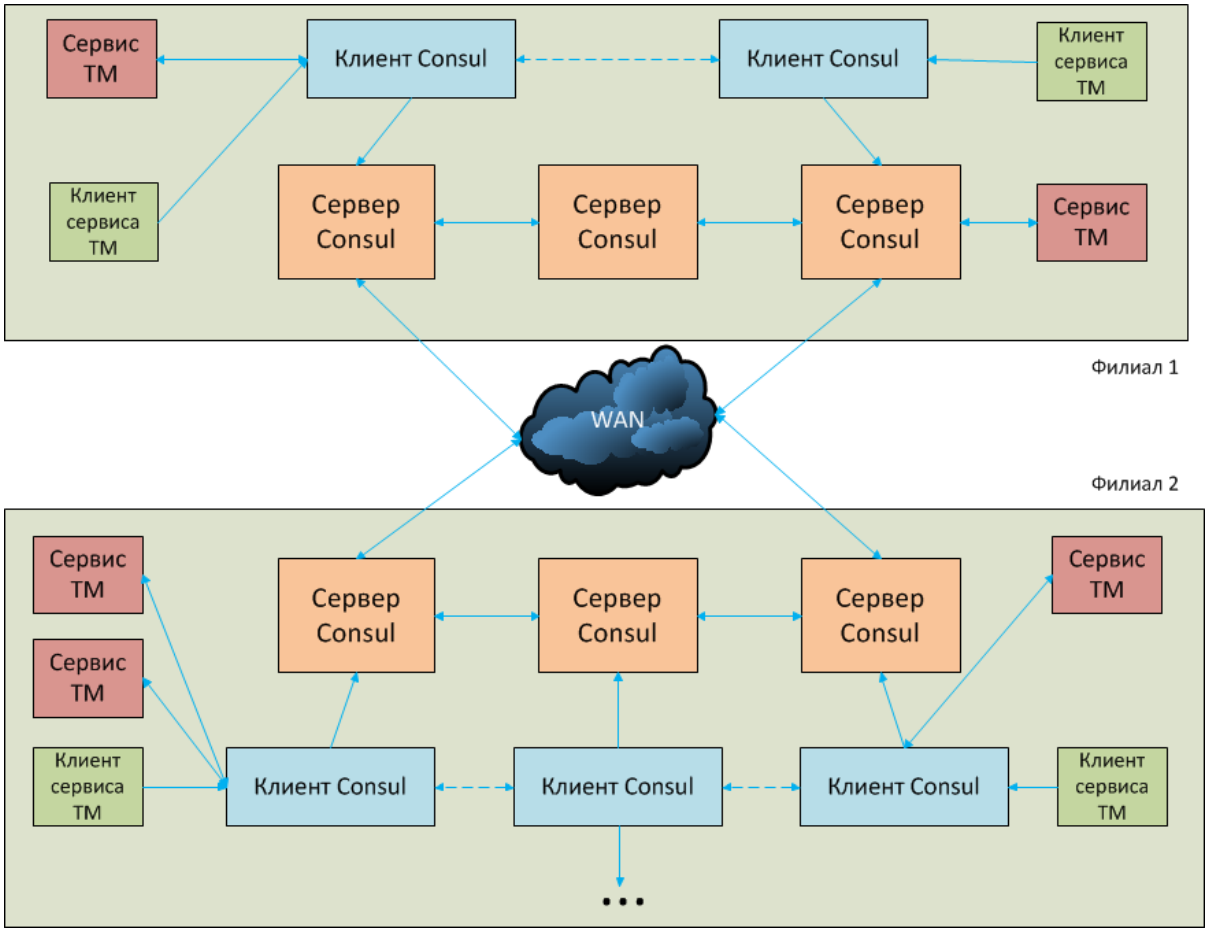
В случае распределенной установки ТМ не должно быть запрета использования TCP и UDP между разными сегментами сети (в том числе нодами) в брендмауэре Windows.

Кластеризация

Агент собирает данные об узле и сервисе и отсылает их серверу. Компоненты системы в поиске сервисов обращаются с запросом к агенту, запущенному на локальной машине, 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 сервера-Лидера, отвечающего 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` рекомендуется 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 рекомендуется, чтобы избежать потери данных, использовать от трех до семи серверов в дата-центре.



> ⚠ **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 конкретной машине
`consul operator raft list-peers -stale=true`	вывод списка всех серверов даже с случае развала кластера

Присоединение к кластеру

Регистрация дополнительных нод на кластере возможна любым из способов:

- Ввести команду: `consul join <ip-адрес>`. При этом нужно убедиться, что у всех серверов и клиентов Consul совпадают параметры `datacenter` и `encrypt` в

конфигурационном файле consul.json (см. Конфигурационный файл consul.json и unit-файл iwtm-consul.service)

- Указать список всех серверов, к которым надо присоединиться в параметре `retry_join` в конфигурационном файле `consul.json`

4.9.4 Настройка сетевых правил доступа в Consul

Для установки сетевого обмена необходимо, чтобы следующие порты между всеми агентами Консул (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

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

Содержимое	Описание
`{`	
`"bootstrap_expect": 1,`	Количество ожидаемых серверов в кластере (только для режима сервера)
`"server": true,`	Запуск агента в режиме сервера (false – 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
`"retry_join": "0.0.0.0",`	В случае распределенной установки содержит список серверов, к которым надо присоединиться
`"ui": 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

Код	Описание
`[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
`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 под пользователем **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 пользователя, указанного в `User`
`ExecReload=/bin/kill -s SIGHUP $MAINPID`	Команда для перезагрузки конфигурации демона, если она доступна. Запускается от 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 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

4.10 Изменение предустановленного пароля в Системе

Для ряда учетных записей в Системе предустановлен стандартный пароль – xxXX1234 (подробнее в статье "Предустановленные серверные параметры"). В процессе эксплуатации Системы его необходимо заменить, следуя требованиям информационной безопасности.

Стандартный пароль изменяется в конфигурационных файлах Системы. Чтобы заменить предустановленный пароль на новый, используйте команду:

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

где `<new_pass>` - новый пароль.

При замене пароля следуйте рекомендациям (подробнее в статье "Приложение А. Рекомендации по составлению имен и паролей").

Стабильная и безопасная работа Системы требует хранить пароли в надежном, недоступном для других месте.

5 Конфигурирование перехватчика Краулер

Подсистема Краулер системы InfoWatch Traffic Monitor позволяет выполнять проверку файлов, находящихся в корпоративной сети, на предмет нарушения корпоративных политик безопасности. Подсистема Краулер работает как один из перехватчиков Traffic Monitor.
В работе Краулера участвуют следующие компоненты системы InfoWatch Traffic Monitor:

- Crawler – программный пакет, обеспечивающий выполнение основных функций. Реализован в виде двух служб Windows:
  - `InfoWatch.Crawler.Scanner` – выполняет сканирование сетевых папок и файловых хранилищ согласно заданным пользователем параметрам;
  - `InfoWatch.Crawler.Server` – управляет службой сканирования и обеспечивает связь с Консолью управления Traffic Monitor;
- База данных – Краулер использует схему БД InfoWatch Traffic Monitor для хранения как объектов, признанных потенциальным нарушением, так и информации о заданиях сканирования.
- Веб-консоль управления InfoWatch Traffic Monitor: Элементы управления Краулер представлены в специальном разделе **Краулер**.

> **Важно!**
>
> Если сервер и сканер Краулер находятся в разных доменах или рабочих группах, необходимо отключить использование шифрованного соединения. Подробнее см. статью "Выключение шифрования трафика между компонентами".

Более подробная информация о настройке Краулер изложена в следующих разделах:

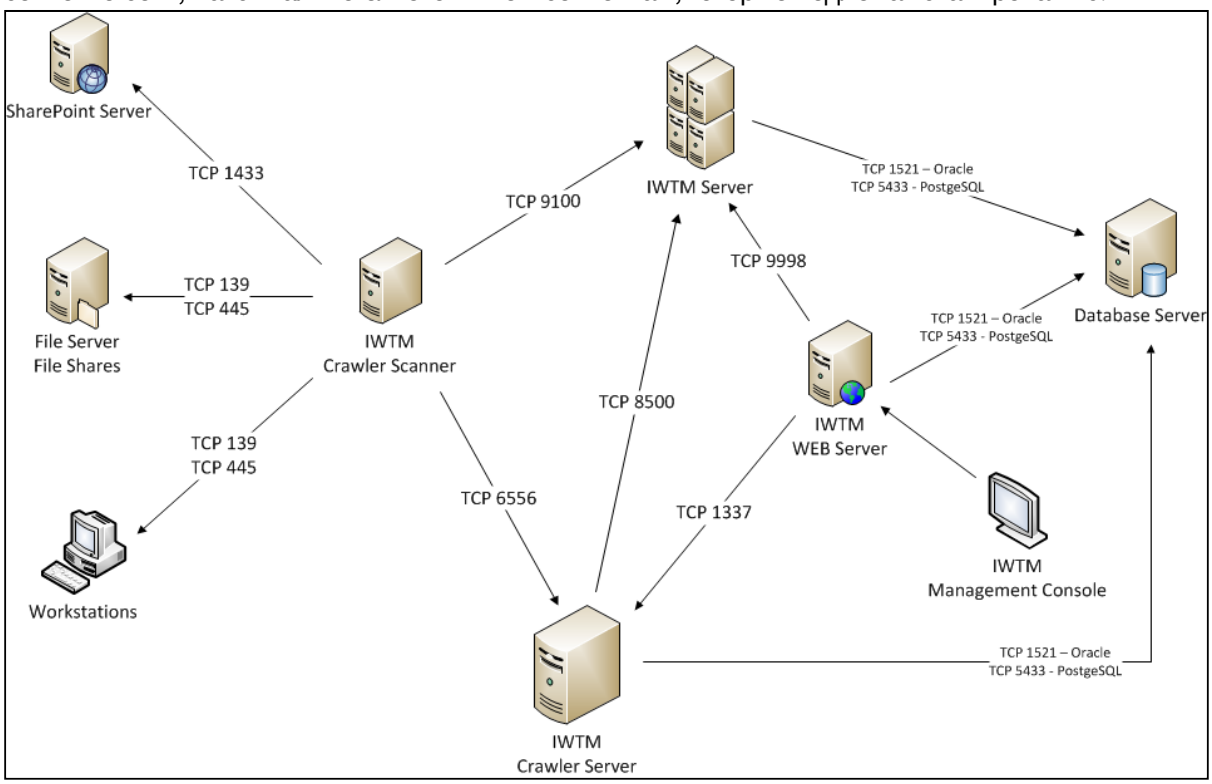
- Настройка сетевых правил доступа;
- Конфигурирование перехватчика Crawler;
- Работа с журналами Краулер;
- Автоматическое удаление событий Краулер.

