

INFOWATCH

# InfoWatch Traffic Monitor

## Руководство администратора

20/01/2023

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

# СОДЕРЖАНИЕ


1 Введение ..... 8
1.1 Аудитория ..... 8
1.2 Комплект документов ..... 8
1.3 Техническая поддержка пользователей ..... 8
2 Обзор Traffic Monitor ..... 9
2.1 Функции InfoWatch Traffic Monitor ..... 9
2.1.1 Перехват трафика в потоке/на шлюзе ..... 9
Схема перехвата SMTP-трафика ..... 9
Схема перехвата POP3-трафика ..... 12
Схема перехвата HTTP-трафика ..... 13
Схема перехвата HTTPS-трафика ..... 16
Схема перехвата ICQ-трафика ..... 17
Схема перехвата NRPC-трафика ..... 18
Схема перехвата IMAP4-трафика ..... 19
2.1.2 Обработка трафика, полученного от сторонних источников ..... 20
2.2 Состав InfoWatch Traffic Monitor (Red Hat Enterprise Linux) ..... 21
2.3 Лицензирование ..... 22
3 Типы установки Системы ..... 27
4 Настройка Системы после установки ..... 28
4.1 Изменение предустановленного пароля ..... 28
4.2 Настройка защиты от подбора паролей ..... 29
4.3 Предварительные настройки ..... 30
4.3.1 Настройка синхронизации времени ..... 30
4.3.2 Конфигурирование работы Sphinx при распределенной установке ..... 31
4.4 Общие настройки ..... 31
4.4.1 Настройка сервера на работу по технологии SPAN, или Port Mirroring ..... 31
Настройка работы сервера Traffic Monitor в качестве Sniffer ..... 32
Настройка сервера Traffic Monitor на прием копии трафика от Sniffer ..... 33
Создание кластера Traffic Monitor ..... 34
Настройка сервера лицензирования (в случае кластера) ..... 35
4.4.2 Перехват трафика, передаваемого по протоколу ICAP ..... 36
Настройка ICAP ..... 37
Рекомендации по настройке Blue Coat SG Series ..... 38

Рекомендации по настройке SQUID ... 39
Рекомендации по настройке Cisco IronPort ... 42
Рекомендации по настройке McAfee Web Gateway ... 45
Рекомендации по настройке Fortinet FortiGate ... 46
Рекомендации по настройке UserGate ... 47
Отключение ICAP ... 50
4.4.3 Настройка работы "в разрыв" для нескольких перехватчиков ... 50
4.5 Настройка перехвата трафика ... 51
4.5.1 Настройка перехвата SMTP-трафика ... 53
SPAN, или Port Mirroring ... 53
Прием копий с почтового сервера ... 53
"В разрыв" ... 54
Настройки почтовых серверов для перехвата SMTP-трафика ... 58
4.5.2 Настройка перехвата POP3-трафика ... 64
4.5.3 Настройка перехвата HTTP-трафика ... 65
SPAN, или Port Mirroring ... 65
"В разрыв" (HTTP) ... 65
4.5.4 Настройка перехвата HTTPS-трафика ... 65
"В разрыв" (HTTPS) ... 65
4.5.5 Настройка перехвата ICQ-трафика ... 66
SPAN, или Port Mirroring ... 66
4.5.6 Настройка перехвата NRPC-трафика ... 66
SPAN, или Port Mirroring ... 66
4.5.7 Настройка перехвата IMAP4-трафика ... 67
4.5.8 Прием объектов, перехваченных InfoWatch Device Monitor ... 67
4.6 Автозапуск процессов ... 67
4.6.1 Проверка автозапуска процессов ... 68
4.6.2 Включение и выключение автозапуска процессов ... 70
4.7 Модуль взаимодействия с удаленной базой данных ... 71
4.7.1 Настройка сбора данных в филиальной сети ... 71
4.7.2 Настройка клиентской части модуля взаимодействия с удаленной БД ... 72
4.7.3 Настройка серверной части модуля взаимодействия с удаленной БД ... 73
4.8 Настройка OCR-экстракторов ... 73
4.9 Настройка отправки уведомлений пользователям и сотрудникам ... 78
4.10 Ограничение количества найденных событий ... 79
4.11 Настройка Сервера InfoWatch Device Monitor ... 79
4.11.1 Раздел <applicationSettings> ... 81
4.11.2 Раздел <system.diagnostics> ... 88
4.11.3 Удаление временных файлов Device Monitor ... 90
4.12 Настройка межсервисного взаимодействия (служба Consul) ... 91
4.12.1 Запуск и остановка службы ... 91

4.12.2 Регистрация сервисов в Consul ... 92
4.12.3 Распределенная установка ... 93
4.12.4 Настройка сетевых правил доступа в Consul ... 95
4.12.5 Конфигурационный файл consul.json и unit-файл iwtm-consul.service ... 95
4.13 Обнаружение рабочих станций для установки агентов ... 98
5 Мониторинг ... 101
5.1 Настройки подсистемы мониторинга ... 101
5.1.1 Настройка подключения Device Monitor ... 101
5.1.2 Ручная настройка индикаторов ... 102
5.1.3 Настройка адреса сервера синхронизации времени для подсистемы мониторинга ... 102
5.1.4 Настройка механизма уведомлений ... 102
6 Администрирование базы данных ... 104
6.1 Oracle ... 104
6.1.1 Изменение предустановленных паролей ... 104
6.1.2 Табличные пространства в базе данных InfoWatch Traffic Monitor ... 104
6.1.3 Управление ежедневными табличными пространствами ... 105
Настройка размещения файлов в файловой системе ... 105
Настройка режимов хранения файлов табличного пространства ... 107
Архивирование ежедневных табличных пространств ... 109
Восстановление ежедневных табличных пространств ... 112
Удаление ежедневных табличных пространств ... 112
6.1.4 Резервное копирование базы данных ... 116
Создание резервной копии базы данных ... 116
Восстановление базы данных из резервной копии ... 121
6.1.5 Проведение регламентных работ на сервере базы данных ... 123
6.1.6 Логирование базы данных ... 125
Ротация логов базы данных ... 126
6.2 PostgreSQL ... 126
6.2.1 Изменение предустановленных паролей ... 127
6.2.2 Табличные пространства в базе данных InfoWatch Traffic Monitor ... 127
6.2.3 Управление ежедневными табличными пространствами ... 128
Архивирование ежедневных табличных пространств ... 128
Восстановление ежедневных табличных пространств ... 131
Настройка размещения файлов в файловой системе ... 131
Настройка режимов хранения файлов табличного пространства ... 133
Удаление ежедневных табличных пространств ... 134
6.2.4 Резервное копирование базы данных ... 138
Создание резервной копии базы данных ... 138
Восстановление базы данных из резервной копии ... 140
6.2.5 Проведение регламентных работ на сервере базы данных ... 142

6.2.6 Логирование базы данных ... 143
Ротация логов базы данных ... 143
7 Администрирование серверной части InfoWatch Traffic Monitor ... 144
7.1 Процессы серверной части Traffic Monitor Server ... 144
7.1.1 Список процессов серверной части Traffic Monitor ... 144
7.1.2 Настройка конфигурационных файлов серверной части Traffic Monitor ... 152
7.1.3 Работа с процессами серверной части Traffic Monitor ... 152
7.2 Настройка использования OCR ... 155
7.2.1 Конфигурационный файл ocr_custom.xml ... 156
7.3 Настройка параметров работы с HTTP-запросами, передаваемыми по протоколу ICAP ... 157
7.4 Настройка параметров обработки архивов вложений ... 158
7.4.1 Конфигурационный файл extractors.xml ... 158
7.5 Архивирование каталога очереди сообщений ... 161
7.6 Логирование работы Системы ... 161
7.7 Файловые очереди ... 163
7.8 Восстановление работоспособности системы в аварийных ситуациях ... 166
7.9 Управление языками с поддержкой морфологии ... 166
7.9.1 Добавление нового языка для поиска событий. Морфология и добавление терминов. ... 167
7.9.2 Обновление установленного языка ... 168
7.9.3 Удаление языка для поиска и терминов ... 168
7.10 Настройка передачи информации в SIEM ... 169
7.10.1 Настройки на стороне SIEM ... 169
Табличное представление событий TM ... 170
Табличное представление аудита пользователей ... 178
7.10.2 Настройки на стороне TM ... 184
Передача логов в SIEM ... 185
Управление логированием сессий пользователей БД TM ... 185
Управление пользователем siem ... 186
7.10.3 Типы логов, передаваемых в SIEM ... 188
7.11 Удаление временных файлов ... 188
8 Настройка сквозной аутентификации между продуктами InfoWatch 190
9 Взаимодействие с внешними системами ... 192
9.1 Загрузка событий в InfoWatch Traffic Monitor (pushAPI SDK) ... 192
9.1.1 Принципы использования pushAPI SDK ... 192
9.1.2 Общее описание программного интерфейса pushAPI SDK ... 195
Типы данных pushAPI SDK ... 195

Исключения pushAPI SDK ... 198
Сервисы Traffic Monitor pushAPI SDK ... 198
Типы контактов Traffic Monitor pushAPI SDK ... 200
Поддерживаемые атрибуты Traffic Monitor pushAPI SDK ... 201
Сервис EventProcessor pushAPI SDK ... 205
9.1.3 Регистрация стороннего компонента pushAPI SDK ... 207
Формат файла регистрации стороннего компонента pushAPI SDK ... 207
9.1.4 Описание примеров PushAPI SDK ... 214
Сборка примеров под Linux pushAPI SDK ... 216
Сборка примеров под Windows pushAPI SDK ... 216
9.2 Загрузка эталонных документов и выгрузок из БД в Traffic Monitor (REST API SDK) ... 216
9.2.1 Конфигурирование программного интерфейса REST API ... 216
9.2.2 Общее описание программного интерфейса REST API ... 217
Создание эталонной выгрузки REST API ... 217
Обновление эталонной выгрузки REST API ... 217
Добавление содержимого к эталонной выгрузке REST API ... 217
Получение состояния эталонной выгрузки REST API ... 218
Инициирование распространения нового содержимого загруженных эталонных документов на модули анализа REST API ... 218
Получение версии интерфейса, который поддерживается Traffic Monitor REST API ... 218
Создание каталога эталонных документов ... 218
Удаление каталога эталонных документов ... 219
Создание эталонного документа ... 219
Удаление эталонного документа ... 219
Добавление содержимого эталонного документа ... 219
Получение состояния эталонного документа ... 219
9.2.3 Регистрация стороннего компонента REST API ... 220
Формат файла регистрации стороннего компонента REST API ... 220
9.2.4 Формат эталонной выгрузки и эталонного документа REST API ... 222
9.2.5 Функциональное описание программного интерфейса REST API ... 222
Общие заголовки GET/POST-запросов ... 223
Работа с конфигурацией REST API ... 223
Работа с эталонными выгрузками REST API ... 223
Общие ошибки REST API ... 228
Работа с эталонными документами REST API ... 235
9.3 Получение доступа к событиям Traffic Monitor внешними системами (DataExport API SDK) ... 250
9.3.1 Функции DataExport API ... 250
9.3.2 Авторизация для доступа к DataExport API ... 252
Работа с плагинами ... 252
Работа с токенами ... 252
9.3.3 Регистрация стороннего компонента DataExport API ... 253

Формат файла регистрации стороннего компонента DataExport API ..... 254
9.3.4 Функциональное описание программного интерфейса DataExport API ..... 258
Общие заголовки GET/POST-запросов для DataExport API ..... 258
Получение списка фич по версии Traffic Monitor ..... 260
Получение данных аудита ..... 261
Получение организационной структуры ..... 269
Получение событий ..... 313
Получение списка пользователей консоли ..... 347
Получение результатов выполнения запроса Traffic Monitor ..... 348
10 Приложение A. Рекомендации по составлению имен и паролей .... 352
11 Приложение B. Индикаторы мониторинга ..... 354

# 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 (Red Hat Enterprise Linux);
- 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 трафика в потоке/на шлюзе - перехват трафика в потоке/на шлюзе, передаваемого по протоколам SMTP, POP3, HTTP, HTTPS, OSCAR (ICQ), NRPC (IBM Notes);
- Перехват трафика на рабочих станциях агентами Device Monitor (подробнее см. *"InfoWatch Device Monitor. Руководство пользователя"*);
- Обработка трафика, полученного от сторонних источников;

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

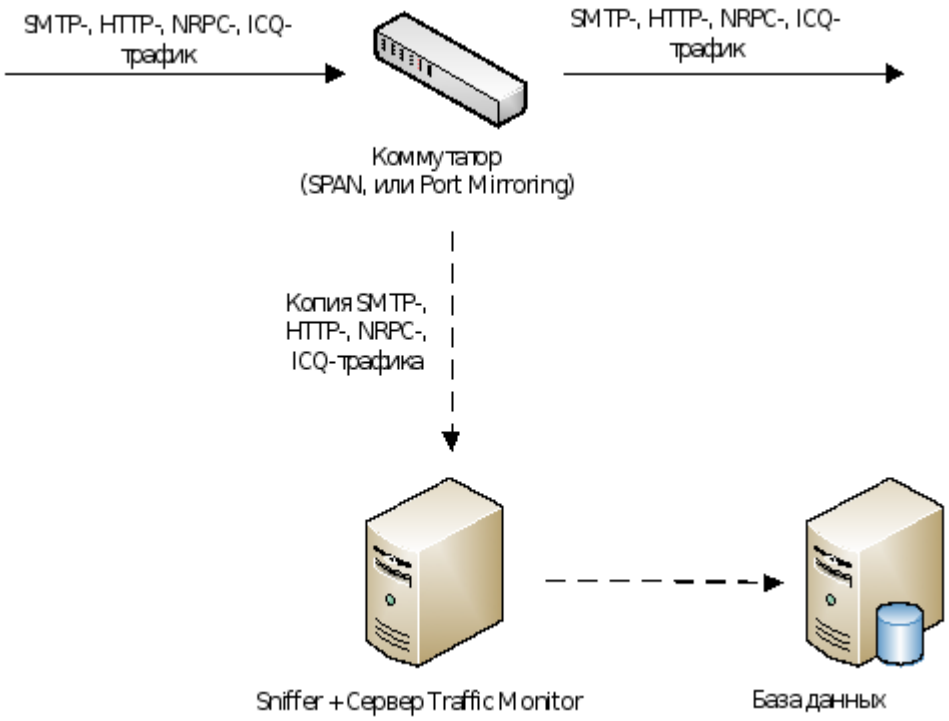
### 2.1.1 Перехват трафика в потоке/на шлюзе

Раздел содержит информацию о видах трафика и схемах его перехвата:


- Схема перехвата SMTP-трафика;
- Схема перехвата POP3-трафика;
- Схема перехвата HTTP-трафика;
- Схема перехвата HTTPS-трафика;
- Схема перехвата ICQ-трафика;
- Схема перехвата NRPC-трафика;
- Схема перехвата IMAP4-трафика.


#### Схема перехвата SMTP-трафика

**Способ №1:**
Трафик снимается с управляемого коммутатора по технологии SPAN Port, или Port Mirroring.
Большое количество управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов или VLAN на отдельно взятый порт.
В данном случае настроенный порт коммутатора подключается к сетевому интерфейсу сервера Traffic Monitor. Интерфейс сервера переводится в «неразборчивый» (promiscuous) режим, что позволяет ему принимать все входящие пакеты. IP-адрес на данном интерфейсе не требуется.
Наиболее эффективным является зеркалирование внутреннего порта шлюза или внутреннего интерфейса прокси-сервера.



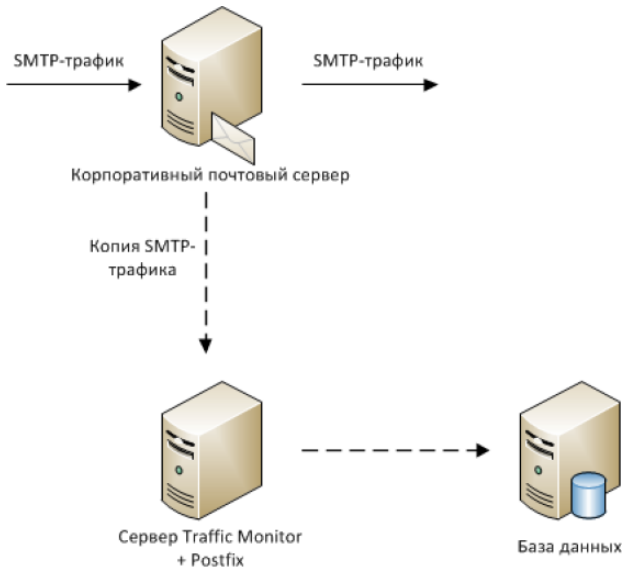

О настройке данного функционала см. "SPAN, или Port Mirroring"
**Преимущества:**

- Способ позволяет безопасно анализировать трафик даже в изолированном сегменте сети. Система никак не может повлиять на анализируемый трафик, независимо от состояния сервера.
- Анализируется также SMTP-трафик внешних серверов

**Недостатки:**

- При большой нагрузке на коммутатор часть пакетов может теряться, особенно если трафик с нескольких портов зеркалируется в один. Чтобы предотвратить потерю пакетов, требуются:
  - коммутатор с соответствующим функционалом;
  - дополнительный сетевой адаптер на сервере Traffic Monitor.
- Внутренняя переписка не контролируется.

**Способ №2:**
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.



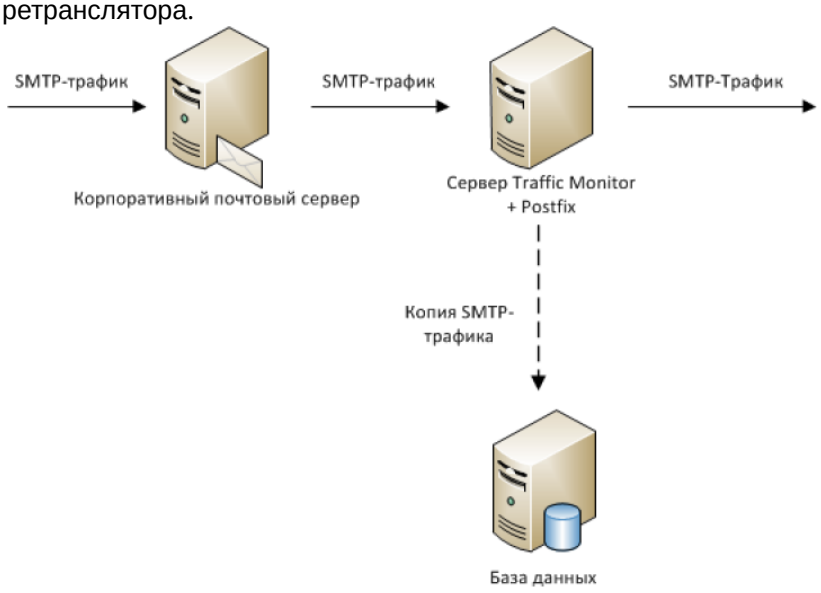

О настройке данного функционала см. "Прием копий с почтового сервера"
**Преимущества:**

- Позволяет анализировать не только внешнюю, но и внутреннюю переписку компании;
- При использовании MS Exchange 2007 и более новых есть возможность анализировать переписку определенной группы пользователей;
- Гарантирует анализ всех писем.

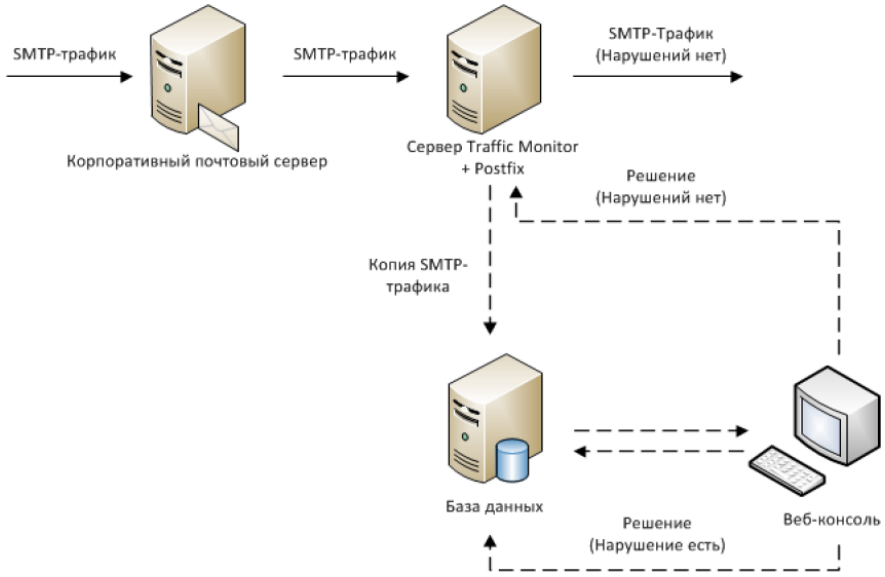
**Недостатки:**

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

**Способ №3**
Сервер Traffic Monitor, использующий настроенный почтовый сервер Postfix, выполняет функцию SMTP-ретранслятора.




Копия

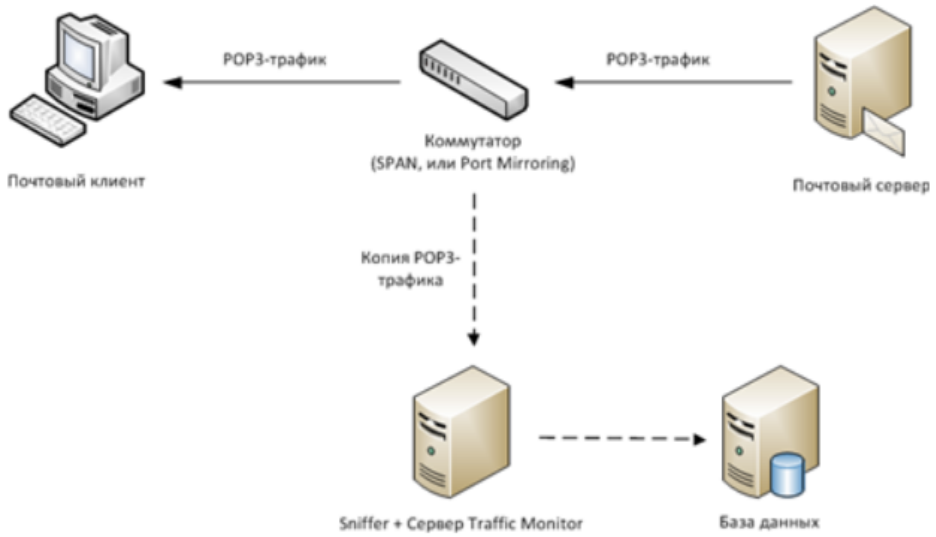



Блокировка
О настройке данного функционала "В разрыв"
**Преимущества:**
Позволяет включить функционал блокировки почтового трафика
**Недостатки:**

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

## Схема перехвата POP3-трафика

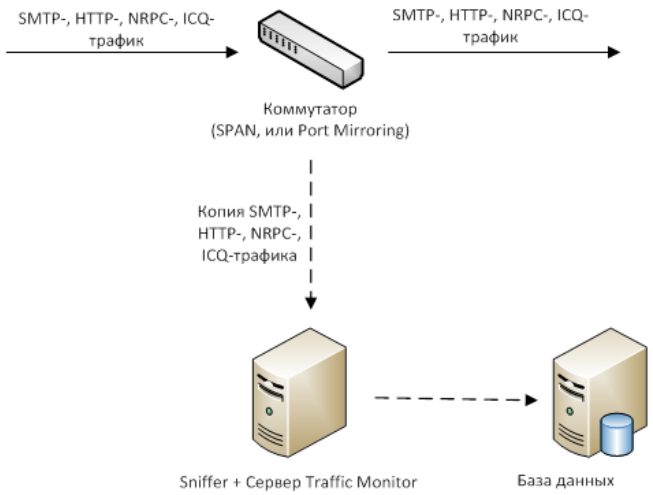
Трафик снимается с управляемого коммутатора по технологии SPAN Port, или Port Mirroring.
Большое количество управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов или VLAN на отдельно взятый порт.
В данном случае настроенный порт коммутатора подключается к сетевому интерфейсу сервера Traffic Monitor. Интерфейс сервера переводится в «неразборчивый» (promiscuous) режим, что позволяет ему принимать все входящие пакеты. IP-адрес при подключении к сетевому интерфейсу не требуется.
Наиболее эффективным является зеркалирование внутреннего порта шлюза или внутреннего интерфейса прокси-сервера.




О настройке данного функционала см. "Настройка перехвата POP3-трафика".

## Схема перехвата HTTP-трафика

**Способ №1:**
Трафик снимается с управляемого коммутатора по технологии SPAN Port, или Port Mirroring.
Большое количество управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов или VLAN на отдельно взятый порт.
В данном случае настроенный порт коммутатора подключается к сетевому интерфейсу сервера Traffic Monitor. Интерфейс сервера переводится в «неразборчивый» (promiscuous) режим, что позволяет ему принимать все входящие пакеты. IP-адрес при подключении к сетевому интерфейсу не требуется.
Наиболее эффективным является зеркалирование внутреннего порта шлюза или внутреннего интерфейса прокси-сервера.




О настройке данного функционала см. "SPAN, или Port Mirroring".
**Преимущества:**

- Позволяет безопасно анализировать трафик даже в изолированном сегменте сети. Система никак не может повлиять на анализируемый трафик, независимо от состояния сервера.

**Недостатки:**

- При большой нагрузке на коммутатор часть пакетов может теряться, особенно если трафик с нескольких портов зеркалируется в один. Чтобы предотвратить потерю пакетов, требуется:
    - коммутатор с соответствующим функционалом;
    - дополнительный сетевой адаптер на сервере Traffic Monitor.

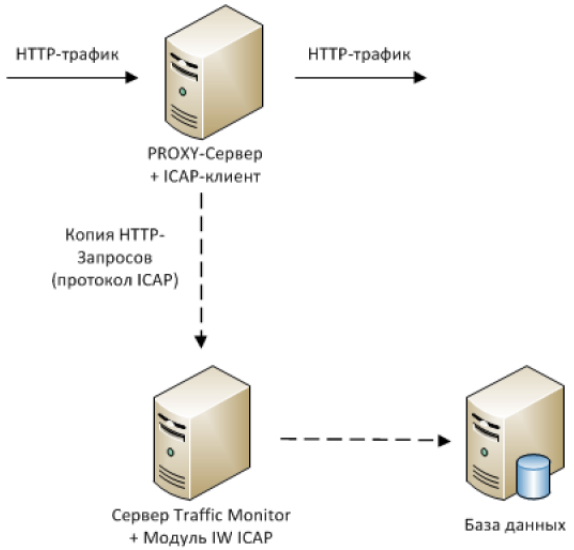
**Частный случай №1:**
Если сервер Traffic Monitor находится в виртуальной среде, то в дополнение к настройке порта коммутатора, для анализа трафика создается отдельный виртуальный свитч, на котором включается режим широковещания (promiscuous mode), связанный с отдельным физическим интерфейсом. Этот способ позволяет анализировать трафик виртуальных машин, работающих через такой виртуальный свитч.
Данный способ работает на VMware ESXi серверах. На Hyper-V данный функционал реализован с ограничениями, начиная с версии Hyper-V 2012.

**Частный случай №2:**
Вместо управляемого коммутатора возможно использовать HUB. Недостатком данного варианта является низкая пропускная способность HUB-устройства, а также отсутствие подобных устройств в продаже в связи со снятием с производства.

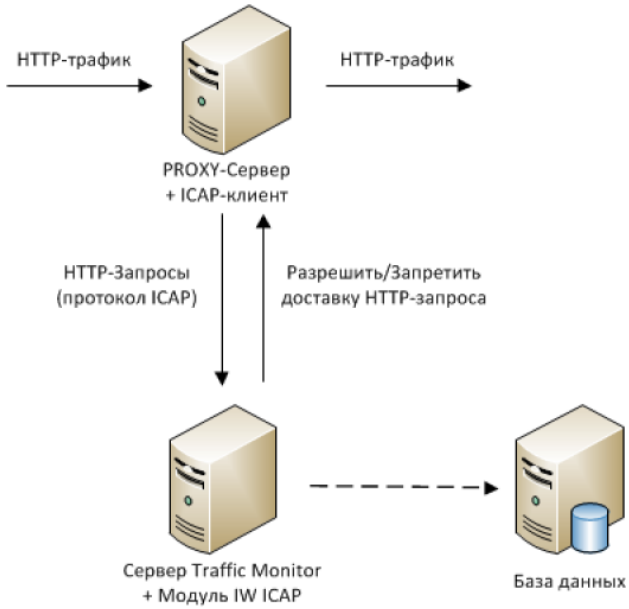
**Способ №2:**
Копия трафика, передаваемого по протоколу ICAP, снимается с корпоративного прокси-сервера. Сервер Traffic Monitor выступает в качестве ICAP-сервера. Если в компании работает прокси-сервер, поддерживающий ICAP-протокол, то можно использовать данный функционал для анализа HTTP-трафика.
Данную функцию поддерживают следующие прокси-серверы:

- Cisco Ironport
- SQUID (при условии, что пакет собран с поддержкой ICAP)
- Blue Coat SG
- Zimbra Proxy (в составе Zimbra ZCS)

> **Примечание:**
>
> Работа с другими прокси-серверами, поддерживающими ICAP, возможна, но требует предварительной проверки на совместимость.




Копия




Блокировка
О настройке данного функционала см. "В разрыв"

**Преимущества:**

- Гарантированная доставка всех пакетов;
- С рядом прокси-серверов возможна работа сервера Traffic Monitor в режиме блокировки ("в разрыв").

**Недостатки:**

- Требуется наличие прокси-сервера с соответствующим функционалом;
- Дополнительная нагрузка на прокси-сервер;
- Внесение изменений в настройки корпоративного прокси-сервера;
- Возможно незначительное увеличение времени отклика интернет-ресурсов.

## Схема перехвата HTTPS-трафика

**Важно!**

При использовании любого способа анализа HTTPS-трафика требуется соблюдать максимальную осторожность. Технология анализа HTTPS основана на подмене сертификата HTTPS-сессии на сертификат, выданный прокси-сервером (**man-in-the-middle attack**). На машине пользователя обязательно должно быть настроено доверие к сертификату прокси-сервера, иначе он не сможет установить соединение с HTTPS-ресурсом. Все HTTPS-ресурсы, использующие для идентификации личные сертификаты, необходимо исключить из перехвата. Примером таких ресурсов могут являться различные клиент-банки.

**Способ №1:**

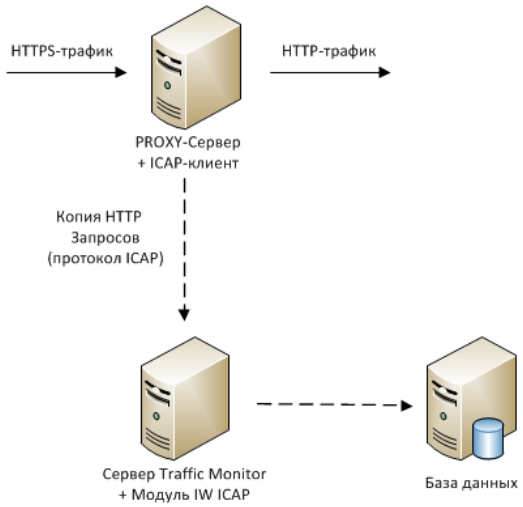
Подмену сертификата и разбор HTTPS-трафика осуществляет корпоративный прокси-сервер. После разбора HTTPS-трафика, прокси-сервер отправляет разобранный трафик в виде HTTP по ICAP протоколу на сервер Traffic Monitor.
Данным функционалом обладают следующие прокси-серверы:

- Cisco Ironport
- SQUID (при условии, что пакет собран с поддержкой ICAP)
- Blue Coat SG
- Zimbra Proxy (в составе Zimbra ZCS)

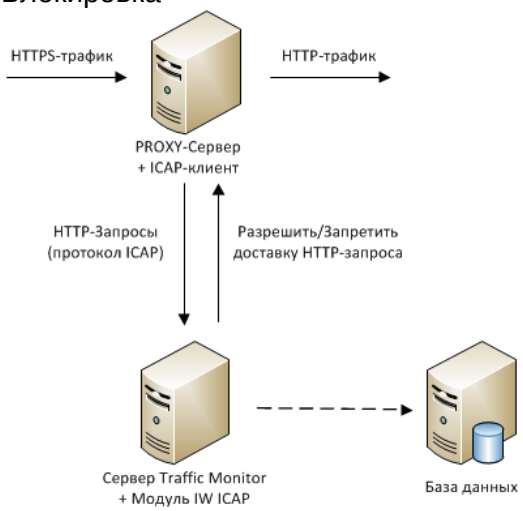
**Примечание:**

Работа с другими прокси-серверами, поддерживающими ICAP, возможна, но требует предварительной проверки на совместимость.

Копия



Блокировка




О настройке данного функционала см. "В разрыв"

**Преимущества:**

- Анализируется весь HTTPS-трафик.

**Недостатки:**

- Нужно учесть потребности всех пользователей, которые пользуются данным прокси-сервером;
- Дополнительная нагрузка на прокси-сервер;
- Требуются серьезные подготовительные мероприятия по созданию списка исключений и распространению сертификата.

**Частный случай:**
Инженеры InfoWatch могут установить бесплатный прокси-сервер SQUID на сервере Traffic Monitor.
**Преимущества:**
Появляется возможность анализировать HTTPS.
**Недостатки:**
Для обслуживания данного сервера требуется специалист со знанием SQUID.
**Способ №2:**
Анализ HTTPS-трафика осуществляется агентом InfoWatch Device Monitor.
О настройке данного функционала см. документ «InfoWatch Traffic Monitor. Руководство пользователя».
**Преимущества:**

- Агент самостоятельно прописывает свой сертификат в доверенные;
- Возможность постепенного внедрения анализа HTTPS-трафика в компании.

**Недостатки:**
Нужно предусмотреть потребности пользователя данной машины.

## Схема перехвата ICQ-трафика

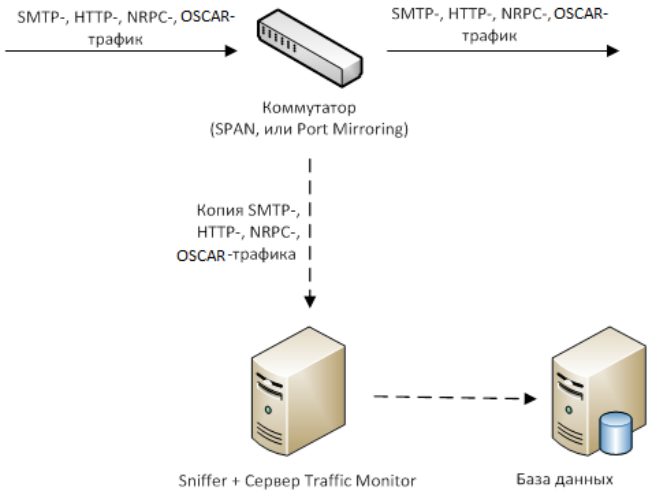
Перехват копии ICQ-трафика (протокол OSCAR), проходящего через оборудование с поддержкой технологии SPAN. Возможен перехват ICQ-трафика поверх HTTP.

> **Важно!**
>
> Не поддерживается перехват и анализ зашифрованного ICQ-трафика, в том числе по протоколу SSL.

**Примечание:**

Не поддерживается прямая передача файлов. По протоколу OSCAR в Traffic Monitor передаётся ссылка на ресурс для обмена файлами, который содержит передаваемый файл.

Трафик снимается с управляемого коммутатора по технологии SPAN Port, или Port Mirroring.
Большое количество управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов или VLAN на отдельно взятый порт.
В данном случае настроенный порт коммутатора подключается к сетевому интерфейсу сервера Traffic Monitor. Интерфейс сервера переводится в «неразборчивый» (promiscuous) режим, что позволяет ему принимать все входящие пакеты. IP-адрес на данном интерфейсе не требуется.
Наиболее эффективным является зеркалирование внутреннего порта шлюза или внутреннего интерфейса прокси-сервера.




О настройке данного функционала см. "SPAN, или Port Mirroring".
**Преимущества:**

Позволяет безопасно анализировать трафик даже в изолированном сегменте сети. Система никак не может повлиять на анализируемый трафик, независимо от состояния сервера.

**Недостатки:**

При большой нагрузке на коммутатор часть пакетов может теряться, особенно если трафик с нескольких портов зеркалируется в один. Чтобы предотвратить потерю пакетов, требуется:

- коммутатор с соответствующим функционалом;
- дополнительный сетевой адаптер на сервере Traffic Monitor.

## Схема перехвата NRPC-трафика

Перехват копии NRPC-трафика (используется в системе IBM Notes), проходящего через оборудование с поддержкой технологии SPAN.

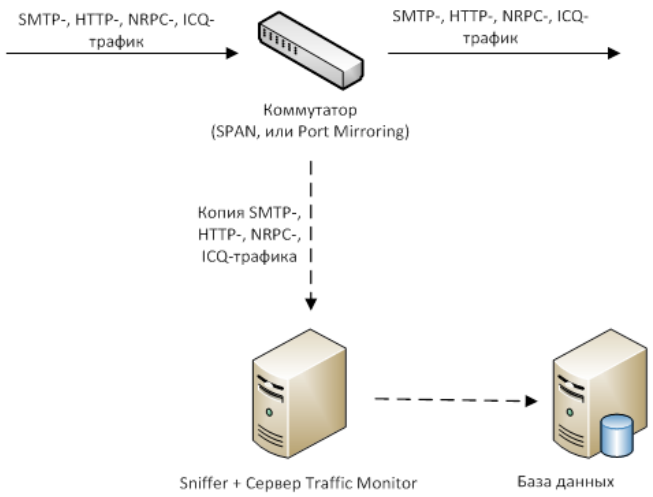
**Способ №1:**

Трафик снимается с управляемого коммутатора по технологии SPAN Port, или Port Mirroring.

Большое количество управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов или VLAN на отдельно взятый порт.

В данном случае настроенный порт коммутатора подключается к сетевому интерфейсу сервера Traffic Monitor. Интерфейс сервера переводится в «неразборчивый» (promiscuous) режим, что позволяет ему принимать все входящие пакеты. IP-адрес при подключении к сетевому интерфейсу не требуется.

Наиболее эффективным является зеркалирование внутреннего порта шлюза или внутреннего интерфейса прокси-сервера.




О настройке данного функционала см. статью "SPAN, или Port Mirroring"

**Преимущества:**

Позволяет безопасно анализировать трафик даже в изолированном сегменте сети. Система никак не может повлиять на анализируемый трафик, независимо от состояния сервера.

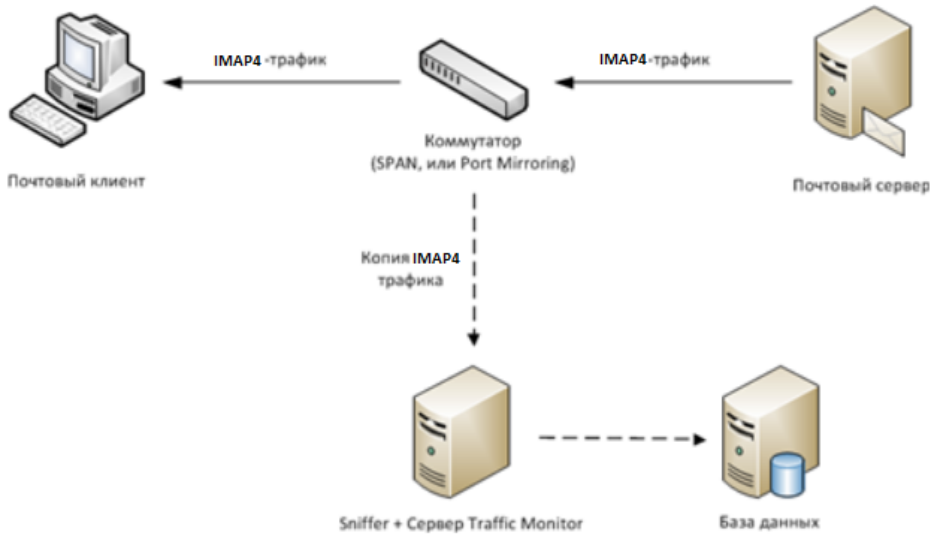
**Недостатки:**

При большой нагрузке на коммутатор часть пакетов может теряться, особенно если трафик с нескольких портов зеркалируется в один. Чтобы предотвратить потерю пакетов, требуются:

- коммутатор с соответствующим функционалом;
- дополнительный сетевой адаптер на сервере Traffic Monitor.

## Схема перехвата IMAP4-трафика

Трафик снимается с управляемого коммутатора по технологии SPAN Port, или Port Mirroring.
Большое количество управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов или VLAN на отдельно взятый порт.
В данном случае настроенный порт коммутатора подключается к сетевому интерфейсу сервера Traffic Monitor. Интерфейс сервера переводится в «неразборчивый» (promiscuous) режим, что позволяет ему принимать все входящие пакеты. IP-адрес при подключении к сетевому интерфейсу не требуется.
Наиболее эффективным является зеркалирование внутреннего порта шлюза или внутреннего интерфейса прокси-сервера.




О настройке данного функционала см. "Настройка сервера на работу по технологии SPAN, или Port Mirroring".

## 2.1.2 Обработка трафика, полученного от сторонних источников

Traffic Monitor поддерживает ряд адаптеров, которые работают по схеме пересылки данных из интегрируемого источника и сохранения их в базе данных:

- **InfoWatch Lotus Domino Adapter**. Рекомендации по установке и администрированию приводятся в документе "InfoWatch Lotus Domino Adapter. Руководство по установке и администрированию";
- **InfoWatch MS Lync Adapter**. Рекомендации по установке и администрированию приводятся в документе "InfoWatch MS Lync Adapter. Руководство по установке и администрированию";
- **InfoWatch TMG Adapter**. Рекомендации по установке и администрированию приводятся в документе "InfoWatch TMG Adapter. Руководство по установке и администрированию";
- **InfoWatch Device Control Adapter**. Рекомендации по установке и администрированию приводятся в документе "InfoWatch Device Control Adapter. Руководство по установке и администрированию";
- **InfoWatch Cisco UCM Adapter**. Рекомендации по установке и администрированию приводятся в документе "InfoWatch Cisco UCM Adapter. Руководство по установке и конфигурированию";
- **InfoWatch Smart Logger II**. Рекомендации по установке и администрированию приводятся в документе "InfoWatch Smart Logger II. Руководство по установке и конфигурированию";
- **InfoWatch HEML Adapter**. Рекомендации по установке и администрированию приводятся в документе "InfoWatch HEML Adapter. Руководство по установке, конфигурированию и запуску";
- **InfoWatch Sample Documents Autoupdate Adapter**. Рекомендации по установке и администрированию приводятся в документе "InfoWatch Sample Documents Autoupdate Adapter. Руководство по установке и конфигурированию".

## 2.2 Состав InfoWatch Traffic Monitor (Red Hat Enterprise Linux)

| Подсистема InfoWatch Traffic Monitor | Назначение подсистемы |
|---|---|
| Подсистема перехвата трафика | Перехват и передача на обработку трафика: объектов или их копий.<br>Состоит из следующих модулей:<br>• Модуль Sniffer;<br>• Модуль ICAP;<br>• Модуль Device Monitor;<br>• Модуль перехвата почты (SMTP). |
| Подсистема обработки | Извлечение из перехваченных объектов значимой информации и вложений, определение форматов вложений и передача извлеченных текстов в подсистему анализа.<br>**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).<br>Состоит из следующих технологий:<br>• Категории и термины;<br>• Текстовые объекты;<br>• Эталонные документы;<br>• Векторные изображения;<br>• Бланки;<br>• Печати;<br>• Выгрузки из БД;<br>• Графические объекты;<br>• Автолингвист. |
| Подсистема применения политик | На основе результатов работы подсистемы анализа и подсистемы обработки выносит вердикт о факте нарушения или не нарушения перехваченным объектом политики информационной безопасности. Также обеспечивает привязку данных о получателе или отправителе объекта к записям справочника сотрудников и рабочих станций.<br>Состоит из следующих модулей: Модуль интеграции с Active Directory, Samba DC и Domino 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 |

| Подсистема InfoWatch Traffic Monitor | Назначение подсистемы |
|---|---|
| | управления. Представляет собой базу данных.<br>Состоит из следующих модулей: Модуль взаимодействия с удаленной БД, Модуль загрузки объектов в БД, Модуль хранения настроек системы, Модуль хранения объектов.<br>**Примечание:** перед сохранением объектов в БД, они преобразуются 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.<br>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.<br>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.<br>Состоит из следующих модулей:<br>• Модуль мониторинга;<br>• Модуль контроля;<br>• Модуль настройки. |

## 2.3 Лицензирование

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, разработанные компанией InfoWatch | | |
|---|---|---|
| Подсистема | Тип событий | Протокол |
| TM | Email | POP3<br>IMAP<br>SMTP<br>NRPC |
| | Web-сообщение | HTTP<br>HTTPS |
| | Web-почта | HTTP<br>HTTPS |
| | ICQ | OSCAR |
| DM | Электронная почта | POP3<br>IMAP<br>Outlook<br>SMTP |
| | Web-сообщение | HTTP<br>HTTPS |
| | Web-почта | HTTP<br>HTTPS |
| | Печать | - |
| | Skype | SKYPE |
| | XMPP | XMPP |
| | Mail.Ru Агент | MMP |

| Модули перехвата, разработанные компанией InfoWatch | | |
|---|---|---|
| Подсистема | Тип событий | Протокол |
| | FTP | FTP |
| | Буфер обмена | - |
| | Снимки экрана | - |
| | Съемные устройства | - |
| | Сетевые ресурсы | - |
| | Терминальная сессия | - |
| | Облачное хранилище | HTTPS |
| | Telegram | - |
| | Vkontakte | HTTPS |
| | Facebook | HTTPS |
| | WhatsApp | - |
| Adapters | MS Lync | SIP |
| | Email (Lotus) | NRPC |
| | Съемные устройства (Lumension Device Control) | - |
| | Печать (Lumension Device Control) | - |
| | Web-сообщение (ICAP) | ICAP |
| | Web-почта (ICAP) | ICAP |

| Модули перехвата сторонних разработчиков | |
|---|---|
| Тип событий | Протокол |
| Электронная почта | POP3<br>MAPI<br>SMTP/ESMTP |

| Модули перехвата сторонних разработчиков | |
|---|---|
| Тип событий | Протокол |
| | IMAP<br>NRPC |
| Web-почта | HTTP<br>HTTPS<br>ICAP |
| ICQ | OSCAR |
| Mail.ru Агент | MMP |
| Skype | Skype |
| XMPP | XMPP |
| MS Lync | SIP |
| Web-сообщение | HTTP<br>HTTPS<br>ICAP |
| FTP | FTP |
| Съемные устройства | - |
| Печать | - |
| SmartLogger | XMPP |
| Cisco UCM | XMPP |

Модули анализа:

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

Дополнительные возможности:

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

**Ограничение:**

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

# 3 Типы установки Системы

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

- *"Все-в-одном" Standard* - базовый тип установки всех компонентов Системы на один компьютер с использованием СУБД PostgreSQL. Подробнее см. документ "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Установка TM Enterprise и TM Standard в режиме "Все-в-одном";
- *"Все-в-одном" Enterprise* - тип установки Системы с расширенными возможностями, включая: использование СУБД PostgreSQLи Oracle, 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 (*компоненты Traffic Monitor и СУБД устанавливаются на разные машины*)* - тип установки Системы для функционирования под большой нагрузкой и работой с большим объемом данных. Подробнее см. 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_bookworm, iw_deliver, iw_licensed, iw_indexer, iw_is, iw_image_autoling, iw_text_autoling**) и пользовательской консоли (**iw_kicker, iw_configerator**) должны быть запущены в единственном экземпляре на кластере (подробнее см. "Список процессов серверной части Traffic Monitor")

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

- InfoWatch Device Monitor - предназначен для настройки схем безопасности, системы мониторинга компьютеров, контроля доступа к компьютерам компании и др. (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;
- Общие настройки - порядок настроек для снятия трафика с управляемого коммутатора по технологии SPAN Port, перехвата трафика, передаваемого по протоколу ICAP, а также системные настройки для переключения перехватчиков на работу в режиме "в разрыв" с возможностью блокировки 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 (подробнее см. документ *"InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию"*);
- Настройка сбора данных в филиальной сети - настройки конфигурационных файлов служб, осуществляющих сбор данных в филиальной сети;
- Настройка межсервисного взаимодействия (служба Consul) - настройки конфигурационного файла и службы, осуществляющей управление процессами Системы;
- Обнаружение рабочих станций для установки агентов - сканирование сети на наличие рабочих станций вне Active Directory.

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

Также имеется возможность настроить защиту от подбора паролей при авторизации в консолях Traffic Monitor и Device Monitor (подробнее в статье Настройка защиты от подбора паролей).

## 4.1 Изменение предустановленного пароля

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

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

1. Остановите процессы Traffic Monitor:
   `iwtm stop`
2. Перейдите в директорию /opt/iw/tm5:
   `cd /opt/iw/tm5`
3. Выполните команду:
   `egrep -lir --include=\*.{cfg,conf} 'xxXX1234' | xargs -l sed -i -e 's/xxXX1234/<new_pass>/g'` где `<new_pass>` - новый пароль.
4. Измените предустановленные стандартные пароли используемой СУБД. Подробнее см. в статьях "Изменение предустановленных паролей (Oracle)", "Изменение предустановленных паролей (PostgreSQL)".
5. Запустите процессы Traffic Monitor:
   `iwtm start`

При замене пароля следуйте рекомендациям, приведенным в статье "Приложение A. Рекомендации по составлению имен и паролей".

## 4.2 Настройка защиты от подбора паролей

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

По умолчанию защита отключена.

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

Чтобы включить защиту для сервера Traffic Monitor:

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

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

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

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

**Пример** настроек защиты для Traffic Monitor:

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

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

## 4.3 Предварительные настройки

После установки системы необходимо выполнить следующие настройки:

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

### 4.3.1 Настройка синхронизации времени

1. Установите системное время с помощью команды `date`. Например, для установки 11 сентября 2013 13:30 запустите команду со следующими параметрами:
   `date 09111330`
2. Скопируйте системное время для настройки аппаратных часов с помощью команды:
   `hwclock --systohc`
3. Проверьте, что системное и аппаратное время настроены корректно:
   `hwclock ; date`
4. Время должно быть одинаковым, допустимы небольшие отклонения.Остановите службу ntpd:
   `systemctl stop ntpd`
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 ntpd:
   `systemctl start ntpd`
8. Проверьте текущее состояние службы ntpd с помощью команды:
   `systemctl status ntpd`
9. Включите автоматическую синхронизацию времени:
   `chkconfig --level 345 ntpd on`

### 4.3.2 Конфигурирование работы Sphinx при распределенной установке

При полнотекстовом поиске по запросам в Traffic Monitor используется механизм Sphinx. Служба **sphinx** устанавливается в режиме All-in-one или при установке шаблона Индексер**.** Сведения о режимах установки Системы приведены в документе «*InfoWatch Traffic Monitor. Руководство по установке*», статья "Схемы развертывания Системы и выбор типа установки".

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

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

## 4.4 Общие настройки

Раздел содержит информацию о настройке Системы и ее компонентов в случае различных вариантов установки:

- Настройка сервера на работу по технологии SPAN, или Port Mirroring;
- Перехват трафика, передаваемого по протоколу ICAP;
- Настройка работы "в разрыв" для нескольких перехватчиков.

### 4.4.1 Настройка сервера на работу по технологии SPAN, или Port Mirroring

Трафик снимается с управляемого коммутатора по технологии SPAN Port, или Port Mirroring.
Возможно несколько вариантов развертывания:
**Вариант 1**. Перехват и анализ копии трафика выполняется на одном компьютере (установка **All-in-one**). Кластер не создается:

1. Настройте сервер на работу в качестве Sniffer (см. "Настройка работы сервера Traffic Monitor в качестве Sniffer", вариант 2)
2. Настройте параметры приема копии трафика от Sniffer (см. "Настройка сервера Traffic Monitor на прием копии трафика от Sniffer").

**Вариант 2**. Перехват и анализ копии трафика выполняется на разных компьютерах, кластеризация не используется:

1. На одном компьютере (шаблон установки **Перехватчики**):
    a. Настройте сервер на работу в качестве Sniffer (см. "Настройка работы сервера Traffic Monitor в качестве Sniffer", вариант 1).
2. На другом компьютере (установка **All-in-one**):
    a. Настройте параметры приема копии трафика от Sniffer (см. "Настройка сервера Traffic Monitor на прием копии трафика от Sniffer").

**Вариант 3**. Перехват и анализ копии трафика выполняются на разных компьютерах. Для увеличения производительности создан кластер из двух экземпляров сервера Traffic Monitor:

1. Установите и настройте сервер СУБД ((шаблоны установки **База данных** и **Индексер**).
2. На компьютере, где будет работать Sniffer (шаблон установки **Перехватчики**):

a. Настройте его на работу в качестве Sniffer (см. "Настройка работы сервера Traffic Monitor в качестве Sniffer", вариант 1).

3. На компьютере, где будет работать экземпляр кластера Traffic Monitor (установка **All-in-one**):
   a. Настройте параметры приема копии трафика от Sniffer (см. "Настройка сервера Traffic Monitor на прием копии трафика от Sniffer").
   b. Укажите параметры кластеризации (см. "Создание кластера Traffic Monitor").
   c. Настройте сервер лицензирования (см. "Настройка сервера лицензирования (в случае кластера)")

Повторите п.3, чтобы добавить в кластер еще один экземпляр сервера Traffic Monitor.

## Настройка работы сервера Traffic Monitor в качестве Sniffer

Для того чтобы сервер Traffic Monitor работал в качестве Sniffer, следует выполнить ряд настроек конфигурационного файла.

В конфигурационном файле **sniffer.conf** укажите требуемые параметры в секции каждого из перехватчиков (секции `http`, `icq` и `smtp`):

| **Параметр** | **Пояснения** |
|---|---|
| `Interface` | Сетевой интерфейс, через который будут поступать данные от коммутатора |
| `OpenInSec (подсекция Timeouts)` | Время сохранения соединения (в сек) при отсутствии пакетов. Рекомендуемое значение – `600` |
| `LiveInSec (подсекция Timeouts)` | Время ожидания (сек), в течение которого соединение должно перейти в состояние *ESTABLISHED*. Если состояние не изменилось, то соединение автоматически прекращается. Рекомендуемое значение – 86400 |
| `CloseInSec (подсекция Timeouts)` | Время сохранения соединения (в сек) при переходе в состояние *TIME_WAIT*. Рекомендуемое значение – `300` |
| `TailInSec (подсекция Timeouts)` | Время ожидания доставки отправленных пакетов (в сек) после прекращения соединения |
| `QueueMemorySizeInBytes` | Объем памяти (в байтах), используемой для приема пакетов. При высокой загруженности канала, можно увеличить значение. Диапазон значений: от 1 до 500 Мб. Рекомендуемое значение – `16777216` |

1. Остановите серверные процессы Traffic Monitor:
   `iwtm stop`
2. Настройте автозапуск процессов:
   - Вариант 1. Перехват и анализ трафика будет выполняться на разных компьютерах.Настраиваемый экземпляр сервера Traffic Monitor будет работать только как Sniffer (перехват трафика):
     a. Включите автозапуск процесса **iw_sniffer**.

b. Отключите автозапуск других процессов.

> **Примечание:**
>
> Подробнее о включении и выключении автозапуска процессов см. "Автозапуск процессов".

- Вариант 2. Перехват и анализ копии трафика будет выполняться на одном компьютере. Сервер Traffic Monitor будет принимать копию трафика от коммутатора (функция Sniffer), анализировать полученные данные и загружать их в базу данных (функции сервера Traffic Monitor):
  a. Включите автозапуск процессов **iw_sniffer, iw_x2db, iw_updater, iw_warpd и iw_adlibitum**.
  b. Отключите автозапуск других процессов.

> **Примечание:**
>
> Подробнее о включении и выключении автозапуска процессов см. "Автозапуск процессов".

3. В файле **/opt/iw/tm5/etc/sniffer.conf**, в секции `iscp`, задайте параметры перехвата трафика:
   - `ListenHost`. IP-адрес, на который нужно принимать входящие соединения.
   - `ListenPort`. Порт, через который нужно принимать входящие соединения
4. Запустите процессы Traffic Monitor:
   `iwtm start`

### Настройка сервера Traffic Monitor на прием копии трафика от Sniffer

Настройка выполняется на компьютере с сервером Traffic Monitor. Настройка необходима также и в том случае, когда Sniffer и сервер Traffic Monitor установлены на одном компьютере.
Перейдите в директорию `/opt/iw/tm5/etc` и выполните настройки:

1. Включите автозапуск для нужных перехватчиков трафика (настройка для SMTP,HTTP(S), ICQ-трафика:
   i `wtm enable iw_proxy_http iw_proxy_smtp iw_proxy_icq`
   Чтобы настроить автозапуск перехватчика NRPC, смотрите "SPAN, или Port Mirroring".
2. Убедитесь, что в конфигурационном файле **proxy.conf** для параметра `SkipNegotiate` указано значение `false`.
3. Если необходимо перехватывать ICQ-трафик, передаваемый через прокси-сервер (поверх HTTP), то в конфигурационном файле **proxy.conf** установите `true` для параметра `IcqFilter`.
4. В конфигурационном файле **proxy.conf** в разделе `Iscp` секций `Smtp`, `Icq`, `Http` укажите значение параметров и `Host` и `Port`.

> **Пример:**

Для настройки взаимодействия с компьютером, имеющим IP-адрес 10.20.30.40 и порт **1234**, раздел `Iscp` для перехватчика ICQ будет выглядеть следующим образом:

```
"iscp": {
"ListenArea": "icq",
"Host": 10.20.30.40,
"Port": 1234
}
```

## Создание кластера Traffic Monitor

При перехвате копии трафика через Sniffer для увеличения производительности Системы можно создавать кластеры серверов Traffic Monitor.

**Важно!**

При использовании кластера сетевое соединение между Sniffer и сервером Traffic Monitor должно обеспечивать скорость передачи, в два раза превышающую ту скорость, с которой трафик поступает на Sniffer.

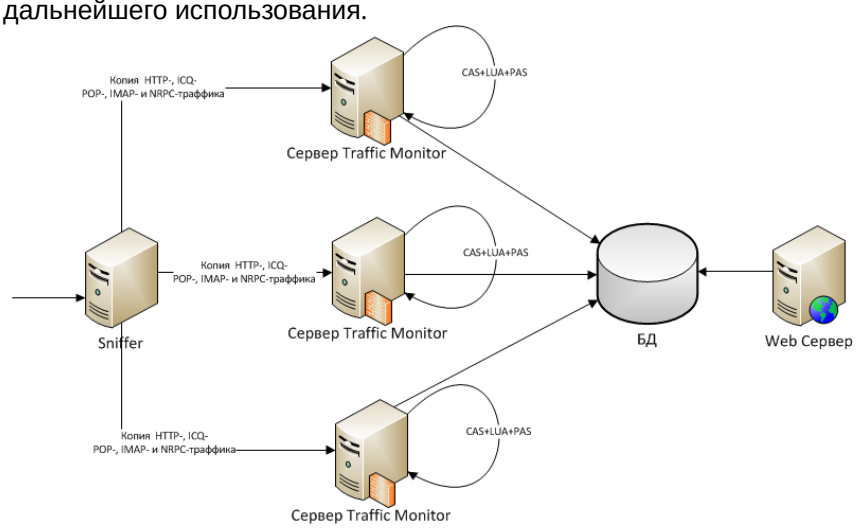
**Чтобы создать кластер серверов Traffic Monitor, на каждом экземпляре сервера Traffic Monitor, который будет входить в кластер, в конфигурационном файле /opt/iw/tm5/etc/sniffer.conf задайте параметры кластеризации:**

1. Убедитесь, что в конфигурационном файле секция `Usedareas` имеет следующий вид:
   ```
   "UsedAreas": [
   "capstack",
   "http",
   "icq",
   "smtp"
   ]
   ```
   По умолчанию данная настройка выполнена.
2. В конфигурационном файле **proxy.conf**, в разделе `Iscp` секций `Smtp`, `Icq`, `Http` укажите значение параметров `Host` и `Port`.
   Например,
   Для настройки взаимодействия с компьютером, имеющим IP-адрес 10.20.30.40 и порт **4301** (по умолчанию), раздел Iscp для перехватчика ICQ будет выглядеть следующим образом:
   ```
   "iscp": {
   "ListenArea": "icq",
   "Host": 10.20.30.40,
   "Port": 4301
   }
   ```
3. В конфигурационном файле **sniffer.conf** для каждой из секций `Smtp`, `Icq`, `Http` укажите значение параметра `Balancer`. Возможные значения:

- `Easy`. Для каждого нового TCP-соединения выбирается экземпляр Traffic Monitor Server с **iw_proxy**. Таким образом, поочередно задействуются все экземпляры сервера Traffic Monitor.
- `IpPref`. Распределение трафика между несколькими экземплярами сервера Traffic Monitor с **iw_proxy** выполняется на основании IP-адреса клиента. Это значит, что все данные с одинаковым IP-адресом клиента будут передаваться на один экземпляр сервера Traffic Monitor.

По умолчанию указан параметр `IpPref`.

**Пример. Создание кластера из нескольких (до трех) экземпляров сервера Traffic Monitor**
Система перехватывает копию SMTP-, ICQ- и HTTP-трафика через Sniffer. Для повышения производительности создается кластер из нескольких (в данном случае - трех) экземпляров сервера Traffic Monitor. С помощью параметра `Balancer` выбирается оптимальный тип нагрузки серверов Traffic Monitor. Эта опция позволяет избежать задержек в обработке данных и потерь пакетов данных. Сервера анализируют трафик с помощью технологий, и затем происходит запись данных в БД для дальнейшего использования.




## Настройка сервера лицензирования (в случае кластера)

Для корректного получения данных от перехватчиков в полном объеме необходимо настроить сервер лицензирования. Он должен быть включен на основном сервере Traffic Monitor и выключен на остальных нодах кластера.
Для этого на ноде:

1. Остановите службу **iw_licensed**:
   `iwtm stop licensed`
2. Выключите автозапуск службы **iw_licensed**:
   `iwtm disable iw_licensed`

На основном сервере Traffic Monitor:

1. Включите автозапуск службы **iw_licensed:**
   `iwtm enable iw_licensed`
2. Запустите службу **iw_licensed**:
   `iwtm start licensed`

Для установки, удаления, проверки валидности или запроса лицензии ознакомьтесь с разделом "Управление лицензиями" Руководства пользователя Traffic Monitor.

### 4.4.2 Перехват трафика, передаваемого по протоколу ICAP

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

> **Примечание:**
>
> Если в качестве прокси-сервера используется Blue Coat, то возможен также перехват HTTPS-трафика. Для этого прокси-сервер Blue Coat должен быть настроен так, чтобы полученный HTTPS-трафик обрабатывался и передавался на сервер Traffic Monitor как HTTP-трафик.

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

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

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

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

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

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

В этом разделе:


- Настройка ICAP;
- Рекомендации по настройке Blue Coat SG Series;
- Рекомендации по настройке SQUID;

- Рекомендации по настройке Cisco IronPort;
- Рекомендации по настройке McAfee Web Gateway;
- Рекомендации по настройке Fortinet FortiGate;
- Рекомендации по настройке UserGate;
- Отключение ICAP.

## Настройка ICAP

Модуль IW ICAP автоматически устанавливается вместе с сервером Traffic Monitor (установка All in one или шаблон Перехватчики). Автозапуск процесса **iw_icap** на сервере TM включен по умолчанию.

Перехват HTTP- и HTTPS-трафика осуществляется с использованием одних и тех же средств Системы, но различается настройка сторонних механизмов (см. ниже).
Для обеспечения перехвата HTTP(S)-трафика, передаваемого по протоколу ICAP, необходимо настроить параметры перехвата HTTP и HTTPS-запросов на прокси-сервере.

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

Возможны следующие варианты настройки ICAP:

1. Чтобы трафик передавался в режиме «Копия»:
   a. В конфигурационном файле **luaengined.conf**, расположенного в директории `/opt/iw/tm5/etc`, в секции `TransportModes` в свойстве `Icap` укажите действительное имя сервера TM (например, `tm-server1`) и значение режима `Copy`. Допускается указывать несколько пар значений:
   `"Icap": [{"Server": "tm-server1", "Mode": "Copy"}, {"Server":"tm-server2", "Mode": "Copy"}]`
   b. Сохраните изменения в файле **luaengined.conf.**
2. Чтобы трафик передавался вне зависимости от вынесенного вердикта:
   a. Задайте значение `Transparent` в вышеуказанном коде.
   b. Сохраните изменения в файле **luaengined.conf.**
3. Чтобы трафик передавался в режиме «Блокировка»:
   a. Задайте значение `Normal` в вышеуказанном коде.
   b. Сохраните изменения в файле **luaengined.conf.**
4. В конфигурационном файле **icap.conf**, расположенном в директории `/opt/iw/tm5/etc/`, укажите значение параметра `AsyncCheck` секции `Icap:`
   - `true` - режим "Копия",
   - `false` - режим "Блокировка".
5. Сохраните конфигурационный файл.
6. Перезапустите сервер Traffic Monitor:
   `iwtm restart`

> **Важно!**

Транспортный режим, настроенный в конфигурационном файле **luaengined.conf**, будет применен к SMTP- и HTTP(S)-перехватчикам. Чтобы выполнить более гибкую настройку см. "Настройка работы "в разрыв" для нескольких перехватчиков".

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

**Примечание:**

Данная настройка зависит от модификации прокси-сервера. Актуальную информацию по настройке Вы можете получить из документации к прокси-серверу.

В случае необходимости используйте рекомендации для настройки Blue Coat SG Series (см. "Рекомендации по настройке ICAP для Blue Coat SG Series ") и SQUID (см. "Рекомендации по настройке SQUID")

## Рекомендации по настройке Blue Coat SG Series

На прокси-сервере должно быть разрешено использование ICAP в режиме Request Mode, настроены параметры взаимодействия с сервером Traffic Monitor. Настройки выполняются через Web-интерфейс, от имени учетной записи администратора.

**Примечание:**

Процедура настройки, описанная ниже, может отличаться, в зависимости от версии и модели прокси-сервера.
Для перехвата HTTPS-трафика необходимо, чтобы в прокси-сервере была реализована возможность ssl инспекции (ssl-bump). Подробную информацию по этому вопросу Вы можете получить из документации к прокси-серверу.

1. Перейдите на вкладку **Configuration**.
2. Перейдите в раздел **External Services ► ICAP**. Создайте сервис **tm**. Задайте параметры сервиса:

- **Service URL**: `icap://<TM_server_IP>/reqmod`
  `Например: icap://10.60.0.20/reqmod`
- **Maximum number of connections**: `10`
- **Connection timeout**: `70`
- Установите флажок **This service supports plain ICAP connection**. В поле **Plain ICAP port** укажите порт **1344**.

**Важно!**

Значение поля **Plain ICAP port** должно совпадать со значением параметра `ListenPort` в файле `/opt/iw/tm5/etc/icap.conf`, секция Icap. Если параметр `ListenPort` имеет другое значение, то откорректируйте его.

    - На панели **ICAP v1.0 Options** настройте параметры:
    - **Method supported**: выберите **request modification**
    - **Send**: установите флажки **Authenticated User**, **Client address** и **Server address**.
- Перейдите в раздел **Health Checks ► General**. Убедитесь, что включена проверка состояния для серверов – на вкладке **Health Checks** отображаются адреса: `icap.tm`
- Проверьте доступность всех перечисленных серверов, нажав кнопку **Perform health check**.

## Рекомендации по настройке SQUID

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

В этой главе:

- Установка SQUID;
- Настройка ICAP;
- Настройка перехвата и раскрытия SSL;
- Настройка аутентификации пользователей.

### Установка SQUID

Перед установкой прокси-сервера SQUID нужно скачать rmp-пакет или архив (с последующей распаковкой) из репозитория или CD/DVD.

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

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

**При успешной установке пакета вы увидите:**

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

**Для доступа к конфигурационному файлу введите:**

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

### Настройка ICAP

Для настройки ICAP выполните:

1. Чтобы настроить ICAP, добавьте в конфигурационном файле **squid.conf** строчки для обработки ICAP:
   ```
   icap_enable on
   icap_service service_req reqmod_precache bypass=1 icap://10.60.7.7:1344/request
   adaptation_access service_req allow all
   icap_send_client_ip on
   icap_send_client_username on
   ```

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

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

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

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

3. Перезапустите **Squid**:
   `sudo service squid3 restart`

Настройка перехвата и раскрытия SSL

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

1. Создайте каталог для хранения сертификатов SQUID и измените его права так, чтобы пользователь **squid** владел ее содержимым:
   ```
   cd /etc/squid
   mkdir ssl_cert
   chown -R squid:squid /etc/squid/ssl_cert/
   ```
2. Сгенерируйте корневой сертификат для браузеров рабочих станций, трафик с которых будет прослушиваться.
3. Перенесите файл с расширением **.der** на Windows машины и установите его как доверенный сертификат в хранилище компьютера:
   ```
   openssl req -new -newkey rsa:1024 -days 720 -nodes -x509 -keyout /etc/
   squid/ssl_cert/IW.pem -out
   /etc/squid/ssl_cert/IW.pem
   openssl x509 -in /etc/squid/ssl_cert/IW.pem -outform DER -out /etc/squid/
   ssl_cert/IW.der
   ```
4. Создайте базу данных для подменяемых сертификатов и сделайте пользователя **squid** ее владельцем:
   ```
   /usr/lib64/squid/ssl_crtd -c -s /var/lib/ssl_db/
   chown -R squid:squid /var/lib/ssl_db/
   squid -k reconfigure
   ```

5. В конфигурационном файле **squid.conf** Закомментируйте настройку `http_port` и добавьте следующие строки:
```
#http_port 3128
http_port 3128 ssl-bump generate-host-certificates=on
dynamic_cert_mem_cache_size=4MB  cert=/etc/squid/ssl_cert/IW.pem
sslproxy_flags DONT_VERIFY_PEER
sslproxy_cert_error allow all
always_direct allow all
ssl_bump client-first all
ssl_bump server-first all
ssl_bump none all
sslcrtd_program /usr/lib64/squid/ssl_crtd -s /var/lib/ssl_db -M 4MB
```
6. Проверьте конфигурацию и перезапустите сервер **squid**:
```
squid -k reconfigure
service squid restart
```
7. Настройте браузер для использования нового прокси-сервера.

Настройка аутентификации пользователей

Работа SQUID по аутентификации заключается в декодировании HTTP заголовка `Authorization` и передаче декодированной информации стороннему модулю. Если предоставленная информация верна, то доступ пользователю предоставляется, если же она не верна или отсутствует, то SQUID возвращает клиенту HTTP ошибку с кодом 407. Таким образом, всю основную работу по проверке подлинности пользователей выполняют сторонние модули. Расположение этих модулей зависит от дистрибутива и версии SQUID. Например в Debian+SQUID3 они расположены в каталоге `/usr/lib/squid3`, в Red Hat скорее всего их расположение будет в `/usr/lib/squid`. Чтобы просмотреть, какие методы проверки подлинности поддерживает SQUID, размещение сторонних модулей и многие другие параметры, используйте команду `squid3 -v`:

```
squid -v
Squid Cache: Version 3.4.0.2
configure options: '--host=x86_64-redhat-linux-gnu' '--build=x86_64-redhat-
linux-gnu' '--program-prefix='
'--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin'
'--sysconfdir=/etc' '--datadir=/usr/share'
'--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec'
'--sharedstatedir=/var/lib'
'--mandir=/usr/share/man' '--infodir=/usr/share/info' '--exec_prefix=/usr' '--
libexecdir=/usr/lib64/squid'
'--localstatedir=/var' '--datadir=/usr/share/squid' '--sysconfdir=/etc/squid'
'--with-logdir=$(localstatedir)/log/squid' '--with-pidfile=$(localstatedir)/
run/squid.pid'
'--disable-dependency-tracking' '--enable-eui' '--enable-follow-x-forwarded-
for' '--enable-auth'
'--enable-auth-basic=DB,LDAP,MSNT,MSNT-multi-
domain,NCSA,NIS,PAM,POP3,RADIUS,SASL,SMB,getp
wnam' '--enable-auth-ntlm=smb_lm,fake' '--enable-auth-
digest=file,LDAP,eDirectory'
'--enable-auth-negotiate=kerberos,wrapper'
'--enable-external-acl-helpers=wbinfo_group,kerberos_ldap_group,AD_group' '--
enable-cache-digests'
'--enable-cachemgr-hostname=localhost' '--enable-delay-pools' '--enable-epoll'
'--enable-icap-client'
'--enable-ident-lookups' '--enable-linux-netfilter' '--enable-removal-
policies=heap,lru' '--enable-snmp'
```

```
'--enable-ssl' '--enable-ssl-crtd' '--enable-storeio=aufs,diskd,ufs,rock' '--
enable-wccpv2' '--enable-esi'
'--with-aio' '--with-default-user=squid' '--with-filedescriptors=16384' '--
with-dl' '--with-openssl' '--with-pthreads'
'--disable-arch-native' 'build_alias=x86_64-redhat-linux-gnu'
'host_alias=x86_64-redhat-linux-gnu'
'CFLAGS=-O2 -g' 'CXXFLAGS=-O2 -g -fPIC'
'PKG_CONFIG_PATH=/usr/lib64/pkgconfig:/usr/share/pkgconfig'
```

Взаимодействие и описание настроек сторонних модулей аутентификации производится с помощью параметра `auth_param`. Клиент будет поочередно пытаться использовать схемы аутентификации в том порядке, в котором они заданы в **squid.conf**. Новая настроенная схема аутентификации вступит в силу после перезапуска сервиса squid. Чтобы изменить существующие схемы без перезапуска сервиса, используйте команды `squid3 -k reconfigure` или `/etc/init.d/squid3 reload`.

Для контроля доступа в интернет, создайте acl, который будет задействовать настроенный модуль аутентификации. Для этого, acl в поле `тип_отбора` должен иметь значение `proxy_auth`, `proxy _auth_regex` или `external` с использованием переменной `%LOGIN`. Установите разрешение на доступ в параметре `http_access` для заданного acl. Ниже приведен формат указания типа используемой аутентификации (формат использования параметра `auth_param`):

```
auth_param схема_аутентификации параметры_схемы [значения_параметров]
```

## Рекомендации по настройке Cisco IronPort

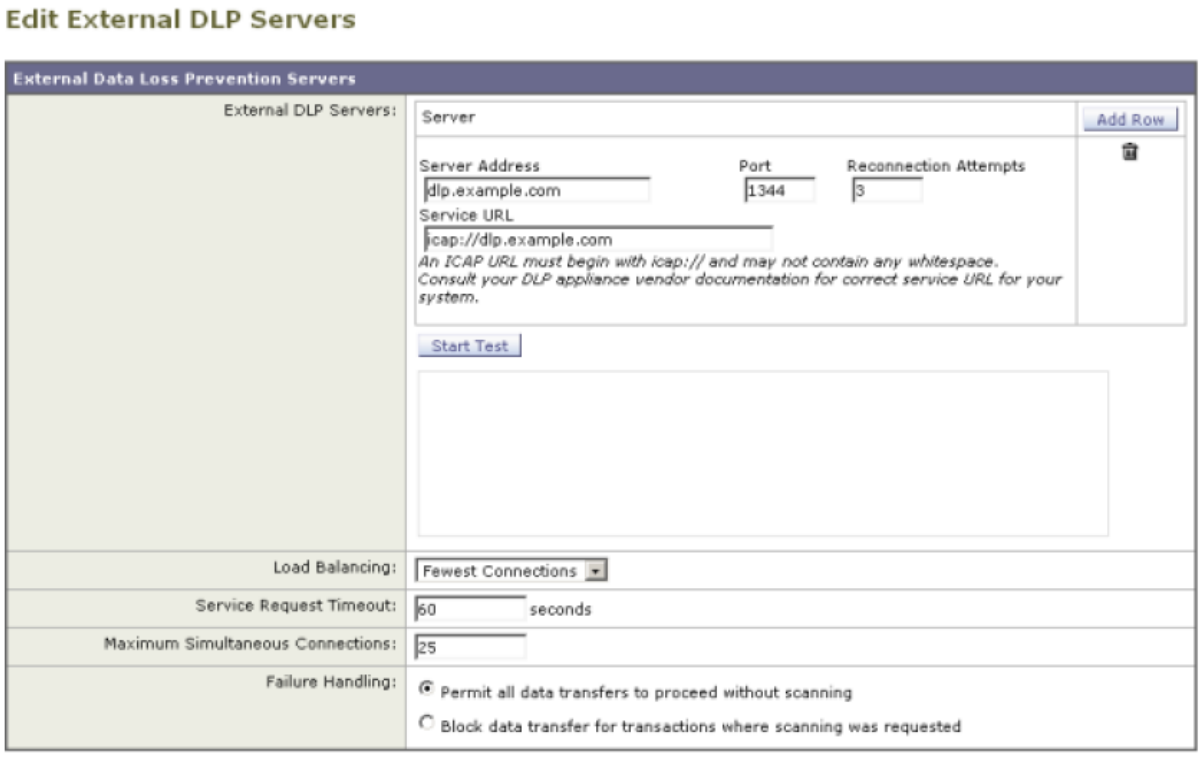
Для настройки Cisco IronPort как ICAP-клиента:

- Добавьте Traffic Monitor в качестве внешнего DLP сервера
- Создайте и настройте внешнюю DLP политику

**Чтобы добавить внешний DLP сервер:**

1. В веб-браузере откройте консоль управления Cisco IronPort:
   `https://<Cisco IronPort hostname or IP-address>:8443`
2. Перейдите в раздел **Network > External DLP Servers**.

3. В открывшемся окне нажмите кнопку **Edit Settings**.




4. Заполните поля в соответствии с таблицей:

| **Параметр настройки** | **Необходимое значение** |
|---|---|
| External DLP Servers | Необходимо заполнить следующие поля, касающиеся внешнего сервера фильтрации исходящего трафика (в данном случае это Traffic Monitor):<br>• **Server address and port**. Доменное имя машины и номер порта, на которой работает ICAP-сервер Traffic Monitor<br>• **Reconnection attempts**. Количество попыток соединения с ICAP-сервером Traffic Monitor. Рекомендуется указать значение 5.<br>• **DLP Service URL.** Адресная строка ICAP-сервера Traffic Monitor. Необходимо, чтобы данный URL начинался с `icap://`. Пример: `icap://FQDN:1344/reqmod` |
| Load Balancing | Балансировка нагрузки. В том случае, если для фильтрации трафика используется только один ICAP-сервер Traffic Monitor необходимо указать значение Fewest Connections. |
| Service Request Timeout | Таймаут, в течении которого Cisco IronPort ожидает отклика от ICAP-сервера Traffic Monitor. Значение по умолчанию `60` секунд. |

| | |
|---|---|
| Maximum Simultaneous Connections | Максимальное количество одновременных соединений Cisco IronPort с ICAP-сервером Traffic Monitor. Значение по умолчанию `25`, рекомендуется не изменять. |
| Failure Handling | Параметр, позволяющий задать поведение Cisco IronPort в том случае, если ICAP-сервер Traffic Monitor по каким-либо причинам недоступен. Рекомендуется установить значение Permit all data transfers to proceed without scanning. |

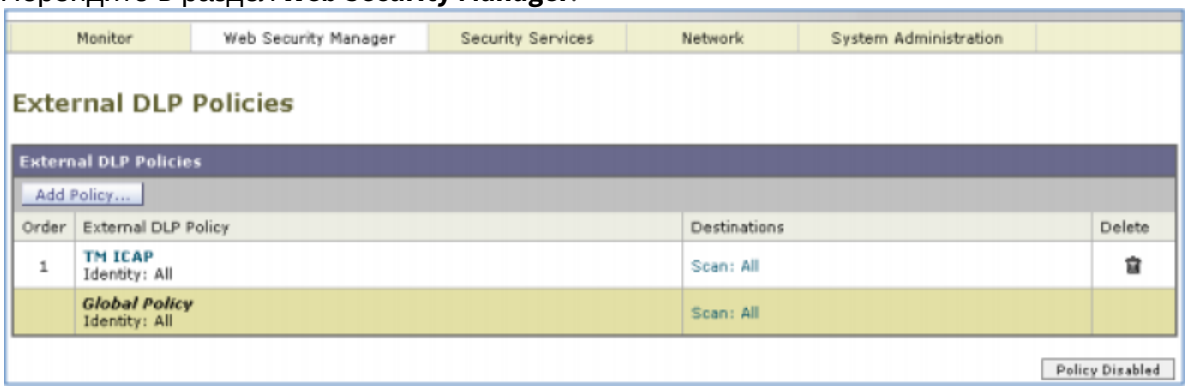
5. При необходимости задайте дополнительный ICAP-сервер, путем нажатия кнопки **Add Row**.
6. Проверьте связь с ICAP-сервером с помощью нажатия кнопки **Start Test**.
7. Нажмите **Submit** чтобы сохранить внесенные изменения.

**Чтобы создать внешнюю DLP политику:**

1. Перейдите в раздел **Web Security Manager**.
2. Нажмите кнопку **Add Policy**.
3. В поле **Policy Name** введите имя политики (например, TM ICAP)
4. В секции **Identities and Users** выберите пользователей или группу пользователей, которая будет контролироваться данной политикой.
5. Нажмите **Advanced** и в поле **Protocols** выберите HTTP.
6. Сохраните внесенные изменения.

**Чтобы настроить внешнюю DLP политику:**

1. Перейдите в раздел **Web Security Manager**:




2. Выберите политику в колонке **Destinations**.
3. В выпадающем списке **Edit Destination Settings** выберите значение **Define Destinations Scanning Custom Settings**.
4. В разделе **Destinations to scan** выберите **Scan All Uploads**.
5. Нажмите **Submit** чтобы сохранить внесенные изменения.

> **Примечание:**
>
> Cisco IronPort способен анализировать HTTPS-трафик. В этом случае осуществляется подмена сертификата, в результате чего HTTPS-трафик может быть дешифрован и обработан как HTTP. При этом взаимодействие между Cisco IronPort и Traffic Monitor по

протоколу ICAP остается неизменным. Дополнительная информация по настройке дешифрации HTTPS-трафика представлена в документации Cisco IronPort (см. раздел «Decryption Policies»).

## Рекомендации по настройке McAfee Web Gateway

Чтобы настроить интеграцию McAfee Web Gateway с Infowatch Traffic Monitor для мониторинга HTTP-трафика с использованием протокола ICAP:

1. Убедитесь, что на сервере Traffic Monitor работает служба **iw_icap**:
   `iwtm status`
2. В списке статусов найдите строку:
   ```
   Service iw_icap.service is active (running); enabled state: loaded (enabled)
   ```
3. Выполните вход в в веб-консоль McAfee Web Gateway.
4. Перейдите в раздел **Политика (Policy)**, а затем откройте вкладку **Настройки** (**Settings)**.
5. Выполните действия, чтобы создать клиент ICAP REQMOD:
   a. Щелкните правой кнопкой мыши на элементе **Клиент ICAP (ICAP Client)** и нажмите **Добавить (Add).**
   b. Введите имя, например *ICAP-REQMOD-Client.*
   c. На панели **Настройки для (Settings for)** выберите **Клиент Icap (ICAP Client).**
   d. На панели **Служба Icap (ICAP Service)** нажмите **Добавить (Add)**.
   e. Введите имя и нажмите **OK и Изменить (OK & Edit).**
   f. Щелкните **+Добавить сервер ICAP (+Add ICAP Server)**, затем введите IP-адрес и порт устройства MCAfee DLP Prevent.
   g. Нажмите **OK** три раза подряд.
6. Добавьте набор правил:
   a. Перейдите на вкладку **Наборы правил (Rule Sets)**.
   b. Выберите **Добавить (Add)** -> **Набор правил из библиотеки (Rule Set from Library)**.
   c. Выберите набор правил **Клиент ICAP (ICAP Client)** и нажмите **OK.**
7. Настройте параметры REQMOD:
   a. На вкладке **Наборы правил (Rule Sets)** разверните набор правил **Клиент ICAP (ICAP Client)** и выберите **ReqMod**.
   b. Выберите **Вызвать сервер ReqMod (Call ReqMOd Server)** и нажмите **Изменить (Edit)**.
   c. Выберите этап **Критерии выбора (Rule Criteria)**.
   d. Выберите **При соблюдении следующих условий (If the following criteria is mached).**
   e. Выберите критерий и нажмите **Изменить (Edit)**.
   f. В раскрывающемся списке **Настройки (Settings)** выберите созданный вами клиент ICAP REQMOD.
   g. Нажмите **OK**, а затем **Готово (Finish).**
8. Включите правило:
   a. На вкладке **Наборы правил (Rule Sets)** выберите правило **Клиент ICAP (ICAP Client)**.
   b. Выберите **Включить (Enable)**.
9. Нажмите **Сохранить изменения (Save settings)**.

## Рекомендации по настройке Fortinet FortiGate

FortiGate, как ICAP-клиент, позволяет передавать HTTP/HTTPS на ICAP-сервер в Traffic Monitor. Чтобы настроить работу FortiGate с ICAP-сервером выполните следующие шаги:

Шаг 1. Добавление нового ICAP-сервера:

1. В боковом меню перейдите в раздел **Security Profiles > ICAP Servers**.
2. Нажмите **Create New**.
3. В поле **Name** введите имя ICAP-сервера, например, `tm`.
4. Выберите используемую версию IP. По умолчанию: `Ipv4`.
5. В поле IP Adress укажите IP-адрес сервера Traffic Monitor, например, `10.60.20.30`.
6. В поле **Port** укажите номер порта. По умолчанию: `1344`.
7. Нажмите **OK**.

> **Важно!**
>
> Значение поля **Port** должно совпадать со значением параметра `ListenPort` в файле `/opt/iw/tm5/etc/icap.conf`, секция Icap. Если параметр `ListenPort` имеет другое значение, то откорректируйте его.
>
> Максимальное количество одновременных подключений к ICAP-серверу можно настроить в интерфейсе командной строки FortiGate (по умолчанию установлено 100 подключений). Например:
>
> ```
> config icap server
>     edit "tm"
>         set max-connections 200
> end
> ```

Шаг 2. Создание ICAP-профиля:

1. Перейдите в раздел настроек **Security Profiles > ICAP**.
2. Нажмите **Create New**.
3. В поле **Name** введите новое имя ICAP-профиля, например, `prof-tm`.
4. Включите настройку **Request Processing** и далее заполните данные:
    a. **Server** - укажите сервер Traffic Monitor : tm
    b. **Path** - укажите строку на выбор: `icap://10.60.20.30:1344/reqmod` (или `icap://10.60.20.30:1344/request)`
    c. **On Failure** - выберите:
        i. **Error**, чтобы заблокировать запрос (если сообщение не может быть обработано, оно не будет заблокировано)
        ii. **Bypass**, чтобы пропустить запрос.
5. Настройку **Response Processing** включать не требуется.
6. Включите настройку **Streaming Media Bypass,** чтобы не выгружать потоковые данные на ICAP-сервер.
7. Нажмите **OK**.

Шаг 3. Добавление ICAP-профиля в политику брендмауэра:

1. Перейдите в раздел настроек **Policy&Objects > IPv4 Policy**.
2. Нажмите **Create New**.
3. Настройте политику контроля трафика в соответствии с вашими потребностями.

4. Установите режим проверки **Proxy-based**.
5. В списке **Security Profiles** включите **ICAP** с профилем `prof-tm`.
6. Нажмите **OK**.

## Рекомендации по настройке UserGate

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

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

| Поле | Действие |
|---|---|
| Название | Введите название ICAP-сервера |
| Описание | Укажите описание ICAP-сервера (необязательное поле) |
| Адрес сервера | Введите IP-адрес ICAP-сервера |
| Порт | Введите TCP-порт ICAP-сервера. Значение по умолчанию: `1344` |
| Максимальный размер сообщения | Определяет максимальный размер сообщения, передаваемого на ICAP-сервер в килобайтах. Установите размер сообщения больше 0.<br>**Пример.** `35840` |
| Период проверки доступности сервера ICAP | Устанавливает время в секундах, через которое UserGate посылает OPTIONS-запрос на ICAP-сервер, чтобы убедиться, что сервер доступен.<br>**Пример.** `60` |
| Пропускать при ошибках | Если эта опция включена, то UserGate не будет посылать данные на ICAP-сервер в случаях, когда он недоступен (не отвечает на запрос OPTIONS). Включение не требуется. |
| Reqmod путь | Включите использование режима Reqmod, установив флаг **Вкл**.<br>Далее задайте **Путь на сервере ICAP для работы в режиме Reqmod** вида:<br>`icap://icap-server:port/path` - указание полного URI для режима reqmod.<br>**Пример.** `icap://FQDN:1344/reqmod` |

| Поле | Действие |
| --- | --- |
| Respmod путь | Включение режима Respmod не требуется. |
| Посылать имя пользователя | Установите флаг **Вкл,** чтобы включить отсылку имени пользователя на ICAP-сервер.<br>Далее задайте **Название заголовка**, которое будет использоваться для отправки имени пользователя на ICAP-сервер. Значение по умолчанию: `X-Authenticated-User`<br>При необходимости выберите **Кодировать в base64** - кодировать имя пользователя в base64. Это может потребоваться, если имена пользователей содержат символы национальных алфавитов. |
| Посылать IP-адрес | Если установлен флаг **Вкл,** то включается отсылка IP-адреса пользователя на ICAP-сервер.<br>Далее задайте **Название заголовка**, которое будет использоваться для отправки IP-адреса пользователя на ICAP-сервер. Значение по умолчанию: `X-Client-Ip`<br>Включение  не требуется. |
| Посылать MAC-адрес | Если установлен флаг **Вкл,** то включается отсылка MAC-адреса пользователя на ICAP-сервер.<br>Далее задайте **Название заголовка**, которое будет использоваться для отправки MAC-адреса пользователя на ICAP-сервер. Значение по умолчанию: `X-Client-Mac`<br>Включение не требуется. |

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

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

3. Создайте правило ICAP:

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

| Поле | Описание |
|---|---|
| Вкл/Выкл | Включает или отключает правило |
| Название | Название правила |
| Описание | Описание правила |
| Действие | Возможны следующие варианты:<br>• **Пропустить** - не посылать данные на ICAP-сервер. Создав правило с таким действием, администратор может явно исключить определенный трафик из пересылки на серверы ICAP;<br>• **Переслать** - переслать данные на ICAP-сервер и ожидать ответа ICAP-сервера. Стандартный режим работы ICAP-серверов;<br>• **Переслать и игнорировать** - переслать данные на ICAP-сервер и игнорировать ответ от ICAP-сервера. В этом случае, вне зависимости от ответа ICAP-сервера, данные к пользователю уходят без модификации, но сервер ICAP получает полную копию пользовательского трафика. |
| ICAP-серверы | Список ICAP-серверов, созданных на предыдущем шаге, на которые будет распределяться нагрузка |
| Источник | Зона источника трафика и/или списки IP-адресов источника трафика. |
| Пользователи | Список пользователей и групп, для которых применяется данное правило. Могут быть использованы пользователи типов: **Any, Unknown, Known**. Для применения правил к конкретным пользователям или к пользователям типа **Known** необходимо настроить идентификацию пользователей |
| Назначение | Зона назначения трафика и/или списки IP-адресов назначения трафика. |
| MIME-типы контента | Списки MIME-типов. Предусмотрена возможность управления видео-контентом, аудио-контентом, изображениями, исполняемыми файлами и другими типами. Также администратор может создать собственные группы MIME-типов. |
| Категории | Списки категорий UserGate URL filtering |

| Поле | Описание |
|---|---|
| URL | Списки URL |
| HTTP-метод | Метод, используемый в HTTP-запросах. Как правило, это POST или GET |
| Сервис | Возможны варианты:<br>• **HTTP** - веб-трафик;<br>• **SMTP** - почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа;<br>• **POP3** - почтовый трафик. Письма будут переданы на сервер ICAP в виде соответствующего MIME-типа |

**Важно!**

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

### Отключение ICAP

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

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

После отключения модуля верните исходные настройки прокси-сервера.

## 4.4.3 Настройка работы "в разрыв" для нескольких перехватчиков

Если в Системе одновременно используются схемы работы "в разрыв" для SMTP- и HTTP(S)-трафика, то для более гибкой настройки Системы внесите следующие изменения:

1. Войдите в систему от имени пользователя **root**
   `su - root`
2. Остановите процесс **iw_luaengined**:
   `iwtm stop iw_luaengined`

3. Откройте файл **luaengined.conf**, расположенный в директории `/opt/iw/tm5/etc`, на редактирование.
4. Для HTTP(S)-перехватчика в секции `TransportMode` в свойстве `Icap` укажите имя сервера Traffic Monitor с перехватчиком (например, `tm-server1`) и значение режима `Normal` (режим "Блокировка"). Допускается ввести несколько пар значений серверов и режимов:
   `"Icap": [{"Server": "tm-server1", "Mode": "Normal"}]`

   > **Важно!**
   >
   > При конфигурировании HTTP-перехватчика необходимо также отредактировать конфигурационный файл **icap.conf** в соответствии с выбранной схемой (см. "Настройка ICAP".)

5. Для SMTP-перехватчика в секции `TransportMode` в свойстве `Smtp` также укажите имя сервера Traffic Monitor с перехватчиком и значение режима `Normal` (режим "Блокировка"):
   `"Smtp": [{"Server": "tm-server1", "Mode": "Normal"}]`
6. Сохраните изменения в файле.
7. Запустите процесс **iw_luaengined**:
   `iwtm start iw_luaengined`

## 4.5 Настройка перехвата трафика

В Системе доступен перехват данных, передаваемых по перечисленным ниже протоколам.

| Протокол | Описание |
|---|---|
| SMTP (Simple Mail Transfer Protocol) | Почтовый протокол, используемый почтовым клиентом для отправки исходящих сообщений электронной почты на сервер. Работает в паре с протоколом POP3. |
| POP3 (Post Office Protocol, version 3) | Почтовый протокол, используемый почтовым клиентом для получения входящих сообщений электронной почты с сервера. Для отправки сообщений применяется протокол SMTP. |
| HTTP (HyperText Transfer Protocol) | Протокол передачи данных на основе технологии «клиент- сервер», используемый для получения текстовой информации, потокового видео и звука с веб-сайтов. Вы сможете осуществлять перехват всех передаваемых данных в сети Интернет (посещенных страниц, порталов, полученных и отправленных электронных писем, сообщений). |
| HTTP(S) | Расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTP, «упаковываются» в криптографический протокол, тем самым обеспечивается защита данных. |

| Протокол | Описание |
|---|---|
| OSCAR | Протокол обмена мгновенными и оффлайновыми текстовыми сообщениями, используемый программами ICQ, AIM, Miranda, QIP. Вы сможете перехватывать текстовые сообщения, передаваемые посредством вышеуказанных программ обмена мгновенными сообщениями.<br><br>**Важно!**<br><br>Перехват ICQ-трафика осуществляется, если используется отдельный сервер ICQ, поддерживающий работу по протоколу OSCAR. |
| NRPC | Протокол передачи почты в IBM Notes. |
| IMAP4 (Internet Mail Access Protocol) | Протокол доступа к электронной почте. Аналогично протоколу POP3, используется для работы с входящими электронными письмами, однако предоставляет более широкие возможности работы с почтовым ящиком. Например, доступ для обработки входящих сообщений, находящихся на сервере, как если бы они располагались на локальном компьютере получателя, без необходимости постоянной пересылки файлов с содержанием писем с сервера и обратно. Для отправки сообщений используется протокол SMTP. Вы сможете осуществлять перехват входящих электронных писем, передаваемых посредством почтовых клиентов. |

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

- Настройка перехвата SMTP-трафика;
- Настройка перехвата POP3-трафика;
- Настройка перехвата HTTP-трафика;
- Настройка перехвата HTTPS-трафика;
- Настройка перехвата ICQ-трафика;
- Настройка перехвата NRPC-трафика;
- Настройка перехвата IMAP4-трафика;
- Прием объектов, перехваченных InfoWatch Device Monitor.