5.1 Настройка сетевых правил доступа

Если сегменты сети, где развернута система InfoWatch Traffic Monitor с Краулер, разделены между собой межсетевыми экранами, для корректной работы Краулер должны быть открыты TCP порты **6556** (подключение сканера Краулер к серверу Краулер) и **1337** (подключение Веб-сервера InfoWatch Traffic Monitor к серверу Краулер).
Более подробно информацию о сетевых портах, доступность которых необходима для эффективной работы системы, смотрите на следующей схеме и в таблице с пояснениями.

> **Примечание:**
>
> На схеме не указаны порты подключения:
>
> - веб-консоли управления к веб-серверу IWTM;
> - веб-сервера IWTM к серверу IWTM.
>
> Порты не указаны, поскольку при установке с использованием kickstart указанные компоненты Системы устанавливаются на один компьютер.

Если какие-либо компоненты системы принадлежат разным контроллерам доменов, то для работы Краулер в такой системе должно быть настроено доверительное отношение (Domain Trust) этих контроллеров. Однако необходимо учитывать, что удаленность сканера Краулер от сканируемых объектов может существенно увеличить нагрузку на сеть. Поэтому рекомендуется выбирать расположение компьютера, на котором будет работать сканер Краулер, так, чтобы он находился в сегменте сети, максимально близком к тем сегментам, которые подлежат сканированию.



Подключение	Порт
Сканер Краулер – сервер Краулер	TCP 6556
Сервер Краулер – БД IWTM	TCP 5433 - для PostgreSQL
Сервер Краулер – IWTM	TCP 8500
Сканер Краулер – сервер IWTM	TCP 9100
Веб-сервер IWTM – сервер Краулер	TCP 1337
Сканер Краулер – рабочие станции и файловые сервера	TCP 139 TCP 445
Сканер Краулер – файловое хранилище SharePoint (сервер MS SQL)	TCP 1443

Важно!

Если выполняется настройка сети внутри домена, то, кроме отключения межсетевого экрана для домена, требуется отключить брандмауэр также в профиле домена.

Чтобы отключить брандмауэр в профиле домена:

1. В меню **Пуск** выберите **Панель управления -> Брандмауэр Windows**.
2. В левой области открывшегося окна выберите пункт **Дополнительные параметры**.

   Прмиечание:

   Если на экране появится запрос на ввод пароля администратора или его подтверждения, укажите пароль или предоставьте подтверждение.

3. В средней области открывшегося окна **Брандмауэр Windows в режиме повышенной безопасности** выберите пункт **Свойства брандмауэра Windows**.
4. В блоке **Состояние** выберите в выпадающем списке **Состояние брандмауэра** значение **Отключить**.
5. Нажмите **ОК**.

5.2 Конфигурационные файлы Краулер

Администратор, обслуживающий систему, может выполнять некоторые низкоуровневые настройки компонентов Краулер с помощью конфигурационных файлов:

- **Сервер Краулер** – `InfoWatch.Crawler.Server.exe.config`. Расположен в том же каталоге, что и исполняемый файл `InfoWatch.Crawler.Server.exe` (по умолчанию – `C:\Program Files\InfoWatch\Crawler\Server` для 32-битных систем и `C:\Program Files (x86)\InfoWatch\Crawler\Server` для 64-битных). Подробнее см. "Конфигурационный файл сервера Краулер".
- **Сканер Краулер** – `InfoWatch.Crawler.Scanner.exe.config`. Расположен в том же каталоге, что и исполняемый файл `InfoWatch.Crawler.Scanner.exe` (по умолчанию – `C:\Program Files\InfoWatch\Crawler\Scanner` для 32-битных систем и `C:\Program Files (x86)\InfoWatch\Crawler\Scanner` для 64-битных). Подробнее см. "Конфигурационный файл сканера Краулер".

Конфигурационные файлы можно просматривать и редактировать при помощи любого текстового или XML-редактора. Кодировка файлов - UTF-8.

5.2.1 Конфигурационный файл сервера Краулер

Администратор, обслуживающий систему, может выполнить некоторые низкоуровневые настройки сервера Краулер с помощью конфигурационного файла `InfoWatch.Crawler.Server.exe.config`. Конфигурационный файл размещается в том же каталоге, что и исполняемый файл `InfoWatch.Crawler.Server.exe` (по умолчанию - `C:\Program Files\Infowatch\Crawler\Server` для 32-битных систем и `C:\Program Files (x86)\Infowatch\Crawler\Server` для 64-битных).
Конфигурационный файл можно просматривать и редактировать при помощи любого текстового или XML-редактора. Кодировка файла - UTF-8.
Первоначальная настройка параметров выполняется во время установки Краулер (см. документ

"InfoWatch Traffic Monitor. Руководство по установке").
Далее описаны параметры, которые может потребоваться изменять. Изменять остальные параметры настоятельно не рекомендуется.

- **Строка соединения с базой данных**. Если изменились параметры подключения к БД Oracle/Prostgre SQL с используемой схемой IWTM (раздел `<connectionStrings>`, параметр `CrawlerEntities`), внесите соответствующие изменение в значение `connectionString`.
- **Пароль учетной записи владельца схемы IWTM**, от имени которой выполняется подключение к БД. Если пароль изменился, укажите новый пароль в разделе `<appSettings>`:
  `<add key="NewDbPassword" value="новый_пароль" />`

После этого сохраните измененный файл `InfoWatch.Crawler.Server.exe.config` и перезапустите сервис Краулер. В результате новый пароль будет зашифрован и сохранен в качестве значения параметра `DbPassword`. Параметр `NewDbPassword` будет снова обнулен.

> **Примечание:**
>
> Если требуется сменить учетную запись, от имени которой запускается сервер, то перед первым запуском службы сервера необходимо ввести пароль от БД в поле `NewDbPassword`, так как зашифрованный пароль может быть расшифрован только пользователем, зашифровавшим его. Подробнее см. п. "Изменение учетной записи, от имени которой запускается служба сервера Краулер".

- **Номера портов, используемые для подключения сканера и Консоли управления ТМ к серверу Краулер**. Данные параметры указываются в секции `<userSettings>`, параметры `ScannerPort` и `ConsolePort`. Значения указываются следующим образом:
  `<value>номер_порта</value>`

Изменение учетной записи, от имени которой запускается служба сервера Краулер

Чтобы изменить учетную запись, от имени которой запускается служба сервера Crawler:

1. На компьютере, где работает сервер Краулер, в списке служб Windows найдите службу **iw_crawler_server** и остановите ее.
2. В конфигурационном файле сервера `InfoWatch.Crawler.Server.exe.config` (подробнее см. "Конфигурационный файл сервера Краулер"), в параметре `NewDbPassword` введите пароль учетной записи владельца схемы IWTM, от имени которой выполняется подключение к БД. Сохраните изменения в конфигурационном файле.
3. Вернитесь к службе **iw_crawler_server** и вызовите ее **Свойства** (**Действия -> Свойства** или выберите в контекстном меню, открывающемся по нажатию правой кнопки мыши на строке сервиса). На вкладке Вход в систему укажите параметры учетной записи, от имени которой должна запускаться служба сервера Краулер.
4. Запустите службу сервера.

Скрипты сканирования SharePoint

Сканирование SharePoint сетевым сканером происходит путем выполнения SQL-запроса к Базе Данных SharePoint с предустановленными параметрами. В новых версиях сканера скрипты могут быть изменены.

По умолчанию скрипты хранятся в папке `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts`.

Чтобы обновить скрипты:

1. В папке `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts` удалите старые скрипты и замените их на новые.
2. Перезапустите службу **InfoWatch Crawler Server Service**.

> **Примечание:**
>
> Если в процессе эксплуатации в скрипты сканирования были внесены изменения и при последующем обновлении Краулера их необходимо перенести в новую версию:
>
> 1. Сохраните измененные скрипты.
> 2. Произведите обновление Системы.
> 3. В папке `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts` замените скрипты на сохраненные ранее.
> 4. Перезапустите службу **InfoWatch Crawler Server Service**.