**Важно!**

Предполагается, что Система уже установлена до начала настройки.
Сведения об установке для каждой из схем развертывания приведены в документе "InfoWatch Traffic Monitor. Руководство по установке".

**Важно!**

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

**Важно!**

На Агентах Device Monitor, установленных на компьютерах по управлением ОС Astra Linux или РЕД ОС, перехват почтового трафика осуществляется только по каналам SMTP, POP3 и IMAP.

### 4.5.1 Настройка перехвата SMTP-трафика

Раздел содержит информацию о том, как настроить перехват SMTP-трафика с использованием следующих технологий:

- SPAN, или Port Mirroring;
- Прием копий с почтового сервера;
- "В разрыв";
- Настройки почтовых серверов для перехвата SMTP-трафика.

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

#### SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. "Настройка сервера на работу по технологии SPAN, или Port Mirroring").
2. Включите возможность автозапуска для процесса iw_proxy_smtp, осуществляющего перехват SMTP-трафика:
   `iwtm enable iw_proxy_smtp`
3. Убедитесь, что включен автозапуск для процессов, участвующих в перехвате и обработке почты: **iw_sniffer**, **iw_proxy_smtp**, **iw_messed**, **iw_warpd**, **iw_cas**, **iw_x2db** (см. "Включение и выключение автозапуска процессов").
4. Чтобы избежать дублирования перехваченных данных, отключите процесс **iw_smtpd** (см. "Включение и выключение автозапуска процессов").

#### 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 Postfix реализуется следующим образом. Почтовый сервер Postfix, 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. На почтовом сервере настройте пересылку скрытых копий SMTP-сообщений (BCC - Blind Carbon Copy) на сервер Traffic Monitor. Пример настройки для Microsoft Exchange Server

2007 и 2010 приведен в статье "Настройка пересылки скрытых копий Microsoft Exchange Server 2007 и 2010".

3. Настройте встроенный в Систему Postfix (см. "Настройка сервера Postfix в системе Traffic Monitor").
4. Убедитесь, что включен автозапуск для процессов, участвующих в перехвате и обработке почты:
**postfix, iw_smtpd, iw_messed, iw_warpd,iw_luaengined, iw_cas, iw_pas, iw_x2x, iw_x2db, iw_tech-tools** (см. "Автозапуск процессов").
5. Убедитесь, что в **/opt/iw/tm5/etc/luaengined.conf** в параметре `"TransportModes"/" Sm t p"` установлен режим `Copy` или пустое значение.

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

**Важно!**

Выбранный режим будет применен и для SMTP-, и для HTTP(S)-перехватчиков. Описание более гибкой настройки приведено в статье "Настройка работы "в разрыв" для нескольких перехватчиков".

**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:

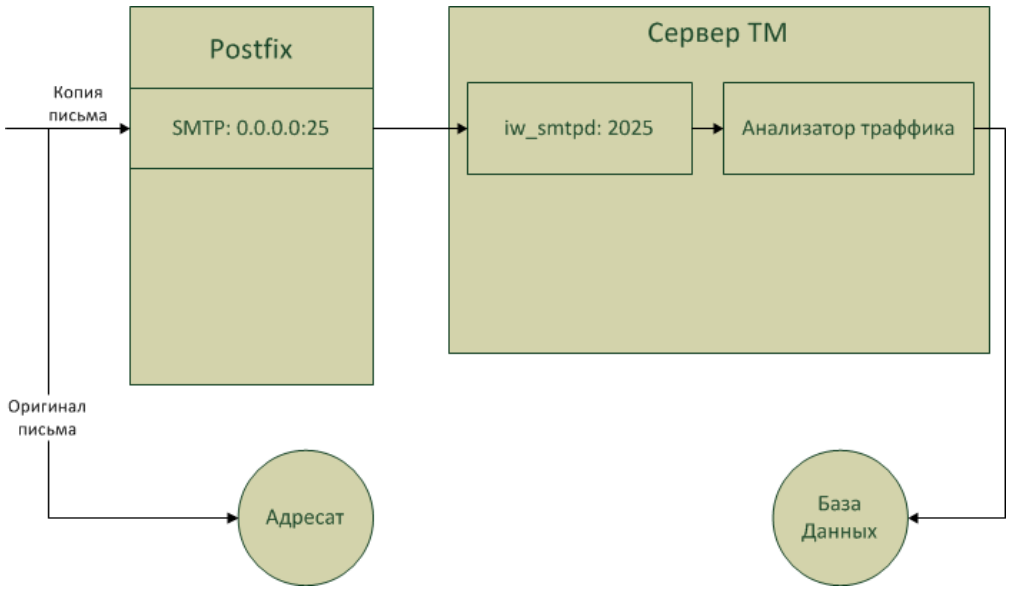
```
"ExchangeJournalReports": true,
```

Чтобы опция стала активной, повторно загрузите конфигурацию или перезапустите службу.

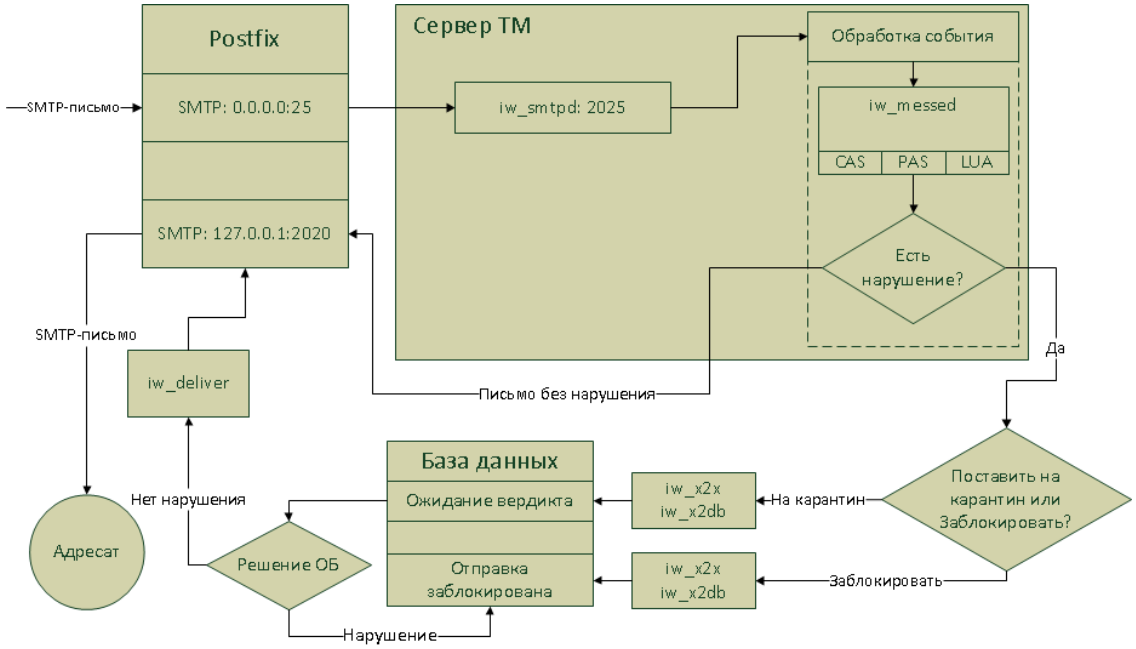
## "В разрыв"

Сервер Traffic Monitor используется как промежуточный почтовый сервер. В его состав входит почтовый сервер Postfix.
Интеграция сервера Traffic Monitor с почтовым сервером реализуется следующим образом. Почтовый сервер Postfix, встроенный в систему Traffic Monitor, принимает входящие SMTP-письма на **25** порт. Далее входящие SMTP-письма передаются процессу **iw_smtpd** на порт **2025**. В Системе создается событие для каждого из писем. В зависимости от схемы работы (Копия или Блокировка), возможны следующие варианты движения SMTP-трафика:

- Режим Копия – SMTP-трафик передается адресату, а также с помощью Postfix - в InfoWatch Traffic Monitor.




- Режим Блокировка – SMTP-трафик анализируется системой Traffic Monitor, и
  - если нарушение отсутствует, SMTP-трафик с помощью встроенного сервера Postfix передается адресату или следующему relay-серверу в почтовой системе организации. Доставка осуществляется так: процесс **iw_messed** передает письма на порт **2020** почтового сервера Postfix. Почтовый сервер Postfix либо напрямую доставляет письма адресатам, либо передает их следующему почтовому relay-серверу;
  - если обнаружено нарушение, и в политиках указан вердикт *Поместить на карантин*, то Система выставляет письму вердикт *Карантин*. Письмо будет доставлено только в том случае, если Офицер безопасности выставит вердикт *Нет нарушения,* разрешая доставку письма в Консоли управления (см. документ «InfoWatch Traffic Monitor. Руководство пользователя»). Доставка осуществляется следующим образом: процесс **iw_deliver** передает письма на порт **2020** почтового сервера Postfix, встроенного в Систему. Почтовый сервер Postfix либо напрямую доставляет письма адресатам, либо передает их следующему почтовому relay-серверу;
  - если обнаружено нарушение, и в политиках указан вердикт *Заблокировать*, то Система выставляет письму вердикт *Заблокировано*. Доставка письма в данном случае будет заблокирована, а событие помещено в Базу данных.




**Чтобы настроить работу "в разрыв", выполните следующие действия:**

1. На корпоративном почтовом сервере в качестве relay-сервера настройте сервер Traffic Monitor.

   > **Примечание:**
   >
   > Если в организации используется более одного почтового сервера, каждый из них должен быть настроен на отправку исходящих сообщений на встроенный в Систему сервер Postfix. В зависимости от того, какой почтовый сервер используется в компании, данная настройка может различаться

   В результате данной настройки весь почтовый трафик от корпоративного почтового сервера будет направляться только на сервер Traffic Monitor.
2. Убедитесь, что включен автозапуск процессов **iw_smtpd** и **iw_deliver** (см. "Автозапуск процессов").
3. Настройте встроенный в Систему Postfix (см. "Настройка сервера Postfix в системе Traffic Monitor").
4. Остановите процесс **iw_luaengined**:
   `iwtm stop iw_luaengined`
5. Откройте файл **luaengined.conf**, расположенный в директории `/opt/iw/tm5/etc`, на редактирование.
6. В секции `TransportMode` в свойстве `Smtp` укажите имя сервера Traffic Monitor с перехватчиком (например, `tm-server1`) и значение режима `Normal` (режим "Блокировка"):
   `"Smtp": [{"Server": "tm-server1", "Mode": "Normal"}]`

**Важно!**

При распределенной установке режим определяется процессом **iw_luaengined**, расположенному локально или на другой ноде кластера. Поэтому на каждой ноде в файле `/opt/iw/tm5/etc/luaengined.conf` в секции `TransportModes` в свойстве `Smtp` укажите несколько пар значений действительных адресов серверов ТМ и нужных режимов. Например:

```
"Smtp": [{"Server": "tm-server1", "Mode": "Copy"},
{"Server":"tm1.org.ru", "Mode": "Normal"}]
```

**Важно!** Файл **iwssid.lua** при этом должен быть одинаковым на всех нодах.

7. Сохраните файл.
8. Перезагрузите Систему:
   `iwtm restart`

Чтобы трафик передавался вне зависимости от вынесенного вердикта:

1. В коде, указанном выше в пункте 5, задайте параметру `TransportMode` значение `'Transparent'` .
2. Выполните шаги 6 и 7.

**Важно!**

Выбранный режим будет применен только для SMTP-перехватчика. Описание более гибкой настройки приведено в статье " Настройка работы "в разрыв" для нескольких перехватчиков ".

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

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

SMTP-письмо будет досылаться при соблюдении одновременно всех условий:

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

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

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

## Настройки почтовых серверов для перехвата SMTP-трафика

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

- Настройка пересылки скрытых копий Microsoft Exchange Server 2007 и 2010;
- Настройка пересылки скрытых копий ZCS Zimbra;
- Настройка пересылки скрытых копий MDaemon;
- Настройка сервера Postfix в системе Traffic Monitor.

### Настройка пересылки скрытых копий Microsoft Exchange Server 2007 и 2010

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

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

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

Окно мастера создания коннектора будет закрыто.

**Создание контакта, на который будут перенаправляться копии почтовых сообщений**

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

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

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

Окно мастера создания контакта будет закрыто.

**Важно!**

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

**Создание транспортного правила для копирования писем**

1. Выберите узел **Organization Configuration -> HubTransport** и нажмите **New Transport Rule**.
2. В открывшемся окне мастера создания транспортного правила введите имя создаваемого правила и установите флажок в поле **EnableRule**. Нажмите **Next**.
3. На шаге **Conditions** установите флажок для условия **from users inside or outside the organization**. В качестве параметра условия выберите **Inside**. Нажмите **Next**.
4. На шаге **Actions** установите флажок для действия **Blind carbon copy (Bcc) the message to address**. Нажмите на гиперссылку с параметром **address** и в открывшемся окне **Select Recepient** выберите ранее созданный контакт, затем нажмите **OK**. В окне мастера создания транспортного правила нажмите **Next**.
5. При необходимости на шаге **Exceptions** Вы можете настроить исключения из правила. Например, чтобы не выполнять копирование писем, отправляемых определенными пользователями, установите флажок в поле **except when the message is from people** и в параметрах исключения выберите желаемых пользователей. Нажмите **Next**.
6. На шаге **Create Rule** убедитесь, что параметры правила заданы верно, и нажмите **New**. Дождитесь окончания процесса создания и нажмите **Finish**.

**Блокирование отправки сообщений при недоступности сервера TM**

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

**Важно!**

Если в MS Exchange используется правило журналирования, для корректной обработки этих писем включите 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.

Настройка пересылки скрытых копий ZCS Zimbra

**Важно!**

Все команды должны выполняться из-под пользователя **zimbra**.

**Настройка транспортной таблицы**

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

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

**Важно!**

Данная команда должна быть выполнена через **zmlocalconfig**. В данной ситуации редактирования **main.cf** будет недостаточно.

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

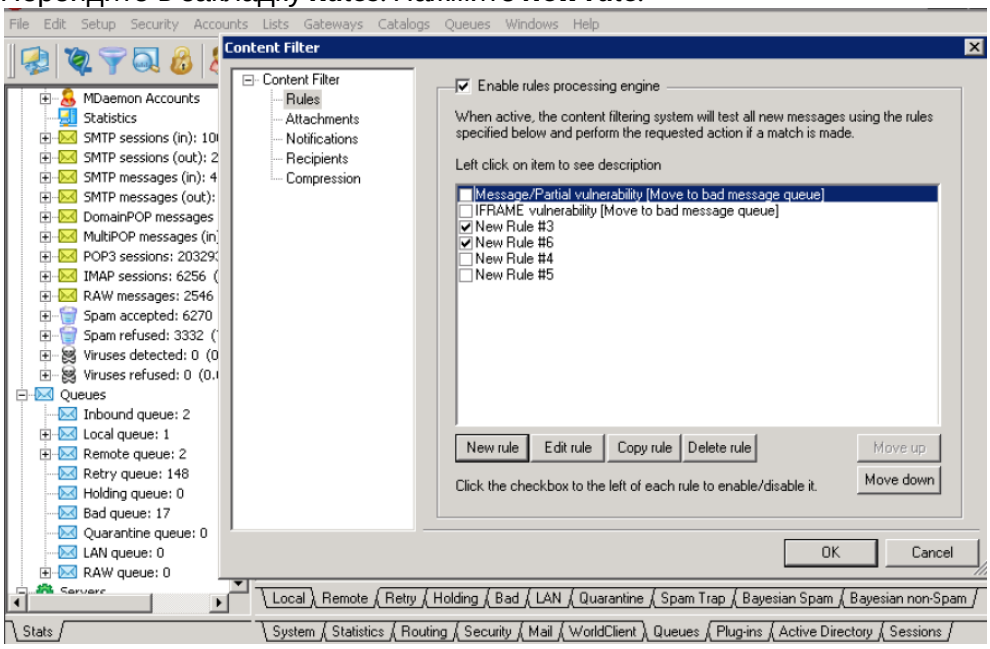
**Настройка отправки BCC**

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

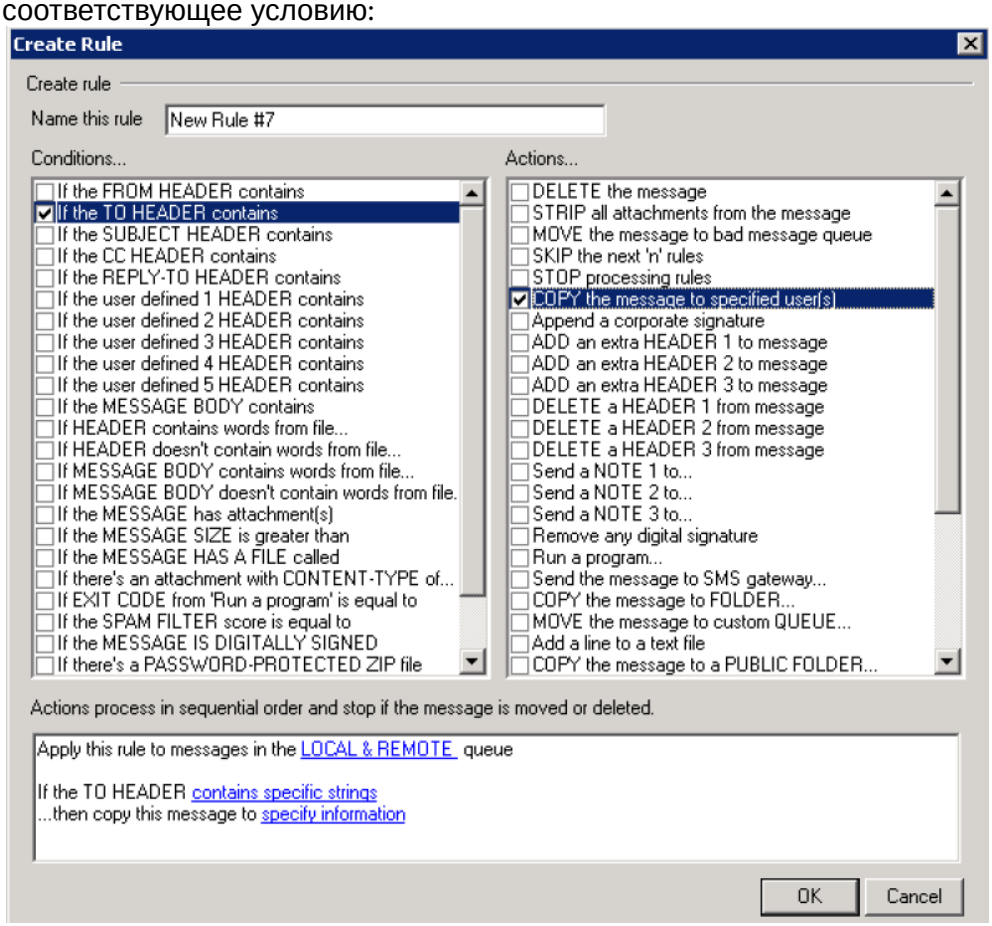
Настройка пересылки скрытых копий MDaemon

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

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



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




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

Настройка сервера Postfix в системе Traffic Monitor

Необходимость настройки встроенного в Систему Postfix определяется в зависимости от схемы развертывания Системы и от того, установлен ли сервер ТМ на один компьютер с базой данных:

| **Вариант развертывания Системы** | | **Настройка Postfix** |
|---|---|---|
| Доставка SMTP-трафика осуществляется корпоративной почтовой системой. Система Traffic Monitor получает только копию SMTP-трафика. Для корректного приема копии трафика рекомендуется выполнить настройку Postfix | Сервер ТМ установлен отдельно от базы данных | Обязательна |
| | Все компоненты установлены на один сервер | Выполнена по умолчанию |

| Вариант развертывания Системы | | Настройка Postfix |
|---|---|---|
| Система Traffic Monitor осуществляет перехват и доставку SMTP-трафика посредством интеграции с Postfix | Сервер TM установлен отдельно от базы данных | Обязательна |
| | Все компоненты установлены на один сервер | Выполнена по умолчанию |
| Система получает копию SMTP-трафика через Sniffer | | Не требуется |
| Перехват SMTP-трафика не требуется (например, Traffic Monitor будет использоваться только как Sniffer) | | Не требуется |

Для корректного взаимодействия системы InfoWatch Traffic Monitor со встроенным в Систему почтовым сервером Postfix внесите следующие изменения в конфигурационные файлы **/etc/postfix/main.cf** и **/etc/postfix/master.cf**:

1. Войдите в систему от имени пользователя **root**:
   `su - root`
2. В файле **main.cf** настройте значения параметра `inet_interfaces` в соответствии с рекомендациями, указанными на сайте Postfix: http://www.postfix.org/postconf.5.html. В большинстве случаев достаточно указать значение параметра: `inet_interfaces = all`
3. В файле **main.cf** настройте значения параметра `message_size_limit` в соответствии с рекомендациями, указанными на сайте Postfix: http://www.postfix.org/postconf.5.html. Значение параметра по умолчанию: `message_size_limit = 50000000`
4. Если InfoWatch Traffic Monitor будет участвовать в доставке SMTP-трафика (см. "В разрыв"):

- в файле **main.cf** задайте параметр `relayhost`. В качестве значения введите IP-адрес корпоративного почтового сервера, на который будут передаваться SMTP-письма после анализа в Traffic Monitor, и пароль доступа к почтовому серверу. Например:
  `relayhost = [smtp.organization.ru]:password`
- отредактируйте файл **master.cf**, дописав в конец файла следующие строки:

> **Важно!**
>
> Строки, задающие опции сервиса, должны начинаться с пробела. Например: " `-o <спецификация опции>` "

```
127.0.0.1:2020   inet  n   -   n  -   21   smtpd
     -o content_filter=
     -o local_recipient_maps=
     -o relay_recipient_maps=
     -o smtpd_restriction_classes=
     -o smtpd_client_restrictions=
     -o smtpd_helo_restrictions=
```

```
    -o smtpd_sender_restrictions=
    -o mynetworks=127.0.0.0/8
    -o strict_rfc821_envelopes=yes
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o myhostname=<полное_доменное_имя_сервера>
```

- В файле **main.cf** проверьте, что в параметре `mynetworks` корректно указана подсеть, где расположены почтовые серверы.
- В файле **master.cf** для обеспечения пересылки почты на проверку в TM добавьте следующую строку:
`smtp inet n - n - - smtpd -o content_filter=smtp:127.0.0.1:2025`

> **Примечание:**
>
> При установке с помощью инсталлятора данная настройка устанавливается автоматически.

- Проверьте корректность синтаксиса файлов конфигурации:
`postfix check`
- Перезапустите Postfix:
`systemctl restart postfix`
- Проверьте доступность почтового сервера Postfix по порту **25** с помощью следующей команды в командной строке:
`telnet <TM_ip> 25`
где `<TM_ip>` - IP-адрес сервера Traffic Monitor, на котором настроен Postfix.
В ответ на данную команду в командной строке должно отобразиться сообщение:
`Connected to mail.server.com`

> **Примечание:**
>
> Если клиент Telnet не установлен, Вы можете установить его как компонент MS Windows 2008-2012, либо использовать вместо него приложение Putty.

Если установить соединение не удалось, поэтапно проверьте настройки подсетей и портов в зависимости от конфигурации сети

.

### 4.5.2 Настройка перехвата POP3-трафика

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. "Настройка сервера на работу по технологии SPAN, или Port Mirroring").
2. Убедитесь, что в конфигурационном файле **/opt/iw/tm5/etc/sniffer.conf** поле `Hi Port` секции `capstack` имеет значение `110`:

```
"ListenAreas": {
 "capstack": {
 "Balancer": "IpPref",
 "Interface": "eth1",
 "MaxClient": 16,
 "QueueMemorySizeInBytes": 67108864,
 "Rules": [
```

```
{
"HiPort": 110,
"IP": "0.0.0.0",
"LoPort": 110,
"Mask": "0.0.0.0",
"Policy": "ACCEPT"
```

3. В конфигурационном файле **/opt/iw/tm5/etc/capstack.conf** укажите значение `true` для поля `pop3` в секции `UsedProcessor`.

### 4.5.3 Настройка перехвата HTTP-трафика

Описание данного способа перехвата трафика см. в статье "Схема перехвата HTTP-трафика".

#### SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. "Настройка сервера на работу по технологии SPAN, или Port Mirroring").
2. Включите автозапуск перехватчика HTTP-трафика:
   `iwtm enable iw_proxy_http`
3. Убедитесь, что включен автозапуск для служб, участвующих в перехвате и обработке HTTP-трафика:
   **iw_sniffer**, **iw_warpd**, **iw_cas**, **iw_x2db** (см. "Включение и выключение автозапуска процессов").

#### "В разрыв" (HTTP)

> **Примечание:**
>
> В данном пункте описана схема "в разрыв" для трафика, передаваемого по протоколу ICAP - не путайте со схемой "в разрыв" для трафика, передаваемого по протоколу SMTP.

**Чтобы настроить работу "в разрыв", выполните следующие действия:**

1. Ознакомьтесь с описанием данной схемы работы (см. "Перехват трафика, передаваемого по протоколу ICAP").
2. Настройте параметры перехвата HTTP-запросов на прокси-сервере (см. "Настройка ICAP").

### 4.5.4 Настройка перехвата HTTPS-трафика

Описание данного способа перехвата трафика см. в статье "Схема перехвата HTTPS-трафика".

#### "В разрыв" (HTTPS)

> **Примечание:**

В данном пункте описана схема "в разрыв" для трафика, передаваемого по протоколу ICAP - не путайте со схемой "в разрыв" для трафика, передаваемого по протоколу SMTP.

**Чтобы настроить работу "в разрыв", выполните следующие действия:**

1. Ознакомьтесь с описанием данной схемы работы (см. "Перехват трафика, передаваемого по протоколу ICAP").
2. Настройте параметры перехвата HTTPS-запросов на прокси-сервере (см. "Настройка ICAP").
3. Включите разбор HTTPS-трафика на прокси-сервере.

   **Примечание:**

   Данная настройка зависит от модификации прокси-сервера. Актуальную информацию по настройке вы можете получить из документации к прокси-серверу.

4. Добавьте сертификат в список доверенных корневых сертификатов браузера каждой рабочей станции, контроль исходящего HTTPS-трафика с которой планируется.

   **Примечание:**

   Информацию по настройке вы можете получить из документации к браузеру.

### 4.5.5 Настройка перехвата ICQ-трафика

Описание данного способа перехвата трафика см. в статье "Схема перехвата ICQ-трафика".

#### SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. "SPAN, или Port Mirroring").
2. Включите автозапуск перехватчика ICQ-трафика:
   `iwtm enable iw_proxy_icq`

### 4.5.6 Настройка перехвата NRPC-трафика

Описание данного способа перехвата трафика см. в статье "Схема перехвата NRPC-трафика".

#### SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. "SPAN, или Port Mirroring").
2. Откройте на редактирование конфигурационный файл **capstack.conf**, расположенный в директории `/opt/iw/tm5/etc`.
3. Убедитесь, что в секции `Usedprocessors` включен перехватчик NRPC-трафика:
   ```
   "UsedProcessors": {
   "nrpc": true,
   ```

4. Убедитесь, что в секции `Processors` включена передача NRPC-трафика:
```
"processors": {
"nrpc": {
"TrackExternal": true,
"TrackInternal": true
},
```
5. Сохраните файл **capstack.conf**.
6. Включите автозапуск процесса **iw_capstack**:
```
iwtm enable iw_capstack
```
7. Перезапустите процесс **iw_capstack**:
```
iwtm restart capstack
```

### 4.5.7 Настройка перехвата IMAP4-трафика

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. "SPAN, или Port Mirroring").
2. Убедитесь, что в конфигурационном файле **/opt/iw/tm5/etc/sniffer.conf** поле `HiPort` секции `capstack` имеет значение `143`:
```
"ListenAreas": {
"capstack": {
"Balancer": "IpPref",
"Interface": "eth1",
"MaxClient": 16,
"QueueMemorySizeInBytes": 67108864,
"Rules": [
{
"HiPort": 143,
"IP": "0.0.0.0",
"LoPort": 110,
"Mask": "0.0.0.0",
"Policy": "ACCEPT"
```
3. В конфигурационном файле **/opt/iw/tm5/etc/capstack.conf** укажите значение `true` для поля `imap4` в секции `UsedProcessor`.

### 4.5.8 Прием объектов, перехваченных InfoWatch Device Monitor

1. Установите и настройте серверную часть Traffic Monitor (см. документ "*InfoWatch Traffic Monitor. Руководство по установке*", статья "Установка InfoWatch Traffic Monitor").
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").

## 4.6 Автозапуск процессов

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

- Проверка автозапуска процессов;
- Включение и выключение автозапуска процессов.

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

### 4.6.1 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<br>**Примечание:** Процесс должен работать только на основном сервере |
| iw_agent | Да |
| iw_analysis | Да |
| iw_kicker | Да<br>**Примечание:** Процесс должен работать только на сервере с веб-консолью |
| iw_blackboard | Да |
| iw_bookworm | Да<br>**Примечание:** Процесс должен работать только на основном сервере |
| iw_capstack | Нет |
| iw_cas | Да |
| iw_configerator | Да<br>**Примечание:** Процесс должен работать только на сервере с веб-консолью |
| iw_deliver | Да<br>**Примечание:** Процесс должен работать только на основном сервере |

| Процесс | По умолчанию автозапуск включен |
| --- | --- |
| iw_icap | Да |
| iw_is | Да<br>**Примечание:** Процесс должен работать только на основном сервере |
| iw_indexer | Да<br>**Примечание:** Процесс должен работать только на основном сервере |
| iw_image_autoling | Да<br>**Примечание:** Процесс должен работать только на сервере с веб-консолью |
| iw_text_autoling | Да<br>**Примечание:** Процесс должен работать только на сервере с веб-консолью |
| iw_licensed | Да<br>**Примечание:** Процесс должен работать только на основном сервере |
| iw_luaengined | Да |
| iw_messed | Да |
| iw_proxy_http<br>iw_proxy_icq<br>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 |

| Процесс | По умолчанию автозапуск включен |
|---|---|
| iw_tech_tools | Да |
| iw_updater | Да |
| iw_warpd | Да |
| iw_x2x | Да |
| iw_x2db | Да |
| iw_xapi_xapi<br>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".

### 4.6.2 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`

## 4.7 Модуль взаимодействия с удаленной базой данных

Если схема развертывания Системы выбрана таким образом, что база данных, в которую передаются перехваченные объекты, находится на удаленном сервере, то 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

### 4.7.1 Настройка сбора данных в филиальной сети

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

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

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

- **iw_qmover_server** - в первую очередь;
- **iw_qmover_client** - во второю 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").

### 4.7.2 Настройка клиентской части модуля взаимодействия с удаленной БД

**Настройка общих параметров**

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

| Параметр | Описание |
|---|---|
| `ListenerIP` | IP-адрес сервера (служба **qmover_server**) |
| `Port` | Порт сервера (центральный офис) |
| `NookDir` | Рабочий каталог службы **qmover_server** |
| `ChannelWidth` | Ширина полосы пропускания канала, скорость закачки данных в Traffic Monitor (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
```

### 4.7.3 Настройка серверной части модуля взаимодействия с удаленной БД

**Настройка конфигурации**

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

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

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

**Настройка автозапуска**

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

## 4.8 Настройка OCR-экстракторов

Настройка OCR для различных перехватчиков производится в 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 анализа событий из которых в Traffic Monitor может использоваться OCR.

| Сервис | Тип события | Протокол |
|---|---|---|
| Почта | Email | POP3<br>SMTP<br>IMAP<br>MAPI<br>NRPC |
| | Web-почта | HTTP |

| Сервис | Тип события | Протокол |
|---|---|---|
| | | HTTPS |
| Мессенджер | ICQ | OSCAR |
| | Skype | SKYPE |
| | XMPP | XMPP |
| | MS Lync | SIP |
| | Telegram | - |
| | Vkontakte | HTTPS |
| | Facebook | HTTPS |
| | WhatsApp | WhatsApp |
| Интернет-активность | Web-сообщение | HTTP<br>HTTPS |
| Обмен файлами | FTP | FTP |
| | Внешнее устройство | - |
| | Облачные хранилища | HTTPS |
| Принтер и МФУ | Печать | - |
| Запись мультимедиа | Фотосъемка | - |

При установке с помощью инсталлятора 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 4.1.1.

Функциональные ограничения экстракторов приведены в таблице ниже:

| Функциональность | ABBYY FineReader Engine 11 | Tesseract 4.1.1 |
|---|---|---|
| Распознавание углов поворота изображения | 0(+/-20) , 90(+/-20), 180(+/-20) и 270( + /-20) градусов | - |
| Распознавание цветного изображения | + | - |

| Функциональность | ABBYY FineReader Engine 11 | Tesseract 4.1.1 |
|---|---|---|
| Коррекция изображения | + | - |
| Рекомендуемое разрешение изображения | 300dpi для текста с размером шрифта от 10pt<br>400-600dpi для текста с размером шрифта 9pt и меньше | 300dpi для текста с размером шрифта от 10pt<br>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 4.1.1:**

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**.

Экстрактор ABBYY FineReader Engine 11 может работать в двух режимах:

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

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

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

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

## 4.9 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 Postfix.

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).

Если письма не отправляются, настройте отправку писем через Postfix.

**Чтобы настроить отправку писем через Postfix:**

1. Откройте файл **/etc/postfix/main.cf**;
2. В качестве значения параметра `relayhost` укажите требуемый почтовый сервер:
   `relayhost = <mail.company.ru>,`
   где `<mail.company.ru>` - требуемый почтовый сервер

   > **Примечание:**
   >
   > Если в файле **/etc/postfix/main.cf** нет строки с параметром `relayhost`, добавьте такую строку.

3. Перезапустите Postfix с помощью команды:
   `service postfix restart`
4. Проверьте, выполняется ли отправка сообщений, с помощью команды:
   `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).

## 4.10 Ограничение количества найденных событий

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

## 4.11 Настройка 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, генерируетс | TCP | Агент | | Модуль Агента в сессии пользователя, процесс `DM.Client.exe` |

| Порт по умолчанию | Поддерживаемые протоколы | Компоненты InfoWatch Device Monitor | | Описание |
|---|---|---|---|---|
| | | Источник | Получатель | |
| я динамически | | | | |
| 15200 | TCP | Сервер | Агент | Скачивание дистрибутива Агента InfoWatch Device Monitor |

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.<br>Редактирование этого раздела не разрешается. |
| <runtime> | Содержит настройки для среды выполнения Microsoft .NET Framework. Эти настройки необходимы для корректной работы Сервера.<br>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).<br>Изменение этого раздела крайне не рекомендуется. |

| Конфигурационный раздел | Описание |
|---|---|
| <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".

### 4.11.1 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>`<br>Настройки ядра Сервера | |
| `RemotingPort` | Порт TCP, обслуживающий подключения Консоли управления.<br>Значение по умолчанию - `15003` (крайне не рекомендуется изменять это значение) |
| `CultureName` | Язык диагностических и других сообщений модуля. Возможные значения:<br>▪ `ru-RU`<br>▪ `en-US` |
| `MachineName` | IP-адрес сетевого интерфейса, посредством которого Сервер принимает соединения с Консолью управления.<br>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 |

| Параметр | Описание |
| --- | --- |
| | 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.<br>Значение по умолчанию - `300`. |
| `<InfoWatch.DeviceMonitor.Server.Database.Properties.Settings>`<br>Настройки модуля, взаимодействующего с базой данных | |
| `DatabaseType` | Тип базы данных.<br>Возможные значения:<br>• `Oracle`<br>• `Microsoft`<br>• `PostgreSql` |
| `ConnectionString` | Строка соединения с базой данных. Должна соответствовать правилам, установленным для строк соединения ADO.NET.<br>Например:<br>`Data Source=isis\s2005;Initial Catalog=g1228_9;Integrated Security=True` |
| `CultureName` | Язык диагностических и других сообщений модуля.<br>Возможные значения:<br>▪ `ru-RU`<br>▪ `en-US` |
| `ConnectionPoolSize` | Количество соединений к БД, которые будут открыты и которые будет использовать сервер в своей работе.<br>Значение по умолчанию - `200`. |
| `CommunicationPort` | Номер порта, используемого при соединении сервера с Агентом распространения при установке Агента через механизм задач. Не рекомендуется менять в процессе работы.<br>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 |

| Параметр | Описание |
| --- | --- |
| | установки продукта, для отображения информации на сервере.<br>Значение по умолчанию - `60`. |
| `EventRelationStoredPeriod` | Интервал времени в днях. Параметр используется в формуле вычисления даты удаления при очистке мусорных событий.<br>Значение по умолчанию - `7`. |
| `DeleteEventCount` | Максимальное количество удаляемых событий из БД за один проход<br>Значение по умолчанию - `10000`. |
| `<InfoWatch.DeviceMonitor.Server.Gui.Properties.Settings>`<br>Настройки модуля, предоставляющего интерфейс для Консоли управления | |
| `CultureName` | Язык диагностических и других сообщений модуля. Возможные значения:<br>▪ `ru-RU`<br>▪ `en-US` |
| `InitialLeaseTime` | Время (в минутах), в течение которого сеанс соединения с Консолью управления считается действительным.<br>Значение по умолчанию - `5`. |
| `RenewOnCallTime` | Время (в минутах), на которое продлевается время жизни сеанса соединения Консоли с сервером.<br>Значение по умолчанию - 2. |
| `<InfoWatch.DeviceMonitor.Server.Client.Properties.Settings>`<br>Настройки модуля, обслуживающего клиентские подключения (контролируемые компьютеры) | |
| `Backlog` | Длина очереди клиентских соединений, ожидающих подключения.<br>Значение по умолчанию - `64`. |
| `CultureName` | Язык диагностических и других сообщений модуля. Возможные значения:<br>• `ru-RU`<br>• `en-US` |
| `ShadowCopyTempDir` | Полный путь к каталогу, в котором хранятся временные теневые копии, ожидающие отправки в InfoWatch Traffic Monitor.<br>Значение по умолчанию: |

| Параметр | Описание |
| --- | --- |
| | `C:\Program Files\InfoWatch\DeviceMonitor\Server\ShadowCopyTempDir` |
| `DmpV1Adress` | Список IP-адресов (разделитель в перечислении – «;»), на которых сервер должен прослушивать порты. Возможны следующие значения:<br>• `AllAny` – порты на всех IP адресах, которые имеются на компьютере (значение по умолчанию);<br>• `AllIp4` – порты на всех IP адресах версии 4;<br>• `AllIp6` – порты на всех IP адресах версии 6. |
| `Dmpv1TraceLevel` | Уровень трассировки протокола взаимодействия клиента и сервера.<br>Возможны следующие значения:<br>▪ 1 – выключить трассировку;<br>▪ 2 – выполнять трассировку только для информации о пакете (значение по умолчанию);<br>▪ 3 – полная трассировка.<br>**Примечание:**<br>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 <system.diagnostics>"). |
| `Dmpv1TraceClients` | Список IP-адресов Агентов (разделитель в перечислении – «;»), взаимодействие с которыми необходимо трассировать.<br>При значении `All` выполняется трассировка для всех Агентов. |
| `Dmpv1ConnectionsLimit` | Количество одновременно обрабатываемых соединений по протоколу TCP/IP с клиентами.<br>Значение по умолчанию - `400`. |
| `Dmpv1ConnectionsQueueLimit` | Максимальное количество соединений, ожидающих обработку. Если значение превышено, то соединения "урезаются" до значения, указанного в параметре `Dmpv1ConnectionsQueueLengthAfterCut`. |

| Параметр | Описание |
| --- | --- |
| | Значение по умолчанию - `700`. |
| `Dmpv1ConnectionsQueueLengthAfterCut` | Количество соединений после урезания очереди при превышении очередью максимального размера.<br>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).<br>Значение по умолчанию - `120`. |
| `SSLPort` | Номер порта для шифрованных соединений.<br>Значение по умолчанию - `15004`. |
| `CheckUpdateTmConfigPeriodMinutes` | Период опроса сервера TM на проверку изменений конфигурации в минутах.<br>Значение по умолчанию - `30`. |
| `<InfoWatch.DeviceMonitor.TrafficMonitor.Connector.Properties.Settings>`<br>Базовые настройки коннектора Traffic Monitor Server | |
| `DBPollTime` | Период (в миллисекундах) опроса базы данных, в процессе которого проверяется наличие событий в базе данных.<br>Значение по умолчанию - `2000`. |
| `CultureName` | Язык диагностических и других сообщений модуля. Возможные значения:<br>• `ru-RU`<br>• `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.<br>Значение по умолчанию - `200`. |
| `MaxSendEventCount` | Максимальное количество событий, вычитываемое за один раз из БД DM для отправки в TM |

| Параметр | Описание |
| --- | --- |
| | Значение по умолчанию - `5000`. |
| `ShadowCopyTrasferBlockSize` | Размер блока данных теневой копии, пересылаемой на сервер Traffic Monitor, в МБ.<br>Значение по умолчанию - `16`. |
| `<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings>`<br>Настройки низкоуровневого драйвера базы данных | |
| `CultureName` | Язык диагностических и других сообщений модуля. Возможные значения:<br>• `ru-RU`<br>• `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`.<br>**Примечание:**<br>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 - `300` (0 - бесконечно).<br>**Примечание:**<br>Данный параметр не работает для СУБД Oracle. |
| `<InfoWatch.DeviceMonitor.EP.Sender.Properties.Settings>`<br>Настройки модуля, взаимодействующего с InfoWatch Activity Monitor | |
| `EPAddress` | Адрес сервера IW Activity Monitor |
| `EPToken` | Токен авторизации IW Activity Monitor |
| `DBPollTime` | Частота опроса БД (в мс).<br>Значение по умолчанию - `5000` |

| Параметр | Описание |
| --- | --- |
| `CultureName` | Язык диагностических и других сообщений модуля.<br>Возможные значения:<br>• `ru-RU`<br>• `en-US` |
| `NumberOfConnections` | Количество подключений сервера IW Device Monitor к серверу IW Activity Monitor.<br>Значение по умолчанию - `4` |
| `MaxSendEventCount` | Количество событий, которое единовременно может быть отправлено из базы данных.<br>Значение по умолчанию - `5000` |
| `RequestEventCount` | Количество событий статистики, допустимое для отправки в одном пакете.<br>Значение по умолчанию - `100` |
| `WriteDisconnectEventLogIntervalMinute` | Интервал записи лог-файла в случае отсутствия или обрыва связи (в мин).<br>Значение по умолчанию - `60` |
| `WaitPlatformDiskErrInitialMinute` | Начальное время ожидания в минутах повторной отправки событий в Платформу в случае получения ошибки 507. Значение по умолчанию - `10` |
| `WaitPlatformDiskErrMaxMinute` | Максимальное время ожидания в минутах повторной отправки событий в Платформу в случае получения ошибки 507. Значение по умолчанию - `60` |
| `<InfoWatch.DeploymentSubSystem.Properties.Settings>`<br>Настройка модуля распространения (установка/обновление/удаление) агентов и диагностики | |
| `NetworkLatency` | Технический параметр, изменять не рекомендуется. |
| `RunningInstallationsLimit` | Максимальное количество одновременных первичных инсталляций на компьютерах.<br>Значение по умолчанию - `0` (вычисляется по формуле) |
| `BandwidthUsagePercentLimit` | Процент занимаемой данными задачами пропускной способности сети, чтобы его можно было контролировать.<br>Значение по умолчанию при отсутствии параметра или ошибки – `0.5 (50%)` |

### 4.11.2 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 <applicationSettings>").

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`.

## 4.11.3 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 <applicationSettings>").

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.

## 4.12 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.

Consul используется во всех типах установки. Сведения о режимах установки Системы приведены в Руководстве по установке, статья "Схемы развертывания Системы и выбор типа установки").

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

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

### 4.12.1 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.

### 4.12.2 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 |

| Сервисы с обязательной регистрацией в Consul | Сервисы, установленные на нодах с присутствием Consul Server или Consul Client |
|---|---|
| iw_xapi_puppy<br>iw_x2x<br>iw_x2db | iw_xapi_puppy<br>iw_x2x<br>iw_x2db<br>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.

### 4.12.3 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!**

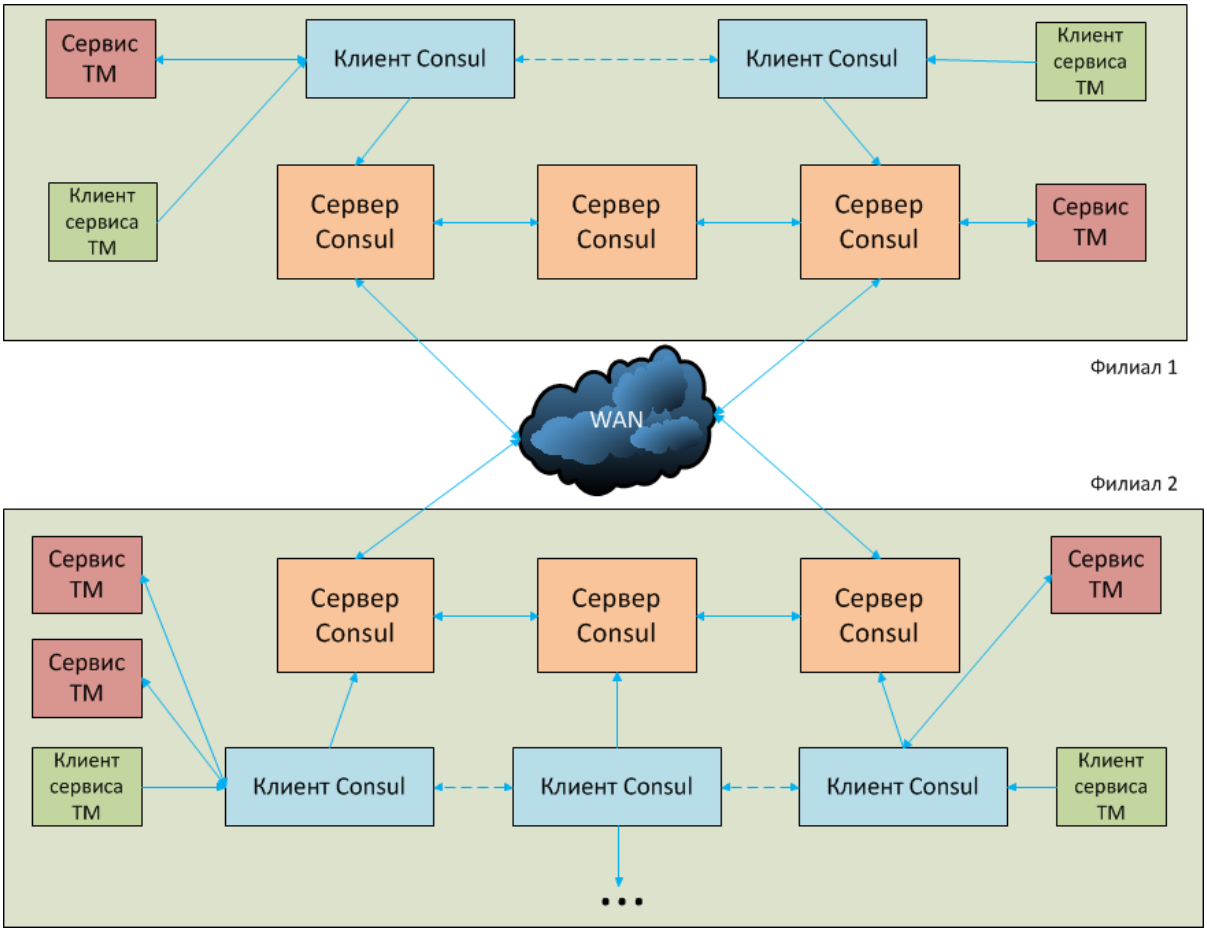
В случае распределенной установки ТМ не должно быть запрета использования TCP и UDP между разными сегментами сети (в том числе нодами) в брендмауэре Windows.

**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`

### 4.12.4 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 |

### 4.12.5 Конфигурационный файл consul.json и unit-файл iwtm-consul.service

| Содержимое | Описание |
|---|---|
| `{` | |
| `"bootstrap_expect": 1,` | Количество ожидаемых серверов в кластере (только для режима сервера) |

| Содержимое | Описание |
| --- | --- |
| `"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 |

| Содержимое | Описание |
| --- | --- |
| } | |

Unit-файл **iwtm-consul.service**

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

| Код | Описание |
| --- | --- |
| `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 |

## 4.13 Обнаружение рабочих станций для установки агентов

В состав дистрибутива для установки Сервера Device Monitor входит утилита сканирования диапазона IP-адресов. Она  устанавливается автоматически вместе с консолью управления DM. Результатом сканирования является текстовый файл, который содержит список "IP-адрес или доменное имя - операционная система" для тех рабочих станций, на которые Агент Device Monitor не установлен.

Утилита не имеет графического интерфейса и запускается из командной строки. Ниже описаны параметры, которые необходимо или возможно указать при запуске. Их описание доступно по вызову справки: `Iw.Util.MachineDiscovery.exe` -- `help`.

| | |
| --- | --- |
| `--mode arg (=icmp)*` | Режим сканирования сети (обязательный параметр):<br>• `nmap` - сканирование сети с помощью утилиты nmap, которая может дополнительно определить тип операционной системы по эвристическим алгоритмам,<br>• `icmp` - сканирование сети по протоколу icmp |
| `--ip-range arg` | Диапазон ip-адресов в одном из форматов, валидных для nmap (обязательный параметр). Например: " `--ip-range 10.60.3-35.1-254` " |

| | |
|---|---|
| `--ip-cidr-range arg` | Диапазон ip-адресов в формате CIDR (обязательный параметр). Например " `--ip-cidr-range 10.60.3.4/24` " |
| `--ipv6-cidr-range arg` | Диапазон IPv6-адресов в формате CIDR (обязательный параметр, если используется протокол IPv6). Например: " `--ipv6-cidr-range fe80::98b9:ec9:f9a9:9104/120` "<br>**Важно!** Для Ipv6-адресов поддерживается только формат CIDR |
| `--threads arg (=2)` | Количество потоков для обработки асинхронных запросов на сканирование сети. |
| `--icmp-attempts arg (=2)` | Количество попыток обратиться по протоколу icmp к ip-адресу, чтобы признать его недоступным. Так как протокол icmp не гарантирует доставку пакетов (в отличии от tcp), то пакеты могут теряться, и для большей уверенности в недоступности адресата нужно несколько попыток. |
| `--icmp-timeout arg (=5000)` | Время ожидания ответа от адресата для каждой попытки проверки его доступности. |
| `--deploy-agent-port arg (=15505)` | Порт агента распространения, на котором он слушает сеть. Следует оставить по умолчанию |
| `--output-file arg` | Путь к файлу с результатами работы утилиты. |
| `--nmap-path arg (nmap mode)` | Путь к кросплатформенной утилите nmap в случае использования режима работы "nmap". |
| `--nmap-os-info arg (=1)` | Определять (=1) или не определять (=0) операционную систему рабочих станций при сканировании в режиме работы "nmap" |
| `--nmap-save-output-to-file arg (=1)` | Сохранить stdout и stderr Nmap'а в файл Nmap_output_%Y-%m-%d_%H-%M-%S.log |
| `--nmap-timing arg (=3)` | Частота сканирования nmap'ом:<br>• от 0 - самое медленное и точное<br>• до 5 - самое быстрое и неточное |
| `--nmap-min-hostgroup arg (=16)` | Минимальный размер группы для параллельного сканирования nmap'ом. |
| `--nmap-max-hostgroup arg (=16)` | Максимальный размер группы для параллельного сканирования nmap'ом (до 1024). |

| | |
|---|---|
| `--nmap-min-parallelism arg (=10)` | Минимальное количество запросов для группы хостов (от 1). |
| `--nmap-max-parallelism arg (=10)` | Максимальное количество запросов для группы хостов. |
| * - в скобках указано установленное по умолчанию значение | |

Чтобы запустить утилиту:

1. В командной строке на рабочей станции с консолью Device Monitor перейдите в директорию с утилитой Iw.Util.MachineDiscovery.exe с помощью команды cd:
   cd <путь_до_утилиты>
2. Запустите утилиту, обязательно указав при этом диапазон IP-адресов, а также другие параметры, если требуется. Например:
   `Iw.Util.MachineDiscovery.exe --ip-range 10.60.3-35.1-254`
3. Дождитесь окончания сканирования.
4. По завершению сканирования результаты будут записаны в текстовый файл `iw_machine_discovery.output.txt` в директории размещения утилиты `C:\Program Files\InfoWatch\Device Monitor\Management Console\Utils`. Полученный файл загрузите в задаче первичного распространения при создании списка компьютеров для установки Агентов на них (см. "Traffic Monitor. Руководство пользователя", раздел "Создание задачи первичного распространения").

# 5 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 инсталлятора. О порядке установки см. документ «InfoWatch Traffic Monitor. Руководство по установке».

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

Также доступна Ручная настройка индикаторов.

## 5.1 Настройки подсистемы мониторинга

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

Настройка подсистемы мониторинга включает следующие задачи:

- Настройка подключения Device Monitor;
- Ручная настройка индикаторов;
- Настройка адреса сервера синхронизации времени для подсистемы мониторинга;
- Настройка механизма уведомлений.

### 5.1.1 Настройка подключения Device Monitor

Чтобы настроить мониторинг для сервера Device Monitor:

1. Отредактируйте файл `/opt/iw/tm5/etc/nagios/iwmon/iwmon-hosts-dm.cfg`:
   - Раскомментируйте секции `host` и `hostgroup`.
   - В параметре `address` секции `host` определите имя хоста или IP-адрес сервера Device Monitor.
- В файле / `opt/iw/tm5` `/etc/nagios/iwmon/iwmon-services-dm.cfg` раскомментируйте секцию `service`.

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

### 5.1.2 Ручная настройка индикаторов

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

- iwmon-services-db-psql.cfg – настройка индикаторов для базы данных 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.

Параметр `service_description` отображает назначение каждого индикатора.

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

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

Чтобы применить изменения, перезапустите процесс nagios:

`systemctl restart iwtm-nagios`

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

### 5.1.4 Настройка механизма уведомлений

Подсистема мониторинга позволяет отправлять уведомления по электронной почте для случаев, когда текущее значение индикатора превышает пороговое значение.

**Чтобы настроить отправку почтовых уведомлений для выбранных индикаторов:**

1. Зайдите в каталог подсистемы Nagios:
```
cd /opt/iw/tm5/etc/nagios/iwmon
```
2. Откройте файл iwmon-services.cfg:
```
mcedit /opt/iw/tm5/etc/nagios/iwmon/iwmon-services.cfg:
```

3. Для того чтобы определить нужный индикатор, посмотрите поле `service_description`.
4. В секции индикатора измените параметр `notifications_enabled` на:

- 1 – если вы хотите включить отправку уведомлений
- 0 – если вы хотите выключить отправку уведомлений

- Сохраните изменения.

> **Примечание:**
>
> В случае если в конфигурационном файле отсутствует параметр `notifications_enabled`, добавьте его вручную.

# 6 Администрирование базы данных

Этот раздел содержит информацию по администрированию:

- Oracle;
- PostgreSQL.

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

## 6.1 Oracle

Раздел содержит инструкции по администрированию Oracle:

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

### 6.1.1 Изменение предустановленных паролей

Чтобы заменить предустановленные пароли пользователей БД:

1. Остановите процессы Traffic Monitor:
   `iwtm stop`
2. Подключитесь к БД Oracle:
   `sqlplus iwtm@iwtm`
3. Введите предустановленный пароль.
4. Получите список пользователей:
   `select * from dba_users;`
5. Измените пароли пользователей:
   `ALTER USER user IDENTIFIED BY password;`
   где `user` - выбранный пользователь БД, `password` - новый пароль для этого пользователя.
6. Выйдите из БД Oracle:
   `exit`
7. Запустите процессы Traffic Monitor:
   `iwtm start`

Чтобы изменить предустановленный пароль Traffic Monitor, смотрите "Изменение предустановленного пароля Traffic Monitor".

### 6.1.2 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.). |

| Тип табличного пространства | Назначение |
|---|---|
| | Управление системой через Консоль управления (роли, учетные записи пользователей и др.) |
| Ежедневное | Хранение объектов, перехваченных в течение одних суток.<br>Хранение информации о результатах анализа и обработки объектов (разобранный объект, категории, термины и др.).<br>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 присваиваются имена:

- *IWTM_YYYY_MM_DD_N* – табличное пространство за день, которое содержит объекты без нарушений.
- *IWTM_YYYY_MM_DD_V* – табличное пространство за день, которое содержит объекты с нарушениями.

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.

## 6.1.3 Управление ежедневными табличными пространствами

В этом разделе:

- Настройка размещения файлов в файловой системе;
- Настройка режимов хранения файлов табличного пространства;
- Архивирование ежедневных табличных пространств;
- Восстановление ежедневных табличных пространств;
- Удаление ежедневных табличных пространств.

### 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 (см. документ "*InfoWatch Traffic Monitor. Руководство по установке*") задается использование одного ежедневного табличного пространства, расположенного в `/u02/oradata/`.

**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

        pkg_part.set_df_path_cnt('4');
 COMMIT;
 END;
 /
```

**Важно!**

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

**Пример сценария, изменяющего пути для расположения ежедневных ТП:**

```
BEGIN

        pkg_part.set_df_path('/test1/', 1);

        pkg_part.set_df_path('/test2/', 2);

        pkg_part.set_df_path('/test3/', 3);

        pkg_part.set_df_path('/test4/', 4);
 COMMIT;
 END;
 /
```

**Примечание:**

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

**Пример сценария просмотра содержимого ежедневных ТП:**

```
select a.tbs_name, a.service_code, power(10, trunc(log(10, a.text_size))) ||
'-' ||
power(10, trunc(log(10, a.text_size)) + 1) size_range,
count(1) cnt, sum(a.text_size) text_size
from
(
select t.tbs_name, o.service_code,
 case
 when length(o.text) > 0 then length(o.text)
 else 1
 end text_size
from object o
inner join object_source os on os.object_id = o.object_id
inner join tbs_list t on o.tbs_id = t.tbs_id
) a
group by a.tbs_name, a.service_code, power(10, trunc(log(10, a.text_size))) ||
'-' ||
power(10, trunc(log(10, a.text_size)) + 1)
order by 1, 2, 3
```

Определение кодов сервиса указано в файле **services.xml**, который находится в каталоге `/opt/iw/tm5/etc/compendiums/`.

> **Примечание:**
>
> Чтобы получить результат анализа размеров перехваченных объектов в табличных пространствах вместе со служебной информацией БД, рекомендуется использовать SQLDeveloper.

## 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 "oradata":
   `mkdir /u03/oradata (` где `/u03/oradata` это путь к быстрому диску)
3. Смените пользователя:
   `chown -R oracle:oinstall /u03`
4. Зайдите в базу данных:
   `su - oracle`
   `sqlplus iwtm@iwtm`
5. Укажите период хранения на быстрых дисках:
   `exec pkg_part.set_fast_days(7);`
6. Укажите путь к быстрому диску:
   `exec pkg_part.set_fast_path('/u03/oradata/',1);`
7. Укажите путь к медленному диску:

```
exec pkg_part.set_df_path('/u02/oradata1/',1);
```

8. При необходимости можно использовать несколько медленных дисков. Данные будут записываться на следующий медленный диск при заполнении предыдущего. Для добавления дополнительных медленных дисков укажите новый путь:
```
exec pkg_part.set_df_path('/u02/oradata2/',2);
```
9. Укажите общее количество медленных дисков:
```
exec pkg_part.set_df_path_cnt('2');
```
10. Поменяйте режим на медленные-быстрые диски:
```
exec pkg_part.set_filesys_type('fast/slow');
```
Данные будут перенесены с быстрых дисков на медленные с помощью ночного задания (джоба).
11. Примените внесенные изменения:
```
commit;
```
12. Чтобы запустить перенос файлов вручную, выполните:
```
exec iwtm.pkg_part.move_fast_tablespaces_to_slow();
```

**Примечание:**

В Системе допустимо использование нескольких медленных дисков.

**Важно!**

Убедитесь, что используемые вами пути разделов соответствуют указанным в данной статье.

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 "oradata"
```
mkdir /u03/oradata
```
3. Смените пользователя:
```
chown -R oracle:oinstall /u03
```
4. Зайдите в базу данных:
```
su - oracle
sqlplus iwtm@iwtm
```
5. Добавьте путь второго раздела:
```
exec pkg_part.set_df_path('/u03/oradata/',2);
```
6. Укажите новое количество путей:
```
exec pkg_part.set_df_path_cnt(2);
```
7. Примените внесенные изменения:
```
commit;
```
8. Переключитесь на режим rotate:
```
exec pkg_part.set_filesys_type('rotate');
```

```
SQL>select * from setting where setting like 'df_path%';
select * from setting where setting like 'df_filesys%';
```

```
setting | value | editable
------------+--------------+----------
df_path1 | /u02/oradata1/ | 1
df_path2 | /u03/oradata/ | 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".

## 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 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 `oracle` должен являться владельцем каталога.

Если каталог установлен неправильно, установите его, выполнив команду:

```
begin
sp_setting_set('archive_path', '/u02/arch/');
commit;
end;
/
```

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
 sp_setting_set('violation_archive_enabled', 1);
 sp_setting_set('violation_archive_period', D);
 commit;
 end;
/
```

- Для ежедневного табличного пространства, хранящего объекты со статусом *Нет нарушений*:

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

- Для ежедневного табличного пространства, хранящего *снимки экрана (скриншоты):*

```
begin
 sp_setting_set('other _archive_enabled', 1);
  sp_setting_set('other _archive_period', D);
 commit;
  end;
/
```

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 архивировано Системой. Это число должно быть меньше устанавливаемого количества дней до удаления ежедневного ТП (см. "Удаление ежедневных табличных пространств").

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. Например, для выборки ежедневных ТП, в которых хранятся объекты, перехваченные более 100 дней назад, можно применить следующий запрос:

```
SELECT t.tbs_id, t.tbs_name, t.part_date
FROM tbs_list t
WHERE t.part_date<trunc(SYSDATE) - 100 + 23 / 24 AND t.status IN (0, 3)
```

**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.

Для выборки файлов данных в этом случае создается следующий запрос:

```
SELECT f.file_name
FROM dba_data_files f
WHERE f.tablespace_name in
(
  SELECT t.tbs_name
  FROM tbs_list t
  WHERE t.part_date<trunc(SYSDATE) - 100 + 23 / 24 AND t.status IN (0, 3)
)
```

где `t.status IN (0, 3)` указывает на то, что для архивации выбраны табличные пространства со статусами *Чтение и запись* (код статуса `0`) и *Только чтение* (код статуса `3`).

**Отключение ежедневных табличных пространств от базы данных**

**Важно!**

Не отключайте ежедневные ТП во время работы заданий IWTM_ADD_PARTS, IWTM_DELETE_TABLESPACES и IWTM_ARCHIVE_TABLESPACES так как это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:
   ```
   begin
   IWTM.pkg_part.archive_tablespace(N);
   end;
   /
   ```
   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 файлы данных, принадлежащие отключенным ежедневным ТП, на другой носитель информации.
Для получения списка отключенных табличных пространств используйте команду:
`select tbs name from tbs_list where NOTE = 'Tablespace is offline'`
где `tbs name` – имя табличного пространства.
`tbs_list` – имя таблицы.
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 *oracle* 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 IWTM_ADD_PARTS и IWTM_DELETE_TABLESPACES. Это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:
   ```
   begin
   pkg_part.restore_tablespace(N);
   end;
   /
   ```
   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 .

## Удаление ежедневных табличных пространств

Если дальнейшее хранение данных не требуется, то Вы можете воспользоваться процедурой удаления ежедневных ТП (**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. Процедура IWTM_DELETE_TABLESPACES не работает с теми табличными пространствами, которые были отключены/подключены вручную.

В результате выполнения этой процедуры удаляются все ежедневные ТП (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 архивированное ежедневное ТП не подлежит восстановлению (т.к. информация о нем была удалена из базы данных), вы можете удалить файлы данных этого ТП из архива.

**Важно!**

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

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 четырех лет, в задании IWTM_DELETE_TABLESPACES укажите интервал 366*4=1464 дня.

**Определение интервала времени для отключения ежедневных ТП**
Для автоматического отключения табличных пространств (по умолчанию функция выключена) вы можете использовать различные сценарии (запускаются от имени владельца схемы данных). Установите срок хранения информации об архивных ТП:

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

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

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

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

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

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

где:
`1` – показатель того, что автоматическое отключение активировано (чтобы выключить, вместо 1 используйте значение 0);
`D` – количество дней, по прошествии которых ежедневное табличное пространство будет отключено от БД. Это число должно быть больше устанавливаемого количества дней до архивирования ежедневного ТП (см. "Автоматическое архивирование ежедневных табличных пространств").

После отключения архивных ТП от БД (статус *Offline*) они становятся недоступны Системе.

**Удаление архивированных ТП**

При отключении от БД архивированных ежедневных ТП в Системе остаются файлы данных (по умолчанию в директории / `u02/arch)`. Чтобы освободить пространство на жестком диске, можно (на выбор):

- удалить их вручную;
- добавить новые задачи, запускаемые по расписанию в файле `/etc/cron.d/iwtm_cleanup` или в другом файле с задачами в этой директории.

**Пример**

Чтобы удалить все архивированные ежедневные ТП старше 150 суток:

1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup` или другой файл с задачами в этой директории.
2. Добавьте строки:
```
35 3 * * * root find /u02/arch/ -type f -mtime +150 -delete > /dev/null 2>&1 &
40 3 * * * root find /u02/arch/ -type d -ctime +10 -empty -delete > /dev/null 2>&1 &
```
3. Сохраните изменения.
4. Примените новые настройки сервиса `cron`:
```
systemctl reload crond
```

**Удаление ежедневных ТП по расписанию**
По умолчанию автоматическое удаление ежедневных ТП отключено. Чтобы включить удаление всех ежедневных ТП согласно расписанию (ежедневно, в 01 ч. 00 мин. 00 с.), от имени владельца схемы базы данных выполните следующий сценарий:

```
BEGIN
 dbms_scheduler.enable('IWTM_DELETE_TABLESPACES');
 COMMIT;
 END;
 /
```

Чтобы отключить автоматическое выполнение процедуры по расписанию, выполните следующий сценарий:

```
BEGIN
 dbms_scheduler.disable('IWTM_DELETE_TABLESPACES');
 COMMIT;
 END;
 /
```

**Удаление ежедневных ТП вручную**

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 сценарий:

```
BEGIN
 dbms_scheduler.run_job('IWTM_DELETE_TABLESPACES');
 END;
 /
```

**Удаление ежедневных ТП с помощью скрипта**

Если вам требуется настроить автоматическое удаление ежедневных ТП, используйте скрипт **/opt/iw/tm5/bin/dbconf-iwdrop-oracle.sh.** Возможны команды:

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

**Пример**

Чтобы удалить все объекты со статусом *"Нет нарушения"*, созданные в течение последних 15 суток, выполните команды:

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

### 6.1.4 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.
Опытные администраторы промышленных баз данных Oracle могут выполнять резервное копирование на работающей БД (процедура «горячего бэкапа») с помощью программы RMAN, рекомендуемой компанией Oracle (см. документацию Oracle), предварительно переведя БД Oracle в режим ARCHIVELOG.
Для специалистов, не являющихся администраторами Oracle, 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 папок для резервной копии;
- Создание вспомогательных файлов на Linux;
- Создание списка файлов, подлежащих резервному копированию;
- Остановка системы IWTM;
- Остановка БД Oracle;
- Копирование файлов БД в хранилище резервных копий.

Определение размера резервной копии

**Чтобы определить размер базы данных:**

1. На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
2. Откройте Oracle SQL*Plus и подключитесь как пользователь *sysdba*:
   `OS> sqlplus / as sysdba`
3. Если система была установлена с помощью инсталлятора, для удобства можете воспользоваться командой **wsqlplus**.

> **Примечание:**
>
> Команда `wsqlplus` является алиасом команды `sqlplus`:
> `alias wsqlplus='rlwrap -b "" -f ~/sql.dict sqlplus'`

Дождитесь подключения – об этом будет свидетельствовать сообщение **Connected**

4. Скопируйте (или введите) в командную строку и выполните следующий SQL запрос:
   ```
   SQL> SELECT ROUND(SUM(bytes)/1024/1024/1024,4) GB FROM ( SELECT SUM(bytes) bytes FROM dba_data_files union SELECT SUM(bytes) bytes FROM dba_temp_files union SELECT SUM(bytes) bytes FROM v$log);
   ```
5. Запишите получившийся размер базы данных.
6. Выйдите из Oracle SQL*Plus:
   ```
   SQL> exit
   ```

Проверка хранилища резервной копии

Проверьте приемлемость выбранного хранилища резервной копии. Оно должно соответствовать следующим требованиям:

- Размещаться на компьютере, отличном от того, где работает база данных.
- Доступно с компьютеров, где работают сервера и базы данных, подлежащие резервному копированию.
- На жестком диске больше свободного места, чем размер резервной копии:

**Чтобы определить количество свободного места на жестком диске**
от имени **root** выполните следующую команду:
```
OS> df -h
```
Убедитесь, что это число больше размера БД.

Создание папок для резервной копии

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

**Чтобы создать структуру папок для бэкапа:**

1. Войдите в систему от имени пользователя **root.**
2. Создайте директорию для хранения файлов резервной копии:
   ```
   OS> mkdir /opt/IWTM_Backup_Files
   ```
3. Создайте следующие поддиректории:
   ```
   OS> mkdir /opt/IWTM_Backup_Files/Oradata
   OS> mkdir /opt/IWTM_Backup_Files/IWTM
   OS> mkdir /opt/IWTM_Backup_Files/Recovery_Aid
   ```
4. Назначьте права на эти директории для пользователя **Oracle**:
   ```
   OS> chmod 777 /opt/IWTM_Backup_Files/ -R
   ```

Создание вспомогательных файлов на Linux

Для обеспечения возможности восстановления из резервной копии, помимо самих файлов данных, вам потребуются вспомогательные файлы: **trace**–файл контрольного файла и копия файла **init.ora**.
**Trace**–файл контрольного файла содержит имена и пути для всех файлов данных и дополнительных файлов данных, добавленных в БД. Также содержит файлы **redo log** и команды, которые можно использовать для восстановления структуры БД.
Файл **init.ora** содержит инициализационные параметры Oracle, в частности, имена и пути для

контрольных файлов базы данных.

**Чтобы создать `trace`-файл для контрольного файла, spfile-файл и скопировать их:**

1. На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
2. Откройте Oracle SQL*Plus и подключитесь как пользователь **sysdba**:
   `OS> sqlplus / as sysdba`
   Если система была установлена с помощью инсталлятора, для удобства Вы можете использовать команду **wsqlplus**.

   > **Примечание:**
   >
   > Команда `wsqlplus` является алиасом команды `sqlplus`:
   > `alias wsqlplus='rlwrap -b "" -f ~/sql.dict sqlplus'`

   Дождитесь подключения – об успешном подключении будет свидетельствовать сообщение **Connected**.
3. Скопируйте (или введите) в командную строку и выполните следующий SQL запрос**:**
   `SQL> alter database backup controlfile to trace;`
4. Найдите путь к директории, в которой был создан trace-файл, выполнив команду:
   `SQL> show parameter user_dump;`
   В данной директории находятся файлы `trc` и `alert_iwtm.log` (alert_INSTANCE_NAME).
   В `log`-файле указано имя созданного `trace`-файла.
   Выйдите из Oracle SQL*Plus:
   `SQL> exit`
5. Если система была установлена с помощью инсталлятора и были оставлены параметры по умолчанию, Вы можете проверить последние записи в файле журнала `alert_iwtm.log` с помощью команды:
   `OS> tail -f /u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log`
   Чтобы выйти из режима просмотра, нажмите CTRL+C
6. Создайте копию файла параметров **spfile** (**pfile**):
   `OS> sqlplus / as sysdba`
   `SQL> CREATE PFILE from SPFILE;`
7. Найдите путь к директории, в которой был создан `pfile`-файл. Для этого выполните команду:
   `SQL> show parameter PFILE`
   Будет возвращен путь к директории, в которой был создан `pfile` (по умолчанию `/u01/app/oracle/product/db_1/dbs/`).
   В этой же директории находится файл initiwtm.ora, для которого нужно также создать резервную копию.
   Выйдите из Oracle SQL*Plus:
   `SQL> exit`
8. Скопируйте файлы `trace` и `spfile` на компьютер с резервной копией, в ранее созданную поддиректорию **/opt/IWTM_Backup_Files/Recovery_Aid**.
9. Вам нужно скопировать самые актуальные файлы. Чтобы найти файлы с самой поздней датой и временем изменения, выполните:
   `OS> ll`
10. Переименуйте файл так, чтобы впоследствии его можно было легко найти, например:
    `controlfilebackupMMDDYY.trc`

Создание списка файлов, подлежащих резервному копированию

Вы можете создать список файлов, подлежащих резервному копированию. Эти списки будут использоваться впоследствии.

1. На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
2. Откройте Oracle SQL*Plus и подключитесь как пользователь **sysdba**:
   OS> sqlplus / as sysdba
   Дождитесь подключения – об этом будет свидетельствовать сообщение **Connected**.
3. Создайте список директорий и файлов, подлежащих резервному копированию. Это можно сделать с помощью следующих команд SQL:
   ```
   SQL> SELECT file_name FROM dba_data_files UNION SELECT file_name FROM dba_temp_files UNION SELECT name FROM v$controlfile union select member name from v$logfile;
   ```
   В результате получится список приблизительно следующего вида:
   ```
   /u01/app/oracle/fast_recovery_area/iwtm/control02.ctl
   /u01/app/oracle/oradata/iwtm/control01.ctl
   /u01/app/oracle/oradata/iwtm/redo01.log
   /u01/app/oracle/oradata/iwtm/redo02.log
   /u01/app/oracle/oradata/iwtm/redo03.log
   /u01/app/oracle/oradata/iwtm/redo04.log
   /u01/app/oracle/oradata/iwtm/redo05.log
   /u01/app/oracle/oradata/iwtm/redo06.log
   /u01/app/oracle/oradata/iwtm/redo07.log
   /u01/app/oracle/oradata/iwtm/redo08.log
   /u01/app/oracle/oradata/iwtm/redo09.log
   /u01/app/oracle/oradata/iwtm/redo10.log
   /u01/app/oracle/oradata/iwtm/redo11.log
   /u01/app/oracle/oradata/iwtm/redo12.log
   /u01/app/oracle/oradata/iwtm/redo13.log
   /u01/app/oracle/oradata/iwtm/sysaux01.dbf
   /u01/app/oracle/oradata/iwtm/system01.dbf
   /u01/app/oracle/oradata/iwtm/temp01.dbf
   /u01/app/oracle/oradata/iwtm/undotbs01.dbf
   /u01/app/oracle/oradata/iwtm/users01.dbf
   /u02/oradata/IWTM_2012_06_25_1.dbf
   /u02/oradata/IWTM_2012_06_26_1.dbf
   /u02/oradata/IWTM_2012_06_27_1.dbf
   /u02/oradata/IWTM_2012_06_28_1.dbf
   /u02/oradata/IWTM_2012_06_29_1.dbf
   /u02/oradata/IWTM_2012_06_30_1.dbf
   /u02/oradata/IWTM_2012_07_01_1.dbf
   /u02/oradata/IWTM_2012_07_02_1.dbf
   /u02/oradata/IWTM_2012_07_03_1.dbf
   /u02/oradata/IWTM_2012_07_04_1.dbf
   /u02/oradata/iwtm_1.dbf
   ```
4. Выйдите из Oracle SQL*Plus:
   ```
   SQL> exit
   ```

### Остановка системы IWTM

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

**Чтобы остановить систему IWTM:**

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

### Остановка БД Oracle

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

**Чтобы остановить БД Oracle:**

1. На компьютере, где работает база данных, зайдите в систему от имени пользователя oracle.
2. В командной строке введите:
   `OS> dbshut $ORACLE_HOME`
   По окончании процедуры резервного копирования сервисы можно запустить с помощью следующей команды:
   `OS> dbstart $ORACLE_HOME`

### Копирование файлов БД в хранилище резервных копий

1. Остановите все сервисы Oracle (см. "Остановка БД Oracle"). Чтобы убедиться в этом, выполните команду:
   `ps aux | grep ora`
   Если сервисы Oracle 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 (см. "Создание списка файлов, подлежащих резервному копированию").
   Если система была установлена с помощью инсталлятора и были оставлены параметры по умолчанию, то:
   a. скопируйте содержимое директории **/u01/app/oracle/oradata/iwtm/** - в директорию **/opt/IWTM_Backup_Files/IWTM**
   b. скопируйте содержимое директории **/u02/oradata/** - в директорию **/opt/IWTM_Backup_Files/Oradata**

> **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.

3. С компьютера, где установлена БД, скопируйте файл **/u01/app/oracle/product/db_1/dbs/orapwiwtm** в директорию **/opt/IWTM_Backup_Files/Recovery_Aid** компьютера, где расположены файлы резервной копии.

## 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 БД".
- Если старая БД не может больше использоваться, создайте новую и восстановите данные на ней: см. "Восстановление на новой БД".

### Восстановление на той же БД

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

**Чтобы восстановить БД с помощью создания новой БД:**

1. Убедитесь в работоспособности БД. Проверьте существующую схему БД, сервер БД, где размещена эта схема, и компьютер, на котором работает сервер БД.
2. Остановите БД:
   ```
   OS> dbshut $ORACLE_HOME
   ```
3. Установите БД Oracle согласно инструкции, приведенной в документе «*InfoWatch Traffic Monitor. Руководство по установке*».
4. Выполните следующие шаги:
   a. Удалите все содержимое папок **/u02/oradata/, /u02/oradata1/** и **/u01/app/oracle/oradata/iwtm/**
   b. Скопируйте содержимое директории **/opt/IWTM_Backup_Files/Oradata/** в директорию **/u02/**
   c. Скопируйте содержимое директории **/opt/IWTM_Backup_Files/IWTM/** в директорию **/u01/app/oracle/oradata/iwtm/**
   d. Переименуйте файл **control01.ctl**, расположенный в директории **/opt/IWTM_Backup_Files/IWTM/**, в **control02.ctl** и скопируйте его в директорию **/u01/app/oracle/oradata/iwtm/**
   e. Проверьте права.
5. При необходимости, измените их:
   ```
   OS> chown -R oracle:oinstall /u02/
   OS> chown -R oracle:oinstall /u01/app/oracle/oradata/iwtm/
   ```
6. Запустите БД
   ```
   OS> dbstart $ORACLE_HOME
   ```

Восстановление на новой БД

**Если структура каталогов на новой БД отличается от структуры старой БД, выполните следующие шаги:**

1. В директории **/opt/IWTM_Backup_Files/Recovery_Aid** отредактируйте файл **initiwtm.ora** так, чтобы он соответствовал структуре каталогов новой БД.
2. Скопируйте отредактированный файл **initiwtm.ora** в директорию **$ORACLE_HOME/dbs** на компьютер, где расположена новая БД.
3. На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
4. Откройте Oracle SQL*Plus и подключитесь как пользователь **sysdba**:
   ```
   OS> sqlplus / as sysdba
   ```
5. Сгенерируйте файл параметров
   ```
   SQL> create spfile from pfile;
   ```
6. Если нужно переименовать какие-либо файлы, воспользуйтесь следующим сценарием:
   ```
   OS> sqlplus / as sysdba
   SQL> startup mount
   SQL> alter database rename file '/<path_to_proddb_files>/<filename1>' to '/<path_to_clonedb_files>/<filename1>';
   …
   SQL> alter database rename file '/<path_to_proddb_files>/<filenameN>' to '/<path_to_clonedb_files>/<filenameN>';
   SQL> shutdown immediate
   ```
   Здесь `path_to_proddb_files` – это путь к директории, где размещены файлы новой БД, в которой восстанавливается резервная копия, а `path_to_clonedb_files` - путь к директории, где размещены файлы резервной копии.

### 6.1.5 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 sqlplus, из-под учетной записи владельца схемы выполните запрос:

```
select JOB_NAME, STATE

from user_scheduler_jobs u

where u.enabled = 'TRUE'
```

4. Выключите задания, выполнив сценарий:

```
BEGIN

dbms_scheduler.disable('JOB_1');

…

dbms_scheduler.disable('JOB_N');

COMMIT;
```

```
END;

/
```

где `JOB_1… JOB_N` – имена выключаемых заданий.

5. Убедитесь, что ни одно задание не выполняется. Для этого выполните запрос:

```
SELECT job_name

FROM user_scheduler_running_jobs
```

Будет выведен перечень запущенных заданий. Если какое-либо задание выполняется, Вы можете остановить его, выполнив сценарий:

```
BEGIN

dbms_scheduler.stop_job('имя_задания');

COMMIT;

END;

/
```

6. Для предотвращения зависания остановите сервер Device Monitor:
`net stop iwdms`
7. Выполните необходимые работы с базой данных.
8. По окончании необходимых работ, с сервера Traffic Monitor проверьте соединение с сервером базы данных:

```
sqlplus db_login/db_password@tns_name
```

Здесь `db_login` и `db_password` – имя и пароль владельца схемы базы данных, а `tns_name` – имя службы TNS.
Если проверка пройдена успешно, то в ответ на выполнение команды будет выведено приглашение SQL *Plus:

```
SQL>
```

9. Запустите Device Monitor Server:
`net start iwdms`
10. Запустите процессы Traffic Monitor Server:
`iwtm start`

```
service iwtm-php-fpm start
```

```
service nginx start
```

11. Проверьте системный журнал на наличие ошибок. Путь к файлу журнала:

```
/var/log/messages
```

12. Если в системном журнале содержится информация об ошибках, то обратитесь в службу технической поддержки.
13. Включите выполнение ранее отключенных заданий:

```
BEGIN
dbms_scheduler.enable('JOB_1');
…
dbms_scheduler.enable('JOB_N');
COMMIT;
END;
/
```

где `JOB_1… JOB_N` – имена ранее остановленных заданий.

### 6.1.6 Логирование базы данных

Логированием работы СУБД Oracle в Traffic Monitor управляет скрипт, который позволяет устанавливать уровень логирования и выгружать данные лога в CSV-файл. При работе скрипта используются настройки текущего конфигурационного файла `/opt/iw/tm5/csw/database.conf`. Запускать скрипт следует из директории его местонахождения: `/opt/iw/tm5/csw/oracle/scripts/sys_log/sys_log.sh`.

Скрипт поддерживает следующие команды:

- чтобы установить уровень логирования: `debug, info, warning, error –` выполните команду:
  `level`
  при этом выводится текущий уровень логирования при запуске без второго параметра;

- чтобы выгрузить тело лога (представление V_SYS_LOG) в CSV-файл, выполните команду:
  `export`
  при этом, если требуется, можно задать количество выгружаемых строк:
  `export <кол-во строк>`

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

### Ротация логов базы данных

Ротация логов базы данных - это процесс архивирования, хранения и удаление старых данных в журналах, нужный для экономии и освобождения свободного дискового пространства. В Traffic Monitor ротация настроена на:

1. Логи базы данных:
   a. xml-файл, содержащий журнал ошибок и важных сообщений в папке `/u01/app/oracle/diag/rdbms/iwtm/iwtm/alert.` Срок хранения файла - 1 год. Он ротируется по 10 Мб и удаляется автоматически;
   b. trc-, trm-файлы, содержащие подробную информацию об ошибках БД (trace files) в папке `/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace.` Срок хранения файлов - 30 дней, после которых удаляются автоматически;
   c. `alert_iwtm.log` - лог БД в текстовом формате в папке `/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace.` Он ротируется службой **logrotate** по 100 Мб и удаляется после превышения количества в 1000 файлов.
2. Логи сетевой службы **listener**:
   a. xml-файл, содержащий логи службы **listener** в папке `/u01/app/oracle/diag/tnslsnr/hostname/listener/alert.` Срок хранения файла - 1 год. Он ротируется по 10 Мб и удаляется службой **crond**.
   b. trc-, trm-файлы, содержащие подробную информацию об ошибках службы listener. Срок хранения файлjd - 30 дней, после которых удаляются службой **crond**.
   c. `listener.log` - лог службы **listener** в текстовом формате в папке `/u01/app/oracle/diag/tnslsnr/hostname/listener/alert` . Он ротируется службой **logrotate** по 100 Мб и удаляется после превышения количества в 100 файлов.

Настройки службы **crond** для удаления старых файлов находятся в `/etc/cron.daily/delete_old_oracle_logs.cron.`

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

## 6.2 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:

- Изменение предустановленных паролей;

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

### 6.2.1 Изменение предустановленных паролей

Чтобы заменить предустановленные пароли пользователей БД:

1. Остановите процессы Traffic Monitor:
   `iwtm stop`
2. Подключитесь к БД PostgreSQL:
   `psql -p 5433 -h 127.0.0.1 postgres iwtm`
3. Получите список пользователей:
   `\du`
4. Измените пароли пользователей:
   `alter user 'iw_user' with password 'new_password';`
   где `'iw_user'` - выбранный пользователь БД, `'new_password'` - новый пароль для этого пользователя.
5. Выйдите из БД PostgreSQL:
   `\q`
6. Запустите процессы Traffic Monitor:
   `iwtm start`

Чтобы изменить предустановленный пароль Traffic Monitor, смотрите "Изменение предустановленного пароля Traffic Monitor".

### 6.2.2 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.).<br>Управление системой через Консоль управления (роли, учетные записи пользователей и др.) |
| Ежедневное | Хранение объектов, перехваченных в течение одних суток.<br>Хранение информации о результатах анализа и обработки объектов (разобранный объект, категории, термины и др.).<br>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 *IWTM_X*, где *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.

## 6.2.3 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 iwtm_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 `postgres` 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 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;
  ```
- 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;
  ```
- 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 архивировано Системой. Это число должно быть меньше устанавливаемого количества дней до удаления ежедневного ТП (см. "Удаление ежедневных табличных пространств").

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 iwtm_iwtm_add_parts, iwtm_iwtm_delete_tablespaces, iwtm_iwtm_archive_tablespaces так как это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:
   `select pkg_part_archive_tablespace(N);`
   где `N` – это значение атрибута `tbs_id` целевого ТП из таблицы `tbs_list`.
   После выполнения этого сценария статус 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 iwtm_iwtm_add_parts, iwtm_iwtm_delete_tablespaces и iwtm_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 (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('/u03/pgdata/',1);`
7. Укажите путь к медленному диску:
   `select pkg_part_set_df_path('/u02/pgdata1/',1);`
8. При необходимости можно использовать несколько медленных дисков. Данные будут записываться на следующий медленный диск при заполнении предыдущего. Для

добавления дополнительных медленных дисков укажите новый путь:
`select pkg_part_set_df_path('/u02/pgdata2/',2);`

9. Укажите общее количество медленных дисков:
`select pkg_part_set_df_path_cnt('2');`
10. Поменяйте режим на медленные-быстрые диски:
`select pkg_part_set_filesys_type('fast/slow');`
Данные будут перенесены с быстрых дисков на медленные с помощью ночного задания (джоба).
11. Чтобы запустить перенос файлов вручную, выполните:
`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 (iwtm_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. Процедура iwtm_iwtm_delete_tablespaces не работает с теми табличными пространствами, которые были отключены/подключены вручную.

В результате выполнения этой процедуры удаляются все ежедневные ТП (в т.ч. информация об архивированных 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 архивированное ежедневное ТП не подлежит восстановлению (т.к. информация о нем была удалена из базы данных), вы можете удалить файлы данных этого ТП из архива.

**Важно!**

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

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 iwtm _iwtm_delete_tablespaces укажите интервал 366*4=1464 дня.

**Определение интервала времени для отключения ежедневных ТП**
Для автоматического отключения табличных пространств (по умолчанию функция выключена) вы можете использовать различные сценарии (запускаются от имени владельца схемы данных). Установите срок хранения информации об архивных ТП:

- 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;
```

- 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;
```
- 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, используйте значение 0);
`D` – количество дней, по прошествии которых ежедневное табличное пространство будет отключено в БД. Это число должно быть больше устанавливаемого количества дней до архивирования ежедневного ТП (см. "Автоматическое архивирование ежедневных табличных пространств").
После отключения архивных ТП от БД (статус *Offline*) они становятся недоступны Системе.

**Удаление архивированных ТП**

При отключении в БД архивированных ежедневных ТП в Системе остаются файлы данных (по умолчанию в директории / `u02/arch)`. Чтобы освободить пространство на жестком диске, можно (на выбор):

- удалить их вручную;
- добавить новые задачи, запускаемые по расписанию в файле `/etc/cron.d/iwtm_cleanup` или в другом файле с задачами в этой директории.

> **Пример**
>
> Чтобы удалить все архивированные ежедневные ТП старше 150 суток:
>
> 1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup` или другой файл с задачами в этой директории.
> 2. Добавьте строки:
> ```
> 35 3 * * * root find /u02/arch/ -type f -mtime +150 -delete > /dev/null 2>&1 &
> 40 3 * * * root find /u02/arch/ -type d -ctime +10 -empty -delete > /dev/null 2>&1 &
> ```
> 3. Сохраните изменения.
> 4. Примените новые настройки сервиса `cron`:
> ```
> systemctl reload crond
> ```

**Удаление ежедневных ТП вручную**

Если вам требуется немедленно удалить ежедневные 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 сценарий:

```
select pkg_part_delete_tablespaces();
```

Если требуется удалить одно ЭТП, выполните сценарий, указав его номер ( `tbs_id` ):

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

**Удаление ежедневных ТП с помощью скрипта**

Если вам требуется настроить автоматическое удаления ежедневных ТП, используйте скрипт **/opt/iw/tm5/bin/dbtools/dbconf-iwdrop-postgres.sh** или **/opt/iw/tm5/bin/dbtools/dbconf-jobs-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]` |
| Удалить все ЕТП | `/opt/iw/tm5/bin/dbtools/dbconf-jobs-postgres.sh start iwtm_delete_tablespace` |

**Пример**

Чтобы удалить все объекты со статусом *"Нет нарушения"*, старше 15 суток, выполните команды:

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

## 6.2.4 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 PostgreSQL;
- Копирование файлов БД в хранилище резервных копий.

#### Определение размера резервной копии

Чтобы рассчитать размер будущего архива, необходимо узнать суммарный размер каталога с базой PostgreSQL, 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/pgdata1  /u02/arch
   ```

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

#### 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 PostgreSQL

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

**Чтобы остановить БД PostgreSQL:**

1. На компьютере, где работает база данных, зайдите в систему от имени пользователя **root**.
2. В командной строке введите:
   `service pgagent-13 stop`

```
service postgresql-13 stop
```
По окончании процедуры резервного копирования сервисы можно запустить с помощью следующей команды:
```
service pgagent-13 start
service postgresql-13 start
```

Копирование файлов БД в хранилище резервных копий

1. Остановите все сервисы PostgreSQL (см. "Остановка PostgreSQL"). 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 инсталлятора и были оставлены параметры по умолчанию, то:
   - скопируйте содержимое директории **/u01/postgres/** в директорию **/opt/IWTM_Backup_Files/postgres**
   - скопируйте содержимое директории **/u02/pgdata/** в директорию **/opt/IWTM_Backup_Files/pgdata**
   - скопируйте содержимое директории **/u02/pgdata1/** в директорию **/opt/IWTM_Backup_Files/pgdata1**
   - скопируйте содержимое директории **/u02/arch/** в директорию **/opt/IWTM_Backup_Files/arch**

   > **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 PostgreSQL:
   ```
   service postgresql-13 stop
   service pgagent-13 stop
   ```
3. Установите БД PostgreSQL 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-13 start
   service pgagent-13 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").

### 6.2.5 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-13 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.

### 6.2.6 Логирование базы данных

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

Скрипт поддерживает следующие команды:

- чтобы установить уровень логирования: `debug, info, warning, error –` выполните команду:
  `level`
  при этом выводится текущий уровень логирования при запуске без второго параметра;
- чтобы выгрузить тело лога (представление V_SYS_LOG) в CSV-файл, выполните команду:
  `export`
  при этом, если требуется, можно задать количество выгружаемых строк:
  `export <кол-во строк>`

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

#### Ротация логов базы данных

Ротация логов базы данных - это процесс архивирования, хранения и удаление старых данных в журналах, нужный для экономии и освобождения свободного дискового пространства. В Traffic Monitor ротация настроена на  лог БД в текстовом формате: `/u01/postrges/pg_log/*.log.` Он ротируется службой **logrotate** по 100 МБ и удаляется после превышения количества в 1000 файлов.

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

# 7 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 работы с HTTP-запросами, передаваемыми по протоколу ICAP;
- 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

## 7.1 Процессы серверной части Traffic Monitor Server

В этом разделе:

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

### 7.1.1 Список процессов серверной части Traffic Monitor

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

| Назначение | Имя процесса | Описание процесса | Конфигурационный файл |
|---|---|---|---|
| **Сбор данных** | iw_icap | Обрабатывает HTTP-трафик. Принимает HTTP-запросы от ICAP-клиента. Извлекает данные из HTTP-запросов. Затем извлеченные данные добавляются в XML-контекст. Готовый XML-контекст передается подсистеме анализа и принятия решения для проверки. По окончании анализа передает ICAP-клиенту ответ с разрешением/ запрещением на доставку HTTP-запроса. Также передает HTTP-запрос процессу **iw_x2db** для сохранения в базу данных | /opt/iw/tm5/etc/icap.conf |

| Назначение | Имя процесса | Описание процесса | Конфигурационный файл |
|---|---|---|---|
| | | | |
| | 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:<br>• 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**.<br>• 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**.<br>• iw_proxy_smtp - процесс, принимающий копию SMTP-трафика. Принимает SMTP-письмо, формирует XML-контекст из | /opt/iw/tm5/etc/proxy.conf |

| Назначение | Имя процесса | Описание процесса | Конфигурационный файл |
|---|---|---|---|
| | | 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 | |
| | 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 | /opt/iw/tm5/etc/messed.conf |

| Назначение | Имя процесса | Описание процесса | Конфигурационный файл |
|---|---|---|---|
| | | 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 | |
| | iw_xapi | Включает в себя две службы: **iw_xapi_xapi** и **iw_xapi_puppy**. Получает объекты от Infowatch Device Monitor и внешних систем (через адаптеры) по thrift-интерфейсу, 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 | /opt/iw/tm5/etc/analysis.conf |

| Назначение | Имя процесса | Описание процесса | Конфигурационный файл |
|---|---|---|---|
| | | файловую очередь для отправки в базу данных процессом **iw_x2db** | |
| **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 |

| Назначение | Имя процесса | Описание процесса | Конфигурационный файл |
|---|---|---|---|
| | 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 | /opt/iw/tm5/etc/adlibitum.conf |

| Назначение | Имя процесса | Описание процесса | Конфигурационный файл |
|---|---|---|---|
| | | Directory, Domino Directory, Samba DC, Astra Linux Directory, Astra Linux Directory Pro и FreeIPA | |
| | 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_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 | /opt/iw/tm5/etc/indexer.conf |

| Назначение | Имя процесса | Описание процесса | Конфигурационный файл |
|---|---|---|---|
| | | данных для ее индексации и складывает индексы в файловое хранилище. При выполнении поискового запроса **sphinx** получает из файлового хранилища индексов id объектов | |
| | 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, 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 |

| Назначение | Имя процесса | Описание процесса | Конфигурационный файл |
|---|---|---|---|
| | consul | Производит обнаружение, регистрацию и мониторинг доступности сервисов, взаимодействующих с интерфейсом пользователя | /opt/iw/tm5/etc/consul/consul.json |
| | iw_system_check | 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 |

### 7.1.2 Настройка конфигурационных файлов серверной части Traffic Monitor

Полный перечень конфигурационных файлов Системы и описание настроек, которые вы можете изменять для отражения специфики работы Системы в вашей инфраструктуре, находятся в документе "*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*").

### 7.1.3 Работа с процессами серверной части Traffic Monitor

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

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

**Примечание:**

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

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

**Примечание:**

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 |

| Ключ запуска | Назначение |
| --- | --- |
| `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:<br>`service iw_cas start` (если требуется просмотр логов)<br>`iwtm start cas`<br>`iwtm start iw_cas`<br>`iwtm start iw_cas.service`<br>`systemctl start iw_cas` (без возможности просмотра логов)<br>`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".

## 7.2 Настройка использования OCR

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

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

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.

### 7.2.1 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>
</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">
```

## 7.3 Настройка параметров работы с HTTP-запросами, передаваемыми по протоколу ICAP

В файле **/opt/iw/tm5/etc/icap.conf** задаются параметры взаимодействия с ICAP сервером.