5.2.2 Конфигурационный файл сканера Краулер

Конфигурационный файл службы сканирования Crawler `InfoWatch.Crawler.Scanner.exe.config` размещается в том же каталоге, что и исполняемый файл `InfoWatch.Crawler.Scanner.exe` (по умолчанию - `C:\Program Files\Infowatch\Crawler\Scanner\`).
Конфигурационный файл можно просматривать и редактировать при помощи любого текстового или XML-редактора. Кодировка файла UTF-8.

При необходимости администратор Системы может изменить следующие параметры:

Содержимое	Описание
`<client> <endpoint name="ScannerEndpoint" binding="netTcpBinding" bindingConfiguration="EncryptedBinding" address="net.tcp://localhost:6556/Scanner" contract="InfoWatch.Crawler.Contracts.Server.IScannerDispatcher"/> </client>`	Строка соединения с сервером Краулер. Данный параметр указывается в следующем блоке. При изменении расположения сервера Краулер укажите в параметре **address** вместо указанного в примере значения localhost необходимый **IP-адрес** или **имя сервера**.
`<setting name="SendEmptyFileToTm" serializeAs="String"> <value>False</value> </setting>`	Передача файлов в базу данных. Данный параметр указывается в следующем блоке. Если требуется, чтобы Краулер передавал в Traffic Monitor только результаты анализа файлов и не передавал теневые копии файлов, измените параметр `value` на `True`. В этом случае в Traffic Monitor будут передаваться файлы нулевой длины.

<setting name="SyncronizeHashes" serializeAs="String"> <value>False</value> </setting>	Синхронизация локальной базы хешей с базой данных. Данный параметр указывается в следующем блоке. Если требуется, чтобы Краулер синхронизировал хеши с базой данных, измените параметр value на True.
<setting name="ResolveSIDs" serializeAs="String"> <value>True</value> </setting>	Разрешение SID. Данный параметр указывается в следующем блоке. Если требуется отключить разрешение SID, измените параметр value на False. При этом вместо отправителя подставляется имя-заглушка, а получатель не известен.
<setting name="MaxRecipients" serializeAs="String"> <value>0</value> </setting>	Ограничение максимального количества получателей. Данный параметр указывается в следующем блоке. По умолчанию ограничения нет (0 - отключено).
<setting name="UserLimitInExpandedGroup" serializeAs="String"> <value>0</value> </setting>	Ограничение максимального количества получателей при раскрытии группы. При значении 0 группы не раскрываются.
<setting name="LimitRunningTasksNumber" serializeAs="String"> <value>True</value> </setting>	Флаг, который указывает, ограничивать ли число одновременно запускаемых задач Краулера. Если True, то ограничивается, если False - нет.
<setting name="MaxRunningTasksNumber" serializeAs="String"> <value>5</value> </setting>	Максимальное разрешенное количество одновременно запущенных задач. Функционирует, если флаг LimitRunningTasksNumber установлен в True. В случае, если число запущенных задач равно MaxRunningTasksNumber и флаг LimitRunningTasksNumber установлен в True, то новые задачи запускаться не будут.
<setting name="ProcessSymLinkFolders" serializeAs="String"> <value>False</value> </setting>	Обработка папок, являющихся символьными ссылками (симлинками). При включении (true) сканируются пути с симлинком, превышающие максимальную длину пути без симлиинков

Для применения настроек перезапустите сервис сканера в Панель управления -> Администрирование -> Службы.

Изменять остальные параметры настоятельно не рекомендуется.

5.2.3 Выключение шифрования трафика между компонентами

Если сервер и сканер Краулер находятся в разных доменах или рабочих группах, необходимо отключить **использование шифрованного соединения**:

1. Измените значение параметра `bindingConfiguration` в конфигурационном файле серверной части
   Краулер `InfoWatch.Crawler.Server.exe.config` с `EncryptedBinding` на `PlainBinding`:
   ```
   <system.serviceModel>
   <services>
   <service name="InfoWatch.Crawler.Server.ScannerDispatcher"
   behaviorConfiguration="CrawlerServerBehavior">
   <endpoint binding="netTcpBinding" address="net.tcp://0.0.0.0:6556/
   Scanner" bindingConfiguration="PlainBinding"
   contract="InfoWatch.Crawler.Contracts.Server.IScannerDispatchr"/>
   ```
2. Измените значение параметра `bindingConfiguration` в конфигурационном файле сканера
   Краулер `InfoWatch.Crawler.Scanner.exe.config`
   с `EncryptedBinding` на `PlainBinding`:
   ```
   <system.serviceModel>
   <client>
   <endpoint name="ScannerEndpoint"
   binding="netTcpBinding" bindingConfiguration="PlainBinding" address="net.tcp
   ://10.60.3.138:6556/Scanner"
   contract="InfoWatch.Crawler.Contracts.Server.IScannerDispatcher"/>
   ```
3. Перезапустите службы сервера и сканера Краулер.

5.3 Работа с журналами Краулер

Администратор системы может получить информацию о работе сканера и сервера Краулер из файлов журналов, которые расположены в директориях `C:\Program Files\Infowatch\Crawler\Scanner\Logs` и `C:\Program Files \Infowatch\Crawler\Server\Logs` для для 32-битных систем, а также `C:\Program Files (x86)\Infowatch\Crawler\Scanner\Logs` и `C:\Program Files (x86)\Infowatch\Crawler\Server\Logs` для 64-битных систем.

Настройка уровня логирования Краулер
Настройка уровня логирования выполняется в конфигурационных файлах (см. "Конфигурационные файлы Краулер").
Уровень логирования по умолчанию: `Error`. Чтобы изменить уровень логирования:

1. В секции `<specialSources>` для трех параметров `listeners` закомментируйте верхнюю строку и раскомментируйте нижнюю;
2. В параметре `switchValue` задайте нужный уровень логирования. Например, `All`:
   ```
   <allEvents switchValue="All" name="All Events">
           <listeners>
            <!--<add name="Rolling Flat File Trace Listener"/>->
            <add name="Flat File Trace Listener" />
           </listeners>
   ```
   Уровни логирования (перечислено в порядке уменьшения подробности): `All, Verbose, Information, Warning, Error, Critical, Off`.
3. Перезапустите сервис краулера при помощи стандартных средств операционной системы.

5.4 Автоматическое удаление событий Краулер

Система по умолчанию удаляет объекты, на которые не сработала ни одна политика TM или не найден ни один объект защиты. Чтобы сохранять такие объекты, отключите настройку удаления:

1. Подключитесь к серверу TM.
2. В каталоге `/opt/iw/tm5/etc/scripts/` откройте конфигурационный файл **iwssid.lua**.
3. Для отключения автоматического удаления объектов измените значение `set_text ('true')` на `set_text('false')`. Должно получиться так:

```
function IWSSID_HookCrawler(root)
    if root:xFind('/root/processing[count(postanalysis/*|policies/
policy)>0]').count == 0
    then
         -- RM: Не удаляем объекты с ошибками анализа
         if root:xFind('//object/processing/messages/
message[@module="cas"][@severity="fatal" or
@severity="error"]').count == 0 then

processing(root):find_or_add_child('delete_content'):set_text('false
');
         end
    end
end
```

4. Сохраните изменения.
5. Перезапустите службу **iw_luaengined**:

```
iwtm restart luaengined
```

6 Мониторинг

Подсистема мониторинга выполняет следующие функции:

- мониторинг работы всех серверов, входящих в состав решения InfoWatch 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 сравнение значения индикатора 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 системы InfoWatch Traffic Monitor с помощью программы-инсталлятора (**kickstart**). О порядке установки см. документ «InfoWatch Traffic Monitor. Руководство по установке и конфигурированию».

Если система InfoWatch Traffic Monitor установлена так, что все серверные компоненты расположены на одном компьютере (**All-in-one**) или сервер базы данных (**DB server**) установлен отдельно от сервера Traffic Monitor (**Node server**), диагностика серверов будет настроена автоматически.

Если система имеет более двух серверов Traffic Monitor (**Node server**), выполните дополнительные настройки (см. "Ручная настройка индикаторов").

6.1 Настройки подсистемы мониторинга

> **Важно!**
>
> Если система InfoWatch Traffic Monitor установлена так, что все серверные компоненты расположены на одном компьютере (**All-in-one**) или сервер базы данных (**DB server**) установлен отдельно от сервера Traffic Monitor (**Node server**), диагностика серверов будет настроена автоматически.

Настройка подсистемы мониторинга включает следующие задачи:

- Настройка подключения Device Monitor;
- Ручная настройка индикаторов;
- Настройка адреса сервера синхронизации времени для подсистемы мониторинга;
- Настройка порогов срабатывания для индикатора нагрузки;

6.1.1 Настройка подключения Device Monitor

Чтобы настроить мониторинг для сервера Device Monitor:

1. Отредактируйте файл **/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 `/etc/nagios/iwmon/iwmon-services-dm.cfg` раскомментируйте секцию `service`.

- В файле `/etc/nagios/iwmon/iwmon-commands.cfg` раскомментируйте секцию `Check Dm server`.
- Перезапустите процесс nagios:
  ```
  service nagios restart
  ```

6.1.2 Ручная настройка индикаторов

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

- iwmon-services-db-psql.cfg – настройка индикаторов для базы данных Postgre SQL;
- iwmon-services-db.cfg – настройка индикаторов для базы данных Oracle;
- 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;
- iwmon-services-traffic.cfg – настройка индикатора трафика из подсетей.