**Примечание:**

Файл **icap.conf** создается только после установки модуля интеграции с ICAP.

## 7.4 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.

### 7.4.1 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`<br>**Примечание:** Обработка файлов размером меньше 10 байт не поддерживается.<br>Данное ограничение также распространяется на тип событий Буфер обмена. |

| | |
|---|---|
| `MaxTextPlainSizeInKb` | Верхняя граница размера файла, сигнатура которого не определена. При превышении порогового значения файл автоматически считается бинарным и не отправляется на анализ в **iw_cas**. Значение по умолчанию – `25600` |
| `SpeedInKBs` | Предположительная скорость работы экстрактора в расчете на 1 ГГц частоты процессора (в Кб/с). Может принимать целочисленные значения от 1 и выше. Значение по умолчанию – `100` |
| `TimeoutInSec` | Время ожидания до завершения обработки файла (в секундах). Значение по умолчанию – `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

**Пример**

Время работы экстрактора можно вычислить по формуле:

Время работы экстрактора = Размер файла в Кб / 1024 / ( `SpeedInKBs` * Тактовая_частота процессора в МГц / 1000)

Остальные секции содержат сигнатуры, при помощи которых детектируются типы файлов, находящиеся во вложениях и архивах. Секции имеют следующий набор параметров:

| Параметр | Описание и примеры настройки |
|---|---|
| `Extension` | Расширение файла архива. Необязательный параметр, необходим для корректной работы некоторых архиваторов, которые требуют наличия правильного расширения входных файлов<br>**Пример**<br>`Ext = arj` |
| `Name` | Имя формата. Используется для точного определения имени формата при распаковке файла.<br>Для определения/уточнения формата может включать также список имен:<br>`"defaultname, name1(code1), name2(code2)"`<br>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:<br>**Пример 1 (одно имя формата)**<br>`text/xml` |

| | |
|---|---|
| | **Пример 2 (список имен формата)**<br>`"application/arj, UNKNOWN(9), text/encrypted(4)"`<br>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<br>Сигнатура может включать до 16 триад вида:<br>`[OFFSET]:BYTE_VALUE/[MASK]`<br>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.<br>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?'`.<br>Параметр MASK, также является необязательным и равен `0xFF` по умолчанию.<br>**Пример** (сигнатура заголовка WAV-формата):<br>`Sign = "'RIFF', 0x8: 'WAVEfmt'"`<br>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:<br>`Comment = "bzip2 v. 1.0.x"` |
| `Command` | Строка команды для извлечения файлов. Например,<br>`Extract = "/usr/bin/bzip2 -f -dc ${SRC} > ${OUTDIR}/${SRC}"`<br>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:<br>• assurance - достоверность определения формата файла этой сигнатурой,<br>• offset - смещение, на котором нужно начинать поиск этой сигнатуры,<br>• max_length - длина проверяемого участка,<br>• 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. |

## 7.5 Архивирование каталога очереди сообщений

При ошибках в очереди входящих SMTP-писем:

1. Заархивируйте каталог очереди SMTP-писем **queue/smtp** и сохраните его для последующего анализа.
2. Удалите каталог.

## 7.6 Логирование работы Системы

Для удобства отслеживания работы процессов, подсистема протоколирования имеет шесть уровней:

| Название уровня | Описание |
|---|---|
| `fatal` | Показывает ошибки, которые препятствуют дальнейшей работе процесса |

| Название уровня | Описание |
|---|---|
| `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.

## 7.7 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` |
| `iwtm start proxy_smtp` | `iwtm stop proxy_smtp` |
| `iwtm start capstack` | `iwtm stop capstack` |

Объекты в Системе перемещаются посредством файловых очередей:

| Путь к директории очереди | Формат файлов в очереди |
|---|---|
| queue/analysis | .xml & .dat |
| queue/smtp | .xml & .dat |
| queue/db | .xml & .dat |
| queue/blackboard | .dat |
| queue/blackboard_errors | .dat |
| queue/is | .xml & .dat |
| queue/x2x | .xml & .dat |
| 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.`

## 7.8 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=#` Если Traffic Monitor Server работает с установленной СУБД Oracle, то для проверки соединения выполните команду:
   `sqlplus db_login/db_password@tns_name`
   где `db_login` и `db_password` – имя и пароль владельца схемы базы данных, а `tns_name` – имя службы TNS.
   Если проверка пройдена успешно, то в ответ на выполнение указанной команды будет выведено приглашение SQL *Plus:
   `SQL>`
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.

## 7.9 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 языка для поиска событий. Морфология и добавление терминов.;
- Обновление установленного языка;
- Удаление языка для поиска и терминов.

### 7.9.1 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/postgres/database.conf` Если используется СУБД Oracle, то для добавления терминов откройте файл **database.conf**:
   `mcedit /opt/iw/tm5/csw/oracle/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
```

### 7.9.2 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.

### 7.9.3 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` Если используется СУБД Oracle, то для добавления терминов откройте файл **database.conf**:
   `mcedit /opt/iw/tm5/csw/oracle/database.conf`
3. Удалите код языка с поддержкой морфологии из параметра `define cfdb_language`.
4. Удалите файлы индексации из директории `/var/lib/sphinx/`
5. Запустите процессы:

```
iwtm start indexer
iwtm stop is
```

После удаления словаря будет произведена полная переиндексация БД.

**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.

## 7.10 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 Oracle или 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

### 7.10.1 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 присутствует. | 110 |
| `monitorcode` | varchar2(4000) | Атрибут события *Тип события* | Тип события определяет способ передачи данных. Может принимать одно из следующих значений:<br>• Съемные устройства;<br>• Печать;<br>• ICQ;<br>• Skype;<br>• XMPP;<br>• Mail.Ru Агент;<br>• Telegram;<br>• Vkontakte;<br>• Facebook;<br>• WhatsApp;<br>• MS Lync;<br>• FTP;<br>• Email; | Email |

| Наименование атрибута | Тип данных | Описание | Возможные значения | Пример заполнения |
|---|---|---|---|---|
| | | | • Web-почта;<br>• Web-сообщение;<br>• Буфер обмена;<br>• Облачные хранилища;<br>• Ввод с клавиатуры;<br>• Терминальная сессия;<br>• Сетевые ресурсы;<br>• Чтение файла;<br>• Запись файла. | |
| `protocol` | | Атрибут события *Протокол* | Протокол может принимать одно из следующих значений:<br>• OSCAR<br>• Skype<br>• XMPP<br>• MMP<br>• SIP<br>• FTP<br>• POP3<br>• IMAP<br>• MAPI<br>• SMTP<br>• HTTP<br>• HTTPS<br>• NRPC<br>• WhatsApp<br>• Отсутствует | |
| `verdict` | varchar2(12) | Атрибут события *Вердикт* | Возможны значения:<br>• *Quarantined* (*Карантин*)<br>• *Forbidden*<br>( | Forbidden |

| Наименование атрибута | Тип данных | Описание | Возможные значения | Пример заполнения |
|---|---|---|---|---|
| | | | *Заблокировано*)<br>• *Allowed* (*Пропущено*) | |
| `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. | Kingston USB Drive 5.0 |

| Наименование атрибута | Тип данных | Описание | Возможные значения | Пример заполнения |
|---|---|---|---|---|
| | | | Либо наименование принтера, на который был отправлен на печать документ из перехваченного события.<br>Может быть не заполнено. | |
| `websource` | varchar2(256) | Атрибут события *Ресурс* | Адрес посещенного веб-ресурса или адрес облачного хранилища.<br>Может быть не заполнено. | Yahoo.com |
| `recipientscontacts` | clob | Атрибут события *Получатели* | Список контактов получателей через запятую. Контакты указанны в формате `<тип контакта>:<значение контакта>`.<br>Может быть не заполнено. | email:ivanov@infowatch.ru, email:petr.petrov@infowatch.ru |
| `recipientsfullname` | clob | Атрибут события *Получатели* | Список полных имен получателей через запятую.<br>Указаны в том же порядке, что и в `recipients`.<br>Указаны только в том случае, если получателей удалось проидентифицировать.<br>Поле может быть не заполнено. | Ivanov Ivan Ivanovich,<br>Petrov Petr Petrovich |

| Наименование атрибута | Тип данных | Описание | Возможные значения | Пример заполнения |
|---|---|---|---|---|
| `recipientsdomainaccountname` | clob | Атрибут события *Получатели* | Список ключей идентификации типа `auth` всех получателей через запятую. Указаны в том же порядке, что и в `recipients`.<br>Может быть не заполнено. | Ivanov@iw,<br>Petrov@iw |
| `senderdomainaccountname` | clob | Атрибут события *Отправители* | Ключ идентификации типа `auth` отправителя.<br>Поле может быть не заполнено. | Petrov@iw |
| `senderfullname` | clob | Атрибут события *Отправители* | Полное имя отправителя.<br>Поле может быть не заполнено. | Petrov Petr Petrovich |
| `sendercontacts` | clob | Атрибут события *Отправители* | Контакт отправителя, указанный в формате `<тип контакта>:<значение контакта>`.<br>Может быть не заполнено. | email:petr.petrov@infowatch.ru |
| `sendermachinedomainname` | clob | Атрибут события *Рабочая станция* | Доменное имя `dnshostname` рабочей станции отправителя.<br>Может быть не заполнено. | XP-PETROV |
| `sendermachineip` | clob | Атрибут события *Рабочая станция* | IP-адрес рабочей станции отправителя.<br>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.<br>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.<br>Может быть не заполнено. | Периметр компании |
| `tags` | clob | Атрибут события *Тег* | Список тегов через запятую.<br>Может быть не заполнено. | New |
| `categories` | clob | Атрибут события *Категория* | Список категорий через запятую.<br>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.<br>Может быть не заполнено. | special control |
| `fingerprints` | clob | Атрибуты события *Бланк*, | Список названий форм, эталонных документов | Бланк заявки.doc |

| Наименование атрибута | Тип данных | Описание | Возможные значения | Пример заполнения |
|---|---|---|---|---|
| | | *Эталонный документ*, *Печать*, *Выгрузка из БД* | , печатей и выгрузок из БД, обнаруженных в перехваченном объекте. Элементы в списке указаны через запятую.<br>Может быть не заполнено. | |
| `protecteddocuments` | clob | Атрибут события *Объект защиты* | Список объектов защиты, обнаруженных в перехваченном объекте. Объекты защиты в списке указаны через запятую.<br>Может быть не заполнено. | Договор аренды |
| `policies` | clob | Атрибут события *Политика* | Список названий политик, сработавших на перехваченном объекте. Политики в списке указаны через запятую.<br>Может быть не заполнено. | Политика контроля новых сотрудников |
| `violationtype` | varchar2(40) | Атрибут события *Группа правил* | Может принимать следующие значения:<br>▪ *Copy* (*Нарушение копирования*)<br>▪ *Placement* (*Нарушение хранения*)<br>▪ *Transfer* (*Нарушение передачи*)<br>Может быть не заполнено. | Copy |

| Наименование атрибута | Тип данных | Описание | Возможные значения | Пример заполнения |
|---|---|---|---|---|
| `violation_level` | Список | Атрибут события *Уровень нарушения* | Может принимать следующие значения:<br>▪ *High* (*Высокий*)<br>▪ *Medium* (*Средний*)<br>▪ *Low* (*Низкий*)<br>▪ *No violation* (*Отсутствует*)<br>Может быть не заполнено. | Medium |
| `userdecision` | varchar2(27) | Атрибут события *Решение пользователя* | Решение пользователя консоли.<br>Может принимать следующие значения:<br>▪ *Violation* (*Нарушение*)<br>▪ *NoViolation* (*Нет нарушения*)<br>▪ *NotProcessed* (*Решение не принято*)<br>▪ *AdditionalProcessingNeeded* (*Требует дополнительной обработки*)<br>Может быть не заполнено. | Violation |
| `filepath` | clob | Атрибут события *Путь к файлу* | Список путей к файлам. Пути в списке указаны через запятую.<br>Может быть не заполнено. | \\xp-petrov\C$\666.txt |

| Наименование атрибута | Тип данных | Описание | Возможные значения | Пример заполнения |
|---|---|---|---|---|
| `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.<br>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.<br>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.<br>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 |

| Атрибут | Тип данных | Описание | Пример заполнения |
|---|---|---|---|
| `change_date` | Varchar2(50) | Дата и время зарегистрированного действия пользователя | 05.08.2015 09:35:10.641446000 |
| `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 |
| `operation` | varchar2(40) | Тип действия, которое было произведено пользователем.<br>Возможны значения:<br>• restart (перезапуск)<br>• delete_hash (удаление хэша)<br>• sync (синхронизировать)<br>• add_tag (добавить тег)<br>• remove_tag (удалить тег)<br>• run (выполнение запроса)<br>• start (запуск)<br>• stop (остановка)<br>• view (просмотр)<br>• create (создание)<br>• update (редактирование)<br>• delete (удаление)<br>• login_failure (неуспешная попытка входа) | Edit |

| Атрибут | Тип данных | Описание | Пример заполнения |
| --- | --- | --- | --- |
| | | • login (успешный вход)<br>• logout (выход)<br>• change_password (изменение пароля)<br>• decision_update (изменение пользовательского решения)<br>• remove_tag (изменение тегов события)<br>• delete_ref (удаление ссылки)<br>• copy (копирование )<br>• move (перемещение)<br>• commit (применение изменений в конфигурации системы)<br>• rollback (откат изменений в конфигурации системы)<br>• draft (сохранение изменений в конфигурации системы)<br>• add (добавление)<br>• import (импорт)<br>• export (экспорт) | |
| `entity_type` | varchar2(40) | Тип объекта, над которым осуществлялось действие.<br>Возможны значения:<br>• AgentJob (диагностические данные)<br>• Adlibitum (адлибитум) | Dashboard |

| Атрибут | Тип данных | Описание | Пример заполнения |
| --- | --- | --- | --- |
| | | • Agent (служба)<br>• Classifier (классификатор)<br>• NetworkSettings (сетевые параметры)<br>• NotificationSettings (состояние системы)<br>• ObjectReport (выгрузка событий)<br>• Query (запуск поиска событий)<br>• QueryReportRun (агрегация отчета)<br>• Setting (настройки)<br>• UpdateSystem (обновление системы)<br>• Category (категория)<br>• Dashboard (дашборд)<br>• DashboardWidget (виджет)<br>• EtForm (эталонные формы)<br>• EtStamp (эталонные печати)<br>• EtTable (эталонные выгрузки)<br>• Fingerprint (эталонные документы)<br>• LdapContact (LDAP контакт)<br>• LdapGroup (LDAP группа)<br>• LdapPerson (LDAP персона)<br>• LdapStatus (LDAP статус персоны) | |

| Атрибут | Тип данных | Описание | Пример заполнения |
| --- | --- | --- | --- |
| | | • LdapWorkstation (LDAP рабочая станция)<br>• Perimeter (периметр)<br>• Policy (политика)<br>• ProtectedDocuments (объект защиты)<br>• Report (отчет)<br>• Role (роль)<br>• Selection (запрос)<br>• ServiceLog (лог сервиса)<br>• SystemList (список тематик ресурсов)<br>• SystemListItem (список ресурсов заданной тематики)<br>• Tag (тег)<br>• Term (термин)<br>• TextObject (текстовый объект)<br>• User (пользователь)<br>• VisibilityArea (область видимости)<br>• Config (Конфигурация)<br>• License (Лицензия)<br>• Object (Событие)<br>• 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 | |

| Атрибут | Тип данных | Описание | Пример заполнения |
| --- | --- | --- | --- |
| | | видимости и при осуществлении входа в консоль управления.<br><br>Возможны три формата заполнения поля. | |
| | - | **Формат №1.**<br>Актуален только для событий управления ролями и областями видимости. | |
| | | {<br>“old”: {<br>“<ТИП ОБЪЕКТА>”:{<br>{<br>“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,<br>“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”<br>}<br>}<br>}<br>{<br>“new”: {<br>“<ТИП ОБЪЕКТА>”:{<br>{<br>“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,<br>“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”<br>}<br>}<br>}<br>} | {<br>"old":{<br>"visibilityareas":{<br>}<br>},<br>"new":{<br>"visibilityareas":[<br>{<br>"VISIBILITY_AREA_ID":"F00207A1E7E7743EE0433D003C0A5DD400000000",<br>"DISPLAY_NAME":"<idclip>",<br>"NOTE":"<idclip>",<br>"VISIBILITY_AREA_CONDITION":"{"data":{"link_operator":"and","children":[]}}",<br>"IS_SYSTEM":1<br>}<br>}<br>} |
| | - | **Формат №2.**<br>Актуален только для событий управления пользователями. | |

| Атрибут | Тип данных | Описание | Пример заполнения |
|---|---|---|---|
| | | | |
| | | {<br>“old”:{<br>“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,<br>“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”<br>}<br>“new”:{<br>“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,<br>“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”<br>}<br>} | {<br>"old":{<br>"EMAIL":"asdasd@asdasd.ru",<br>"CHANGE_DATE":"01-07-2014 09:46:29.000000"<br>},<br>"new":{<br>"EMAIL":"asdasd11@asdasd.ru",<br>"CHANGE_DATE":"01-07-2014 09:46:44.000000"<br>}<br>} |
| | - | **Формат №3.**<br>Актуален только для событий входа пользователя в систему.<br>- | |
| | | {<br>"request":{<br>"hostname": “<ИМЯ ХОСТА>”,<br>"ip":"<IP-АДРЕС>",<br>"login":"<ЛОГИН ПОЛЬЗОВАТЕЛЯ>"<br>}<br>} | {<br>"request":{<br>"hostname":*null*,<br>"ip":"127.0.0.1",<br>"login":"officer"<br>}<br>} |

## 7.10.2 Настройки на стороне ТМ

**Чтобы настроить передачу консолидированной информации из ТМ:**

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 ТМ в SIEM (см. "Передача логов в SIEM");
4. Отрегулируйте настройку **Nagios** и компонент ТМ из меню;
5. Отрегулируйте настройки логирования аудита сессий пользователей БД ТМ.

### Передача логов в SIEM

**Чтобы настроить передачу записей из лог файлов Linux-сервера ТМ 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 логированием сессий пользователей БД ТМ

Включение и выключение логирования сессий пользователей БД ТМ в системном журнале ОС осуществляется через **rsyslog**.

**Чтобы включить логирование сессий пользователей Базы Данных ТМ**:

1. Запустите скрипт: `/opt/iw/tm5/bin/config/iwtm-siem.conf.py`
2. Выберите опцию **DB audit logging management**.
3. Введите учетные данные администратора БД:
   - **Enter login for DB administrative account** - логин для учетной записи;
   - **Enter password for DB administrative account** - пароль для учетной записи.
4. Нажмите **Check logging status**.
5. Если:
   - **DB audit logging to OS journal: OFF** - нажмите **Change logging status**, чтобы включить логирование.
   - **DB audit logging to OS journal: ON** - нажмите **Change logging status**, чтобы выключить логирование.

> **Примечание:**
>
> Если используется БД Oracle, то при смене статуса логирования будут перезапущены IWTM-сервисы. Это может занять некоторое время.

## 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 Oracle/PostgreSQL<br>**Примечание:** используются следующие логины:<br>• для Oracle - `sys`<br>• для PostgreSQL - `postgres` |

| Параметр | Описание |
| --- | --- |
| `Enter password for DB administrative account` | Пароль для учетной записи администратора Oracle/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 Oracle/PostgreSQL<br>**Примечание:** используются следующие логины:<br>• для Oracle - `sys`<br>• для PostgreSQL - `postgres` |
| `Enter password for DB administrative account` | Пароль для учетной записи администратора Oracle/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 Oracle/PostgreSQL |

| Параметр | Значение |
| --- | --- |
| `Enter password for DB administrative account` | Пароль для учетной записи администратора Oracle/PostgreSQL |

5. Нажмите **Delete**.

### 7.10.3 Типы логов, передаваемых в SIEM

Rsyslog формирует общий системный журнал и является протоколом, по которому логи передаются в SIEM.

Существует пять основных типов 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 подключения и отключения от **БД Oracle**:
   `Mar 11 14:28:20 iw-VMware-4224da3ab Oracle Audit[17786]: LENGTH : '153' ACTION :[7] 'STARTUP' DATABASE USER:[1] '/' PRIVILEGE :[4] 'NONE' CLIENT USER:[4] 'root' CLIENT TERMINAL:[13] 'Not Available' STATUS:[1] '0' DBID:[0]`
4. 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)`
5. Логи **Nagios**:
   `Feb 10 20:05:39 iw-VMware-4224289a4 nagios: SERVICE ALERT: IWTM;TM_DAEMONS_STATE;CRITICAL;SOFT;1;CRITICAL - updater(3)`

## 7.11 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`

# 8 Настройка сквозной аутентификации между продуктами InfoWatch

Сквозная аутентификация позволяет вам переходить между установленными продуктами InfoWatch без повторного ввода логина и пароля. В данной версии InfoWatch Traffic Monitor поддерживается технология единого входа с продуктом InfoWatch Vision версии 2.5 и возможна только при явном переходе из одного продукта в другой и только для пользователей, созданных на основании одинаковой учетной записи в Active Directory.

Чтобы настроить сквозную аутентификацию:

1. В командной строке на сервере Vision введите команду:
   ```
   kubectl get secret guardkeys-central -n infowatch -o 'go-template={{index .data "ec256-public.pem"}}' | base64 -d
   ```
2. Скопируйте выданный системой публичный ключ в pem-формате. Пример ключа:
   ```
   -----BEGIN PUBLIC KEY-----
   MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAExqBY7YcuTlucSX6s8LBTrBmWRuxT
   WkEmnwCBkurgc9Ntm+o+QOOmCZube3M8yimt2Xqy3sgq/WJe+PoGjvhVCg==
   -----END PUBLIC KEY-----
   ```
3. Подключитесь к БД Traffic Monitor:
   a. Если используется БД PostgreSQL:
      `psql postgres iwtm`
   b. Если используется БД Oracle:
      `sqlplus iwtm@iwtm`
4. Укажите в Traffic Monitor список доверенных систем с их открытыми ключами, которые могут авторизоваться в Traffic Monitor, используя свою учетную запись. Для каждой доверенной системы задайте название доверенной системы и открытый ключ доверенной системы. Например, выполните команду:
   ```
   insert into trusted_system(system_name, public_key)
   values('my system','-----BEGIN PUBLIC KEY-----
   MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAExqBY7YcuTlucSX6s8LBTrBmWRuxT
   WkEmnwCBkurgc9Ntm+o+QOOmCZube3M8yimt2Xqy3sgq/WJe+PoGjvhVCg==
   -----END PUBLIC KEY-----');
   commit;
   ```
5. Выйдите из БД:
   a. Если используется БД PostgreSQL:
      `\q`
   b. Если используется БД Oracle:
      `exit`
6. Откройте новую вкладку браузера и войдите в консоль Traffic Monitor.
7. Настройте и запустите синхронизацию с Active Directory для импорта пользователя, который и будет работать в обеих системах. Дождитесь успешного завершения синхронизации.
8. В разделе **Управление доступом** добавьте нового пользователя из LDAP, назначьте ему роль на просмотр событий и область видимости.
9. Выйдите из учетной записи пользователя.
10. Откройте консоль Vision на другой вкладке браузера.
11. Настройте и запустите ту же синхронизацию с Active Directory для импорта того же пользователя.
12. После успешной синхронизации на вкладке **Пользователи** добавьте нового пользователя из LDAP, назначьте ему роль.

13. Выйдите из учетной записи пользователя и войдите под новым созданным пользователем LDAP.
14. Перейдите в раздел **События** , щелчком мыши выберите в списке одно или несколько событий и нажмите **Просмотр события**.

Будет автоматически открыт раздел **События** консоли Traffic Monitor, а также зарегистрирован вход пользователя из внешней системы в журнале аудита.

# 9 Взаимодействие с внешними системами

Обмен данными между Traffic Monitor и внешними системами осуществляется посредством API. Для удобства работы с ним реализован пакет **iwtm-apidocs-publicapi**, который входит в состав Traffic Monitor и требует установки. Для этого выполните команду на сервере Traffic Monitor: `yum install iwtm-apidocs-publicapi`

При этом будут установлены пакеты:

- **iwtm-apidocs-publicapi**, содержащий OpenAPI-схемы публичного API;
- **iwtm-apidocs-common**, содержащий UI с полным описанием методов, включая модели, коды ответов, параметры запросов. Доступ к нему осуществляется по адресу: <имя_сервера_TM>/doc/

Далее описаны протоколы обмена данными между Traffic Monitor и внешними системами:

- Загрузка событий в InfoWatch Traffic Monitor (pushAPI SDK);
- Загрузка эталонных документов и выгрузок из БД в Traffic Monitor (REST API SDK);
- Получение доступа к событиям Traffic Monitor внешними системами (DataExport API SDK).

## 9.1 Загрузка событий в InfoWatch Traffic Monitor (pushAPI SDK)

Программный интерфейс pushAPI SDK предназначен для интеграции сторонних компонентов с Traffic Monitor для осуществления перехвата информации с различного рода каналов и их последующего анализа.
Сторонние компоненты самостоятельно формируют события перехвата данных и передают их в Traffic Monitor. После этого Traffic Monitor классифицирует события, анализирует их и выносит свой вердикт на основе настроенных политик защиты данных. Переданные события и вердикты можно просматривать в консоли Traffic Monitor.

### 9.1.1 Принципы использования pushAPI SDK

Для организации передачи событий на Traffic Monitor необходимо учитывать следующие принципы:

- События перехвата передаются в Traffic Monitor в виде объектов «событие»;
- Каждое «событие» имеет набор обязательных атрибутов, которые задаются пользователем программного интерфейса;
- Каждое «событие» может иметь набор необязательных атрибутов, которые задаются пользователем программного интерфейса;
- Каждое «событие» имеет «отправителя» и «получателя»;
- Каждый «отправитель» и «получатель» может иметь связанный с ним список «контактов», которые позволяют уникальным образом идентифицировать отправителя и получателя;
- Каждый «получатель» и «отправитель» может иметь связанный с ним набор атрибутов;
- Каждое «событие» имеет связанные с ним «данные», т.е. последовательность байт и/или символов текста, которые представляют собой содержимое перехваченного события;
- Каждый элемент «данных» может иметь связанный с ним набор атрибутов.

Все возможные «события», которые может принимать и анализировать Traffic Monitor, разбиты на группы – классы событий, которые объединены общими характеристиками. Класс события определяет бизнес-логику обработки события, а также правила его отображения в консоли Traffic Monitor.
На данный момент поддерживаются следующие классы событий:

- **Почта** – любые события обмена электронными письмами, включая вложения. Характеризуется списком персон-отправителей и персон-получателей, датой отправки, темой, телом и вложениями к письму. Включает в себя корпоративную почту (IMAP, POP3, SMTP, MAPI, NRPC) и Веб-почту (HTTP, HTTPS). Название сервиса в ТМ: **Почта**;
- **Беседа** – любые события беседы, представляющие собой обмен текстовыми сообщениями или файлами в рамках одного приложения. Приложение может являться как тонким клиентом на рабочих станциях и мобильных устройствах, так и web-приложением. Характеризуется списком реплик. Для каждой реплики должна быть указана персона-отправитель, время отправления и текст сообщения. Следующие сервисы уже предустановлены в этом классе: MS Lync, ICQ, Mail.ru, Jabber, Skype (передача SMS и обычных текстовых сообщений). Название сервиса в ТМ: **Мессенджеры**;
- **Печать, копирование и сканирование** – события преобразования данных на специализированных устройствах ввода и вывода изображений/документов (например: Принтер, Сканер). Характеризуется персоной-отправителем и устройством-получателем, количеством копий, а также файлом с оригиналом документа/образом документа/заданием на печать. В рамках этого класса предустановлен сервис Принтер. Название сервиса в ТМ: **Принтер и МФУ**;
- **Интернет-активность** – события формирования запросов из Web-браузеров и аналогичных программ, осуществляемое по протоколам HTTP, HTTPS. В событие данного типа попадают все данные, для которых не нашлось другого типа. Примером может служить отправка веб-сообщения . Характеризуется персоной-отправителем и ресурсом-получателем в случае POST-запросов или персоной-получателем и ресурсом-отправителем в случае GET-запросов, а также текстом "сырого" запроса. В рамках этого класса предустановлен сервис Интернет-приложение. Название сервиса в ТМ: **Интернет-активность**;
- **Фотосъемка** – события фотосъемки с помощью камеры устройства. Характеризуется персоной-отправителем и устройством-получателем, а также перехваченным изображением. Название сервиса в ТМ: **Запись мультимедиа**;
- **Обмен файлами** – любые события, связанные с передачей файлов между произвольными отправителями и получателями. Характеризуется персоной-отправителем и персоной-/устройством-/ресурсом-получателем, а также перехваченным файлом. Включает в себя копирование на USB-устройство, в облачное хранилище, обмен файлами по FTP-протоколу.Следующие сервисы уже предустановлены в этом классе: FTP, Съемное устройство, MS Lync, ICQ, Mail.ru, Jabber, Skype, Облачные хранилища, Терминальная сессия, Сетевые ресурсы. Название сервиса в ТМ: **Мессенджеры** (если отправители и получатели события являются персонами) или **Обмен файлами** (если хотя бы один отправитель или получатель события не является персоной);
- **Звонок** – любое событие голосового или видеоразговора между людьми, который может происходить по мессенджеру или телефону. Характеризуется персоной-отправителем (инициатор звонка) и персонами-получателями, а также файлом и длиной записи разговора. Примером могут служить отправка/получение SMS и MMS или перехват разговоров в сотовых сетях. Следующие сервисы уже предустановлены в этом классе: MS Lync, Mail.ru, Jabber, Skype. Название сервиса в ТМ: **Мессенджеры**;
- **Запись мультимедиа** – события создания аудио- и видеозаписи с помощью устройства. Характеризуются персоной-отправителем и устройством-получателем, а также перехваченным изображением. Примером могут служить записи с микрофонов/диктофонов или записи на видеокамеру, а также любые события, связанные с

фотографированием потенциально конфиденциальных документов на камеру устройства. Название сервиса в TM: **Запись мультимедиа**;

Пользователь SDK должен обязательно определить «Тип» для своих перехваченных объектов и «Протокол» перехваченного объекта. «Протокол» определяет, что именно было перехвачено с точки зрения пользовательского сервиса, который использовал «отправитель» для передачи информации.

Пользователь SDK может выбрать сервис из числа встроенных в Traffic Monitor или определить и зарегистрировать свой собственный. На основании «Протокола» объекта и идентификатора компании-производителя перехватчика реализуются политики лицензирования внутри Traffic Monitor. «Протокол» объекта представляет собой последовательность символов и определяется пользователем SDK.

**Пример:**

Если пользователь SDK реализовал перехватчик для клиента Viber, он может определить и зарегистрировать сервис "Viber". На каждый сервис одного производителя будет выдаваться отдельная лицензия.

«Протокол» перехваченного события может задаваться как одно из условий в формировании «политики» Traffic Monitor и аналитических запросах.
У каждого «События» должны быть определены «отправитель(и)» и «получатель(и)».
Поддерживаются следующие типы «получателей» и «отправителей»:

- «Персона» – представляет собой «пользователя», который определяется как создатель, отправитель или получатель перехваченного объекта. Для персоны можно определить набор «контактов» для её идентификации. Тип контакта можно выбрать из списка, который поддерживается SDK. В качестве примера типа контакта можно привести email, телефон или учётную запись Windows;
- «Компьютеры» – представляет собой компьютер, мобильное устройство или терминальный сервер, на котором был «создан» перехваченный объект. Для данного типа «отправителя» можно определить список «контактов»;
- «Ресурс» – представляет собой адрес в сети Интернет, на который были переданы данные;
- «Устройство» – представляет собой устройство, которое получает данные при копировании файлов на съёмные носители;

Список контактов, связанных с «Персоной», позволяет идентифицировать её по любому её контакту. Таким образом, любые перехваченные действия «Персоны», в которых определён хотя бы один её контакт, позволяет идентифицировать конкретного пользователя в Traffic Monitor.
Интерфейс SDK позволяет связывать различные типы контактов между собой логическими связями, например, отправителя «Персону» с отправителем «Компьютеры». Это позволяет точно определить контекст перехватываемой операции, т.е. кто и где инициировал действие по передаче данных.
Добавление собственных «Протоколов» осуществляется через специальный файл заданного формата. Этот файл загружается в Систему через консоль Traffic Monitor и обновляет внутренние структуры данных. После этого новые «Протоколы» смогут принимать участие в создании правил и аналитических запросов.
Интерфейс SDK позволяет передавать данные в сеть по частям. Это позволяет внешним разработчикам самим определять стратегию ограничения нагрузки на сеть.
Общий алгоритм передачи события через интерфейс SDK выглядит так:

- Создать объект «Событие» и установить его атрибуты;
- Создать отправителей/получателей события, а также установить их контакты и атрибуты;
- Создать данные события и установить его атрибуты;
- Создать соединение с Traffic Monitor;

- Проверить доступ к Traffic Monitor и лицензию плагина внешнего разработчика;
- Передать «метаданные» события;
- Передать по частям содержимое данных события;
- Закрыть соединение;
- Удалить объект «Событие».

Более подробно процесс передачи событий можно посмотреть в Примерах SDK.

### 9.1.2 Общее описание программного интерфейса pushAPI SDK

Программный интерфейс реализован в виде Thrift-сервиса. Подробнее о Thrift-сервисах можно прочитать тут: https://thrift.apache.org. В состав примеров SDK входит Thrift схема, которая описывает сервис, реализованный в Traffic Monitor. Ниже приведено описание этой схемы.

#### Типы данных pushAPI SDK

| Код | **Описание** |
|---|---|
| Структура Identity | |
| `typedef i32 ItemId` | Идентификатор элемента в событии |
| `enum IdentityItemType { kPerson, kWorkstation, kDevice, kResource, }` | Вид элемента идентификации |
| `struct Attribute { 1: required string name, 2: required string value }` | Отдельный атрибут любой сущности события (самого события, идентификации, потока данных):<br>1. контакт;<br>2. метаинформация о контакте |
| `struct ContactWithMeta { 1: required Attribute contact, 2: optional string meta }` | Контакты идентификации с метаинформацией:<br>1. контакт;<br>2. метаинформация о контакте |
| `struct Identity { 1: required ItemId identity_id, 2: required IdentityItemType identity_type, 3: required list<Attribute> identity_contacts, 4: optional list<Attribute> identity_attributes, 5: optional` | Идентификация получателя или отправителя объекта:<br>1. уникальный номер идентификации внутри объекта, используется для ссылок на идентификацию;<br>2. вид элемента идентификации;<br>3. набор контактов идентификации;<br>4. не обязательный набор атрибутов идентификации; |

| Код | **Описание** |
| --- | --- |
| `list<ContactWithMeta> identity_contacts_with_meta }` | 5. набор контактов идентификации с метаинформацией |
| `struct EventData { 1: required ItemId data_id, 2: optional list<Attribute> data_attributes }` | Описание потока данных события:<br>1. уникальный идентификатор потока данных внутри события, используется для ссылок на поток;<br>2. необязательный набор атрибутов потока данных |
| `struct ChatMessage { 1: required ItemId sender_id, 2: required string sent_time, 3: required string utf8_text, 4: optional ItemId mes_data_id }` | Описание одного сообщения класса "Беседа":<br>1. ссылка на идентификацию, которая является отправителем сообщения;<br>2. локальное время передачи сообщения в формате ГГГГ-ММ-ДДТЧЧ:ММ:СС+ЧЧ:ММ (ISO 8601 с форматированием yyyy-MM-ddTHH:mm:sszzz);<br>3. текст сообщения в кодировке UTF-8;<br>4. идентификатор данных объекта, в которых будет передано содержимое сообщения, если utf8_text пустой |
| `typedef string LinkNameType struct ItemLink { 1: required ItemId id, 2: required ItemId link_to_id, 3: required LinkNameType link_name }` | Описание связи между различными сущностями события:<br>1. идентификатор сущности события, от которой идёт связь;<br>2. идентификатор сущности события, к которой идёт связь;<br>3. имя (тип) связи |
| `const LinkNameType link_name_ws = "workstation_link"` | Список имён поддерживаемых связей между сущностями:<br>• имя для задания связи идентификаций типа "Персона" и "Рабочая станция" |
| `struct Event { 1: required EventClass evt_class, 2: required TmServiceType evt_service, 3: optional list<Attribute> evt_attributes, 4: required list<Identity> evt_senders, 5: required list<Identity>` | Описание события, которое нужно передать в Traffic Monitor:<br>1. класс события;<br>2. сервис события;<br>3. атрибуты события;<br>4. отправители события;<br>5. получатели события;<br>6. данные события; |

| Код | **Описание** |
| --- | --- |
| `evt_receivers,`<br>`6: required list<EventData> evt_data,`<br>`7: optional list<ChatMessage> evt_messages,`<br>`8: optional list<ItemLink> evt_links,`<br>`9: optional Identity evt_source,`<br>`10: optional Identity evt_destination`<br>`}` | 7. сообщения события для класса "Беседа";<br>8. связи между сущностями в событии;<br>9. источник события;<br>10. приемник события |
| `struct Credentials {`<br>`1: required string company_name,`<br>`2: required string token`<br>`}` | Структура, описывающая параметры доступа к Traffic Monitor:<br>1. название клиента (или компании в нашем случае). Этот параметр связывает плагин внешнего разработчика с лицензией;<br>2. токен авторизации. Эта строка является «секретом», который знают плагин и Traffic Monitor. Так реализована авторизация источника данных |
| `typedef i64 EventId` | Идентификатор загружаемого события |
| `typedef i64 StreamId` | Идентификатор загружаемого потока данных события |
| `typedef i32 InterfaceVersion`<br>`const InterfaceVersion pushapi_version = 1` | Версия PushAPI интерфейса |
| `enum EventClass {`<br>`kChat,`<br>`kEmail,`<br>`kMfp,`<br>`kWeb,`<br>`kFileExchange,`<br>`kPhoto,`<br>`kMultimedia,`<br>`kVoiceTalk`<br>`}` | Поддерживаемые "классы" событий в PushAPI:<br>• Беседа<br>• Почта<br>• Печать, копирование и сканирование<br>• Интернет-активность<br>• Обмен файлами<br>• Фотосъемка<br>• Запись мультимедиа<br>• Звонок |

## Исключения pushAPI SDK

| Код | **Описание** |
|---|---|
| `exception EventNotFound { 1: string message, }` | EventId, указанный в списке параметров, не найден в рамках текущей сессии передачи события |
| `exception DataNotFound { 1: string message, }` | DataId для указанного EventId некорректный, т.е. указанный DataId не найден в рамках текущей сессии передачи события |
| `exception StreamNotFound { 1: string message, }` | StreamId для указанного EventId некорректный, т.е. указанный StreamId не найден в рамках текущей сессии передачи события |
| `exception InvalidEventFormat { 1: string message, }` | Некорректный формат события, т.е. не прошла проверка на содержимое атрибутов события. Каждый класс события имеет набор обязательных атрибутов |
| `exception InvalidCredentials { 1: string message }` | Некорректные параметры доступа к интерфейсу. Нужно указать правильный токен |
| `exception LicenseError { 1: string message }` | На сервере Traffic Monitor нет правильной лицензии для передачи событий |
| Примечание: message – уточняет причину возникновения исключения | |

## Сервисы Traffic Monitor pushAPI SDK

Встроенные в Traffic Monitor сервисы, которые можно использовать для событий:

```
const TmServiceType service_email = "email" //!< Почта на Клиенте
const TmServiceType service_email_web = "email_web" //!< Почта в Браузере
const TmServiceType service_im_icq = "im_icq" //!< ICQ
const TmServiceType service_im_skype = "im_skype" //!< Skype
const TmServiceType service_im_xmpp = "im_xmpp" //!< XMPP
const TmServiceType service_im_mmp = "im_mail_ru" //!< MMP
const TmServiceType service_im_lync = "im_lync" //!< MS Lync
const TmServiceType service_web = "web_common" //!< Web-сообщения
const TmServiceType service_file_removable_storage = "file_copy_removable" //!< Обмен файлами с внешним устройством (съёмным устройством хранения)
const TmServiceType service_file_ftp = "ftp" //!< Обмен файлами по FTP
const TmServiceType service_print = "print" //!< Печать
const TmServiceType service_cloud_storage = "cloud_storage" //!< Обмен файлами с облачным хранилищем
const TmServiceType service_terminal_session = "terminal_session" //!< Обмен
```

файлами через терминальную сессию
`const TmServiceType service_network_resource = "network_resource" //!< Обмен файлами с сетевыми ресурсами`

| Наименование сервиса | Классы | Описание |
|---|---|---|
| email | «Электронная почта» | Сервис перехвата корпоративной почты, который не зависит от используемого протокола или типа почтового сервера. При расширении класса «Электронная почта» рекомендуется добавлять к названию сервиса префикс "email_", например "email_google" |
| email_web | «Электронная почта» | Сервис перехвата почты в браузере |
| im_icq | «Беседа», «Голосовая беседа», «Обмен файлами» | Сервис перехвата программы обмена сообщениями "ICQ" (протокол "OSCAR") |
| im_skype | «Беседа», «Голосовая беседа», «Обмен файлами» | Сервис перехвата программы обмена сообщениями "Skype" |
| im_xmpp | «Беседа», «Голосовая беседа», «Обмен файлами» | Сервис перехвата любой программы обмена сообщениями, которая работает по протоколу XMPP (Jaber) |
| im_mail_ru | «Беседа», «Голосовая беседа», «Обмен файлами» | Сервис перехвата любой программы обмена сообщениями, которая работает по протоколу MMP(Mail.ru Agent) |
| im_lync | «Беседа», «Голосовая беседа», «Обмен файлами» | Сервис перехвата программы обмена сообщениями "MS Lync" |
| web_common | «Интернет-активность» | Сервис перехвата неразобранных POST-запросов |
| file_copy_removable | «Обмен файлами» | Сервис, который создаёт копии файлов, копируемых на съёмные устройства хранения данных |
| ftp | «Обмен файлами» | Сервис, который создаёт копии файлов, копируемых на съёмные устройства хранения данных |
| print | «Принтеры и МФУ» | Сервис, который создаёт «образы» распечатываемых на принтере документов |

| Наименование сервиса | Классы | Описание |
|---|---|---|
| cloud_storage | «Обмен файлами» | Сервис, который создаёт копии файлов, копируемых на облачные хранилища |
| terminal_session | «Обмен файлами» | Сервис, который создаёт копии файлов, передаваемых через терминальную сессию |
| network_resource | «Обмен файлами» | Сервис, который создаёт копии файлов, копируемых на сетевые ресурсы |
| **Примечание:** При добавлении нового сервиса, который представляет собой программу обмена сообщениями, рекомендуется добавить к его названию префикс "im_". Например "im_viber" | | |

**Примечание:**

Сервисы с другими типами событий могут быть зарегистрированы с помощью плагинов

### Типы контактов Traffic Monitor pushAPI SDK

Типы контактов, поддерживаемые бизнес-логикой Traffic Monitor:

| Код | Описание |
|---|---|
| `const TmContactType contact_type_email = "email"` | Почтовый адрес. Используется для идентификаций с типом «Персона» |
| `const TmContactType contact_type_auth = "auth"` | Логин в ОС в формате login@domain. Используется для идентификаций с типом «Персона» |
| `const TmContactType contact_type_dnshostname = "dnshostname"` | DNS имя. Используется для отправителей с типом «Рабочая станция» |
| `const TmContactType contact_type_icq = "icq"` | Icq-номер. Используется для идентификаций с типом «Персона» |
| `const TmContactType contact_type_skype = "skype"` | Skype-логин. Используется для идентификаций с типом «Персона» |
| `const TmContactType contact_type_phone = "phone"` | Номер телефона. Используется для идентификаций с типом «Персона» |
| `const TmContactType contact_type_ip = "ip"` | IPv4-адрес. Используется для отправителей с типом «Рабочая станция» |

| Код | **Описание** |
| --- | --- |
| `const TmContactType contact_type_sid = "sid"` | Security Identifier в операционной системе Windows, представленный в текстовом формате. Используется для идентификаций с типом «Персона» |
| `const TmContactType contact_type_webaccount = "webaccount"` | Название учетной записи на сетевом ресурсе |
| `const TmContactType contact_type_lotus = "lotus"` | Почтовый адрес в Lotus. Используется для идентификаций с типом «Персона» |
| `const TmContactType contact_type_domain = "domain"` | Домен |

## Поддерживаемые атрибуты Traffic Monitor pushAPI SDK

Список имён атрибутов, которые поддерживаются в Traffic Monitor:

| Код | Описание атрибута |
| --- | --- |
| **`typedef string EventAttributeType`** | **Атрибуты события:** |
| `const EventAttributeType event_attr_capture_date = "capture_ts"` | Локальное время перехвата события в формате ГГГГ-ММ-ДДТЧЧ:ММ:СС+ЧЧ:ММ (ISO 8601 с форматированием yyyy-MM-ddTHH:mm:sszzz) (*) |
| `const EventAttributeType event_attr_capture_server_ip = "capture_server_ip"` | IP-адрес сервера перехвата (позволяет различать различные экземпляры одного плагина) (*) |
| `const EventAttributeType event_attr_capture_server_fqdn = "capture_server_fqdn"` | DNS-имя сервера перехвата (позволяет различать различные экземпляры одного плагина) (*) |
| `const EventAttributeType event_attr_inteceptor_id = "interceptor_id"` | Идентификатор объекта в перехватчике |
| `const EventAttributeType event_attr_inteceptor_protocol = "protocol_mnemo"` | Протокол, по которому передавался объект |

| Код | Описание атрибута |
| --- | --- |
| `const EventAttributeType event_attr_print_copies = "print_copies"` | Количество копий, целое число в строковом представлении |
| `const EventAttributeType event_attr_destination_type = "destination_type"` | Тип приёмника |
| **`typedef string DataAttributesType`** | **Общие атрибуты потока данных:** |
| `const DataAttributesType data_attr_mimetype = "mimetype"` | MIME-тип содержимого (заполняется только для узлов, которые уже разобраны клиентом) |
| `const DataAttributesType data_attr_size = "data_size"` | Размер данных, если он известен заранее |
| `const DataAttributesType data_attr_sent_date = "sent_date"` | Дата отправки объекта в формате ГГГГ-ММ-ДДТЧЧ:ММ:СС+ЧЧ:ММ.<br>Позволяет независимо устанавливать время формирования события и время реальной передачи данных |
| `const DataAttributesType data_attr_comment = "data_comment"` | Комментарий |
| | **Атрибуты потока данных для класса "Электронная почта":** |
| `const DataAttributesType data_attr_email_subject = "subject"` | Тема письма |
| `const DataAttributesType data_attr_email_is_encrypted = "encrypted"` | Признак шифрования (строки "true" или "false") |
| `const DataAttributesType data_attr_email_is_signed = "is_signed"` | Признак наличия цифровой подписи (строки "true" или "false") |
| | **Атрибуты потока данных для класса "Обмен файлами":** |

| Код | Описание атрибута |
| --- | --- |
| `const DataAttributesType data_attr_file_filename = "filename"` | Короткое имя файла (*) |
| `const DataAttributesType data_attr_file_source_file_path = "source_path"` | Полный путь к файлу источнику события |
| `const DataAttributesType data_attr_file_destination_file_path = "destination_path"` | Полный путь к переданному или скопированному файлу или полный адрес веб-ресурса |
| | **Атрибуты потока данных для класса "Сотовая связь":** |
| `const DataAttributesType data_attr_voice_duration_sec = "call_duration"` | Длительность в секундах (целое число в строковом представлении) |
| | **Атрибуты потока данных для класса "Принтер и МФУ":** |
| `const DataAttributesType data_attr_print_job_name = "print_job_name"` | Название задания на печать |
| `const DataAttributesType data_attr_print_copies = "event_attr_print_copies"` | Количество копий (целое число в строковом представлении) |
| **`typedef string IdentityAttrType`** | **Общие атрибуты идентификаций:** |
| `const IdentityAttrType identity_attr_comment = "identity_comment"` | Комментарий |
| **`typedef string TWorkstation`** | **Атрибуты идентификаций типа "Компьютеры":** |

| Код | Описание атрибута |
| --- | --- |
| `const IdentityAttrType identity_attr_ws_type = "workstation_type"` | Тип рабочей станции: |
| `const TWorkstation ws_type_computer = "ws_type_computer"` | Компьютер |
| `const TWorkstation ws_type_mobile = "ws_type_mobile"` | Мобильное устройство |
| `const TWorkstation ws_type_terminal = "ws_type_terminal"` | Терминальный сервер |
| | **Атрибуты идентификаций типа "Устройство":** |
| `const IdentityAttrType identity_attr_device_name = "device_name"` | Имя устройства (*) |
| `const IdentityAttrType identity_attr_device_type = "device_type"` | Тип устройства |
| | **Атрибуты идентификации типа "Устройство", "Ресурс", "Рабочая станция" для источника и приемника:** |
| `const IdentityAttrType identity_attr_endpoint_name = "name"` | Имя устройства или ресурса (*) |
| `const IdentityAttrType identity_attr_endpoint_path = "path"` | Путь на заданном ресурсе или устройстве (*) |
| `const IdentityAttrType identity_attr_endpoint_type = "type"` | Тип ресурса или устройства. Заполняется мнемониками из справочника |
| `const IdentityAttrType identity_attr_endpoint_device_id` | ID съемного устройства |
| `const string identity_attr_print_location = "print_location"` | Расположение устройства принтера |

| Код | Описание атрибута |
| --- | --- |
| `const string identity_attr_print_port_name = "print_port_name"` | Имя порта устройства принтера |
| `const string identity_attr_print_server = "print_server"` | Имя сервера устройства принтера |
| | **Атрибуты идентификаций типа "Ресурс":** |
| `const IdentityAttrType identity_attr_resource_url = "res_destination_url"` | URL ресурса (*) |
| `const IdentityAttrType identity_attr_resource_address = "res_destination_host"` | DNS или IP адрес ресурса (*) |
| **Примечание:** (*) - обязательный атрибут | |

**Примечание:**

Если внешняя система присылает в Traffic Monitor событие, в котором атрибут `destination_path` заполнен несколькими значениями, то в Traffic Monitor событие будет сохранено с первым значением этого атрибута, а все остальные значения будут отброшены.

## Сервис EventProcessor pushAPI SDK

| Код | Описание |
| --- | --- |
| `InterfaceVersion GetVersion()` | Функция получения текущей версии интерфейса |
| `void VerifyCredentials(1: Credentials cred) throws(1: InvalidCredentials ex);` | Функция проверки параметров доступа к интерфейсу pushAPI SDK.<br>Позволяет проверить возможность передачи данных до их реальной передачи: |
| `ventId BeginEvent (1: Event event, 2: Credentials cred) throws(1: InvalidEventFormat ex1, 2: InvalidCredentials ex2, 3: LicenseError ex3, 4: EventNotFound ex4, 5: DataNotFound ex5);` | Функция инициирует процесс передачи события перехвата на Traffic Monitor, используя pushAPI SDK, где:<br>• event – заполненная структура содержащая все «метаданные», которые описывают событие перехвата. Атрибуты: |

| Код | Описание |
| --- | --- |
| | отправителя, получателя, списка потоков данных, которые связаны с событием;<br>• cred – структура, которая позволяет авторизовать процесс передачи события;<br>• return – идентификатор события с сессии передачи данных (в одной и той же TCP-сессии можно передавать несколько событий) |
| `StreamId BeginStream (1: EventId event_id, 2: ItemId event_data_id) throws(1: EventNotFound ex1, 2: DataNotFound ex2);` | Функция инициирует передачу потока данных, который связан с событием перехвата данных, где:<br>• event_id – идентификатор события, с которым связан данный поток данных. Возвращается функцией `BeginEvent`;<br>• event_data_id – идентификатор передаваемых данных. Этот идентификатор передаётся в составе «метаданных» события, в поле evt_data;<br>• return – идентификатор загружаемого потока |
| `void SendStreamData(1: EventId object_id, 2: StreamId stream_id, 3: binary chunk) throws(1: EventNotFound ex1, 2: StreamNotFound ex2, 3: InvalidEventFormat ex3);` | Функция передаёт буфер данных в составе потока данных, который связан с событием перехвата данных, где:<br>• event_id – идентификатор события, с которым связан данный поток данных. Возвращается функцией `BeginEvent`;<br>• stream_id – идентификатор потока данных, в составе которого передаётся буфер. Возвращается функцией `BeginStream`;<br>• chunk – буфер данных. Пользователь SDK сам должен выбирать разумный размер буфера данных, чтобы обеспечить достаточную скорость загрузки событий, но не перегружать сетевую инфраструктуру |
| `void EndStream(1: EventId event_id, 2: StreamId stream_id) throws(1: EventNotFound ex1, 2: StreamNotFound ex2, 3: InvalidEventFormat ex3);` | Функция фиксирует конец передачи потока данных, связанного с событием перехвата, где:<br>• event_id – идентификатор события, с которым связан данный поток данных. Возвращается функцией `BeginEvent`;<br>• stream_id – идентификатор потока данных, в составе которого передаётся буфер. Возвращается функцией `BeginStream` |

| Код | Описание |
| --- | --- |
| `string GetEventDatabaseId(1: EventId object_id) throws(1: EventNotFound ex1);` | Функция получения уникального идентификатора события перехвата в системе Traffic Monitor, где:<br>• event_id – идентификатор события, полученный вызовом `BeginEvent`.<br>Это значение можно использовать для ссылки на загруженное событие. Функцию можно вызывать после удачного выполнения функции `BeginEvent` |
| `void EndEvent(1: EventId event_id, 2: bool abort) throws(1: EventNotFound ex1, 2: InvalidEventFormat ex2, 3: LicenseError ex3);` | Функция фиксирует конец передачи события перехвата, где:<br>• event_id – идентификатор события, передача которого завершается;<br>• abort – флаг прекращения обработки события в Traffic Monitor. Если выставлен флаг, то событие не попадает в БД |

### 9.1.3 Регистрация стороннего компонента pushAPI SDK

Для интеграции стороннего модуля перехвата данных с системой Traffic Monitor нужно выполнить следующие шаги:

1. Зарегистрировать в компании InfoWatch строку идентификатор компании-производителя компонента. Это позволит связывать компанию-производителя с лицензией, которая будет устанавливаться в систему Traffic Monitor;
2. Получить лицензию разработчика, связанную с идентификатором компании. Это позволит загружать в Traffic Monitor события перехвата этого производителя. Лицензия разработчика позволяет загружать произвольные типы (Сервисы) событий;
3. Создать файл регистрации стороннего компонента в описанном ниже формате. К этому моменту должны быть определены названия сервисов, которые будут перехватываться сторонним компонентом. В файл регистрации добавляется лицензия, полученная на шаге 2;
4. Загрузить файл регистрации стороннего компонента в систему Traffic Monitor через интерфейс консоли Traffic Monitor. Раздел «Управление» - «Плагины». (см. "InfoWatch Traffic Monitor. Руководство пользователя");
5. Получить токен доступа в свойствах загруженного стороннего компонента.

Система готова принимать события от заданной компании производителя с указанным сервисом перехвата.

#### Формат файла регистрации стороннего компонента pushAPI SDK

Плагин представляет собой архив в формате .zip. В состав архива входят:

- папка **licenses**, содержащая файлы лицензий;
- папка **icon**, содержащая файлы с используемыми пиктограммами для регистрируемых событий;
- файл **manifest.json**, содержащий информацию о плагине.

**Примечание:**

Папки **licenses** и **icon** не являются обязательными. Файлы лицензий и файлы с используемыми пиктограммами могут находиться в корне.

Для внешних систем-источников событий файл **manifest.json** должен содержать следующую информацию:

| Содержимое | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| `{` | | | |
| `"PLUGIN_ID": "",` | Строка | Да | Уникальный идентификатор (UUID) плагина, который создается его разработчиком. До 40 символов. Идентификатор используется для обновления плагина.<br>**Пример:** `"PLUGIN_ID": "189C38D390396EB6E0530100007F1CA200000001",` |
| `"DISPLAY_NAME": "",` | Строка | Да | Отображаемое имя плагина.<br>**Пример:** `"DISPLAY_NAME": "Имя плагина",` |
| `"DESCRIPTION": "",` | Строка | Нет | Отображаемое описание плагина.<br>**Пример:** `"DESCRIPTION": "Тестовый плагин для демонстрации",` |
| `"VERSION": "",` | Строка | Да | Версия плагина.<br>**Пример:** `"VERSION": "1.0.0",` |
| `"VENDOR": "",` | Строка | Да | Идентификатор компании-разработчика, соответствующий названию компании в лицензии.<br>**Пример:** `"VENDOR": "infowatch",` |
| `"LICENSE": [ { "PATH":"" } ],` | Массив<br><br>Строка | Да | Файлы лицензии. Должны быть указаны пути к файлам лицензий относительно корня архива.<br><br>**Пример**<br>`"LICENSE": [ { "PATH": "licenses/файл лицензии 1.license"` |

| Содержимое | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| | | | <pre>    },<br>    {<br>        "PATH": "licenses/файл лицензии 2.license"<br>    },<br>],</pre> |
| `"PATTERN_SEARCH_LICENSE": "",` | Строка | Нет | Шаблон для поиска загруженных ранее лицензий для привязки их к плагину. Имеет формат: `{operator:or\|and,child[{name:value}]}"`. **Пример:** `"PATTERN_SEARCH_LICENSE": "{\"operator\":\"or\",\"conditions\":[{\"origin\":\"dm\"},{\"origin\":\"dmmobile\"}]}",` |
| `"ADDS_EVENTS": {`<br>`"OBJECT_TYPE": [`<br>`{`<br>`"MNEMO": "",`<br>`"SERVICE_MNEMO": "",`<br>`"ICON": "",`<br>`"LOCALE": {`<br>`"": ""`<br>`}`<br>`}`<br>`],`<br>`"PROTOCOL": [`<br>`{`<br>`"MNEMO": "",`<br>`"LOCALE": {`<br>`"": ""`<br>`}`<br>`}`<br>`]`<br>`},` | Объект<br>Массив<br><br>Строка<br>Строка<br>Строка<br>Объект<br><br><br>Массив<br><br>Строка<br>Объект | Да | Регистрируемые типы событий и протоколы.<br>Массив типов регистрируемых событий с указанием типов сервисов, к которым они относятся.<br><br>Тип события.<br>Сервис.<br>Файлы с иконками регистрируемых контактов.<br>Локализации наименований типов контактов хотя бы на одном языке.<br><br>**Пример**<br><pre>"ADDS_EVENTS": {<br>    "OBJECT_TYPE": [<br>        {<br>            "MNEMO": "cloud_storage",<br>            "SERVICE_MNEMO": "file",<br>            "LOCALE": {<br>                "rus": "Облачное хранилище",<br>                "eng": "Cloud storage"<br>            }<br>        },<br>        {<br>            "MNEMO": "im_telegram",<br>            "SERVICE_MNEMO": "im",</pre> |

| Содержимое | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| | | | <pre>"ICON": "icon/event_icon_telegram.png",<br>"LOCALE": {<br>"rus": "Telegram",<br>"eng": "Telegram"<br>}<br>}<br>],<br>"PROTOCOL": [<br>{<br>"MNEMO": "telegram",<br>"LOCALE": {<br>"rus": "Telegram",<br>"eng": "Telegram"<br>}<br>}<br>]<br>},</pre> |
| <pre>"USES_EVENTS": {<br>"OBJECT_TYPE": [<br>{<br>"MNEMO": "",<br>"PROTOCOL": [<br>{ "MNEMO": "" }<br>],<br>"ORIGIN": [<br>"" ]<br>}<br>]<br>},</pre> | Объект<br>Массив<br><br>Строка<br>Массив<br>Строка<br><br>Массив<br>Строка | Да | Существующие типы событий.<br>Массив типов регистрируемых событий с указанием типов сервисов, к которым они относятся.<br><br>Тип события.<br>Массив протоколов, относящихся к данному типу события.<br>Протоколы.<br><br>Массив кодов типов перехватчиков для Плагинов InfoWatch.<br>Коды.<br><br>**Пример**<br><pre>"USES_EVENTS": {<br>"OBJECT_TYPE": [<br>{<br>"MNEMO": "email",<br>"PROTOCOL": [<br>{<br>"MNEMO": "pop3"<br>},<br>{<br>"MNEMO": "imap"<br>},<br>{<br>"MNEMO": "mapi"<br>},</pre> |

| Содержимое | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| | | | <pre>{<br>"MNEMO": "smtp"<br>}<br>],<br>"ORIGIN": ["dm", "dmmobile"]<br>},<br>{<br>"MNEMO": "email_web",<br>"PROTOCOL": [<br>{<br>"MNEMO": "http"<br>},<br>{<br>"MNEMO": "https"<br>}<br>],<br>"ORIGIN": ["dm", "dmmobile"]<br>},<br>{<br>"MNEMO": "im_whatsapp",<br>"PROTOCOL": [<br>{<br>"MNEMO": "whatsapp"<br>}<br>],<br>"ORIGIN": ["dm", "dmmobile"]<br>}<br>]<br>},</pre> |
| <pre>"ADDS_SERVICES": {<br>"SERVICE_TYPE": [<br>{<br>"SERVICE_MNEMO": "",<br>"DATA_CLASS": [""],<br>"ICON": "",<br>"LOCALE": {<br>"": "",<br>"": ""<br>}<br>}<br>],<br>},</pre> | Объект<br>Массив<br><br>Строка<br>Массив строк<br>Строка<br>Объект | Да | Регистрируемые типы событий через сервисы SDK.<br>Регистрируемые типы перехватываемых сервисов.<br><br>Имя перехватываемого сервиса.<br>Список классов данных, которые перехватывает данный перехватчик в сервисе.<br>Файл с иконкой регистрируемого сервиса.<br>Локализации наименований типов регистрируемого сервиса хотя бы на одном языке.<br>**Пример:**<br><br>**Пример**<br><pre>"ADDS_SERVICES": {</pre> |

| Содержимое | Тип данных | Является обязательным | Описание |
| --- | --- | --- | --- |
| | | | "SERVICE_TYPE": [{<br>"SERVICE_MNEMO": "newservice",<br>"DATA_CLASS": ["kChat", "kFileExchange"],<br>"ICON": "icon/TM_icon.png",<br>"LOCALE": {<br>"rus": "сервис#5",<br>"eng": "service#5"<br>}<br>},<br>{<br>"SERVICE_MNEMO": "newservice2",<br>"DATA_CLASS": ["kPhoto"],<br>"ICON": "icon/TM_icon.png",<br>"LOCALE": {<br>"rus": "сервис#5+2",<br>"eng": "service#5+2"<br>}<br>}<br>]<br>}, |
| `"OBJECT_HEADER": [`<br>`{`<br>`"NAME": "",`<br><br>`"NOTE": {`<br>`"": "",`<br>`"": ""`<br>`},`<br>`"TYPE": "",`<br>`"FORMAT": "",`<br><br>`"DATA_CLASS": [""],`<br>`"USE_IN_POLICY": "",`<br>`"USE_IN_NOTIFICATION": "",`<br>`"USE_IN_QUERY": "",`<br>`"USE_IN_LIST": "",`<br>`"USE_IN_SHOW": "",`<br>`"USE_IN_DETAIL": "",` | Массив<br><br>Строка<br><br>Объект<br>Строка<br><br>Перечисление<br>Перечисление<br><br>Массив строк<br>Перечисление<br>Перечисление<br><br>Перечисление<br>Перечисление<br>Перечисление | Нет | Пользовательские атрибуты событий.<br><br>Уникальный код атрибута, который будет использован в заголовках события и для идентификации в xAPI/PushAPI.<br>Если идентификатор разработчика не "IW", код должен начинаться с префикса "`<Идентификатор компании-разработчика>_`".<br>**Пример:** CISCO_CALL_DURATION<br>Название атрибута, отображаемое в консоли Traffic Monitor.<br><br><br>Тип значения.<br>Формат записи. Возможны значения: число (целое, дробное), строка, дата и время в UTC + указание смещение часового пояса, длительность, гиперссылка, перечисление, логический тип.<br>Сервисы, к событиям которых будет добавлен новый пользовательский атрибут.<br>Использование атрибута в политиках. `"1"` - да, `"0"` - нет. |

| Содержимое | Тип данных | Является обязательным | Описание |
| --- | --- | --- | --- |
| `"IS_MULTIPLE_VALUE": "",`<br>`}`<br>`]` | Перечисление<br><br>Перечисление | | Использование атрибута в почтовых уведомлениях. `"1"` - да, `"0"` - нет.<br><br>Использование атрибута в запросах. `"1"` - да, `"0"` - нет.<br>Использование атрибута в табличной форме просмотра списка событий. `"1"` - да, `"0"` - нет.<br>Использование атрибута в краткой форме просмотра события. `"1"` - да, `"0"` - нет.<br>Использование атрибута в детальной форме просмотра события. `"1"` - да, `"0"` - нет.<br><br>Множественное значение. `"1"` - да, `"0"` - нет.<br><br>**Пример**<br><br>`"OBJECT_HEADER": [`<br>`{`<br>`"NAME": "header_multi_string",`<br>`"NOTE": {`<br>`"rus": "Заголовок строк1",`<br>`"eng": "Header strings1"`<br>`},`<br>`"DATA_CLASS": ["kEmail"],`<br>`"USE_IN_POLICY": "1",`<br>`"USE_IN_QUERY": "1",`<br>`"USE_IN_NOTIFICATION": "1",`<br>`"USE_IN_LIST": "1",`<br>`"USE_IN_SHOW": "1",`<br>`"USE_IN_DETAIL": "1",`<br>`"TYPE": "string",`<br>`"FORMAT": "string",`<br>`"IS_MULTIPLE_VALUE": "1"`<br>`},`<br>`{`<br>`"NAME": "header_date",`<br>`"NOTE": {`<br>`"rus": "Заголовок дата1",`<br>`"eng": "Header date1"`<br>`},`<br>`"DATA_CLASS": ["kEmail"],`<br>`"USE_IN_POLICY": "1",`<br>`"USE_IN_QUERY": "1",`<br>`"USE_IN_NOTIFICATION": "1",`<br>`"USE_IN_LIST": "0",`<br>`"USE_IN_SHOW": "1",`<br>`"USE_IN_DETAIL": "1",` |

| Содержимое | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| | | | <pre>"TYPE": "string",<br>"FORMAT": "date",<br>"IS_MULTIPLE_VALUE": "0"<br>}<br>]</pre> |
| } | | | |

Полная JSON-схема входит в состав примеров SDK (см. раздел "Описание примеров PushAPI SDK"). Пример файла регистрации модуля входит в состав SDK.

**Важно!**

В состав файла входит просроченная лицензия. Для регистрации плагина на основании файла примера нужно будет получать новую лицензию.

### 9.1.4 Описание примеров PushAPI SDK

Примеры представляют собой исходные коды консольных утилит, которые реализуют загрузку событий в Traffic Monitor, используя Thrift-интерфейс pushAPI SDK.

Первая утилита – pushapi-cpp. Реализована на языке C++. Подготовлена к сборке в операционных системах Windows и Linux. Данная утилита демонстрирует сценарии загрузки всех типов событий, которые уже зарегистрированы в системе Traffic Monitor.

Вторая утилита – pushapi-csharp. Реализована на языке C#. Подготовлена к сборке в операционной системе Windows. Данная утилита демонстрирует сценарии загрузки всех типов событий, которые уже зарегистрированы в системе Traffic Monitor.

Третья утилита – pushapi-demo.py. Реализована на языке Python. Подготовлена к сборке в операционных системах Windows и Linux. Демонстрирует сценарии загрузки всех типов событий, которые уже зарегистрированы в системе Traffic Monitor.

Четвертая утилита – pushapi-util. Реализована на языке C++. Подготовлена к сборке в операционных системах Windows и Linux. Данная утилита имеет развитый интерфейс командной строки, который позволяет загружать произвольные события в систему Traffic Monitor, в том числе те, которые зарегистрированы внешней системой. Вот описание командной строки:

```
./pushapi-util
--host <pushapi address > [--port <pushapi port>]
--token <plugin token>
--id <company>
--class <event class>
--service <event service>
--evtattr <attr_name:attr_value,…, attr_name:attr_value>
--sender
<contact type:contact_value,attr_name:attr_value,…,attr_name:attr_value>
--receiver
<contact type:contact value,attr name:attr value,…,attr name:attr value>
--data file:<data_falie_name>, attr_name:attr_value,…, attr_name:attr_value
```

```
--mes <contact_type:contact_value,"message text"
[-addctx]
```

Где:

- <pushapi address > – адрес pushAPI-сервера;
- <pushapi port> – порт pushAPI-сервера, если не указан, используется значение по умолчанию;
- <plugin token> – токен авторизации плагина. Берётся из консоли в разделе данного плагина;
- <company> – идентификатор компании-производителя плагина. Произвольная строка, обязательно совпадающая с той, что использовалась для генерации лицензии для плагина;
- <event class> – класс передаваемого события;
- <event service> – сервис передаваемого события. Плагин может зарегистрировать свои перехватываемые сервисы по имени и передавать их;
- --evtattr – атрибуты передаваемого события. Посмотреть можно в списке команд с примером. Некоторые имена атрибутов имеют фиксированные значения и бизнес-смысл;
- --sender – отправитель события. Первая пара параметров определяет контакт отправителя. Далее указываются атрибуты отправителя. Существуют три «особых» типа контактов: dev (отправитель/получатель является устройством), res (отправитель/получатель является ресурсом), ws (отправитель/получатель является «Рабочей станцией»). Если не задан ни один отправитель, то будет сгенерировано два отправителя с типом «Персона» и контактом типа «auth»; и с типом «Рабочая станция» и контактом dnshostname. Задан может быть только один отправитель;

  **Пример:**

  Для события с отправителем с аккаунтом Вконтакте и указанием мета-информации:
  ```
  --sender "vkontakte:349051292:'{\"display_name\":\"some name\",\"url\":
  \"some_url\",\"login\":\"some_login\"}'"
  ```

- --receiver – получатель события. Параметры аналогичны отправителю;
- --data – данные события. Первая пара атрибутов указывает на путь к файлу, где содержится тело события. Остальные параметры описывают атрибуты этих данных. Для некоторых типов событий некоторые атрибуты обязательны;
- --mes – передача сообщений класса «Беседа». Указывается контакт отправителя сообщения и его содержимое. Сообщений может быть несколько;
- --addctx – необязательный параметр. Автоматически добавляет к событию двух отправителей с типом «Персона» и контактом типа «auth»; и с типом «Рабочая станция» и контактом типа dnshostname.

Примеры вызова этой утилиты есть в исходных кодах примеров.
Кроме этого в состав примеров SDK входит:

- файл pluging.json – JSON-схема файла manifest.json, который включается в состав файла регистрации внешнего плагина;
- файл plugin.zip – пример файла регистрации внешнего плагина.

**Важно!**

В состав файла входит просроченная лицензия. Для регистрации плагина на основании файла примера нужно будет получать новую лицензию.

### Сборка примеров под Linux pushAPI SDK

Для сборки примеров под Linux нужно иметь установленный пакет **cmake** и компилятор с поддержкой стандарта C++11. Все остальные зависимости определяются **cmake**-скриптом. Для сборки может понадобиться установка Thrift Runtime-библиотек, библиотеки Boost и OpenSSL, а именно:

- boost 1.62
- openssl 1.0.1
- thrift 0.11.0

### Сборка примеров под Windows pushAPI SDK

Для сборки примеров под Windows нужно иметь установленную программу Visual Studio 2013. В состав примеров входит Toolchain, который содержит boost, OpenSSL, а также исходники Thift Runtime-библиотек, которые собираются в составе примера. В Toolchain входит утилита thrift, которая компилирует thift-схему в соответствующий исходный код. Пользователь может использовать свою реализацию boost, OpenSSL и Thrift – для этого нужно определить свои переменные окружения:

```
$(BOOST_ROOT)
$(OPENSSL_ROOT_DIR)
$(THRIFT_INSTALL_DIR)
```

**Важно!**

Самостоятельную сборку Thrift необходимо осуществлять с OpenSSL, т.к. pushAPI работает по SSL-соединению.

## 9.2 Загрузка эталонных документов и выгрузок из БД в Traffic Monitor (REST API SDK)

Данный программный интерфейс предназначен для интеграции сторонних компонентов с Traffic Monitor. Сторонние компоненты могут самостоятельно формировать документы, представляющие собой «Эталонные выгрузки баз данных» и «Эталонные документы» и далее, используя предоставленный интерфейс, передавать их в Traffic Monitor. После этого переданные выгрузки и эталонные документы будут детектироваться в анализируемых Traffic Monitor потоках данных. Правила детектирования выгрузок и ЭД задаются в консоли Traffic Monitor. Сторонний компонент только загружает или обновляет содержимое выгрузки или ЭД. Сторонний компонент должен быть зарегистрирован в системе согласно процедуре, которая описана в разделе «Регистрация стороннего компонента REST API».

### 9.2.1 Конфигурирование программного интерфейса REST API

В конфигурировании программного интерфейса участвуют следующие параметры:

- Адрес подключения с сервису SDK (сетевой адрес, порт);
- Токен авторизации. Строка символов, которая позволяет авторизовать компоненты, использующие SDK. Данная строка может быть получена в разделе "Управление" (вкладка "Токены") в консоли управления Traffic Monitor;
- Идентификатор передаваемых данных. Строка, которую производитель внешнего компонента получает от InfoWatch. Данная строка характеризует тип передаваемых данных и используется в политике лицензирования;
- Идентификатор компании-производителя внешнего компонента. Строка, которую производитель внешнего компонента получает от InfoWatch. Данная строка характеризует компанию-производителя и используется в политике лицензирования.

## 9.2.2 Общее описание программного интерфейса REST API

Программный интерфейс представляет собой REST API, т.е. последовательность запросов к Web-серверу. Программный интерфейс предоставляет следующие возможности:

- Создание эталонной выгрузки REST API;
- Обновление эталонной выгрузки REST API;
- Добавление содержимого к эталонной выгрузке REST API;
- Получение состояния эталонной выгрузки REST API;
- Инициирование распространения нового содержимого загруженных эталонных документов на модули анализа REST API;
- Получение версии интерфейса, который поддерживается Traffic Monitor REST API;
- Создание каталога эталонных документов;
- Удаление каталога эталонных документов;
- Создание эталонного документа;
- Удаление эталонного документа;
- Добавление содержимого эталонного документа;
- Получение состояния эталонного документа.

### Создание эталонной выгрузки REST API

```
FingerPrintDsc Create(string name, string[] columns)
```

Функция создаёт эталонную выгрузку с заданным именем и списком имён колонок эталонной выгрузки. Возвращается описание созданного эталонного объекта (FingerPrint).

### Обновление эталонной выгрузки REST API

```
FingerPrintDsc UpdateContent(string FingerPrintId,string[]content)
```

Функция позволяет загрузить в существующий эталонный объект (выгрузку) его содержимое. Эталонный объект определяется его идентификатором (поле структуры FingerPrintDsc). Возвращается описание эталонного объекта (FingerPrint). После загрузки содержимого начинается процесс преобразования и сохранения содержимого эталонного объекта. Данная функция целиком заменяет содержимое эталонного объекта.

### Добавление содержимого к эталонной выгрузке REST API

```
FingerPrintDsc AddContent(string FingerPrintId, string[] content)
```

Функция позволяет добавить в существующий эталонный объект (выгрузку) дополнительное содержимое. Эталонный объект определяется его идентификатором (поле структуры FingerPrintDsc).

Возвращается описание эталонного объекта (FingerPrint). После загрузки содержимого начинается процесс преобразования и сохранения содержимого эталонного объекта. Данная функция целиком заменят содержимое эталонного объекта.

### Получение состояния эталонной выгрузки REST API

```
FingerPrintDsc GetInfo(string FingerPrintId)
```

Функция позволяет получить информацию о существующей эталонной выгрузке. Возвращается описание эталонного объекта (FingerPrint). Важным полем результата вызова этой функции является поле статуса эталонной выгрузки.

### Инициирование распространения нового содержимого загруженных эталонных документов на модули анализа REST API

```
Void Ditribute()
```

Функция инициирует процедуру распространения нового содержимого эталонных выгрузок по модулям анализа. Функция синхронная. После её выполнения система Traffic Monitor готова к детектированию нового содержимого в анализируемых потоках данных.

### Получение версии интерфейса, который поддерживается Traffic Monitor REST API

```
VersionInfo GetInterfaceVersion()
```

Функция позволяет получить информацию об интерфейсе, который поддерживает Traffic Monitor.

Каждая часть выгрузки, которая загружается в Traffic Monitor, проходит этапы преобразования во внутренний формат и сохранения в базе данных. После этого сторонний компонент должен дать команду о передаче новой выгрузки системам анализа Traffic Monitor. Таким образом можно загрузить по частям достаточно большую выгрузку. Т.е. выгрузка загружается в несколько запросов, а затем одной командой распространяется по системам анализа.

Каждый этап обработки загруженной эталонной выгрузки занимает некоторое время. На каждом этапе могут произойти ошибки.

Программный интерфейс позволяет отслеживать этапы обработки выгрузки и реагировать на ошибки, которые могут произойти во время обработки.

### Создание каталога эталонных документов

```
CatalogId CreateEtDocCatalog(CatalogId parentCatalog, string name);
```

Функция создания каталога эталонных документов, возвращающая идентификатор созданного каталога, где:

- `parentCatalog` – идентификатор родительского каталога, в котором создаётся каталог (0 - создать в корневом каталоге);
- `name` - имя каталога эталонных документов. Под этим именем каталог появится в консоли ТМ.

```
CatalogId GetEtDocCtalogIdByName(string name);
```

Функция получения идентификатора каталога по имени, возвращающая идентификатор каталога.

```
CatalogList GetEtDocCtalogs();
```

Функция получения каталогов, созданных плагином, возвращающая список каталогов.

### Удаление каталога эталонных документов

```
void DeleteEtDocCatalog(CatalogId id)
```

Функция удаления каталога эталонных документов в том случае, если он не входит в Объект защиты. Функция возвращает идентификатор удаляемого каталога.

### Создание эталонного документа

```
DocumentId CreateEtDoc(CatalogId parentCatalog, string name, Type type);
```

Функция создания эталонного документа, возвращающая идентификатор эталонного документа, где:

- `parentCatalog` - идентификатор каталога, в котором создаётся эталонный документ. Не может быть "0", так как создавать документы в корневом каталоге запрещено;
- `name` - имя эталонного документа. Под этим именем документ появится в консоли ТМ;
- `type` - тип эталонного документа. Эталонный документ может быть создан на основании извлечённого текста или своего бинарного представления.

### Удаление эталонного документа

```
void DeleteEtDoc(DocumentId doc);
```

Функция удаления эталонного документа в том случае, если он не входит в Объект защиты.

### Добавление содержимого эталонного документа

```
void AddEtDocContent(DocumentId doc, Buffer buf);
```

Функция добавления содержимого эталонного документа, которая позволяет также загружать содержимое по частям, где:

- `doc` - идентификатор эталонного документа, к которому добавляется содержимое;
- `buf` - буфер данных, добавляемый к документу.

```
void UpdateEtDocContent(DocumentId doc, Buffer buf);
```

Функция обновления или замены содержимого эталонного документа, где:

- `doc` - идентификатор эталонного документа, в котором меняется содержимое;
- `buf` - буфер данных, который будет представлять собой новое содержимое эталонного документа.

### Получение состояния эталонного документа

```
DocState GetEtDocState(DocumentId doc);
```

Функция получения состояния эталонного документа, где:

- `doc` - идентификатор эталонного документа.

### 9.2.3 Регистрация стороннего компонента REST API

Для интеграции стороннего модуля перехвата данных с системой Traffic Monitor нужно выполнить следующие шаги:

1. Зарегистрировать в компании InfoWatch строку-идентификатор компании-производителя компонента. Это позволит связывать компанию-производителя с лицензией, которая будет устанавливаться в систему Traffic Monitor.
2. Получить лицензию разработчика, связанную с идентификатором компании. Это позволит загружать в Traffic Monitor эталонные выгрузки и эталонные документы указанного производителя. Лицензия разработчика позволяет загружать произвольные эталонные выгрузки и эталонные документы.
3. Создать файл регистрации стороннего компонента в описанном ниже формате. К этому моменту должны быть определены названия источника данных эталонной выгрузки и эталонного документа, которая будет формироваться сторонним компонентом. В файл регистрации добавляется лицензия, полученная на шаге 2.
4. Загрузить файл регистрации стороннего компонента в систему Traffic Monitor через интерфейс консоли Traffic Monitor. Раздел «Управление» - «Плагины». (см. "InfoWatch Traffic Monitor. Руководство пользователя").
5. Получить токен доступа в свойствах загруженного стороннего компонента.

Система готова принимать сформированные эталонные выгрузки и эталонные документы от заданной компании-производителя с указанным источником эталонной выгрузки или эталонного документа.

#### Формат файла регистрации стороннего компонента REST API

Плагин представляет собой архив в формате .zip. В состав архива входят:

- папка **licenses**, содержащая файлы лицензий;
- папка **icon**, содержащая файлы с используемыми пиктограммами для регистрируемых событий;
- файл **manifest.json**, содержащий информацию о плагине.

> **Примечание:**
>
> Папки **licenses** и **icon** не являются обязательными. Файлы лицензий и файлы с используемыми пиктограммами могут находиться в корне.

Для внешних систем-источников событий файл **manifest.json** должен содержать следующую информацию:

| **Содержимое** | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| `{` | | | |
| `"PLUGIN_ID": "",` | Строка | Да | Уникальный идентификатор (UUID) плагина. До 40 символов. **Пример:** `"PLUGIN_ID":` |

| **Содержимое** | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| | | | `"189C38D390396EB6E0530100007F1CA200000001",` |
| `"DISPLAY_NAME": "",` | Строка | Да | Отображаемое имя плагина. **Пример:** `"DISPLAY_NAME": "Имя плагина",` |
| `"DESCRIPTION": "",` | Строка | Нет | Отображаемое описание плагина. **Пример:** `"DESCRIPTION": "Тестовый плагин для демонстрации",` |
| `"VERSION": "",` | Строка | Да | Версия плагина. **Пример:** `"VERSION": "1.0.0",` |
| `"VENDOR": "",` | Строка | Да | Идентификатор компании-разработчика, соответствующий названию компании в лицензии. **Пример:** `"VENDOR": "infowatch",` |
| `"LICENSE": [ { "PATH":"" } ],` | Массив<br><br>Строка | Да | Файлы лицензии. Должны быть указаны пути к файлам лицензий относительно корня архива. **Пример:** `"LICENSE": [ { "PATH":"licenses/файл лицензии 1.license" }, { "PATH":"licenses/файл лицензии 2.license" }, ],` |
| `"PATTERN_SEARCH_LICENSE": "",` | Строка | Нет | Шаблон для поиска загруженных ранее лицензий для привязки их к плагину. Имеет формат: `{operator:or\|and,child[{name:value}]}"` . **Пример:** `"PATTERN_SEARCH_LICENSE":` |

| **Содержимое** | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| | | | `"{\"operator\":\"or\", \"conditions\": [{\"origin\":\"dm\"}, {\"origin\": \"dmmobile\"}]}",` |
| `"DATATYPE": [ { "VALUE": "" } ]` | Массив<br><br>Строка | Да | Список типов данных с указанием систем-источников.<br>**Пример:**<br>`"DATATYPE": [ { "VALUE": "type1_s1", "VALUE": "type2_s2" } ],` |
| `}` | | | |

**Важно!**

В состав файла входит просроченная лицензия. Для регистрации плагина на основании файла примера нужно будет получать новую лицензию.

### 9.2.4 Формат эталонной выгрузки и эталонного документа REST API

Эталонная выгрузка представляет собой последовательность строк в кодировке UTF-8. Строки должны быть разделены символами CRLF или LF. Значения ячеек в строке должны быть разделены символами TAB или ‘,’(Comma). Данные ограничения соответствуют формату TSV (Tab separated values) или CSV (Comma separated values). Число ячеек во всех строках должно совпадать. При создании выгрузки указывается число ячеек. Оно равно числу имён столбцов, которые передаются в функцию Create. В существующую эталонную выгрузку можно загружать только содержимое, где число ячеек в строке равно числу, которое было указано при создании. Любое другое число ячеек сделает выгрузку невалидной.

Эталонный документ представляет собой файл любого формата. Если файл является незашифрованным архивом, Система извлекает файлы из архива, обрабатывает их независимо друг от друга и создает отдельный эталонный документ на основе каждого извлеченного файла (эталонный документ на основе всего архива не создается). Все созданные эталонные документы помещаются в каталог, выбранный при создании эталонного документа. Если файл является зашифрованным архивом, Система не создает эталонный документ. Если файл является файлом типа "контейнер", Система создает один эталонный документа на основе файла.

### 9.2.5 Функциональное описание программного интерфейса REST API

Программный интерфейс представляет собой REST API, т.е. последовательность GET/POST-запросов к Web-серверу на определенный ресурс и ответов на них. Формат оформления запросов и формат ответов представлен ниже. Защита данных во время их передачи осуществляется по протоколу SSL/

TLS без авторизации клиента. Передача данных в открытом виде программным интерфейсом не поддерживается. При передаче данных используется кодировка UTF-8.

## Общие заголовки GET/POST-запросов

Каждый запрос к серверу должен содержать следующие обязательные заголовки:

- X-API-Auth-Token – указывается токен авторизации;
- X-API-DataType – указывается идентификатор передаваемого типа данных;
- X-API-CompanyId – указывается идентификатор компании-производителя;
- X-API-Version – указывается номер версии программного интерфейса. Сейчас используется номер: «1».

## Работа с конфигурацией REST API

После того, как содержимое эталонной выгрузки передано на сервер SDK и удачно скомпилировано, можно дать команду на распространение изменённой конфигурации на системы анализа.

### Распространение конфигурации REST API

Описание: метод нужен для распространения конфигурации на системы анализа.

Характеристики метода: POST, синхронный.

Ресурс: xapi/configuration..

JSON Scheme тела запроса:

```
{
    "STATUS": "distribute"
}
```

В случае успеха – код возврата «200» и тело ответа:

```
{
    "STATUS": "distributed"
}
```

В случае ошибки – код возврата «500». Возможные значение поля code:

- error – конфигурация не может быть применена.

## Работа с эталонными выгрузками REST API

Глава содержит следующую информацию:

- Создание выгрузки REST API;
- Обновление данных выгрузки REST API;
- Добавление данных выгрузки REST API;
- Получение состояния выгрузки REST API;
- Получение текущей версии REST API.

### Создание выгрузки REST API

Описание: метод нужен для добавления новой выгрузки без наполнения её данными. Сами данные будут добавлены через отдельный метод.

Характеристики метода: POST, синхронный.

Ресурс: `xapi/etalonTable`.

JSON Scheme тела запроса:

```
{
    "properties": {
        "DISPLAY_NAME": {
            "description": "Название выгрузки",
            "type": "string",
            "errors": ["required", "not_match", "not_unique_field"]
        },
        "CONDITION_COLUMNS": {
            "description": "строка, закодированный JSON-массив с названием столбцов, например: [\"first_column\", \"second_column\"]",
            "type": "string",
            "errors": ["required", "not_valid_json"]
        },
        "NOTE": {
            "description": "Произвольное описание выгрузки",
            "type": "string"
        }
    },
    "required": [
        "DISPLAY_NAME",
        "CONDITION_COLUMNS"
    ]
}
```

В случае успеха – код возврата «200» и тело ответа:

```
{
    "FINGERPRINT_ID":    "string",
    "TYPE":              "string",
    "SOURCE":            "string",
    "DISPLAY_NAME":      "string",
    "NOTE":              "string",
    "CONDITION_COLUMNS": "string",
    "CREATE_DATE":       "string",
    "CHANGE_DATE":       "string",
    "STATUS":            "string"
```

```
}
```

> **Важно!**
>
> Число столбцов, которые указываются при создании выгрузки, не может быть изменено. При загрузке содержимого число ячеек в загружаемых стоках должно совпадать с тем значением, которое было указано при создании эталонной выгрузки.

Обновление данных выгрузки REST API

Описание: метод предназначен для обновления содержимого выгрузки. Все записи эталонной выгрузки будут удалены, и после этого добавится новая запись. Данный метод можно использовать для первичного наполнения.

> **Важно!**
>
> Наполнение должно иметь целое число строк, минимум 2 строки.
> Минимальное количество колонок – 2.
> Минимальный байтовый размер загружаемого контента – 128 байт.
> Максимальный байтовый размер загружаемого контента – 2 ГБ.

Характеристики метода: POST, асинхронный.

Ресурс: `xapi/etalonTable/{id}/content/replace`.

Параметры:

- id – fingerprint_id редактируемого объекта.

Например: `enatalonTable/0123456789ABCDEF/content/replce`

Content-type тела запроса должно быть не `application/json`, а `multipart/form-data` ( подробнее см.: https://ru.wikipedia.org/wiki/Multipart/form-data).

Content-Disposition, который будет содержать файл, должен иметь поле `name` со значением CONTENT и атрибут `filename` с названием файла с расширением TSV или CSV в зависимости от формата файла, разделенного Tab или запятыми соответственно.

Возможные значение ошибок поля CONTENT:

- not_valid – файл имеет неверную сигнатуру;
- not_allowed_file_extension – неразрешенное расширение файла, на данный момент разрешены 2 формата: TSV и CSV;
- too_long_size – слишком большой размер файла;
- duplicate – такой файл уже существует в системе.

В случае успеха – код возврата «200» и тело ответа:

```
{
    "FINGERPRINT_ID":    "string",
    "TYPE":              "string",
    "SOURCE":            "string",
    "DISPLAY_NAME":      "string",
```

```
    "NOTE":              "string",
    "CONDITION_COLUMNS": "string",
    "CREATE_DATE":       "string",
    "CHANGE_DATE":       "string",
    "STATUS":            "string"
}
```

После получения кода возврата «200» нужно взять поле FINGERPRINT_ID и по нему проверять состояние выгрузки, пока статус не перейдет в состояние ready.

**Важно!**

Число ячеек в загружаемых строках должно совпадать со значением числа столбцов, которое было указано при создании выгрузки.
При удалении выгрузки через консоль TrafficMonitor она считается существующей до момента распространения конфигурации, т.е. с этой выгрузкой возможны операции обновления и добавления содержимого.
При загрузке «ошибочного» содержимого, т.е. содержимого, которое является дубликатом уже загруженной выгрузки (части выгрузки) или содержимого, строки которого содержат неправильное количество ячеек, весь эталонный объект получает невалидный статус. Внешняя подсистема должна перестать загружать такое содержимое и перейти к следующему содержимому. Загрузка корректного содержимого исправляет общий статус эталонного объекта. Некорректное содержимое никогда не попадает на модули анализа.

Добавление данных выгрузки REST API

Описание: метод предназначен для добавления содержимого в выгрузку. Все записи содержимого будут сохранены, будет добавлена новая запись.

Характеристики метод: POST.

Ресурс: `xapi/etalonTable/{id}/content`.

Подробнее см. статью "Обновление данных выгрузки REST API"

Получение состояния выгрузки REST API

Описание: метод нужен для получения сведений о состоянии одной выгрузки.

Характеристики метода: GET.

Ресурс: `xapi/etalonTable/{id}`.

Параметры:

- id – fingerprint_id редактируемого объекта.

Например: `etalonTable/0123456789ABCDEF`

Тело ответа:

```
{
    "FINGERPRINT_ID":    "string",
    "TYPE":              "string",
    "SOURCE":            "string",
```

```
    "DISPLAY_NAME":      "string",
    "NOTE":              "string",
    "CONDITION_COLUMNS": "string",
    "CREATE_DATE":       "string",
    "CHANGE_DATE":       "string",
    "STATUS":            "string"
    "content":           [
        {
            "CONTENT_ID":   "string",
            "CHECKSUM":     "string",
            "CONTENT_SIZE": "integer",
            "CONTENT_MIME": "string"
        }
    ]
}
```

Поле статус может иметь следующие значения:

- sending – отправка данных на компилятор;
- sent – данные отправлены на компилятор, и начинается компиляция;
- compiling – идёт компиляция документа;
- compiled – документ готов;
- saving – идет сохранение;
- ready – документ сохранён, готов для дальнейшего внесения в него изменений и не блокирует применение конфигурации;
- fatal_error – произошла ошибка во время сохранения документа, и операция не может быть повторена или продолжена;
- duplicate – произошло дублирование данных content (можно продолжать загружать содержимое);
- not_match_delimiter – строки в выгрузке не содержат разделителя символов (COMMA или TAB);
- wrong_column_count – количество колонок в строке не совпадает с количеством колонок, которое было указано при создании выгрузки;
- error – временная ошибка, можно попробовать ещё раз через некоторое время (лучше через час);
- max_words - превышено допустимое количество слов;
- max_columns - превышено допустимое количество столбцов.

Получение текущей версии REST API

Описание: метод нужен для получения поддерживаемых версий.

Если код возврата будет «200», то можно продолжать работу.

Метод может использоваться для проверки лицензии, версии и авторизации. В случае успеха – код возврата «200». В случае неисправности возвращается код ошибки.

Характеристики метод: GET.

Ресурс: `xapi/version`.

Тело ответа:

```
{
    "data":       [
        {
            "NAME":    "string",
            "STATUS": "supported|deprecated|removed"
        }
    ]
}
```

Пример ответа при указании неправильной версии:

HTTP/1.1 400 Bad Request

Content-Type: application/json

```
{
    "error": {
        "code": "unsupported_version",
        "meta": {
            "versions": [
                {
                    "NAME":   "1.0.0",
                    "STATUS": "removed"
                },
                {
                    "NAME":   "2.0.0",
                    "STATUS": "deprecated"
                },
                {
                    "NAME":   "3.0.0",
                    "STATUS": "supported"
                }
            ]
        }
    }
}
```

## Общие ошибки REST API

Описание возможных ошибок:

- not_unique_field – неуникальное значение;
- unique – уникальное значение;

- too_short – слишком короткое значение;
- too_long – слишком длинное значение;
- wrong_length – значение неправильной длины;
- repeat_exactly – значение не совпадает со значением в другом поле;
- required – у поля обязательно должно быть значение;
- not_exist_in_list – значение не входит в список;
- invalid – значение невалидно;
- contains_child – узел является не листовым;
- contains_items – узел категории содержит сущности;
- parent_own_child – родитель содержит детей;
- parent_self_set_current – попытка установить родителем самого себя;
- not_valid_json – JSON невалиден;
- invalid_cron_format – не правильный формат cron;
- read_only – объект доступен только для чтения;
- empty – значение не может быть пустым.

Успешный ответ REST API

Код возврата: «200».

Формат ответа:

```
{
    "data": "mixed",
    "meta": "mixed"
}
```

Ошибка валидации данных/версии REST API

Код возврата: «400».

**Формат ответа в случае неправильной версии API (JSON Scheme) REST API**

```
{
    "properties": {
        "error": {
            "description": "Контейнер ошибки",
            "properties":  {
                "code":       {
                    "description": "Общее описание ошибки",
                    "type":        "string",
                    "value":       "unsupported_version"
                },
                "meta": {
                    "description": "Дополнительные данные об ошибке",
                    "type":        "object",
                    "properties":  {
```

```
                        "supported_versions": {
                            "description": "Массив поддерживаемых версий",
                            "type":        "array",
                            "items": {
                                "description": "Поддерживаемая версия",
                                "type": "string"
                            }
                        }
                    }
                }
            }
        }
    }
}
```

**Формат ответа в случае ошибки валидации запроса (JSON Scheme) REST API**

```
{
    "properties": {
        "error": {
            "description": "Контейнер ошибки",
            "properties":  {
                "code":       {
                    "description": "Общее описание ошибки",
                    "type":        "string",
                    "value":       "validation"
                },
                "meta": {
                    "description": "Дополнительные данные об ошибке",
                    "type":        "object",
                    "properties":  {
                        "validation": {
                            "description": "Название полей модели",
                            "type":        "object",
                            "properties":  {
                                "field":     {
                                    "description": "Поле модели",
                                    "type":        "array",
                                    "items":       {
```

```
                                        "description": "Ошибка",
                                        "type":        "string",
                                        "values": [
                                            "not_unique_field",
                                            "too_short",
                                            "too_long",
                                            "wrong_length",
                                            "repeat_exactly",
                                            "required",
                                            "not_exist_in_list",
                                            "invalid",
                                            "contains_child",
                                            "contains_items",
                                            "parent_own_child",
                                            "unique",
                                            "not_valid_json",
                                            "invalid_cron_format",
                                            "read_only",
                                            "parent_self_set_current",
                                            "empty"
                                        ]
                                    }
                                },
                                "sub_model": {
                                    "description": "Название вложенной модели",
                                    "type":         "object",
                                    "$ref":       "#/properties/error/
properties/meta/properties/validation"
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
```

**Пример ошибки при указании неправильной версии REST API**

```
{
    "error": {
        "code": "unsupported_version",
        "meta": {
            "supported_versions": ["2", "3"]
        }
    }
}
```

**Пример ошибки проверки на уникальность имени эталонной выгрузки REST API**

```
{
    "error": {
        "code": "validation",
        "meta": {
            "validation":    {
                "DISPLAY_NAME": ["unique"]
            },
            "unique_models": [
                {
                    "FINGERPRINT_ID": "0123456789ABCDEF",
                    "DISPLAY_NAME":   "test"
                }
            ]
        }
    }
}
```

Необходима авторизация REST API

Код возврата: «401».

Описание: возвращается в любом запросе, где требуется авторизация.

Тело ответа: нет.

Недостаточно прав REST API

Код возврата: «403».

Описание: возвращается в любом запросе, если у текущего пользователя недостаточно прав для выполнения данной операции.

Тело ответа: нет.

Сущность в системе не найдена REST API

Код возврата: «404».

Описание: возвращается, если определенная модель не найдена в системе. Например, не найдена эталонная выгрузка.

Тело ответа: нет.

Тело запроса слишком большое REST API

Код возврата: «413».

Описание: возвращается, если передан слишком большой запрос.

Тело ответа: нет.

Превышено количество запросов к серверу REST API

Код возврата: «429».

Описание: возвращается, если на сервер отправлено слишком много запросов за определенный промежуток времени. Может сопровождаться заголовком Retry-After, указывающим, через какое время можно повторить запрос.

Тело ответа (JSON Scheme):

```
{
    "properties": {
        "error": {
            "description": "Контейнер ошибки",
            "properties":  {
                "code": {
                    "description": "Общее описание ошибки",
                    "type":        "string",
                    "value":       "too_many_requests "
                },
                "meta": {
                    "description": "Дополнительные данные об ошибки",
                    "type":        "object",
                    "properties":  {
                        "time": {
                            "description": "HTTP-дата, либо целое число в секундах, через которые можно повторить запрос",
                            "type":        "string"
                        }
                    }
                }
```

```
            }
        }
    }
}
```

Ошибка системы REST API

Код возврата: «500».

Описание: возвращается, если в системе произошла логическая ошибка, и далее невозможно выполнение запроса.

Тело ответа (JSON Scheme):

```
{
    "properties": {
        "error": {
            "description": "Контейнер ошибки",
            "properties":  {
                "code": {
                    "description": "Общее описание ошибки",
                    "type":        "string"
                },
                "meta": {
                    "description": "Дополнительные данные об ошибке",
                    "type":        "object"
                }
            }
        }
    }
}
```

Сервер временно не доступен REST API

Код возврата: «503».

Описание: информирует, что в данный момент невозможно выполнить запросы, и сервер находится на техническом обслуживании. Приблизительное время окончания технического обслуживания содержится в заголовке Retry-After (значением этого заголовка может быть либо HTTP-дата, либо целое число в секундах).

Тело ответа (JSON Scheme):

```
{
    "properties": {
        "error": {
```

```
            "description": " Контейнер  ошибки ",
            "properties":  {
                "code": {
                    "description": " Общее  описание  ошибки ",
                    "type":         "string",
                    "value":        "maintains"
                },
                "meta": {
                    "description": " Дополнительные  данные  об  ошибке ",
                     "type":         "object",
                    "properties":  {
                        "time": {
                            "description": "HTTP-дата, либо цело число в секундах, через которые можно повторить запрос",
                            "type":         "string"
                        }
                    }
                }
            }
        }
    }
}
```

## Работа с эталонными документами REST API

Глава содержит следующую информацию:

- Создание каталога эталонных документов REST API;
- Просмотр каталогов эталонных документов REST API;
- Редактирование каталога эталонных документов REST API;
- Удаление каталога эталонных документов REST API;
- Создание эталонного документа REST API;
- Просмотр эталонных документов REST API;
- Обновление и замена содержимого эталонного документа REST API;
- Удаление эталонного документа REST API.

### Создание каталога эталонных документов REST API

**Метод**: `POST`

**Ресурс**: `etalonDocumentCategory`

**Тело запроса** :

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
```

```
    "definitions": {},
    "id": "http://infowatch.com/tm/etalonDocumentCategory/edit",
    "type": "object",
    "properties": {
        "PARENT_CATEGORY_ID": {
            "examples": [
                "AC3DF073B60107890A4C704A10577FE700000000"
            ],
            "title": "GUID категории родителя, если null, то проставляется папка
автоматических эталонных документов",
            "type": "string"
        },
        "DISPLAY_NAME": {
            "title": "Название",
            "type": "string"
        },
        "DIR_PATH (возможно изменение в названии)": {
            "title": "Полное имя директории",
            "type": "string"
        },
        "FP_BIN_VALUE_THRESHOLD": {
            "title": "Порог цитируемости бинарных данных",
            "type": "integer"
        },
        "FP_TEXT_VALUE_THRESHOLD": {
            "title": "Порог цитируемости текстовых данных",
            "type": "integer"
        },
        "NOTE": {
            "title": "Описание",
            "type": [
                "null",
                "string"
            ]
        }
    }
}
```


**Тело ответа :**


```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "definitions": {},
    "id": "http://infowatch.com/tm/etalonDocumentCategory",
    "type": "object",
    "properties": {
        "CATEGORY_ID": {
            "examples": [
                "AC3DF073B60107890A4C704A10577FE700000000"
            ],
            "title": "GUID категории",
            "type": "string"
        },
```

```
        "PARENT_CATEGORY_ID": {
            "examples": [
                "AC3DF073B60107890A4C704A10577FE700000000"
            ],
            "title": "GUID категории родителя",
            "type": "string"
        },
        "DISPLAY_NAME": {
            "title": "Название",
            "type": "string"
        },
        "DIR_PATH (возможно изменение в названии)": {
            "title": "Полное имя директории",
            "type": "string"
        },
        "FP_BIN_VALUE_THRESHOLD": {
            "title": "Порог цитируемости бинарных данных",
            "type": "integer"
        },
        "FP_TEXT_VALUE_THRESHOLD": {
            "title": "Порог цитируемости текстовых данных",
            "type": "integer"
        },
        "NOTE": {
            "title": "Описание",
            "type": [
                "null",
                "string"
            ]
        },
        "OWNER": {
            "title": "ID токена",
            "type": "integer"
        },
        "CREATE_DATE": {
            "examples": [
                "2017-07-04 10:45:45.000000"
            ],
            "title": "Дата создания",
            "type": "string"
        },
        "CHANGE_DATE": {
            "examples": [
                "2017-07-04 10:45:45.000000"
            ],
            "title": "Дата изменения",
            "type": "string"
        }
    }
}
```

Просмотр каталогов эталонных документов REST API

**Метод**: `GET`

**Ресурс**: `etalonDocumentCategory[ /{category_id}]`

**Параметры**:

- `filter` — список фильтрации:
  - `create_date[from]` — начало диапазона для фильтрации по дате создания в формате UNIX-timestamp (включая передаваемую дату, можно использовать отдельно от `create_date[to]` )
  - `create_date[to]` — окончание диапазона для фильтрации по дате создания в формате UNIX-timestamp (включая передаваемую дату, можно использовать отдельно от `create_date[from]` )
  - `change_date[from]` — начало диапазона для фильтрации по дате изменения в формате UNIX-timestamp (включая передаваемую дату, можно использовать отдельно от `change_date[to]` )
  - `change_date[to]` — окончание диапазона для фильтрации по дате изменения в формате UNIX-timestamp (включая передаваемую дату, можно использовать отдельно от `change_date[from]` )
  - `display_name[]` — имя каталога, можно использовать * в конце, чтобы включить поиск по `LIKE` , например: `?filter[display_name][]=foo*`
  - `dir_path[]` — полный путь до каталога, можно использовать * в конце, чтобы включить поиск по `LIKE` , например: `?filter[dir_path][]=foo*`
  - `fingerprint_id []` — GUID эталонного документа, например: `?filter[ fingerprint_id ] []= 82EAE496A1686E407B1162E3C3159999F404F559&filter[fingerprint_id] []=AF8EAC3C3C8532C3C780481B7D8C5B8E68D0148F`
- `with[]` — список дополнительных сущностей, которые должны быть добавлены к объекту:
  - `etalonDocumentsCount` — количество эталонных документов в каталоге
- `sort[]` — поле, позволяющее сортировать результат. Возможные ключи:
  - `create_date` — `desc/asc` , например: `?sort[create_date]=desc`
  - `change_date` — `desc/asc , например: ?sort[change_date]=asc`

**Ответ**:

Массив объектов, отдаваемых при создании/редактировании

**Примеры** :

```
GET /xapi/etalonDocumentCategory?filter[create_date][to]=1&filter[display_name]
[]=foo*&filter[display_name][]=bar&with[]=etalonDocumentsCount&sort[create_date]=desc
GET /xapi/etalonDocumentCategory/FAB85F61531BB9E428088EFC81F266FA3C2959E6
```

Редактирование каталога эталонных документов REST API

**Метод**: PUT

**Ресурс**: `etalonDocumentCategory/{category_id}`

**Тело запроса** :

```
{
```

```
    "$schema": "http://json-schema.org/draft-04/schema#",
    "definitions": {},
    "id": "http://infowatch.com/tm/etalonDocumentCategory/edit",
    "type": "object",
    "properties": {
        "PARENT_CATEGORY_ID": {
            "examples": [
                "AC3DF073B60107890A4C704A10577FE700000000"
            ],
            "title": "GUID категории родителя, если null, то проставляется папка
автоматических эталонных документов",
            "type": "string"
        },
        "DISPLAY_NAME": {
            "title": "Название",
            "type": "string"
        },
        "DIR_PATH (возможно изменение в названии)": {
            "title": "Полное имя директории",
            "type": "string"
        },
        "FP_BIN_VALUE_THRESHOLD": {
            "title": "Порог цитируемости бинарных данных",
            "type": "integer"
        },
        "FP_TEXT_VALUE_THRESHOLD": {
            "title": "Порог цитируемости текстовых данных",
            "type": "integer"
        },
        "NOTE": {
            "title": "Описание",
            "type": [
                "null",
                "string"
            ]
        }
    }
}
```


**Тело ответа**:


```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "definitions": {},
    "id": "http://infowatch.com/tm/etalonDocumentCategory",
    "type": "object",
    "properties": {
        "CATEGORY_ID": {
            "examples": [
                "AC3DF073B60107890A4C704A10577FE700000000"
            ],
            "title": "GUID категории",
            "type": "string"
```

```
        },
        "PARENT_CATEGORY_ID": {
            "examples": [
                "AC3DF073B60107890A4C704A10577FE700000000"
            ],
            "title": "GUID категории родителя",
            "type": "string"
        },
        "DISPLAY_NAME": {
            "title": "Название",
            "type": "string"
        },
        "DIR_PATH (возможно изменение в названии)": {
            "title": "Полное имя директории",
            "type": "string"
        },
        "FP_BIN_VALUE_THRESHOLD": {
            "title": "Порог цитируемости бинарных данных",
            "type": "integer"
        },
        "FP_TEXT_VALUE_THRESHOLD": {
            "title": "Порог цитируемости текстовых данных",
            "type": "integer"
        },
        "NOTE": {
            "title": "Описание",
            "type": [
                "null",
                "string"
            ]
        },
        "OWNER": {
            "title": "ID токена",
            "type": "integer"
        },
        "CREATE_DATE": {
            "examples": [
                "2017-07-04 10:45:45.000000"
            ],
            "title": "Дата создания",
            "type": "string"
        },
        "CHANGE_DATE": {
            "examples": [
                "2017-07-04 10:45:45.000000"
            ],
            "title": "Дата изменения",
            "type": "string"
        }
    }
}
```


**Пример редактирования каталога CURL**

```
curl 'https://example.com/xapi/etalonDocumentCategory/0123456789ABCDEF123400000000' \
  -X PUT \
  -H 'X-API-Auth-Token: 1792jmclf7fer1ikuhby' \
  -H 'X-API-Version: 1' \
  -H 'X-API-CompanyId: IW' \
  -H 'X-API-DataType: sap' \
  -H 'Content-Type: application/json' \
  --data-
binary
'{"PARENT_CATEGORY_ID":"0123456789ABCDEF123400000000","DISPLAY_NAME":"world.txt","DIR_
PATH":"c:\\hello\
\world.txt","FP_BIN_VALUE_THRESHOLD":10,"FP_TEXT_VALUE_THRESHOLD":10,"NOTE":null}'
```

Удаление каталога эталонных документов REST API

**Метод**: `DELETE`
**Ресурс**: `etalonDocumentCategory /{category_id}`

Создание эталонного документа REST API

Предполагается, что сначала создаётся эталонный документ, с помощью `POST /xapi/ etalonDocument` со статусом new, а дальше происходит его компиляция, статус которой нужно проверять с помощью получения эталонного документа ( `GET /xapi/ etalonDocument/{id}` ) и его отслеживания. При получении дубликатов эталонного документа (STATUS=duplicate), такие файлы будут удалены.

**Метод**: `POST`
**Ресурс**: `etalonDocument`
**Тело запроса**:

Поля:

| Название поля | Описание |
|---|---|
| DISPLAY_NAME | Имя эталонного документа (если не указано, то берётся из поля FILE) |
| FILE_PATH* | Путь к эталонному документу в источнике, например: smb://example.com/top_secret/etalon.docx, \\example\test\text.rtf, ftp://example.com/foo/bar.txt, oracle://example.com:1521/database/table/row, https://examlpe.com/same/html/document<br>По факту, это просто подсказка для автоматического загрузчика, по-которой он может искать |
| NOTE | Описание эталонного документа |
| BIN_VALUE_THRESHOLD | Порог цитируемости бинарных данных (по умолчанию берется из первого указанного каталога) |
| TEXT_VALUE_THRESHOLD | Порог цитируемости текстовых данных (по умолчанию берется из первого указанного каталога) |

| Название поля | Описание |
| --- | --- |
| CATEGORY_ID* | Список GUID-ов категорий, разделенных запятой, например: "E77D893219A24EEAB3D049804FD86751,C743F88121B8449DAF37291474830679,A7AF8EFCF4D54E9393A9B3D750E5ABBB" |
| FILE* | Сам файл (Передаётся сам файл, а не путь к нему. Сервер не сможет подключиться к вашему компьютеру и забрать его сам. Поэтому весь файл передаётся в запросе) |
| COMPILE_TYPE* | Тип цифрового отпечатка:<br>• TEXT — Извлекать только текст<br>• ALL — Извлекать и компилировать всё что возможно |

* — поле обязательно для заполнения

**Ответ**: JSON-Schema:

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "definitions": {},
    "id": "http://infowatch.com/tm/etalonDocument",
    "type": "object",
    "properties": {
        "FINGERPRINT_ID": {
            "examples": [
                "139C7026ED48BE13459669024786F7517E5687AE"
            ],
            "title": "Идентификатор эталонного документа",
            "type": "string"
        },
        "DISPLAY_NAME": {
            "title": "Название",
            "type": "string"
        },
        "FILE_PATH": {
            "title": "Полное имя файла",
            "type": "string"
        },
        "FILE_SIZE": {
            "title": "Размер файла в байтах",
            "type": "integer"
        },
        "MIME": {
            "title": "Mime-type файла",
            "type": "string"
        },
        "BIN_VALUE_THRESHOLD": {
            "title": "Порог цитируемости бинарных данных",
            "type": "integer"
        },
        "TEXT_VALUE_THRESHOLD": {
```

```
        "title": "Порог цитируемости текстовых данных",
        "type": "integer"
    },
    "NOTE": {
        "title": "Описание",
        "type": [
            "null",
            "string"
        ]
    },
    "OWNER": {
        "title": "ID токена",
        "type": "integer"
    },
    "STATUS": {
        "examples": [
            "new",
            "compiled",
            "compiling",
            "sending",
            "sent",
            "saving",
            "ready",
            "fatal_error",
            "duplicate",
            "error"
        ],
        "title": "Статус обработки",
        "type": "string"
    },
    "CREATE_DATE": {
        "examples": [
            "2017-07-04 10:45:45.000000"
        ],
        "title": "Дата создания",
        "type": "string"
    },
    "CHANGE_DATE": {
        "examples": [
            "2017-07-04 10:45:45.000000"
        ],
        "title": "Дата изменения",
        "type": "string"
    },
    "categories": {
        "type": "array",
        "title": "Массив категорий",
        "items": {
            "type": "object",
            "properties": {
                "CATEGORY_ID": {
                    "examples": [
                        "AC3DF073B60107890A4C704A10577FE700000000"
```

```
                        ],
                        "title": "GUID категории",
                        "type": "string"
                    },
                    "DISPLAY_NAME": {
                        "title": "Название",
                        "type": "string"
                    },
                    "DIR_PATH (возможно изменение в названии)": {
                        "title": "Полное имя директории",
                        "type": "string"
                    },
                    "FP_BIN_VALUE_THRESHOLD": {
                        "title": "Порог цитируемости бинарных данных",
                        "type": "integer"
                    },
                    "FP_TEXT_VALUE_THRESHOLD": {
                        "title": "Порог цитируемости текстовых данных",
                        "type": "integer"
                    },
                    "NOTE": {
                        "title": "Описание",
                        "type": [
                            "null",
                            "string"
                        ]
                    },
                    "OWNER": {
                        "title": "ID токена",
                        "type": "integer"
                    },
                    "CREATE_DATE": {
                        "examples": [
                            "2017-07-04 10:45:45.000000"
                        ],
                        "title": "Дата создания",
                        "type": "string"
                    },
                    "CHANGE_DATE": {
                        "examples": [
                            "2017-07-04 10:45:45.000000"
                        ],
                        "title": "Дата изменения",
                        "type": "string"
                    }
                }
            }
        }
    }
}
```


**Пример**:

```
POST /xapi/etalonDocument HTTP/1.1
Host: tm.example.com
X-API-Auth-Token: brse99dugp1cdbr69axz
X-API-Version: 1
X-API-DataType: cap
X-API-CompanyId: liw
Content-Type: multipart/form-data; boundary=Asrf456BGe4h
Content-Length: (суммарный объём, включая дочерние заголовки)
(пустая строка)
(отсутствующая преамбула)
--Asrf456BGe4h
Content-Disposition: form-data; name="CATEGORY_ID"
(пустая строка)
2ABECC84F2360B94E0533D003C0A80AE00000000
--Asrf456BGe4h
Content-Disposition: form-data; name="COMPILE_TYPE"
(пустая строка)
ALL
--Asrf456BGe4h
Content-Disposition: form-data; name="FILE"; filename="foo.doc"
Content-Type: application/msword
(пустая строка)
(двоичное содержимое документа)
```

**Пример создания файла с помощью CURL**

```
curl -i -X POST \
   -H "Content-Type:multipart/form-data" \
   -H "X-API-Auth-Token:brse99dugp1cdbr69axz" \
   -H "X-API-Version:1" \
   -H "X-API-DataType:cap" \
   -H "X-API-CompanyId:liw" \
   -F "CATEGORY_ID=2ABECC84F2360B94E0533D003C0A80AE00000000" \
   -F "FILE=@\"./foo.doc\";filename=\"foo.doc\"" \
   -F "COMPILE_TYPE=ALL" \
 'https://tm.example.com/xapi/etalonDocument'
```

Просмотр эталонных документов REST API

**Метод**: `GET`
**Ресурс**: `etalonDocument[/{fingerprint_id}]`
**Параметры**:

- `filter` — список фильтрации:
  - `create_date[from]` — начало диапазона для фильтрации по дате создания в формате UNIX-timestamp (включая передаваемую дату, можно использовать отдельно от `create_date[to]`)
  - `create_date[to]` — окончание диапазона для фильтрации по дате создания в формате UNIX-timestamp (включая передаваемую дату, можно использовать отдельно от `create_date[from]`)

    - `change_date[from]` — начало диапазона для фильтрации по дате изменения в формате UNIX-timestamp (включая передаваемую дату, можно использовать отдельно от `change_date[to]`)
    - `change_date[to]` — окончание диапазона для фильтрации по дате изменения в формате UNIX-timestamp (включая передаваемую дату, можно использовать отдельно от `change_date[from]`)
    - `display_name[]` — имя файла, можно использовать * в конце, чтобы включить поиск по `LIKE`, например: `?filter[display_name][]=foo*`
    - `file_path[]` — полный путь до файла, можно использовать * в конце, чтобы включить поиск по `LIKE`, например: `?filter[file_path][]=foo*`
    - `category_id[]` — GUID категории, например: `?filter[category_id][]=82EAE496A1686E407B1162E3C3159999F404F559&filter[category_id][]=AF8EAC3C3C8532C3C780481B7D8C5B8E68D0148F`
    - `category_path[]` — полный путь до папки категории, можно использовать * в конце, чтобы включить поиск по `LIKE`, например: `?filter[category_path][]=bar*`
- `with[]` — список дополнительных сущностей, которые должны быть добавлены к объекту:
    - `categories` — список категорий, в которые входит эталонный документ
- `sort[]` — поле, позволяющее сортировать результат. Возможные ключи:
    - `create_date` — `desc/asc`, например: `?sort[create_date]=desc`
    - `change_date` — `desc/asc`, например: `?sort[change_date]=asc`

**Ответ**:

Массив объектов, отдаваемых при создании/редактировании

**Примеры**:

```
GET /xapi/etalonDocument?filter[create_date][to]=1&filter[display_name]
[]=foo*&filter[display_name][]=bar&with[]=categories&sort[create_date]=desc
GET /xapi/etalonDocument/FAB85F61531BB9E428088EFC81F266FA3C2959E6
```

Обновление и замена содержимого эталонного документа REST API

**Метод**: POST

**Ресурс**: `etalonDocument/{fingerprint_id}/update`

**Тело запроса**:

Поля:

| Название поля | Описание |
|---|---|
| DISPLAY_NAME | Имя эталонного документа (если не указано, то берётся из поля FILE) |
| FILE_PATH | Путь к эталонному документу в источнике, например: smb://example.com/top_secret/etalon.docx, \\example\test\text.rtf, ftp://example.com/foo/bar.txt, oracle://example.com:1521/database/table/row, https://examlpe.com/same/html/document |
| NOTE | Описание эталонного документа |

| Название поля | Описание |
|---|---|
| BIN_VALUE_THRESHOLD | Порог цитируемости бинарных данных (по умолчанию берется из первого указанного каталога) |
| TEXT_VALUE_THRESHOLD | Порог цитируемости текстовых данных (по умолчанию берется из первого указанного каталога) |
| CATEGORY_ID | Список GUID-ов категорий, разделенных запятой, например: "E77D893219A24EEAB3D049804FD86751,C743F88121B8449DAF37291474830679,A7AF8EFCF4D54E9393A9B3D750E5ABBB" |
| FILE | Сам файл (Передаётся сам файл, а не путь к нему. Сервер не сможет подключиться к вашему компьютеру и забрать его сам. Поэтому весь файл передаётся в запросе) |
| COMPILE_TYPE | Тип цифрового отпечатка:<br>• TEXT — Извлекать только текст<br>• ALL — Извлекать и компилировать всё что возможно |

Передавать нужно только те поля, которые нужно изменить. Остальные поля нужно опускать.

**Ответ**:


```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "definitions": {},
    "id": "http://infowatch.com/tm/etalonDocument",
    "type": "object",
    "properties": {
        "FINGERPRINT_ID": {
            "examples": [
                "139C7026ED48BE13459669024786F7517E5687AE"
            ],
            "title": "Идентификатор эталонного документа",
            "type": "string"
        },
        "DISPLAY_NAME": {
            "title": "Название",
            "type": "string"
        },
        "FILE_PATH": {
            "title": "Полное имя файла",
            "type": "string"
        },
        "FILE_SIZE": {
            "title": "Размер файла в байтах",
            "type": "integer"
        },
        "MIME": {
            "title": "Mime-type файла",
```

```
            "type": "string"
        },
        "BIN_VALUE_THRESHOLD": {
            "title": "Порог цитируемости бинарных данных",
            "type": "integer"
        },
        "TEXT_VALUE_THRESHOLD": {
            "title": "Порог цитируемости текстовых данных",
            "type": "integer"
        },
        "NOTE": {
            "title": "Описание",
            "type": [
                "null",
                "string"
            ]
        },
        "OWNER": {
            "title": "ID токена",
            "type": "integer"
        },
        "STATUS": {
            "examples": [
                "new",
                "compiled",
                "compiling",
                "sending",
                "sent",
                "saving",
                "ready",
                "fatal_error",
                "duplicate",
                "error"
            ],
            "title": "Статус обработки",
            "type": "string"
        },
        "CREATE_DATE": {
            "examples": [
                "2017-07-04 10:45:45.000000"
            ],
            "title": "Дата создания",
            "type": "string"
        },
        "CHANGE_DATE": {
            "examples": [
                "2017-07-04 10:45:45.000000"
            ],
            "title": "Дата изменения",
            "type": "string"
        },
        "categories": {
            "type": "array",
```

```
"title": "Массив категорий",
"items": {
    "type": "object",
    "properties": {
        "CATEGORY_ID": {
            "examples": [
                "AC3DF073B60107890A4C704A10577FE700000000"
            ],
            "title": "GUID категории",
            "type": "string"
        },
        "DISPLAY_NAME": {
            "title": "Название",
            "type": "string"
        },
        "DIR_PATH (возможно изменение в названии)": {
            "title": "Полное имя директории",
            "type": "string"
        },
        "FP_BIN_VALUE_THRESHOLD": {
            "title": "Порог цитируемости бинарных данных",
            "type": "integer"
        },
        "FP_TEXT_VALUE_THRESHOLD": {
            "title": "Порог цитируемости текстовых данных",
            "type": "integer"
        },
        "NOTE": {
            "title": "Описание",
            "type": [
                "null",
                "string"
            ]
        },
        "OWNER": {
            "title": "ID токена",
            "type": "integer"
        },
        "CREATE_DATE": {
            "examples": [
                "2017-07-04 10:45:45.000000"
            ],
            "title": "Дата создания",
            "type": "string"
        },
        "CHANGE_DATE": {
            "examples": [
                "2017-07-04 10:45:45.000000"
            ],
            "title": "Дата изменения",
            "type": "string"
        }
    }
```

```
            }
        }
    }
}
```

Удаление эталонного документа REST API

**Метод**: DELETE
**Ресурс**: `etalonDocument/{fingerprint_id}`



## 9.3 Получение доступа к событиям Traffic Monitor внешними системами (DataExport API SDK)

Данный программный интерфейс предназначен для интеграции Traffic Monitor с внешними системами-приемниками данных. В рамках реализации DataExport API внешние системы получают из Traffic Monitor содержимое и метаданные событий, данные организационной структуры, списки пользователей Консоли управления и данные аудита их действий. DataExport API поддерживает двусторонний обмен данными между Traffic Monitor и внешними системами.

### 9.3.1 Функции DataExport API

DataExport API поддерживает следующий набор функций:

- Возможность указать набор атрибутов, которые будут включены в результат:
    - ID события;
    - Отправители: список контактов и результат идентификации с учетом возможных конфликтов;
    - Получатели: список контактов и результат идентификации с учетом возможных конфликтов;
    - Компьютер отправителя с учетом возможных конфликтов;
    - Тип события;
    - Дата и время перехвата;
    - Протокол;
    - Уровень нарушения;
    - Вердикт;
    - Путь к файлу или адрес приемника;
    - Путь к файлу или адрес источника;
    - Решение пользователя;
    - Путь к файлу;
    - Адрес веб-ресурса;
    - Объекты защиты и каталоги;
    - Размер события;
    - Теги;
    - Набор пользовательских атрибутов, зарегистрированных через плагин;
    - Набор системных заголовков событий;
    - Дата и время вставки события в БД;
    - Наименование периметра, в которое вошло событие;
    - Наименование периметра, из которых ушло событие ;
    - Список наименований политик (с ID политик), сработавших на перехваченном объекте;

    - Группа правил;
    - Сервер перехвата;
    - Сервер перехвата IP;
    - Имя устройства приемника;
    - Имя устройства источника;
    - Тема письма;
    - Вложение;
    - Мандатный уровень;
    - Мандатная категория.
- Возможность указать набор атрибутов, по которым будет осуществляться фильтрация:
    - Дата и время перехвата;
    - Тип события;
    - Протокол;
    - Каталог ОЗ;
    - Решение пользователя;
    - Размер события;
    - Теги;
    - Дата и время вставки события в БД;
    - Группа правил;
    - Уровень нарушения;
    - Вердикт;
    - Дата и время зарегистрированного действия пользователя;
    - Тип объекта, над которым осуществлялось действие.
- Возможность изменить в Traffic Monitor атрибуты события:
    - Вердикт пользователя по событию;
    - Вердикт пользователя по множеству событий.
- Получение метаданных отдельного события с возможностью указать набор атрибутов, которые будут включены в результат. При этом если в событии есть нескольких вложенных объектов, то весь извлеченный текст будет склеен в один файл;
- Получение всего извлеченного текста отдельного события;
- Получение полного списка системных заголовков и зарегистрированных с помощью плагина пользовательских атрибутов событий;
- Получение бинарных данных отдельного события;
- Получение списка пользователей Консоли управления;
- Запуск на выполнение и получение результатов выполнения запросов в Traffic Monitor:
    - список запросов;
    - статус выполнения запросов;
    - результаты запросов;
- Получение данных аудита пользователей:
    - ID записи в аудите сессий пользователей консоли;
    - Дата и время зарегистрированного действия пользователя в UTC;
    - ID пользователя, осуществившего действие;
    - Полное имя пользователя, осуществившего действие;
    - Тип действия, которое было произведено пользователем;
    - Тип объекта, над которым осуществлялось действие;
    - ID объекта, над которым осуществлялось действие;
    - Наименование объекта, над которым осуществлялось действие;

- Описание произошедших изменений с указанием новых и старых значений.

## 9.3.2 Авторизация для доступа к DataExport API

Авторизация для доступа к DataExport API предоставляется по механизму токенов, аналогичному другим API InfoWatch Traffic Monitor. Для получения токена и просмотра статуса лицензирования DataExport API в Системе необходимо добавить плагин нового типа - Плагин для DataExport API. Все действия по работе с плагинами выполняются в консоли управления Traffic Monitor.

### Работа с плагинами

#### Добавление плагина

Чтобы добавить плагин:

1. Перейдите в раздел **Управление - Плагины**;
2. В области **Плагины** нажмите .
3. Нажмите **Добавить**.
4. Просмотрите описание плагина и нажмите **Установить**.

> **Примечание:**
>
> Чтобы обновить плагин, добавьте его обновленную версию.

#### Удаление плагина

Чтобы удалить плагин:

1. Перейдите в раздел **Управление - Плагины**;
2. В области **Плагины** нажмите .
3. Нажмите **Да**, чтобы подтвердить удаление.

### Работа с токенами

Токен генерируется автоматически после добавления плагина. Все действия по работе с токенами выполняются в консоли управления InfoWatch Traffic Monitor.

#### Добавление токена

Чтобы добавить токен:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите .

**Примечание:**

Значение токена генерируется автоматически при создании токена и не может быть задано пользователем.

Редактирование данных токена

Чтобы изменить данные токена:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. По двойному нажатию левой кнопкой мыши в графе *Имя* или *Описание* введите нужную информацию.

Обновление значения токена

Если токен скомпрометирован или появилась вероятность его утечки третьим лицам, нужно сгенерировать значение токена заново.

Чтобы обновить значение токена:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите  .

Копирование токена

Чтобы скопировать значение токена в буфер обмена:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите  .

Удаление токена

Чтобы удалить токен:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите  .

## 9.3.3 Регистрация стороннего компонента DataExport API

Для интеграции сторонней системы-приемника данных с системой Traffic Monitor нужно выполнить следующие шаги:

1. Зарегистрировать в компании InfoWatch строку-идентификатор компании-потребителя компонента. Это позволит связывать компанию-потребителя с лицензией, которая будет устанавливаться в систему Traffic Monitor;
2. Получить лицензию разработчика, связанную с идентификатором компании. Это позволит выгружать из Traffic Monitor данные о событиях;
3. Создать файл регистрации стороннего компонента в описанном ниже формате. В файл регистрации добавляется лицензия, полученная на шаге 2;
4. Загрузить файл регистрации стороннего компонента в систему Traffic Monitor через интерфейс консоли Traffic Monitor. Раздел «Управление» - «Плагины». (см. "Traffic Monitor. Руководство пользователя");
5. Получить токен доступа в свойствах загруженного стороннего компонента;

Система готова отправлять данные о событиях заданной компании.

## Формат файла регистрации стороннего компонента DataExport API

Плагин представляет собой архив в формате .zip. В состав архива входят:

- папка **licenses**, содержащая файлы лицензий;
- папка **icon**, содержащая файлы с используемыми пиктограммами для регистрируемых событий;
- файл **manifest.json**, содержащий информацию о плагине.

> **Примечание:**
>
> Папки **licenses** и **icon** не являются обязательными. Файлы лицензий и файлы с используемыми пиктограммами могут находиться в корне.

Для внешних систем-приемников данных из Traffic Monitor файл **manifest.json** должен содержать следующую информацию:

| Содержимое | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| `{` | | | |
| `"PLUGIN_ID": "",` | Строка | Да | Уникальный идентификатор (UUID) плагина, который создается его разработчиком. До 40 символов. Идентификатор используется для обновления плагина. **Пример:** `"PLUGIN_ID": "189C38D390396EB6E0530100007F1CA200000001",` |
| `"DISPLAY_NAME": "",` | Строка | Да | Отображаемое имя плагина. **Пример:** `"DISPLAY_NAME": "Имя плагина",` |

| Содержимое | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| `"DESCRIPTION": "",` | Строка | Нет | Отображаемое описание плагина.<br>**Пример:** `"DESCRIPTION": "Тестовый плагин для демонстрации",` |
| `"VERSION": "",` | Строка | Да | Версия плагина.<br>**Пример:** `"VERSION": "1.0.0",` |
| `"VENDOR": "",` | Строка | Да | Идентификатор компании-разработчика, соответствующий названию компании в лицензии.<br>**Пример:** `"VENDOR": "infowatch",` |
| `"LICENSE": [ { "PATH":"" } ],` | Массив<br>Строка | Да | Файлы лицензии. Должны быть указаны пути к файлам лицензий относительно корня архива.<br>**Пример**<br>`"LICENSE": [ { "PATH": "licenses/файл лицензии 1.license" }, { "PATH": "licenses/файл лицензии 2.license" }, ],` |
| `"PATTERN_SEARCH_LICENSE": "",` | Строка | Нет | Шаблон для поиска загруженных ранее лицензий для привязки их к плагину. Имеет формат: `{operator:or\|and,child[{name:value}]}"`.<br>**Пример:**<br>`"PATTERN_SEARCH_LICENSE": "{\"operator\":\"or\", \"conditions\":[{\"origin\": \"dm\"},{\"origin\": \"dmmobile\"}]}",` |
| `"DATA_RECEIVER": [ "" ]` | Массив<br>Строка | Да | Список идентификаторов систем-приемников данных из Traffic Monitor.<br>**Пример**<br>`"DATA_RECEIVER": [` |

| Содержимое | Тип данных | Является обязательным | Описание |
|---|---|---|---|
| | | | "Events reciever1",<br>"Events reciever2"<br>] |
| "OBJECT_HEADER": [<br>{<br>"NAME": "",<br><br>"NOTE": {<br>"": "",<br>"": ""<br>},<br>"TYPE": "",<br>"FORMAT": "",<br><br>"DATA_CLASS": [""],<br>"USE_IN_POLICY": "",<br>"USE_IN_NOTIFICATION": "",<br>"USE_IN_QUERY": "",<br>"USE_IN_LIST": "",<br>"USE_IN_SHOW": "",<br>"USE_IN_DETAIL": "",<br>"IS_MULTIPLE_VALUE": "",<br>}<br>] | Массив<br><br>Строка<br><br>Объект<br>Строка<br><br>Перечисление<br>Перечисление<br><br>Массив строк<br>Перечисление<br>Перечисление<br><br>Перечисление<br>Перечисление<br>Перечисление<br>Перечисление<br><br>Перечисление | Нет | Пользовательские атрибуты событий.<br><br>Уникальный код атрибута, который будет использован в заголовках события и для идентификации в xAPI/PushAPI.<br>Если идентификатор разработчика не "IW", код должен начинаться с префикса " <Идентификатор компании-разработчика>_ ".<br>**Пример:** CISCO_CALL_DURATION<br>Название атрибута, отображаемое в консоли Traffic Monitor.<br><br>Тип значения.<br>Формат записи. Возможны значения: число (целое, дробное), строка, дата и время в UTC + указание смещение часового пояса, длительность, гиперссылка, перечисление, логический тип.<br>Сервисы, к событиям которых будет добавлен новый пользовательский атрибут.<br>Использование атрибута в политиках. "1" - да, "0" - нет.<br>Использование атрибута в почтовых уведомлениях. "1" - да, "0" - нет.<br><br>Использование атрибута в запросах. "1" - да, "0" - нет.<br>Отображение атрибута в табличном режиме просмотра событий. "1" - да, "0" - нет.<br>Отображение атрибута в краткой форме просмотра события. "1" - да, "0" - нет.<br>Отображение атрибута в детальной форме просмотра события. "1" - да, "0" - нет.<br><br>Множественное значение. "1" - да, "0" - нет. |

| Содержимое | Тип данных | Является обязательным | Описание |
| --- | --- | --- | --- |
| | | | **Пример**<br><br>"OBJECT_HEADER": [<br>{<br>"NAME": "header_multi_string",<br>"NOTE": {<br>"rus": "Заголовок строк1",<br>"eng": "Header strings1"<br>},<br>"DATA_CLASS": ["kEmail"],<br>"USE_IN_POLICY": "1",<br>"USE_IN_QUERY": "1",<br>"USE_IN_NOTIFICATION": "1",<br>"USE_IN_LIST": "1",<br>"USE_IN_SHOW": "1",<br>"USE_IN_DETAIL": "1",<br>"TYPE": "string",<br>"FORMAT": "string",<br>"IS_MULTIPLE_VALUE": "1"<br>},<br>{<br>"NAME": "header_date",<br>"NOTE": {<br>"rus": "Заголовок дата1",<br>"eng": "Header date1"<br>},<br>"DATA_CLASS": ["kEmail"],<br>"USE_IN_POLICY": "1",<br>"USE_IN_QUERY": "1",<br>"USE_IN_NOTIFICATION": "1",<br>"USE_IN_LIST": "0",<br>"USE_IN_SHOW": "1",<br>"USE_IN_DETAIL": "1",<br>"TYPE": "string",<br>"FORMAT": "date",<br>"IS_MULTIPLE_VALUE": "0"<br>}<br>] |
| } | | | |

## 9.3.4 Функциональное описание программного интерфейса DataExport API

### Общие заголовки GET/POST-запросов для DataExport API

#### Авторизация

Токен, полученный для Public API, необходимо указывать в заголовке **X-API-Auth-Token** при каждом запросе к API. Токен может быть отозван/заблокирован/удалён через web-интерфейс IWTM. В случае, если это произойдет, токен считается недействительным. При указании недействительным токена возвращается сообщение об ошибке с кодом **401**.

**Пример ответа при недействительном токене**

```
{
    "error": {
        "code": "unauthorized"
    }
}
```

Если токен действующий, но у пользователя API недостаточно прав, то пользователю возвращается сообщение об ошибке с кодом **403**.

**Пример ответа при нехватке прав**

```
{
    "error": {
        "code": "forbidden"
    }
}
```

#### Версионирование

Версия API передается с помощью заголовка **X-API-Version** и может иметь 3 состояния:

- supported — версия поддерживается и активно развивается;
- deprecated — версия доступна, но перестала поддерживаться. Рекомендуется перейти на новую версию, так как в следующих выпусках эта версия может быть удалена;
- removed — версия полностью удалена из продукта.

В случае, если сервер не поддерживает версию, ему возвращается сообщение об ошибке с кодом **400**.

**Ответ в случае некорректной версии**

```
{
    "error": {
        "code": "unsupported_version",
        "meta": {
            "versions": [
                {
                    "NAME":   "1",
```

```
                    "STATUS": "removed"
                },
                {
                    "NAME":   "1.1",
                    "STATUS": "deprecated"
                },
                {
                    "NAME":   "1.2",
                    "STATUS": "deprecated"
                },
                {
                    "NAME":   "1.3",
                    "STATUS": "deprecated"
                },
                {
                    "NAME":   "1.4",
                    "STATUS": "deprecated"
                },
                {
                    "NAME":   "1.5",
                    "STATUS": "deprecated"
                },
                {
                    "NAME":   "1.6",
                    "STATUS": "deprecated"
                },
                {
                    "NAME":   "1.7",
                    "STATUS": "supported"
                }
            ]
        }
    }
}
```

Лицензирование

Для работы модуля требуется лицензия:

```
{
    "common_name": "iw",
    "importer_name": "dome"
}
```

Где `common_name` — это название лицензируемой компании, а `importer_name` — продукт, который принимает данные от TM.

В каждом запросе нужно передавать заголовки **X-API-CompanyId** и **X-API-ProductName**. В случае, если лицензия не проходит проверку, возвращается сообщение об ошибке с кодом **403**.

**Формат ответа при невалидной лицензии**

```
{
    "error": {
```

```
        "code": "licence_not_valid"
    }
}
```

Таким образом, каждый запрос к серверу должен содержать следующие обязательные заголовки:

- X-API-Version – указывается номер версии программного интерфейса. Текущая версия: **1.6**;
- X-API-CompanyId – указывается идентификатор компании-производителя, например: **iw**;
- X-API-ProductName – указывается продукт, принимающий данные, например: **dome**;
- X-API-Auth-Token – указывается токен авторизации.

**Пример запроса**

```
X-API-Version: 1.6
X-API-CompanyId: iw
X-API-ProductName: dome
X-API-Auth-Token: gla20dos1pcdbr69caxz
```

## Получение списка фич по версии Traffic Monitor

**Описание**: Список фич для текущей версии Traffic Monitor.

**Метод**: `GET`

**Ресурс**: `version/features`

**Параметры** :

**Пример запроса:**

```
curl -k -i -X GET    -H "X-Api-Auth-Token:1lap4tvpakbgsbj8tyeu"    -H "X-Api-Version:1.3"    -H "X-Enable-Openapi:1"    -H "X-API-CompanyId:iw"    -H "X-API-ProductName:dome"  'https://qa-797e.infowatch.ru/xapi/version/features'
```

**Пример ответа:**

```
{
  "data": [
    {
      "VERSION_TM": "7.3.0.285",
      "VERSION_API": "1.6",
      "FEATURES": "sso - сквозная авторизация из vision в tm"
    }
  ]
}
```

## Получение данных аудита

> **Примечание:**
>
> В API получения данных аудита могут появляться новые действия. При этом версия API может не меняться.

**Описание**: Список данных аудита, отсортированных по дате и времени зарегистрированного действия пользователя.

**Метод**: `GET`

**Ресурс**: `audit`

**Параметры**:

- `filter` - список фильтрации:
  - `change_date[>]` – дата и время начала зарегистрированного действия пользователя в формате UNIX-timestamp и через точку microtime, например `filter[change_date][>]=1591368000.123456`
  - `change_date[<]` – дата и время окончания зарегистрированного действия пользователя в формате UNIX-timestamp и через точку microtime, например `filter[change_date][<]=1591368000.123456`
  - `change_date[>=]` – дата и время начала зарегистрированного действия пользователя в формате UNIX-timestamp и через точку microtime, например `filter[change_date][>=]=1591368000.123456`
  - `change_date[<=]` – дата и время окончания зарегистрированного действия пользователя в формате UNIX-timestamp и через точку microtime, например `filter[change_date][<=]=1591368000.123456`
  - `entity_type[]` – тип сущности, над которой было выполнено действие (возможно несколько значений);
- `without[] –` получить данные без дополнительных атрибутов:
  - `property_changes` – данные расширенного аудита.
- `sort[]` – параметр для сортировки:
  - `change_date` — сортировать по дате изменения `asc` .
- `start` – с какой позиции начать отдавать данные аудита (по умолчанию 0)
- `limit` – сколько комплектов данных аудита отдавать (по умолчанию 100, не может быть больше 1000)

**OpenAPI-схема отдачи данных аудита**

```
schemas:
    auditCommon:
      type: object
      required: [AUDIT_LOG_ID, CHANGE_DATE, OPERATION, ENTITY_TYPE]
      properties: &common
        AUDIT_LOG_ID:
          type: integer
          description: Audit log id
        USER_ID:
          type: integer
          nullable: true
```

```
          description: |
            User id who performed the action (See /xapi/user).
            USER_ID may be null on login or if changes make by plugin.
        CHANGER_NAME:
          type: string
          nullable: true
          description: |
            User name or Plugin name who performed the action.
            May be null on login.
        CHANGE_DATE:
          type: string
          description: Date and time of the registered user action with format "Y-m-d H:i:s.u" in UTC
          example: "2020-05-14 13:53:52.926560"
        OPERATION:
          type: string
          description: Operation type over which the action was performed. There may be values not from the
enum.
          enum:
            - run
            - canceled
            - start
            - stop
            - restart
            - view
            - create
            - update
            - change
            - delete
            - delete_ref
            - delete_hash
            - copy
            - move
            - login_failure
            - bruteforce
            - login
            - logout
            - change_password
            - commit
            - rollback
            - draft
            - add
            - import
            - export
            - export_object
            - create_widget
            - update_widget
            - delete_widget
            - download
            - sync
            - decision_update
            - add_tag
            - remove_tag
            - add_role
            - remove_role
            - add_visibility_area
            - remove_visibility_area
            - logging
            - apply_inbound
```