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:

```
service nagios restart
```

6.1.3 Настройка адреса сервера синхронизации времени для подсистемы мониторинга

Для корректной синхронизации времени, на всех серверах системы необходимо 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 **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).

6.1.4 Настройка порогов срабатывания для индикатора нагрузки

В файле **/etc/nagios/iwmon/iwmon-services-loadavg.cfg** для индикатора (службы) `Current Load`, который проверяет значения для load average на сервере Traffic Monitor, уточните пороговые значения срабатывания, в зависимости от количества ядер на сервере Traffic Monitor.
Например, для 4-х ядерного процессора пороговые значения должны быть определены следующим образом:
`iwmon_check_load!10.0,8.0,6.0!20.0,16.0,12.0`
Пороговые значения для другого количества ядер вычисляются пропорционально.

7 Администрирование базы данных

Этот раздел содержит информацию по администрированию:

- PostgreSQL.

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

7.1 PostgreSQL

Чтобы подключиться к серверу БД из терминала сервера Traffic Monitor, используйте следующие 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

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

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

Раздел содержит инструкции по администрированию PostgreSQL:

- Проведение регламентных работ на сервере базы данных;
- Табличные пространства в базе данных InfoWatch Traffic Monitor;
- Управление ежедневными табличными пространствами;
- Резервное копирование базы данных.

7.1.1 Проведение регламентных работ на сервере базы данных

> **Важно!**
>
> Категорически не рекомендуется выключать сервер БД кнопкой питания. В некоторых случаях это может привести к повреждению БД.

При выполнении регламентных работ на сервере базы данных 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 TM:
   ```
   iwtm stop
   service iwtm-php-fpm stop
   service nginx stop
   ```
3. На сервере базы данных получите список заданий, запускающихся по расписанию. Для этого в psql, из-под учетной записи 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 осуществить посредством остановки агента из Linux с помощью команды:
`service pgagent-9.6 stop` (остановка всех задач при помощи единой команды)
6. Выполните необходимые работы с базой данных.
7. По окончании необходимых работ с сервера Traffic Monitor проверьте соединение с сервером базы данных:
```
psql -p 5433 -h server_name postgres postgres
```
где `server_name` - имя или ip адрес базы данных
Если проверка пройдена успешно, тогда в ответ на выполнение команды будет выведено следующее приглашение psql:
```
postgre=#
```
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.

7.1.2 Табличные пространства в базе данных InfoWatch Traffic Monitor

В базе данных InfoWatch Traffic Monitor Enterprise имеются два типа табличных пространств (ТП):

Тип табличного пространства	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 др.)

Ежедневное	Хранение объектов, перехваченных в течение одних суток. Хранение информации о результатах анализа и обработки объектов (разобранный объект, категории, термины и др.). Состоит из трех табличных пространств: для хранения объектов со статусами *Нарушение*, *Нет нарушений, Остальное (пространство для хранения снимков экрана)*. Таким образом, достигается возможность раздельного архивирования, восстановления и удаления.

Все данные об объектах, перехваченных в определенный день, находятся в одном ежедневном ТП. Ежедневные ТП создаются каждые сутки с таким расчетом, чтобы в базе данных всегда были ТП для работы в ближайшие шесть суток, не включая текущие. Всем ежедневным ТП автоматически присваивается имя *<Schema Owner>_X*. Здесь

- *Schema Owner* – владелец схемы базы данных.
- *X* – номер ТП (tbs_id из таблицы tbs_list).

Параметры, предназначенные для управления сегментами данных, задаются при настройке схемы базы данных, но могут быть переопределены после создания схемы (см. "Управление ежедневными табличными пространствами").
При использовании типа установки **TM Standard**, события хранятся в едином табличном пространстве. Автоматический расчет свободного места для будущих событий с освобождением пространства происходит еженедельно.

7.1.3 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.

Архивирование ежедневных табличных пространств

Чтобы освободить пространство на жестком диске, Вы можете периодически архивировать устаревшие данные. Архив с данными рекомендуется размещать на внешних носителях информации. При необходимости эти данные могут быть восстановлены.

> **Важно!**
>
> Если в качестве интервала времени используются месяцы или годы, то рекомендуется в расчете использовать максимальное значение интервала. Для месяца – 31 день. Для года – 366 дней. Например, чтобы архивировать ежедневные ТП старше 4-х лет, в задании *<SchemaOwner>*_iwtm_archive_tablespaces укажите интервал 366*4=1464 дня.

Архивирование может выполняться:

- Автоматически после истечения указанного периода (см. "Автоматическое архивирование ежедневных табличных пространств");
- Вручную – для архивирования выбранного ЕТП (см. "Архивирование ежедневных табличных пространств вручную").

Автоматическое архивирование ежедневных табличных пространств

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

```
select value

from setting

where setting = 'archive_path';
```

Пользователь `postgre` должен являться владельцем каталога.

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

```
begin;

select sp_setting_set('archive_path', '/test/archive/');

commit;
```

Для автоматического архивирования табличных пространств (по умолчанию функция выключена) Вы можете использовать следующие сценарии (запускаются от имени владельца схемы данных):

- Для ежедневного табличного пространства, хранящего объекты со статусом *Нарушение*:
  ```
  begin;
  select sp_setting_set('violation_archive_enabled', '1');
  select sp_setting_set('violation_archive_period', 'D');
  commit;
  ```
  1 – показатель того, что автоматическое архивирование включено (чтобы выключить, вместо 1 используйте значение 0);
  D – количество дней, по истечении которого ежедневное табличное пространство будет архивироваться Системой.
- Для ежедневного табличного пространства, хранящего объекты со статусом *Нет нарушений*:
  ```
  begin;
  select sp_setting_set('noviolation_archive_enabled', '1');
  select sp_setting_set('noviolation_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 ежедневное табличное пространство будет архивироваться Системой.
- Для ежедневного табличного пространства, 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 ежедневное табличное пространство будет архивироваться Системой.

Архивирование ежедневных табличных пространств вручную

Архивирование ЕТП вручную производится в порядке, представленном ниже.

Выборка ежедневных табличных пространств и файлов данных

Список отключаемых табличных пространств 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 ежедневных ТП 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 рекомендуется для получения списка файлов использовать запрос, пример которого описывается далее в этом разделе. Это связано с тем, что список файлов данных, полученный другими способами, может оказаться неполным.

Отключение ежедневных табличных пространств от базы данных

Важно!

Не отключайте ежедневные ТП во время работы заданий *<SchemaOwner>*_iwtm_add_parts, *<SchemaOwner>*_iwtm_delete_tablespaces, *<SchemaOwner>*_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 ежедневного ТП изменится на *Отключено от базы данных*.
2. Повторите вызов процедуры для каждого ежедневного ТП, которое нужно отключить.

Перенос файлов данных

Перенесите каталоги с заархивированными табличными пространствами, принадлежащие отключенным ежедневным ТП, на другой носитель информации.

Для получения списка отключенных табличных пространств 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 можно восстанавливать только в той схеме базы данных, в которой оно было отключено (даже если эта схема была обновлена). Восстановить табличное пространство после полной переустановки схемы базы данных невозможно.

Перемещение файлов данных

Для восстановления ежедневного ТП необходимо переместить файлы данных этого табличного пространства с внешнего носителя в каталог, путь к которому можно получить, выполнив запрос:

```
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 ежедневного табличного пространства

> **Важно!**
>
> Не подключайте ежедневное ТП во время работы заданий *<SchemaOwner>*_iwtm_add_parts, *<SchemaOwner>*_iwtm_delete_tablespaces и *<SchemaOwner>*_iwtm_archive_tablespaces. Это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:
   `select pkg_part_restore_tablespace(N);`
   где `N` – ID табличного пространства (указывается в tbs_list).
   После выполнения процедуры статус ежедневного ТП изменится на *Восстановлено*.
2. Повторите вызов процедуры для каждого ежедневного ТП, которое нужно подключить.

Настройка размещения файлов в файловой системе

Ежедневные табличные пространства могут храниться либо в одном каталоге, либо распределенно, в разных каталогах на разных дисках.

При установке Системы с помощью поставляемого инсталлятора (kickstart: см. документ "InfoWatch Traffic Monitor. Руководство по установке ") задается использование одной директории ежедневных табличных пространств, расположенной в `/u02/pgdata1/`.

> **Примечание.**
>
> Для архивирования табличных пространств используется директория `/u02/arch`.

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

Первый день – ежедневное табличное пространство создается в файловой системе 1.
Второй день – ежедневное табличное пространство создается в файловой системе 2.
Третий день – ежедневное табличное пространство создается в файловой системе 3.
Четвертый день – ежедневное табличное пространство создается в файловой системе 1.
…

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

Пример сценария, изменяющего количество отдельных мест хранения ежедневных ТП:

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

> **Важно!**
>
> Изменив количество мест хранения ежедневных ТП, обязательно откорректируйте (добавьте/удалите) пути их расположения.

Пример сценария, изменяющего пути для расположения ежедневных ТП:

```
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:

Рекомендуется при указании пути в конце указывать символ «/».

Пример сценария просмотра содержимого ежедневных ТП:

```
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 табличных пространствах вместе со служебной информацией БД, рекомендуется использовать pgAdmin.

Настройка режимов хранения файлов табличного пространства

Если во время установки Система была настроена на режим переноса данных **Normal** (обычный), в процессе эксплуатации режим хранения может быть изменен.

Для того, чтобы настроить режим хранения **Fast/slow** (быстрые и медленные диски), при котором свежие данные сохраняются в быстром разделе и через указанное количество дней перемещаются на медленные разделы, необходимо выполнить следующие действия:

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 базу данных:
   `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:
   `select pkg_part_set_fast_days(7);`
6. Укажите путь к быстрому диску
   `select pkg_part_set_fast_path('/u02/pgdata/',1);`
7. Укажите путь к медленному диску:
   `select pkg_part_set_df_path('/u03/pgdata/',1);`
8. Укажите второй путь к медленному диску:
   `select pkg_part_set_df_path('/u04/pgdata/',2);`
9. Поменяйте режим на медленные-быстрые диски:
   `select pkg_part_set_filesys_type('fast/slow');`
10. Запустите перенос файлов:
    `select iwtm.pkg_part_move_fast_tablespaces_to_slow();`

Для того, чтобы настроить режим хранения **Rotate** (ежедневное переключение), при котором переход к следующему разделу происходит ежедневно и при переполнении предыдущего, необходимо выполнить следующие действия:

1. Монтируйте раздел и убедитесь, что он способен монтироваться автоматически при перезагрузке
2. Создайте папку "pgdata":
   `mkdir /u03/pgdata`
3. Смените пользователя:
   `chown -R postgres:postgres /u03`
4. Зайдите в базу данных:
   `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:

Особенности режимов хранения данных (**normal**, **fast/slow** и **rotate**) описаны в статье базы знаний "Настройка режима хранения данных в ТП. Хранение данных на разных дисках".

Удаление ежедневных табличных пространств

Если дальнейшее хранение данных не требуется, то Вы можете воспользоваться процедурой удаления ежедневных ТП (<*SchemaOwner*>_iwtm_delete_tablespaces). Данная процедура позволяет автоматически удалить все данные, хранящиеся в табличном пространстве, сегменты, табличное пространство и файлы данных.

Важно!

1. Удаление табличных пространств – необратимая операция. После выполнения этой операции Вы не сможете восстановить удаленные данные.
2. После удаления табличных пространств, которые отключены от базы данных (имеют статус *Offline*), остаются файлы данных. Чтобы освободить пространство на жестком диске, удалите эти файлы вручную.
3. Процедура <*SchemaOwner*>_iwtm_delete_tablespaces не работает с теми табличными пространствами, которые были отключены/подключены вручную.

В результате выполнения этой процедуры удаляются все ежедневные ТП (и в т.ч. информация о заархивированных ежедневных ТП), которые удовлетворяют следующему условию:

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

Примечание:

Если заархивированное ежедневное ТП не подлежит восстановлению (т.к. информация о нем была удалена из базы данных), то Вы можете удалить файлы данных этого ежедневного ТП из архива.

На время удаления табличных пространств работа процессов **iw_deliverd**, **iw_x2db**, **iw_updater** будет автоматически приостановлена. По завершении процедуры удаления, выполняется автоматический перезапуск процессов. Рекомендуется запускать задание на удаление данных ежедневно. В противном случае количество удаляемых данных увеличится, что приведет к большим временным затратам на выполнение данной процедуры и, как следствие, к увеличению времени простоя сервера Traffic Monitor.

Важно!

Если в качестве интервала времени используются месяцы или годы, то рекомендуется в расчете использовать максимальное значение интервала. Для месяца – 31 день. Для года – 366 дней. Например, чтобы удалять ежедневные ТП старше 4-х лет, в задании <*SchemaOwner*>_iwtm_delete_tablespaces укажите интервал 366*4=1464 дня.

Определение интервала времени для удаления ежедневных ТП
Для автоматического удаления табличных пространств (по умолчанию функция выключена) вы можете использовать следующие сценарии (запускаются от имени владельца схемы данных):

- Для ЕТП, хранящего объекты со статусом *Нарушение*:
```
begin;
select sp_setting_set('violation_delete_enabled', '1');
select sp_setting_set('violation_delete_period', 'D');
commit;
```
где:
`1` – показатель того, что автоматическое удаление включено (чтобы выключить, вместо `1` используйте значение `0`);
`D` – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

- Для ЕТП, хранящего объекты со статусом *Нет нарушений*:
```
begin;
select sp_setting_set('noviolation_delete_enabled', '1');
select sp_setting_set('noviolation_delete_period', 'D');
commit;
```
где:
`1` – показатель того, что автоматическое удаление включено (чтобы выключить, вместо `1` используйте значение `0`);
`D` – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

- Для ЕТП, хранящего *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` используйте значение `0`);
`D` – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

Ручной запуск процедуры
Если вам требуется немедленный запуск процедуры удаления ежедневных ТП (например, из-за нехватки места в файловой системе был изменен интервал удаления, но следующий запуск задания произойдет нескоро), от имени владельца схемы базы данных выполните следующий сценарий:

```
select pkg_part_delete_tablespaces();
```

Выполнение процедуры с помощью скрипта

Если вам требуется настроить автоматическое удаления ежедневных ТП, то имеет смысл использовать скрипт **/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh.** Возможны 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]`

Пример.

Задача: удалить все объекты со статусом *"Нет нарушения"*, старше 15 суток.

Решение:

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

7.1.4 Резервное копирование базы данных

Для снижения рисков потери данных рекомендуется ежемесячно выполнять создание резервной копии (бэкапа) базы данных. 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, рекомендуется описанная ниже процедура «холодного бэкапа», выполняемая на остановленной БД. Данная процедура также может применяться для переноса базы данных с одного сервера на другой.

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 Postgre SQL;
- Копирование файлов БД в хранилище резервных копий.

Определение размера резервной копии

Чтобы рассчитать размер будущего архива, необходимо узнать суммарный размер каталога с базой Postgre, каталога основного табличного пространства и ежедневных табличных пространств:

1. Войдите в систему от имени пользователя **root**;

2. Получите суммарный размер каталогов:
   `du -sx -BM /u01/postgres/ /u02/pgdata /u02/arch`

Проверка хранилища резервной копии

Для проверки приемлемости выбранного хранилища резервной копии:

1. Примонтируйте внешнее хранилище к серверу БД. Оно должно соответствовать следующим требованиям:
   - Размещаться на компьютере, отличном от того, где работает база данных.
   - Быть доступно с компьютеров, где работают сервера и базы данных, 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 примонтированном разделе больше, чем размер резервной копии.

Создание каталогов для резервной копии

> **Внимание!**
>
> Директории файлов резервной копии должны находиться на компьютере, отличном от того, где расположена БД.

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/arch
   ```

Остановка системы

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

Чтобы остановить систему:

1. На компьютере, где запущены процессы серверной части Trafic 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 Postgre SQL

> **Важно!**
>
> Перед началом резервного копирования файлов базы данных обязательно нужно остановить БД Postgre SQL.

Чтобы остановить Postgre SQL БД:

1. На компьютере, где работает база данных, зайдите в систему от имени пользователя **root**.
2. В командной строке введите:
   ```
   service pgagent-9.6 stop
   service postgresql-9.6 stop
   ```
   По окончании процедуры резервного копирования сервисы можно запустить с помощью следующей команды:
   ```
   service pgagent-9.6 start
   service postgresql-9.6 start
   ```

Копирование файлов БД в хранилище резервных копий

1. Остановите все сервисы Postgre SQL (см. "Остановка Postgre SQL"). Чтобы убедиться в этом, выполните команду:
   ```
   ps aux | grep postgre
   ```
   Если сервисы Postgre SQL не остановлены, файлы резервной копии могут быть повреждены и оказаться непригодными для восстановления.
2. На компьютере, где установлена БД, скопируйте директории (со всем содержимым) с помощью ранее созданного списка директорий.
   Если система была установлена с помощью программы-инсталлятора (kickstart) 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**

   > **Примечание:**
   >
   > В качестве хранилища файлов необходимо использовать только:
   > - внешний диск с файловыми системами Ext4, XFS;
   > - удаленное блочное устройство, подключенное по протоколам iSCSI, NFS;

- локально подключенное блочное устройство с файловыми системами Ext4, XFS.

Восстановление базы данных из резервной копии

С учетом причины падения вашей базы данных, выберите подходящую процедуру восстановления БД:

- 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").

Восстановление на той же базе данных

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

Чтобы восстановить базу данных с помощью создания новой базы данных:

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 Postgre SQL:
   ```
   service postgresql-9.6 stop
   service pgagent-9.6 stop
   ```
3. Установите БД Postgre SQL согласно инструкции, приведенной в документе «InfoWatch Traffic Monitor. Руководство по установке».
4. 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/**
5. Проверьте права. При необходимости, измените их:
   ```
   chown postgres /u01/postgres/ –R
   chown postgres /u02/pgdata/ –R
   chown postgres /u02/pgdata1/ –R
   chown postgres /u02/arch/ –R
   ```

6. Запустите базу данных:
   ```
   service postgresql-9.6 start
   service pgagent-9.6 start
   ```

Восстановление на новой базе данных

При восстановлении PostgreSQL, необходимо копировать файлы БД в те же каталоги, в которых они были сохранены.

Чтобы восстановить БД, скопируйте каталоги, проверьте права и запустите сервисы БД (см. "Восстановление на той же базе данных").

8 Администрирование серверной части InfoWatch Traffic Monitor

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

- Процессы серверной части Traffic Monitor Server;
- Настройка конфигурационных файлов серверной части Traffic Monitor;
- Настройка параметров обработки архивов вложений;
- Архивирование каталога очереди сообщений;
- Логирование работы Системы;
- Файловые очереди;
- Восстановление работоспособности системы в аварийных ситуациях.
- Настройка передачи информации в SIEM
- Удаление временных файлов

8.1 Процессы серверной части Traffic Monitor Server

В этом разделе:

- Список процессов серверной части Traffic Monitor;
- Работа с процессами серверной части Traffic Monitor.

8.1.1 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_buf	Процесс собирает полный файл из пакетов исходного файла, полученного с proxy-серверов для загрузки во внешнее файловое хранилище, и отправляет на **iw_icap**	/opt/iw/tm5/etc/icap_buf.conf
	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/запрещением на доставку HTTP-запроса. Также передает HTTP-запрос процессу **iw_x2db** для сохранения в базу данных	/opt/iw/tm5/etc/icap.conf

iw_sniffer	Процесс, перехватывающий трафик, который передается по протоколам SMTP, HTTP, ICQ, POP3, IMAP, NRPC	/opt/iw/tm5/etc/sniffer.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 и принятия решения. По окончании анализа копия объекта передается процессу **iw_x2db** для укладки в базу данных	/opt/iw/tm5/etc/proxy.conf
iw_smtpd	Процесс, принимающий SMTP-письма. В случае интеграции с почтовым сервером Postfix принимает входящие сообщения от Postfix. Если интеграция с Postfix отсутствует, 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	Процесс обработки SMTP-писем. 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 интеграция с Postfix отсутствует, то, в зависимости от настроек вашей почтовой системы, таким компонентом может быть корпоративный почтовый сервер или почтовый клиент. Кроме того, копия проверенного SMTP-письма передается процессу **iw_x2db** для сохранения в базу данных	/opt/iw/tm5/etc/messed.conf
	iw_xapi	Включает в себя две службы: **iw_xapi_xapi** и **iw_xapi_puppy**. Получает объекты от Infowatch Device Monitor, Crawler и внешних систем (через адаптеры) по thrift-интерфейсу, складывает 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	Забирает объекты из файловой очереди, в которую их кладет **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 складываются в файловую очередь для отправки в базу данных процессом **iw_x2db**	/opt/iw/tm5/etc/analysis.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 ABBYY FineReader.	/opt/iw/tm5/etc/image2text_fre.conf
	iw_image2text_ts	Осуществляет распознавание текста в 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	Процесс, обеспечивающий выполнение LUA-скрипта согласно действующей политике. Отправляет	/opt/iw/tm5/etc/luaengined.conf
iw_x2x	Процесс получает данные с xml+dat-файлами посредством файловой очереди. Полученные файлы модифицируются и отправляется процессу **iw_x2db**	/opt/iw/tm5/etc/x2x.conf

	iw_tech_tools	Процесс верифицирует условия для выгрузок из БД и регулярные выражения, позволяет нормализовать текст в соответствии с регулярными выражениями	/opt/iw/tm5/etc/tech_tools.conf
Загрузка в БД	iw_qmover_client	Работает на Traffic Monitor Server, установленном в филиале. Отправляет перехваченные объекты в базу данных центрального офиса	/opt/iw/tm5/etc/qmover_client.conf
	iw_qmover_server	Работает на Traffic Monitor Server, установленном в центральном офисе. Принимает объекты, полученные от Агента, установленного в филиале. Передает через **iw_x2x** объекты процессу **iw_x2db** для сохранения в базу данных	/opt/iw/tm5/etc/qmover_server.conf
	iw_x2db	Процесс, загружающий 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	/opt/iw/tm5/etc/adlibitum.conf
	iw_agent	Требуется для управления конфигурацией Системы	/opt/iw/tm5/etc/agent.conf

iw_blackboard	Осуществляет взаимодействие применяемых политик и базы данных	/opt/iw/tm5/etc/blackboard.conf
iw_bookworm	Выполняет роль справочника в Системе	/opt/iw/tm5/etc/bookworm.conf
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_crawler	Процесс для подсистемы Crawler (сама подсистема работает на сервере, отличном от Traffic Monitor Server)	/opt/iw/tm5/etc/web.conf
iw_deliver	Выполняет доставку писем. Отправляет SMTP-письма получателям в случае, если доставка письма разрешена из Management Console (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_indexer	Служит для индексации текста объектов из БД. Получает доступ к базе данных для ее индексации и складывает индексы в файловое хранилище. При выполнении поискового запроса **sphinx** получает из файлового хранилища индексов id объектов	/opt/iw/tm5/etc/indexer.conf
iw_metainfo_fetcher	Осуществляет выборку данных для индексации из БД. Передает данные на индексацию процессу **iw_is.**	-
iw_is	Получает данные для индексации от **iw_metainfo_fetcher** через файловую очередь. Проводит индексацию полученных данных. Отправляет проиндексированные данные в файловое хранилище **sphinx**	/opt/iw/tm5/etc/is.conf
iw_kicker	Служит для корректной работы WebGUI, осуществляет запуск сервисов: agent, blackboard, crawler, 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
iw_rammer	Выполняет досылку писем с ошибками обработки при работе "в разрыв"	/opt/iw/tm5/etc/rammer.conf

iw_sample_compiler	Процесс, создающий цифровые отпечатки из загруженных эталонных файлов	/opt/iw/tm5/etc/sample_compiler.conf
consul	Производит обнаружение, регистрацию и мониторинг доступности сервисов, взаимодействующих с интерфейсом пользователя	/opt/iw/tm5/etc/consul/consul.json
iw_system_check	Процесс, занимающийся сбором данных от службы Nagios и предоставляющий полученные данные для выведения в Консоли управления	/opt/iw/tm5/etc/system_check.conf
iw_updater	Процесс, загружающий конфигурацию из базы данных на Traffic Monitor Server	/opt/iw/tm5/etc/updater.conf

Внимание!

В данной версии ТМ перехват для Astra Linux осуществляется на стороне DM и перехватчиком **iw_smtpd** на стороне ТМ. Поэтому следующие сервисы ТМ должны быть установлены, но отключены по умолчанию до принудительного запуска:

- iw_icap_buf
- iw_icap
- iw_sniffer
- iw_proxy
- iw_capstack

8.1.2 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:**
>
> 1. Для перехвата копии трафика через Sniffer (ICQ- HTTP-, SMTP-трафик) запускаются отдельные процессы **iw_proxy**.
> 2. 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**).
> 3. Процесс **iw_rammer** не установлен по умолчанию. После ручной установки он становится доступен в списке процессов.

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+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`
`systemctl start iw_cas` (без возможности просмотра логов)
`systemctl start iw_cas.service`
	Запустить сервер контентного анализа (CAS)

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".

8.2 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

"*Справочник по конфигурационным файлам*". Файлы, не описанные в данном документе, изменять не рекомендуется.

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 (см. документ "*Справочник по конфигурационным файлам*", статьи: *"Общая секция Bookworm", "Общая секция Discovery", "Общая секция Logging", "Общая секция Statistics", "Общая секция Statistic", "Общая секция ThriftServers"*) и параметры, специфичные для каждого из конфигурационных файлов (см. описание отдельных файлов в документе "*Справочник по конфигурационным файлам*").

8.3 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.

В первом случае извлечением данных из контейнеров, вложенных в перехваченные объекты, занимается процесс **iw_warpd**. Во втором случае процесс **iw_sample_compiler** создает цифровые отпечатки из загруженных эталонных файлов. Включение и настройка технологии OCR осуществляется в их конфигурационных файлах. Подробнее см.Настройка OCR-экстракторов

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

Настройка перехвата на уровне:	**Настройка применяется к содержимому событий,**	**Приоритет выполнения настройки**
Сервиса	Полученных по протоколам типов событий этого сервиса (если для данных типов событий или протоколов не задана своя настройка OCR)	Низкий
Типа события для конкретного сервиса	Полученных по протоколам этого типа события (если для этих протоколов не задана своя настройка OCR)	Средний
Протокола для конкретного типа события	Полученных 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.

Для включения использования технологии OCR при внедрении необходимо 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.

> **Примечание:**
>
> 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`.

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"`).

При необходимости настройки OCR для нескольких нод (распределенная установка) необходимо 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 .

> **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.

8.3.1 Конфигурационный файл ocr_custom.xml

Примеры правил OCR в выключенном состоянии представлены ниже, где:

- `object_type` – тип события;
- `service` – сервисы;
- `protocol` – протоколы;
- `key` - ключи;
- `mnemo` – идентификаторы объектов справочника типов событий, сервисов и протоколов.

При включении правил имеет смысл указывать не все, а только необходимые из них:

```
<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="62E7C68AD1354D118282FAFF07DA59ED00000000" mnemo="multimedia" ocr_enabled="false">
    <object_type key="55E10E81F5C94B3FB742CB61CA9476F800000000" mnemo="multimedia_photo"
 ocr_enabled="false"/>
  </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>
```

Примечание:

Для включения OCR на всех уровнях сразу (на уровне сервиса, типа события и на уровне протокола) необходимо в нижней строке файла `ocr_custom.xml` заменить `<ocr_options node="*" ocr_enabled="false">` на `<ocr_options node="*" ocr_enabled="true">`

8.4 Настройка параметров обработки архивов вложений

Обработка вложений настраивается в двух конфигурационных файлах:

- файл `/opt/iw/tm5/etc/extractors.conf` (см. документ "*Справочник по конфигурационным файлам*", статья "extractors.conf");
- файл `/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml` (см. "Конфигурационный файл extractors.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.

8.4.1 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`
`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 Кб/с, в расчете на 1 ГГц частоты процессора. Значение по умолчанию – `100`
`TimeoutInSec`	Время ожидания (в секундах) до завершения обработки файла. Значение по умолчанию – `1800`
`UseLog`	Логирование экстрактора. Значение по умолчанию – `false`

Если общие значения параметров `TimeoutInSec` и `MinFileSizeInBytes` не подходят для каких-либо типов файлов, включите эти параметры в секции для нужных типов файлов с другими значениями.

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, необходим 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 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.
	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. Например, указание используемой версии архиватора: `Comment = "bzip2 v. 1.0.x"`
Command	Строка команды для извлечения файлов. Например, `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 (`On`), 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 отключен (`Off`)
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. При значении `true` - файлы. При значении `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`	Нужно ли файлы с указанным mime-типом отправлять на анализ.

8.5 Архивирование каталога очереди сообщений

При ошибках в очереди входящих SMTP-писем заархивируйте каталог очереди SMTP-писем и сохраните его для последующего анализа. Затем удалите каталог. Местоположение каталога очереди сообщений указано в конфигурационном файле **/opt/iw/tm5/etc/filequeues.conf** в параметре `Smtppath`.

8.6 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` необходимое 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.

8.7 Файловые очереди

Чтобы обеспечить загрузку имеющихся очередей объектов:

1. Остановите службы iw_icap, iw_deliver, iw_luaengined, iw_is, iw_smtpd, iw_sniffer, 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_sniffer, 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 sniffer`	`iwtm stop sniffer`
`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`
`service iwtm start proxy_smtp`	`service iwtm stop proxy_smtp`
`service iwtm start capstack`	`service 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
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, необходимо 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_luaengined, iw_deliver	iw_blackboard
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`.

8.8 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 очередей ошибок в обычные. Процедура выполняется при помощи утилиты iw_qtool (см. статью базы знаний "Как переместить объекты между очередями при помощи утилиты iw_qtool").
3. Если Traffic Monitor Server работает с установленной СУБД Postgre, 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`

После запуска Traffic Monitor, проверьте системный журнал на наличие ошибок. Путь к файлу журнала: `/var/log/messages`. Если в системном журнале содержится информация об ошибках, обратитесь в службу технической поддержки.

8.9 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 язык для поиска и терминов;
- Обновление установленного языка;
- Удаление языка для поиска и терминов.

8.9.1 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 лежат все пакеты, загруженные при установке:
   ```
   cd /opt/iw/distr
   ```
3. Перейдите в директорию, соответствующую текущей версии Traffic Monitor
4. Выберите необходимый пакет и выполните его установку с помощью команды:
   ```
   rpm –i <название пакета>
   ```
   Например, для установки пакета со словарем французского языка необходимо 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 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 необходимого языка в параметр `sphinx_language` .
   Например, чтобы включить морфологию русского и турецкого языков в Системе, необходимо указать 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/postgresql/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
   ```

8.9.2 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 БД производиться не будет: новые языки с поддержкой морфологии будут использоваться только для новых событий.

8.9.3 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
   ```

> **Примечание:**
>
> После удаления словаря происходит полная переиндексация БД.

В результате удаления языка с поддержкой морфологии при обновлении из Системы также будет удален соответствующий язык БКФ.

> **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.

8.10 Настройка передачи информации в SIEM

Traffic Monitor может интегрироваться с SIEM-системами (ArcSight, Tivoli и др.). Под интеграцией подразумевается поступление в SIEM-систему консолидированной информации со всех установленных в компании компонентов системы TM.

Для интеграции используется скрипт **/opt/iw/tm5/bin/config/iwtm-siem.conf.py**, доступный на сервере Traffic Monitor.

Информация из TM доступна для SIEM системы:

1. Посредством табличного представления:

- События, зарегистрированные в TM;
- Аудит сессий пользователей консоли TM;

- Посредством rsyslog:
  - Вход/выход пользователей Linux-сервера TM;
  - События, зафиксированные в системном журнале Linux-сервера TM, включая информацию о входе/выходе пользователей Базы Данных PostgreSQL;

- Состояние служб Linux-сервера TM или группы серверов.

В этом разделе:

- Настройки на стороне SIEM
- Настройки на стороне TM
- Типы логов, передаваемых в SIEM

8.10.1 Настройки на стороне SIEM

Чтобы подготовить SIEM к получению данных от TM:

1. В SIEM укажите таблицы, из которых необходимо забирать информацию:

- `IWTM.ARC_VIEW_OBJECTS2` - события TM;
- `IWTM.ARC_VIEW_AUDIT _LOG` – аудит пользователей TM

- Создайте учетную запись SIEM для доступа к таблицам БД.
- Настройте обработку данных, извлеченных из БД TM.

Информацию о табличных представлениях (иногда требуется для анализа) см. в статьях:

- "Табличное представление событий TM";
- "Табличное представление аудита пользователей".

> **Важно!**
>
> При настройке интеграции могут понадобиться дополнительные модули от производителя SIEM системы, позволяющие SIEM системе работать с табличными представлениями. Например, для интеграции с HP ArcSight необходим модуль HP Flex Conector.

Табличное представление событий TM

При подключении к БД TM используйте созданного пользователя **siem** (см. "Создание пользователя siem"). Искомые данные содержатся в таблице `IWTM.ARC_VIEW_OBJECTS2`.

> **Примечание:**
>
> Если для импорта в SIEM требуется отфильтровать данные, вы можете выполнить фильтрацию 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 TM. Всегда присутсвует.	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: • Внешнее устройство • Печать • ICQ • Skype • XMPP • Telegram • MS Lync • FTP • Email • Web-почта • Web-сообщение • Crawler • Буфер обмена • Облачные хранилища	Crawler
`protocol`		Атрибут события *Протокол*	Протокол может принимать одно из следующих значений: • OSCAR • Skype • XMPP • MMP • SIP • FTP • POP3 • IMAP • MAPI • SMTP • HTTP • HTTPS • NRPC • Отсутствует	
`verdict`	varchar2 (12)	Атрибут события *Вердикт*	Возможны значения: • *Quarantined* (*Карантин*) • *Forbidden* (*Заблокировано*) • *Allowed* (*Пропущено*)	Forbidden

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`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`. Используется для быстрой фильтрации данных		timestamp
`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 указанны в формате `<тип контакта>:<значение контакта>`. Может быть не заполнено.	email:ivanov@infowatch.ru, email:petr.petrov@infowatch.ru

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`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 проидентифицировать. 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
`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.	10.60.20.184

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
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
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 пользователя*	Решение пользователя консоли. Может принимать следующие значения: ▪ *Violation* (*Нарушение*) ▪ *NoViolation* (*Нет нарушения*) ▪ *NotProcessed* (*Решение не принято*) ▪ *AdditionalProcessingNeeded* (*Требует дополнительной обработки*) Может быть не заполнено.	Violation

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`filepath`	clob	Атрибут события *Путь к файлу*	Список путей к файлам. Пути в списке указаны через запятую. Может быть не заполнено.	\\xp-petrov\C$\666.txt
`attachments`	clob	Атрибут события *Имя файла вложения*	Имена файлов вложений, указанные через запятую.	666.txt, Petrov.doc, 3.jpg
`url`	varchar2 (4000)	Атрибут события *URL*	Полный адрес, с которого осуществлялась передача данных. Может быть не заполнено.	10.60.21.34/3.jpg
`capture_server_ip`	varchar2 (256)	Атрибут события *Сервер перехвата IP*	IP-адрес сервера, на котором были перехвачены данные. Может быть не заполнено.	10.60.21.34
`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 TM 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 TM.	12345
`change_date`	Varchar2(50)	Дата и время зарегистрированного действия пользователя	05.08.2015 09:35:10.641446000

Атрибут	Тип данных	Описание	Пример заполнения
`user_login`	varchar2(256)	Логин пользователя, осуществившего действие.	Admin
`user_fullname`	varchar2(256)	Полное имя пользователя, совершившего действие.	Petrov Petr Petrovich
`user_email`	varchar2(256)	E-mail пользователя, совершившего действие.	petr.petrov@infowatch.ru

Атрибут	Тип данных	Описание	Пример заполнения
`operation`	varchar2(40)	Тип действия, которое было произведено пользователем. Возможны значения: • restart (перезапуск) • delete_hash (удаление хэша) • sync (синхронизировать) • 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 пользовательского решения) • remove_tag (изменение тегов события) • delete_ref (удаление ссылки) • copy (копирование) • move (перемещение) • commit (применение изменений в конфигурации системы) • rollback (откат изменений в конфигурации системы) • draft (сохранение изменений в конфигурации системы) • add (добавление) • import (импорт) • export (экспорт)	Edit

Атрибут	Тип данных	Описание	Пример заполнения
`entity_type`	varchar2(40)	Тип объекта, над которым осуществлялось действие. Возможны значения: • AgentJob (диагностические данные) • Adlibitum (адлибитум) • Agent (служба) • CrawlerScanner (лог сканера Краулер) • CrawlerTask (лог задания Краулер) • Classifier (классификатор) • NetworkSettings (сетевые параметры) • NotificationSettings (состояние системы) • ObjectReport (выгрузка событий) • Query (запуск поиска событий) • QueryReportRun (агрегация отчета) • Setting (настройки) • UpdateSystem (обновление системы) • 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) • Term (термин) • TextObject (текстовый объект) • User (пользователь) • VisibilityArea (область видимости)	Dashboard

Атрибут	Тип данных	Описание	Пример заполнения
		• 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.	

Атрибут	Тип данных	Описание	Пример заполнения

		{
		“old”: {
		“<ТИП ОБЪЕКТА>”:{
		{
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”
		}
		}
		}
		{
		“new”: {
		“<ТИП ОБЪЕКТА>”:{
		{
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”
		}
		}
		}
		}
			{
			"old":{
			"visibilityareas":{
			}
			},
			"new":{
			"visibilityareas":[
			{
			"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.	

Атрибут	Тип данных	Описание	Пример заполнения

		{
		“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"
			}
			}

	-	**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"
			}
			}

8.10.2 Настройки на стороне TM

Чтобы настроить передачу консолидированной информации из TM:

1. Для запуска скрипта выполните команду:
   `/opt/iw/tm5/bin/config/iwtm-siem.conf.py`
2. Создайте учетную запись БД для SIEM (см. "Создание пользователя siem").
3. Настройте передачу информации из TM в SIEM (см. "Передача логов в SIEM");
4. Отрегулируйте настройку **Nagios** и компонент TM из меню;
5. Отрегулируйте настройки логирования аудита сессий пользователей БД TM.

Передача логов в SIEM

Чтобы настроить передачу записей из лог файлов Linux-сервера TM в SIEM:

1. Запустите скрипт:
   `/opt/iw/tm5/bin/config/iwtm-siem.conf.py`
2. Выберите опцию **Log messages forwarding configuration**.
3. Задайте в 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 **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 БД не логируется, поэтому в SIEM данная информация попадать не будет.

Управление пользователем siem

В данном разделе описывается создание, удаление и смена пароля для пользователя **siem**, от имени которого SIEM будет взаимодействовать с TM:

- Создание пользователя siem;
- Смена пароля пользователя siem;
- Удаление пользователя siem.

Создание пользователя siem

Чтобы создать пользователя siem:

1. Для запуска скрипта выполните команду:
   `/opt/iw/tm5/bin/config/iwtm-siem.conf.py`

2. Выберите опцию **DB siem user**.
3. В появившемся меню выберите опцию **Create DB siem user**.
4. Задайте параметры:

Параметр	Описание
`Enter login for DB administrative account`	Логин для учетной записи администратора PostgreSQL **Примечание:** используются логин `postgres`
`Enter password for DB administrative account`	Пароль для учетной записи администратора PostgreSQL
`Enter password DB siem user`	Пароль для новой учетной записи siem

5. Нажмите **Create**.

Смена пароля пользователя siem

Чтобы сменить пароль пользователю siem:

1. Для запуска скрипта выполните команду:
   `/opt/iw/tm5/bin/config/iwtm-siem.conf.py`
2. Выберите опцию **DB siem user** .
3. Выберите опцию **Change password for DB siem user**.
4. Задайте параметры:

Параметр	Описание
`Enter login for DB administrative account`	Логин для учетной записи администратора PostgreSQL **Примечание:** используются логин `postgres`
`Enter password for DB administrative account`	Пароль для учетной записи администратора PostgreSQL
`Enter new password user siem`	Новый пароль для учетной записи siem

5. Нажмите **Change password**.

Удаление пользователя siem

Чтобы удалить пользователя siem:

1. Для запуска скрипта выполните команду:
   `/opt/iw/tm5/bin/config/iwtm-siem.conf.py`

2. Выберите опцию **DB siem user** .
3. Выберите опцию **Delete DB siem user**.
4. Задайте параметры:

Параметр	Значение
`Enter login for DB administrative account`	Логин для учетной записи администратора PostgreSQL
`Enter password for DB administrative account`	Пароль для учетной записи администратора PostgreSQL

5. Нажмите **Delete**.

8.10.3 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 в случае 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)
   ```

8.11 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`

9 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.

10 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.

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` Дополнительная информация в ст. "Использование демона rsyslogd для логирования сообщений от служб iwtm"
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 Alert Log должен осуществляться по наличию слов: • ORA- • Failed to archive • ORACLE Instance .* - Archival Error • ARC[0-9]: I/O error • ARC[0-9]: RFS network connection lost at host • ARC[0-9]: Error 3113 creating • Media Recovery failed with error • Corrupt block • Fractured block • Bad header • Data in bad block • Reread of rdba • log corruption • RESETLOGS 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 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 10 % до 20% 🟢 – свободно > 20%	Подробнее см. "Рекомендации по разбиению дискового пространства серверов при установке в разных режимах"
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	Количество файлов в каталоге /opt/iw/tm5, начинающихся с core_.... (Linux-серверы)	30 мин.	🔴 – есть дамп 🟢 – нет дампов	Обратитесь в службу технической поддержки InfoWatch по адресу support@infowatch.com

Очередь ошибок обработки событий	Количество объектов в очереди **queue/final-errors** (iw_rammer)	1 мин.	🔴 – > 50 объектов
			🟡 – от 1 до 50 объектов
			🟢 = 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_error_queue.`
				2. Уменьшите период очистки очередей в штатном задании cron во всех строках (Значение по умолчанию - 90 дней).
				3. Сохраните изменения и закройте файл.
				Для получения дополнительной информации см. "Каким образом можно дослать письма, если они попали в очереди ошибок?"

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. "Рекомендации по разбиению дискового пространства серверов при установке в разных режимах")

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. "Рекомендации по разбиению дискового пространства серверов при установке в разных режимах"
Свободное место в каталоге ежедневных табличных пространств на быстром диске	Свободное место в партиции хранения ежедневных табличных пространств на быстром диске.	30 мин.	🔴 – < 7% 🟡 – от 7 до 15% 🟢 – > 15%	Индикатор добавляется, если при установке был выбран режим хранения данных *Быстрые и медленные диски* Подробнее см. "Рекомендации по разбиению дискового пространства серверов при установке в разных режимах"
Размер журнала предупреждений БД	Размер журнала предупреждений для СУБД PostgreSQL: System Log	5 мин.	🔴 – > 100 Мб 🟡 – от 50 до 100 Мб 🟢 – < 50 Мб	Обратитесь в службу технической поддержки InfoWatch по адресу support@infowatch.com
Наличие ошибок в журнале базы данных	Наличие ошибок	30 мин.	🔴 – есть ошибки 🟢 – нет ошибок	Необходимо снизить количество ошибок с SEVERITY=Error

Количество запущенных процессов	Количество запущенных процессов (Linux-серверы)	30 мин.	🔴 – > 600 процессов
			🟡 – от 450 до 600 процессов
			🟢 – < 450 процессов
				Необходимо увеличить максимально разрешенное количество процессов. Для этого в файле `/etc/security/limits.d/iwtm.conf` увеличьте значения:
				`* - nproc 8192`
				`@iwtm - nproc 8192`
				Максимально допустимое значение - 100000.

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: `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 об ъектов 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` 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 применен ных политик	Количество об ъектов 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: 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` 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 (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` 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`

Количество ошибок индексации событий службой **iw_indexer**	Количество ошибок индексации (iw_indexer)	30 мин.	🔴 – > 50 ошибок 🟡 – от 1 до 50 🟢 – нет ошибок	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.	🔴 – > 50 ошибок 🟡 – от 1 до 50 ошибок 🟢 – нет ошибок	1. Проверьте статус службы: `systemctl status iw_is` 2. Просмотрите логи службы в `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`
Очередь команд **iw_is**	Количество команд в очереди службы **iw_is**	30 мин.	🔴 – > 100 команд 🟡 – от 50 до 100 команд 🟢 – < 50 команд	
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.	🔴 – есть ошибки 🟢 – нет ошибок	

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 поддержки InfoWatch
Очередь команд для табличного пространства метаинформации	Количество команд в очереди табличного пространства метаинформации	30 мин.	🔴 – > 50 команд 🟡 – от 20 до 50 команд 🟢 – < 20 команд	

Очередь ошибок обработки событий	Количество объектов в очереди ошибок **queue/errors** (Extractors Framework, TMcap-серверы: iw_luaengined, iw_warpd, iw_cas)	30 мин.	🔴 – > 1000 объектов
			🟡 – от 200 до 1000 объектов
			🟢 – < 200 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_error_queue.`
				2. Уменьшите период очистки очередей в штатном задании cron во всех строках (Значение по умолчанию - 90 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.	🔴 – > 50 объектов
			🟡 – от 1 до 50 объектов
			🟢 = 0
				Вариант 1: Очистите очередь, используя команды:
				`su - iwtm`
				`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/x2x-errors`
				`exit`
				Вариант 2:
				1. Откройте на редактирование файл `/etc/cron.d/iwtm_error_queue.`
				2. Уменьшите период очистки очередей в штатном задании cron во всех строках (Значение по умолчанию - 90 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.	🔴 – > 50 объектов
			🟡 – от 1 до 50 объектов
			🟢 = 0
				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_error_queue.`
				2. Уменьшите период очистки очередей в штатном задании cron во всех строках (Значение по умолчанию - 90 дней).
				3. Сохраните изменения и закройте файл.

Очередь ошибок обработки действий примененных политик	Количество объектов в очереди **queue/blackboard_errors** (Linux-серверы)	30 мин.	🔴 – > 50 объектов
			🟡 – от 1 до 50 объектов
			🟢 = 0
				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_error_queue`.
				2. Уменьшите период очистки очередей в штатном задании cron во всех строках (Значение по умолчанию - 90 дней).
				3. Сохраните изменения и закройте файл.