```
            - xapi_decision_update
            - start_scan_job
            - apply_result_scan_job
            - update_job_schedule
            - create_log
            - plugin_register
            - plugin_update
            - privileges_update
            - privileges_create
            - notification
            - notification_template
            - notification_test
            - upload_image
            - delete_image
            - create_contact
            - update_contact
            - delete_contact
            - compile_create
            - compile_update
            - create_template
            - update_template
            - delete_template
            - create_rule
            - update_rule
            - delete_rule
            - notification_test
        ENTITY_TYPE:
          type: string
          description: Entity type over which the action was performed. There may be values not from the
enum.
          enum: *entryTypes
        ENTITY_ID:
          type: string
          nullable: true
          description: |
            ID of the entity which the action was performed. May be GUID or integer as string
            May by null for:
            | OPERATION | ENTITY_TYPE |
            | :--- | :--- |
            | commit | Config |
            | run | QueryReportRun |
            | sync | Adlibitum |
            | login | User |
            | rollback | Config |
          example: "DBAF4F834F7647CBB297BC9DD17B77B100000000"
        ENTITY_DISPLAY_NAME:
          type: string
          nullable: true
          description: The name of the entity over which the action was carried out
          example: "Some name"
        PROPERTY_CHANGES:
          type: object
          nullable: true
          description: Null in default Audit log events
    userLoginLogout:
      type: object
      description: For ENTITY_TYPE User and OPERATION login or logout
      properties:
```

```
    <<: *common
    OPERATION:
      type: string
      enum: [login, logout]
    ENTITY_TYPE:
      type: string
      enum: [User]
    PROPERTY_CHANGES:
      type: object
      nullable: true
      required: [request]
      properties:
        request:
          required:
            - hostname
            - ip
            - result
            - login
          properties:
            hostname:
              type: string
              title: Hostname
              description: Hostname from which authorization passed
            ip:
              type: string
              title: Ip address
              description: Ip address from which authorization passed
            result:
              type: string
              title: Result
              description: Result
              enum:
                - login_failure
                - login
                - logout
            login:
              type: string
              title: User login
              description: Entered user login in input
userBruteForce:
  type: object
  description: For ENTITY_TYPE User and OPERATION login with bruteforce
  properties:
    <<: *common
    OPERATION:
      type: string
      enum: [ bruteforce ]
    ENTITY_TYPE:
      type: string
      enum: [ User ]
    PROPERTY_CHANGES:
      type: object
      nullable: true
      required: [ login ]
      properties:
        request:
          required:
            - login
```

```
            - display_name
          properties:
            login:
              type: string
              title: User login
              description: Entered user login in input
            display_name:
              type: string
              title: User full name
              description: User full name
tagPropertyChanges:
  type: object
  properties:
    <<: *common
    ENTITY_TYPE:
      type: string
      enum: [ Object ]
    OPERATION:
      type: string
      enum: [ add_tag, remove_tag ]
    PROPERTY_CHANGES:
      type: object
      properties:
        new:
          $ref: '#/components/schemas/TagDiffProperties'
        old:
          $ref: '#/components/schemas/TagDiffProperties'
TagDiffProperties:
  type: object
  properties:
    DISPLAY_NAME:
      type: string
    NOTE:
      type: string
userDesicionPropertyChanges:
  type: object
  properties:
    <<: *common
    ENTITY_TYPE:
      type: string
      enum: [ Object ]
    OPERATION:
      type: string
      enum: [ decision_update, xapi_decision_update ]
    PROPERTY_CHANGES:
      type: object
      properties:
        new:
          type: object
          properties:
            USER_DECISION:
              $ref: '#/components/schemas/UserDecisionState'
        old:
          type: object
          properties:
            USER_DECISION:
              $ref: '#/components/schemas/UserDecisionState'
UserDecisionState:
```

```
    type: string
    enum: [ NotProcessed, NoViolation, Violation, AdditionalProcessingNeeded ]
  objectExportPropertyChanges:
    type: object
    properties:
      <<: *common
      ENTITY_TYPE:
        type: string
        enum: [ Object ]
      OPERATION:
        type: string
        enum: [ export_object ]
      PROPERTY_CHANGES:
        type: object
        properties:
          new:
            type: object
            properties:
              PARAMS:
                type: object
                properties:
                  QUERY_ID:
                    type: integer
                    nullable: true
                  DISPLAY_NAME:
                    type: string
                  COMMENT:
                    type: string
                  FILTER:
                    anyOf:
                      - type: object
                      - type: array
                  SORT:
                    type: object
                  IS_ONE_REPORT:
                    $ref: '#/components/schemas/BooleanAsInteger'
                  ONE_LOAD_REPORT:
                    $ref: '#/components/schemas/BooleanAsInteger'
                  FORMAT:
                    type: string
                    enum: [ simple, full ]
                  TYPE:
                    type: object
                    properties:
                      one_report:
                        type: string
                        enum: [ docx, xls, xlsx, pdf ]
                      several_report:
                        type: string
                        enum: [ docx, pdf ]
                  IS_SEVERAL_REPORT:
                    $ref: '#/components/schemas/BooleanAsInteger'
                  SEVERAL_LOAD_REPORT:
                    $ref: '#/components/schemas/BooleanAsInteger'
                  LOAD_ATTACHMENT:
                    $ref: '#/components/schemas/BooleanAsInteger'
                  KEEP_HIERARCHY:
                    $ref: '#/components/schemas/BooleanAsInteger'
```

```
                    LOAD_SNIPPET:
                      $ref: '#/components/schemas/BooleanAsInteger'
                    LOAD_EML:
                      $ref: '#/components/schemas/BooleanAsInteger'
                    LOAD_DEBUG_OBJECT:
                      $ref: '#/components/schemas/BooleanAsInteger'
                    SCOPE:
                      oneOf:
                        - type: string
                          enum: [ all ]
                        - type: array
                          items:
                            type: integer
                    GROUPING:
                      type: array
                      items:
                        type: string
                        enum: [CaptureDate, Computer, Object, ObjectType, Person]
                    IS_REPORT_ARCHIVE:
                      $ref: '#/components/schemas/BooleanAsInteger'
    BooleanAsStringOrInteger:
      $ref: 'common.yaml#/components/schemas/BooleanAsStringOrInteger'
    BooleanAsInteger:
      $ref: 'common.yaml#/components/schemas/BooleanAsInteger'
    BooleanAsString:
      $ref: 'common.yaml#/components/schemas/BooleanAsString'
```

### Пример:

**Запрос**

```
curl -X GET "https://qa-2944.infowatch.ru/xapi/audit?sort[CHANGE_DATE]=asc&filter[ENTITY_TYPE]
[]=Adlibitum&filter[ENTITY_TYPE][]=Audit&filter[ENTITY_TYPE][]=Config&filter[ENTITY_TYPE]
[]=Perimeter&filter[ENTITY_TYPE][]=Policy&start=0&limit=5" -H "accept: application/json" -H "X-Enable-
OpenAPI: 1"
```

**Ответ**


```
{
  "data": [
    {
      "AUDIT_LOG_ID": 0,
      "USER_ID": 0,
      "CHANGER_NAME": "string",
      "CHANGE_DATE": "2020-05-14 13:53:52.926560",
      "OPERATION": "run",
      "ENTITY_TYPE": "Adlibitum",
      "ENTITY_ID": "DBAF4F834F7647CBB297BC9DD17B77B100000000",
      "ENTITY_DISPLAY_NAME": "Some name",
      "PROPERTY_CHANGES": {}
    },
    {
      "AUDIT_LOG_ID": 0,
```

```
    "USER_ID": 0,
    "CHANGER_NAME": "string",
    "CHANGE_DATE": "2020-05-14 13:53:52.926560",
    "OPERATION": "login",
    "ENTITY_TYPE": "User",
    "ENTITY_ID": "DBAF4F834F7647CBB297BC9DD17B77B100000000",
    "ENTITY_DISPLAY_NAME": "Some name",
    "PROPERTY_CHANGES": {
      "request": {
        "hostname": "string",
        "ip": "string",
        "result": "login_failure",
        "login": "string"
      }
    }
  },
  {
    "AUDIT_LOG_ID": 0,
    "USER_ID": 0,
    "CHANGER_NAME": "string",
    "CHANGE_DATE": "2020-05-14 13:53:52.926560",
    "OPERATION": "run",
    "ENTITY_TYPE": "Policy",
    "ENTITY_ID": "DBAF4F834F7647CBB297BC9DD17B77B100000000",
    "ENTITY_DISPLAY_NAME": "Some name",
    "PROPERTY_CHANGES": {
      "old": {
        "DISPLAY_NAME": "string",
        "NOTE": "string",
        "STATUS": 0,
        "START_DATE": "string",
        "END_DATE": "string",
        "DATA": {
          "ITEMS": [
            {
              "TYPE": "catalog",
              "ID": "string",
              "NAME": "string"
            },
            {
              "TYPE": "fileformat",
              "ID": "string",
              "NAME": "string",
              "MIME_TYPE": "string",
              "ENCRYPTED": 0,
              "MERGED": 0,
              "MAX": 0,
              "MIN": 0,
              "MAX_TYPE": 0,
              "MIN_TYPE": 0
            }
          ]
        }
      },
      "new": {
        "DISPLAY_NAME": "string",
        "NOTE": "string",
        "STATUS": 0,
```

```
          "START_DATE": "string",
          "END_DATE": "string",
          "DATA": {
            "ITEMS": [
              {
                "TYPE": "catalog",
                "ID": "string",
                "NAME": "string"
              },
              {
                "TYPE": "fileformat",
                "ID": "string",
                "NAME": "string",
                "MIME_TYPE": "string",
                "ENCRYPTED": 0,
                "MERGED": 0,
                "MAX": 0,
                "MIN": 0,
                "MAX_TYPE": 0,
                "MIN_TYPE": 0
              }
            ]
          }
        },
        "rule": {
          "ENTITY_TYPE": "PolicyRule",
          "ENTITY_ID": "string",
          "ENTITY_DISPLAY_NAME": "string"
        }
      }
    }
  ],
  "meta": {
    "totalCount": 0,
    "start": 0,
    "limit": 0
  }
}
```


## Получение организационной структуры

Получение информации по группам

Получение списка групп

**Описание**: Список групп

**Метод**: `GET`

**Ресурс**: `group`

**Параметры**:

- `filter` — список фильтрации:
  - `change_date[from]` — от даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[to]`)

    - `change_date[to]` — до даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[from]`)
    - `create_date[from]` — от даты создания в формате UNIX-timestamp (можно использовать отдельно от `create_date[to]`)
    - `create_date[to]` — до даты создания в формате UNIX-timestamp (можно использовать отдельно от `create_date[from]`
    - `is_deleted` — флаг 1 или 0. Если параметр указан, то будут выдавать сущности с указанным значением
    - `disabled` — флаг 1 или 0, признак активности. Если выставлен, то сущность неактивна (признак берется из LDAP)
    - `contact_type[]` — фильтрация по типу контакта (можно передать несколько, например: `/xapi/group?filter[contact_type][]=webaccount&filter[contact_type][]=icq`)
    - `contact_value[]` — фильтрация по значению контакта (можно передавать несколько, например: `/xapi/group?filter[contact_value][]=user@ad&filter[contact_value][]=login@example.com`)
    - `parent_group_id[]` — фильтрация по группам (можно передать несколько, например: `/xapi/group?filter[parent_group_id][]=FCE1409680E5D6469E1F7998266CE9E9&filter[parent_group_id][]=918462B6DC2C954BAAF8706F7DC53F14)`
- `with[]` — список дополнительных сущностей, которые должны быть добавлены к объекту:
    - `contacts` — контакты группы
    - `children` — подчиненные группы
- `sort` — параметр для сортировки
    - `change_date` — сортировать по дате изменения `asc` или `desc` (например: `/xapi/group?sort[change_date]=asc`) ⚠️ может замедлить выдачу

- `start` — с какой позиции начать отдавать элементы, по-умолчанию 0
- `limit` — сколько элементов отдавать, по-умолчанию 100, не может быть больше 1000

**Ответ**: Список персон, описанный следующей JSON-Schema:

**JSON схема отдачи**

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "required": [
       "data",
       "meta"
   ],
   "properties": {
       "data": {
           "description": "Массив групп",
           "type": "array",
           "items": {
               "description": "Группа",
               "type": "object",
               "required": [
                   "GROUP_ID",
                   "CREATE_DATE",
```

```
                    "CHANGE_DATE",
                    "DISPLAY_NAME",
                    "DISTINGUISHEDNAME",
                    "GROUP_TYPE",
                    "IS_VISIBLE",
                    "IS_DELETED",
                    "childrenCount"
                ],
                "properties": {
                    "GROUP_ID": {
                        "description": "Уникальный идентификатор группы",
                        "type": "string"
                    },
                    "CREATE_DATE": {
                        "description": "Дата создания записи",
                        "type": "string"
                    },
                    "CHANGE_DATE": {
                        "description": "Дата изменения записи",
                        "type": "string"
                    },
                    "DISPLAY_NAME": {
                        "description": "Название группы",
                        "type": "string"
                    },
                    "DISTINGUISHEDNAME": {
                        "description": "Полное имя",
                        "type": "string"
                    },
                    "GROUP_TYPE": {
                        "description": "Тип группы (tmRoot, tmGroup, adRoot, adGroup,
adContainer, adDomain, adOU from LDAP objectclass)",
                        "type": "string"
                    },
                    "IS_VISIBLE": {
                        "description": "Видимость группы",
                        "type": "integer"
                    },
                    "IS_DELETED": {
                        "description": "Удалена ли группа из TM",
                        "type": "integer"
                    },
                    "childrenCount": {
                        "description": "Количество детей в группе",
                        "type": "integer"
                    },
                    "contacts": {
                        "description": "Массив контактов",
                        "type": "array",
                        "items": {
                            "description": "Контакт",
                            "type": "object",
                            "required": [
```

```
                    "CONTACT_ID",
                    "CREATE_DATE",
                    "CHANGE_DATE",
                    "CONTACT_TYPE",
                    "VALUE",
                    "IS_PERSONAL",
                    "IS_PRIMARY",
                    "SOURCE"
                ],
                "properties": {
                    "CONTACT_ID": {
                        "description": "Уникальный идентификатор объекта",
                        "type": "string"
                    },
                    "CREATE_DATE": {
                        "description": "Дата создания",
                        "type": "string"
                    },
                    "CHANGE_DATE": {
                        "description": "Дата изменения",
                        "type": "string"
                    },
                    "CONTACT_TYPE": {
                        "description": "Тип",
                        "type": "string"
                    },
                    "VALUE": {
                        "description": "Значение",
                        "type": "string"
                    },
                    "IS_PERSONAL": {
                        "description": "Принадлежность (Рабочий, Личный)",
                        "type": "integer"
                    },
                    "IS_PRIMARY": {
                        "description": "Признак основной",
                        "type": "integer"
                    },
                    "SOURCE": {
                        "description": "Тип",
                        "type": "string"
                    }
                }
            }
        },
        "children": {
            "description": "Массив групп принадлежащих текущей группе",
            "type": "array",
            "items": {
                "description": "Группа",
                "type": "object",
                "properties": {
                    "GROUP_ID": {
```

```
                                    "description": "Уникальный идентификатор группы",
                                    "type": "string"
                                },
                                "PARENT_GROUP_ID": {
                                    "description": "Уникальный идентификатор группы
родителя",
                                    "type": "string"
                                },
                                "RELATION_TYPE": {
                                    "description": "Тип связи: 0 - tm, 1 - member, 2 -
distinguishedname",
                                    "type": "integer"
                                }
                            }
                        }
                    }
                }
            },
            "meta": {
                "description": "Дополнительные данные",
                "type": "object",
                "required": [
                    "totalCount",
                    "start",
                    "limit"
                ],
                "properties": {
                    "totalCount": {
                        "type": "integer",
                        "description": "Общее количество"
                    },
                    "start": {
                        "type": "integer",
                        "description": "С какой позиции началось отдаваться"
                    },
                    "limit": {
                        "type": "integer",
                        "description": "Сколько всего отдалось"
                    }
                }
            }
        }
    }
```

**Пример**:

**Запрос**

```
/xapi/group?filter[change_date][from]=1&filter[change_date][to]=2&with[]=contacts&with[
]=children&limit=10&sort[change_date]=asc
```

Получение списка с типами контактов группы

**Описание** : Список всех возможных типов контактов группы

**Метод**: `GET`

**Ресурс**: group `/contact_type`

- `start` — с какой позиции начать отдавать элементы, по-умолчанию 0
- `limit` — сколько элементов отдавать, по-умолчанию 100, не может быть больше 1000

**Пример**:

**Запрос**

```
GET /xapi/group/contact_type?start=0&limit=10
```

Получение статистики по группам

**Описание**: Статистика по группам

**Метод**: `GET`

**Ресурс**: group `/stat`

**Параметры**:

- `filter` — список фильтрации:
  - `change_date[from]` — от даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[to]` )
  - `change_date[to]` — до даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[from]` )

**Ответ**:

**JSON схема отдачи**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Статистика",
    "type": "object",
    "properties": {
        "data": {
            "description": "Не используется",
            "type": "array",
            "items": {}
        },
        "meta": {
            "description": "Статистика",
            "type": "object",
            "properties": {
                "CHANGE_DATE": {
                    "description": "Дата изменения",
                    "type": "object",
                    "properties": {
                        "from": {
                            "description": "Самая ранняя дата изменения",
                            "type": "string"
```

```
                        },
                        "to": {
                            "description": "Самая поздняя дата изменения",
                            "type": "string"
                        }
                    }
                },
                "totalCount": {
                    "description": "Общее количество элементов",
                    "type": "integer"
                }
            }
        }
    }
}
```

**Пример**:

```
GET /xapi/group/stat?filter[CAPTURE_DATE][to]=1494951762&filter[CAPTURE_DATE][from]=14
94951000
```

**Ответ**

```
{
  "data": [],
  "meta": {
    "CHANGE_DATE": {
      "from": "2017-03-24 10:40:03",
      "to": "2017-05-24 12:10:22"
    },
    "totalCount": 539693
  }
}
```

Получение информации по персоне

Получение изображений множества персон

**Метод**: POST

**Ресурс**: `person/images`

**Параметры** (передаются в виде JSON):

- `response_type` — тип ответа:
  - `chunked` — используется `Transfer-Encoding: chunked`, где каждое изображение отдаётся в своём блоке и в порядке, переданном в теле запроса, если изображения нет, то вместо изображения передаётся null символ "\0"
  - `multipart/mixed` — используется формат `multipart/mixed` rfc tech-ms, он не входит в стандарт HTTP, но используется в электронных письмах. Поэтому реализовать его не составляет труда. Так же он очень похож на `multipart/form-data`. Каждое изображение отдаётся в своём блоке и помечено отдельно

заголовком X-Person-ID, к какой персоне оно принадлежит. Если изображения нет, то оно либо не передаётся, либо тело этого изображения отсутствует

- `person_id` — массив ID персон

**Примеры**:

**`chunked`** :

**Запрос**

```
POST /xapi/person/images
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
(пустая строка)
{"response_type": "chunked", "person_id": ["DEF1CC1FA015CA428D5DE3CD5B804B69", "E277B6
24BC988C4C96590A8435F634ED"]}
```

**Ответ**

```
HTTP/1.1 200 OK
Content-Type: image/png
Transfer-Encoding: chunked
(пустая строка)
1
\0 (символ отсутствия изображения для персоны DEF1CC1FA015CA428D5DE3CD5B804B69)
48AC
(содержимое изображения для персоны E277B624BC988C4C96590A8435F634ED)
0
```

**`multipart/mixed`** :

**Запрос**

```
POST /xapi/person/images
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
(пустая строка)
{"response_type": "multipart/mixed", "person_id": ["DEF1CC1FA015CA428D5DE3CD5B804B69",
 "E277B624BC988C4C96590A8435F634ED"]}
```

**Ответ**

```
HTTP/1.1 200 OK
Content-Type: multipart/mixed; boundary=Asrf456BGe4h
Content-Length: (суммарный объём, включая дочерние заголовки, может отсутствовать!)
(пустая строка)
(отсутствующая преамбула)
--Asrf456BGe4h
Content-Type: application/x-empty
Content-Disposition: attachment; filename="DEF1CC1FA015CA428D5DE3CD5B804B69"
```

```
X-Person-ID: DEF1CC1FA015CA428D5DE3CD5B804B69
(пустая строка и после нулевое содержимое)
--Asrf456BGe4h
Content-Disposition: attachment; filename="E277B624BC988C4C96590A8435F634ED.jpg"
Content-Type: image/jpeg
X-Person-ID: E277B624BC988C4C96590A8435F634ED
(пустая строка)
(двоичное содержимое второй персоны E277B624BC988C4C96590A8435F634ED)
--Asrf456BGe4h--
(отсутствующий эпилог - пустая строка)
```

Получение изображения персоны

**Метод**: `GET`

**Ресурс**: `person/image/{person_id}`

**Ответ**: Изображение пользователя

Получение списка персон

**Описание**: Список персон

**Метод**: `GET`

**Ресурс**: `person`

**Параметры**:

- `filter` — список фильтрации:
  - `change_date[from]` — от даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[to]`)
  - `change_date[to]` — до даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[from]`)
  - `create_date[from]` — от даты создания в формате UNIX-timestamp (можно использовать отдельно от `create_date[to]`)
  - `create_date[to]` — до даты создания в формате UNIX-timestamp (можно использовать отдельно от `create_date[from]`
  - is_deleted — флаг 1 или 0. Если параметр указан, то будут выдавать сущности с указанным значением
  - `disabled` — флаг 1 или 0, признак активности. Если выставлен, то сущность неактивна (признак берется из LDAP)
  - `contact_type[]` — фильтрация по типу контакта (можно передать несколько, например: `/xapi/person?filter[contact_type][]=webaccount&filter[contact_type][]=icq`)
  - `contact_value[]` — фильтрация по значению контакта (можно передавать несколько, например: `/xapi/person?filter[contact_value ][]=user@ad&filter[contact_value ][]=login@example.com`)
  - `group_id[]` — фильтрация по группам (можно передать несколько, например: `/xapi/person?filter[group_id][]=webaccount&filter[group_id][]=icq)`
- `with[]` — список дополнительных сущностей, которые должны быть добавлены к объекту:
  - `contacts` — контакты персоны
  - `p2g` — связь персоны с группами
  - `status` — статусы персоны

- `sort` — параметр для сортировки
  - `change_date` — сортировать по дате изменения `asc` или `desc` (например: `/xapi/person?sort[change_date]=asc` ) ⚠️ может замедлить выдачу

- `start` — с какой позиции начать отдавать элементы, по-умолчанию 0
- `limit` — сколько элементов отдавать, по-умолчанию 100, не может быть больше 1000

**Ответ**: Список персон, описанный следующей JSON-Schema:

**JSON схема отдачи списка персон**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "object",
    "required": [
        "data",
        "meta"
    ],
    "properties": {
        "data": {
            "description": "Массив персоны",
            "type": "array",
            "items": {
                "description": "Персона",
                "type": "object",
                "required": [
                    "PERSON_ID",
                    "CREATE_DATE",
                    "CHANGE_DATE",
                    "DISTINGUISHEDNAME",
                    "DISPLAY_NAME",
                    "GIVENNAME",
                    "SN",
                    "DISABLED",
                    "IS_EMPLOYEE",
                    "IS_DELETED"
                ],
                "properties": {
                    "PERSON_ID": {
                        "description": "Уникальный идентификатор объекта",
                        "type": "string"
                    },
                    "CREATE_DATE": {
                        "description": "Дата создания",
                        "type": "string"
                    },
                    "CHANGE_DATE": {
                        "description": "Дата последнего изменения",
                        "type": "string"
                    },
                    "DISTINGUISHEDNAME": {
                        "description": "Полное имя",
```

```
            "type": "string"
        },
        "DISPLAY_NAME": {
            "description": "Имя и фамилия",
            "type": "string"
        },
        "GIVENNAME": {
            "description": "Имя",
            "type": "string"
        },
        "SN": {
            "description": "Фамилия",
            "type": "string"
        },
        "DISABLED": {
            "description": "Состояние персоны",
            "type": "integer"
        },
        "IS_EMPLOYEE": {
            "description": "Является ли сотрудником компании",
            "type": "integer"
        },
        "IS_DELETED": {
            "description": "Удалена ли персона из ТМ",
            "type": "integer"
        },
        "contacts": {
            "description": "Массив контактов",
            "type": "array",
            "items": {
                "description": "Контакт",
                "type": "object",
                "required": [
                    "CONTACT_ID",
                    "CREATE_DATE",
                    "CHANGE_DATE",
                    "CONTACT_TYPE",
                    "VALUE",
                    "IS_PERSONAL",
                    "IS_PRIMARY",
                    "SOURCE"
                ],
                "properties": {
                    "CONTACT_ID": {
                        "description": "Уникальный идентификатор объекта",
                        "type": "string"
                    },
                    "CREATE_DATE": {
                        "description": "Дата создания",
                        "type": "string"
                    },
                    "CHANGE_DATE": {
                        "description": "Дата изменения",
```

```
                                    "type": "string"
                                },
                                "CONTACT_TYPE": {
                                    "description": "Тип",
                                    "type": "string"
                                },
                                "VALUE": {
                                    "description": "Значение",
                                    "type": "string"
                                },
                                "IS_PERSONAL": {
                                    "description": "Принадлежность (Рабочий, Личный)",
                                    "type": "integer"
                                },
                                "IS_PRIMARY": {
                                    "description": "Признак основной",
                                    "type": "integer"
                                },
                                "SOURCE": {
                                    "description": "Тип",
                                    "type": "string"
                                }
                            }
                        }
                    },
                    "p2g": {
                        "description": "Массив связи с группами",
                        "type": "array",
                        "items": {
                            "description": "Связь с группой",
                            "type": "object",
                            "required": [
                                "PERSON_ID",
                                "PARENT_GROUP_ID",
                                "RELATION_TYPE"
                            ],
                            "properties": {
                                "PERSON_ID": {
                                    "description": "Уникальный идентификатор персоны",
                                    "type": "string"
                                },
                                "PARENT_GROUP_ID": {
                                    "description": "Уникальный идентификатор группы",
                                    "type": "string"
                                },
                                "RELATION_TYPE": {
                                    "description": "Тип связи: 0 - tm, 1 - member, 2 -
distinguishedname, 3 - primarygroupsid",
                                    "type": "integer"
                                }
                            }
                        }
                    },
```

```
                    "status": {
                        "description": "Массив статусов",
                        "type": "array",
                        "items": {
                            "description": "Статус персоны",
                            "type": "object",
                            "required": [
                                "IDENTITY_STATUS_ID",
                                "CREATE_DATE",
                                "CHANGE_DATE",
                                "ASSIGNMENT_DATE",
                                "DISPLAY_NAME",
                                "COLOR",
                                "EDITABLE"
                            ],
                            "properties": {
                                "IDENTITY_STATUS_ID": {
                                    "description": "Уникальный идентификатор статуса",
                                    "type": "string"
                                },
                                "CREATE_DATE": {
                                    "description": "Дата создания статуса",
                                    "type": "string"
                                },
                                "CHANGE_DATE": {
                                    "description": "Дата изменения статуса",
                                    "type": "string"
                                },
                                "ASSIGNMENT_DATE": {
                                    "description": "Дата проставления статуса персоне",
                                    "type": "string"
                                },
                                "DISPLAY_NAME": {
                                    "description": "Название статуса",
                                    "type": "string"
                                },
                                "COLOR": {
                                    "description": "Цвет статуса (например #ff0000)",
                                    "type": "string"
                                },
                                "EDITABLE": {
                                    "description": "Признак, что статус не является
системным",
                                    "type": "integer"
                                }
                            }
                        }
                    }
                }
            }
        },
        "meta": {
            "description": "Дополнительные данные",
```

```
            "type": "object",
            "required": [
                "totalCount",
                "start",
                "limit"
            ],
            "properties": {
                "totalCount": {
                    "type": "integer",
                    "description": "Общее количество"
                },
                "start": {
                    "type": "integer",
                    "description": "С какой позиции началось отдаваться"
                },
                "limit": {
                    "type": "integer",
                    "description": "Сколько всего отдалось"
                }
            }
        }
    }
}
```

**Пример**:

**Запрос**

```
GET /xapi/person?start=0&limit=10&filter[change_date][from]=0&filter[change_date][to]=1&
with[]=contacts
```

**Ответ**

```
{
    "data": [{
        "PERSON_ID": "532ECB81F75DDC46BE023478C2E86BD9",
        "WHENCHANGED": "20151229230303.0Z",
        "WHENCREATED": "20151229230303.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
        "DISTINGUISHEDNAME": "CN=Annett Rist,OU=Testou,DC=trafmon,DC=iw",
        "DISPLAY_NAME": "Annett Rist",
        "GIVENNAME": "Annett",
        "SN": "Rist",
        "OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156702",
        "SAMACCOUNTNAME": "AC428097",
        "NETBIOSNAME": "TRAFMON",
        "DNSROOT": "trafmon.iw",
        "USERPRINCIPALNAME": "AC428097@acme.com",
        "MAIL": "Annett.Rist@acme.com",
        "TELEPHONENUMBER": "+49-30-626763",
        "SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
        "CREATE_DATE": "2017-03-07 08:54:56.401138",
```

```
"CHANGE_DATE": "2017-03-10 08:40:35.741001",
"SOURCE": "ad",
"HAS_TM_THUMBNAILPHOTO": false,
"HAS_THUMBNAILPHOTO": false,
"TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
"contacts": [{
    "CONTACT_ID": "4A211BA3896A7620E0530100007F388100000000",
    "IDENTITY_ID": "532ECB81F75DDC46BE023478C2E86BD9",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac428097@acme.com",
    "IS_PRIMARY": 0,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.402060",
    "CHANGE_DATE": "2017-03-07 08:54:56.402060",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA389687620E0530100007F388100000000",
    "IDENTITY_ID": "532ECB81F75DDC46BE023478C2E86BD9",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac428097@trafmon",
    "IS_PRIMARY": 1,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.401926",
    "CHANGE_DATE": "2017-03-07 08:54:56.401926",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA389697620E0530100007F388100000000",
    "IDENTITY_ID": "532ECB81F75DDC46BE023478C2E86BD9",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac428097@trafmon.iw",
    "IS_PRIMARY": 0,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.401998",
    "CHANGE_DATE": "2017-03-07 08:54:56.401998",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA389667620E0530100007F388100000000",
    "IDENTITY_ID": "532ECB81F75DDC46BE023478C2E86BD9",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "email",
    "VALUE": "annett.rist@acme.com",
    "IS_PRIMARY": 1,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.401457",
    "CHANGE_DATE": "2017-03-07 08:54:56.401457",
    "SOURCE": "ad"
```

```
        }, {
            "CONTACT_ID": "4A211BA389677620E0530100007F388100000000",
            "IDENTITY_ID": "532ECB81F75DDC46BE023478C2E86BD9",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "phone",
            "VALUE": "+49-30-626763",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.401670",
            "CHANGE_DATE": "2017-03-07 08:54:56.401670",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA3896B7620E0530100007F388100000000",
            "IDENTITY_ID": "532ECB81F75DDC46BE023478C2E86BD9",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "sid",
            "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156702",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.402130",
            "CHANGE_DATE": "2017-03-07 08:54:56.402130",
            "SOURCE": "ad"
        }],
        "status": []
    }, {
        "PERSON_ID": "92FB7D1EC79A9947938BE582D355B109",
        "WHENCHANGED": "20151229230304.0Z",
        "WHENCREATED": "20151229230303.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
        "DISTINGUISHEDNAME": "CN=Lieselene SchÃ¶nemann,OU=Testou,DC=trafmon,DC=iw",
        "DISPLAY_NAME": "Lieselene SchÃ¶nemann",
        "GIVENNAME": "Lieselene",
        "SN": "SchÃ¶nemann",
        "OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156706",
        "SAMACCOUNTNAME": "AC727058",
        "NETBIOSNAME": "TRAFMON",
        "DNSROOT": "trafmon.iw",
        "USERPRINCIPALNAME": "AC727058@acme.com",
        "MAIL": "Lieselene.SchÃ¶nemann@acme.com",
        "TELEPHONENUMBER": "+49-2183-398305",
        "SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
        "CREATE_DATE": "2017-03-07 08:54:56.402195",
        "CHANGE_DATE": "2017-03-10 08:40:35.741198",
        "SOURCE": "ad",
        "HAS_TM_THUMBNAILPHOTO": false,
        "HAS_THUMBNAILPHOTO": false,
        "TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
        "contacts": [{
            "CONTACT_ID": "4A211BA389707620E0530100007F388100000000",
            "IDENTITY_ID": "92FB7D1EC79A9947938BE582D355B109",
```

```
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac727058@acme.com",
        "IS_PRIMARY": 0,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.403048",
        "CHANGE_DATE": "2017-03-07 08:54:56.403048",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA3896E7620E0530100007F388100000000",
        "IDENTITY_ID": "92FB7D1EC79A9947938BE582D355B109",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac727058@trafmon",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.402920",
        "CHANGE_DATE": "2017-03-07 08:54:56.402920",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA3896F7620E0530100007F388100000000",
        "IDENTITY_ID": "92FB7D1EC79A9947938BE582D355B109",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac727058@trafmon.iw",
        "IS_PRIMARY": 0,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.402984",
        "CHANGE_DATE": "2017-03-07 08:54:56.402984",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA3896C7620E0530100007F388100000000",
        "IDENTITY_ID": "92FB7D1EC79A9947938BE582D355B109",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "email",
        "VALUE": "lieselene.schÃ¶nemann@acme.com",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.402517",
        "CHANGE_DATE": "2017-03-07 08:54:56.402517",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA3896D7620E0530100007F388100000000",
        "IDENTITY_ID": "92FB7D1EC79A9947938BE582D355B109",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "phone",
        "VALUE": "+49-2183-398305",
        "IS_PRIMARY": 1,
```

```
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.402731",
            "CHANGE_DATE": "2017-03-07 08:54:56.402731",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA389717620E0530100007F388100000000",
            "IDENTITY_ID": "92FB7D1EC79A9947938BE582D355B109",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "sid",
            "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156706",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.403117",
            "CHANGE_DATE": "2017-03-07 08:54:56.403117",
            "SOURCE": "ad"
        }],
        "status": []
    }, {
        "PERSON_ID": "F0A3298727D7E0498106AE678CC1F5F8",
        "WHENCHANGED": "20151229230304.0Z",
        "WHENCREATED": "20151229230304.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
        "DISTINGUISHEDNAME": "CN=Kasimir Eggers,OU=Testou,DC=trafmon,DC=iw",
        "DISPLAY_NAME": "Kasimir Eggers",
        "GIVENNAME": "Kasimir",
        "SN": "Eggers",
        "OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156710",
        "SAMACCOUNTNAME": "AC217045",
        "NETBIOSNAME": "TRAFMON",
        "DNSROOT": "trafmon.iw",
        "USERPRINCIPALNAME": "AC217045@acme.com",
        "MAIL": "Kasimir.Eggers@acme.com",
        "TELEPHONENUMBER": "+49-7191-389863",
        "SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
        "CREATE_DATE": "2017-03-07 08:54:56.403185",
        "CHANGE_DATE": "2017-03-10 08:40:35.741388",
        "SOURCE": "ad",
        "HAS_TM_THUMBNAILPHOTO": false,
        "HAS_THUMBNAILPHOTO": false,
        "TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
        "contacts": [{
            "CONTACT_ID": "4A211BA389767620E0530100007F388100000000",
            "IDENTITY_ID": "F0A3298727D7E0498106AE678CC1F5F8",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "auth",
            "VALUE": "ac217045@acme.com",
            "IS_PRIMARY": 0,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.404114",
            "CHANGE_DATE": "2017-03-07 08:54:56.404114",
```

```
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389747620E0530100007F388100000000",
        "IDENTITY_ID": "F0A3298727D7E0498106AE678CC1F5F8",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac217045@trafmon",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.403984",
        "CHANGE_DATE": "2017-03-07 08:54:56.403984",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389757620E0530100007F388100000000",
        "IDENTITY_ID": "F0A3298727D7E0498106AE678CC1F5F8",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac217045@trafmon.iw",
        "IS_PRIMARY": 0,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.404055",
        "CHANGE_DATE": "2017-03-07 08:54:56.404055",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389727620E0530100007F388100000000",
        "IDENTITY_ID": "F0A3298727D7E0498106AE678CC1F5F8",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "email",
        "VALUE": "kasimir.eggers@acme.com",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.403507",
        "CHANGE_DATE": "2017-03-07 08:54:56.403507",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389737620E0530100007F388100000000",
        "IDENTITY_ID": "F0A3298727D7E0498106AE678CC1F5F8",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "phone",
        "VALUE": "+49-7191-389863",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.403722",
        "CHANGE_DATE": "2017-03-07 08:54:56.403722",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389777620E0530100007F388100000000",
        "IDENTITY_ID": "F0A3298727D7E0498106AE678CC1F5F8",
        "IDENTITY_TYPE": "person",
```

```
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "sid",
            "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156710",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.404184",
            "CHANGE_DATE": "2017-03-07 08:54:56.404184",
            "SOURCE": "ad"
        }],
        "status": []
    }, {
        "PERSON_ID": "52BDB45E49090F4D986899E29FEB35CB",
        "WHENCHANGED": "20151229230304.0Z",
        "WHENCREATED": "20151229230304.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
        "DISTINGUISHEDNAME": "CN=Leoni Huck,OU=Testou,DC=trafmon,DC=iw",
        "DISPLAY_NAME": "Leoni Huck",
        "GIVENNAME": "Leoni",
        "SN": "Huck",
        "OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156709",
        "SAMACCOUNTNAME": "AC716847",
        "NETBIOSNAME": "TRAFMON",
        "DNSROOT": "trafmon.iw",
        "USERPRINCIPALNAME": "AC716847@acme.com",
        "MAIL": "Leoni.Huck@acme.com",
        "TELEPHONENUMBER": "+49-9184-802313",
        "SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
        "CREATE_DATE": "2017-03-07 08:54:56.404249",
        "CHANGE_DATE": "2017-03-10 08:40:35.741577",
        "SOURCE": "ad",
        "HAS_TM_THUMBNAILPHOTO": false,
        "HAS_THUMBNAILPHOTO": false,
        "TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
        "contacts": [{
            "CONTACT_ID": "4A211BA3897C7620E0530100007F388100000000",
            "IDENTITY_ID": "52BDB45E49090F4D986899E29FEB35CB",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "auth",
            "VALUE": "ac716847@acme.com",
            "IS_PRIMARY": 0,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.405104",
            "CHANGE_DATE": "2017-03-07 08:54:56.405104",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA3897A7620E0530100007F388100000000",
            "IDENTITY_ID": "52BDB45E49090F4D986899E29FEB35CB",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "auth",
            "VALUE": "ac716847@trafmon",
```

```
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.404978",
        "CHANGE_DATE": "2017-03-07 08:54:56.404978",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA3897B7620E0530100007F388100000000",
        "IDENTITY_ID": "52BDB45E49090F4D986899E29FEB35CB",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac716847@trafmon.iw",
        "IS_PRIMARY": 0,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.405040",
        "CHANGE_DATE": "2017-03-07 08:54:56.405040",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389787620E0530100007F388100000000",
        "IDENTITY_ID": "52BDB45E49090F4D986899E29FEB35CB",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "email",
        "VALUE": "leoni.huck@acme.com",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.404575",
        "CHANGE_DATE": "2017-03-07 08:54:56.404575",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389797620E0530100007F388100000000",
        "IDENTITY_ID": "52BDB45E49090F4D986899E29FEB35CB",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "phone",
        "VALUE": "+49-9184-802313",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.404789",
        "CHANGE_DATE": "2017-03-07 08:54:56.404789",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA3897D7620E0530100007F388100000000",
        "IDENTITY_ID": "52BDB45E49090F4D986899E29FEB35CB",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "sid",
        "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156709",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.405174",
        "CHANGE_DATE": "2017-03-07 08:54:56.405174",
        "SOURCE": "ad"
```

```
        }],
        "status": []
    }, {
        "PERSON_ID": "BE20920FFD837142AAC09C87A874CCD4",
        "WHENCHANGED": "20151229230304.0Z",
        "WHENCREATED": "20151229230304.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
        "DISTINGUISHEDNAME": "CN=Adelgund Krebs,OU=Testou,DC=trafmon,DC=iw",
        "DISPLAY_NAME": "Adelgund Krebs",
        "GIVENNAME": "Adelgund",
        "SN": "Krebs",
        "OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156708",
        "SAMACCOUNTNAME": "AC944381",
        "NETBIOSNAME": "TRAFMON",
        "DNSROOT": "trafmon.iw",
        "USERPRINCIPALNAME": "AC944381@acme.com",
        "MAIL": "Adelgund.Krebs@acme.com",
        "TELEPHONENUMBER": "+49-6392-145757",
        "SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
        "CREATE_DATE": "2017-03-07 08:54:56.405238",
        "CHANGE_DATE": "2017-03-10 08:40:35.741765",
        "SOURCE": "ad",
        "HAS_TM_THUMBNAILPHOTO": false,
        "HAS_THUMBNAILPHOTO": false,
        "TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
        "contacts": [{
            "CONTACT_ID": "4A211BA389827620E0530100007F388100000000",
            "IDENTITY_ID": "BE20920FFD837142AAC09C87A874CCD4",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "auth",
            "VALUE": "ac944381@acme.com",
            "IS_PRIMARY": 0,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.406146",
            "CHANGE_DATE": "2017-03-07 08:54:56.406146",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA389807620E0530100007F388100000000",
            "IDENTITY_ID": "BE20920FFD837142AAC09C87A874CCD4",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "auth",
            "VALUE": "ac944381@trafmon",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.406026",
            "CHANGE_DATE": "2017-03-07 08:54:56.406026",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA389817620E0530100007F388100000000",
            "IDENTITY_ID": "BE20920FFD837142AAC09C87A874CCD4",
```

```
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "auth",
            "VALUE": "ac944381@trafmon.iw",
            "IS_PRIMARY": 0,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.406089",
            "CHANGE_DATE": "2017-03-07 08:54:56.406089",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA3897E7620E0530100007F388100000000",
            "IDENTITY_ID": "BE20920FFD837142AAC09C87A874CCD4",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "email",
            "VALUE": "adelgund.krebs@acme.com",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.405584",
            "CHANGE_DATE": "2017-03-07 08:54:56.405584",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA3897F7620E0530100007F388100000000",
            "IDENTITY_ID": "BE20920FFD837142AAC09C87A874CCD4",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "phone",
            "VALUE": "+49-6392-145757",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.405836",
            "CHANGE_DATE": "2017-03-07 08:54:56.405836",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA389837620E0530100007F388100000000",
            "IDENTITY_ID": "BE20920FFD837142AAC09C87A874CCD4",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "sid",
            "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156708",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.406214",
            "CHANGE_DATE": "2017-03-07 08:54:56.406214",
            "SOURCE": "ad"
        }],
        "status": []
    }, {
        "PERSON_ID": "54C067BB3B8518489D098154447242DB",
        "WHENCHANGED": "20151229230304.0Z",
        "WHENCREATED": "20151229230304.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
```

```
"DISTINGUISHEDNAME": "CN=Kilian Adolph,OU=Testou,DC=trafmon,DC=iw",
"DISPLAY_NAME": "Kilian Adolph",
"GIVENNAME": "Kilian",
"SN": "Adolph",
"OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156707",
"SAMACCOUNTNAME": "AC598197",
"NETBIOSNAME": "TRAFMON",
"DNSROOT": "trafmon.iw",
"USERPRINCIPALNAME": "AC598197@acme.com",
"MAIL": "Kilian.Adolph@acme.com",
"TELEPHONENUMBER": "+49-30-399513",
"SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
"CREATE_DATE": "2017-03-07 08:54:56.406279",
"CHANGE_DATE": "2017-03-10 08:40:35.741957",
"SOURCE": "ad",
"HAS_TM_THUMBNAILPHOTO": false,
"HAS_THUMBNAILPHOTO": false,
"TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
"contacts": [{
    "CONTACT_ID": "4A211BA389887620E0530100007F388100000000",
    "IDENTITY_ID": "54C067BB3B8518489D098154447242DB",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac598197@acme.com",
    "IS_PRIMARY": 0,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.407140",
    "CHANGE_DATE": "2017-03-07 08:54:56.407140",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA389867620E0530100007F388100000000",
    "IDENTITY_ID": "54C067BB3B8518489D098154447242DB",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac598197@trafmon",
    "IS_PRIMARY": 1,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.407000",
    "CHANGE_DATE": "2017-03-07 08:54:56.407000",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA389877620E0530100007F388100000000",
    "IDENTITY_ID": "54C067BB3B8518489D098154447242DB",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac598197@trafmon.iw",
    "IS_PRIMARY": 0,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.407081",
    "CHANGE_DATE": "2017-03-07 08:54:56.407081",
```

```
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA389847620E0530100007F388100000000",
            "IDENTITY_ID": "54C067BB3B8518489D098154447242DB",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "email",
            "VALUE": "kilian.adolph@acme.com",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.406603",
            "CHANGE_DATE": "2017-03-07 08:54:56.406603",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA389857620E0530100007F388100000000",
            "IDENTITY_ID": "54C067BB3B8518489D098154447242DB",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "phone",
            "VALUE": "+49-30-399513",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.406812",
            "CHANGE_DATE": "2017-03-07 08:54:56.406812",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA389897620E0530100007F388100000000",
            "IDENTITY_ID": "54C067BB3B8518489D098154447242DB",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "sid",
            "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156707",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.407217",
            "CHANGE_DATE": "2017-03-07 08:54:56.407217",
            "SOURCE": "ad"
        }],
        "status": []
    }, {
        "PERSON_ID": "D4B1F21E90098D4880ABAB5C81F53F7C",
        "WHENCHANGED": "20151229230305.0Z",
        "WHENCREATED": "20151229230305.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
        "DISTINGUISHEDNAME": "CN=Lene Escher,OU=Testou,DC=trafmon,DC=iw",
        "DISPLAY_NAME": "Lene Escher",
        "GIVENNAME": "Lene",
        "SN": "Escher",
        "OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156712",
        "SAMACCOUNTNAME": "AC673590",
        "NETBIOSNAME": "TRAFMON",
        "DNSROOT": "trafmon.iw",
```

```
"USERPRINCIPALNAME": "AC673590@acme.com",
"MAIL": "Lene.Escher@acme.com",
"TELEPHONENUMBER": "+49-6131-340459",
"SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
"CREATE_DATE": "2017-03-07 08:54:56.407282",
"CHANGE_DATE": "2017-03-10 08:40:35.742722",
"SOURCE": "ad",
"HAS_TM_THUMBNAILPHOTO": false,
"HAS_THUMBNAILPHOTO": false,
"TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
"contacts": [{
    "CONTACT_ID": "4A211BA3898E7620E0530100007F388100000000",
    "IDENTITY_ID": "D4B1F21E90098D4880ABAB5C81F53F7C",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac673590@acme.com",
    "IS_PRIMARY": 0,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.408129",
    "CHANGE_DATE": "2017-03-07 08:54:56.408129",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA3898C7620E0530100007F388100000000",
    "IDENTITY_ID": "D4B1F21E90098D4880ABAB5C81F53F7C",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac673590@trafmon",
    "IS_PRIMARY": 1,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.408006",
    "CHANGE_DATE": "2017-03-07 08:54:56.408006",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA3898D7620E0530100007F388100000000",
    "IDENTITY_ID": "D4B1F21E90098D4880ABAB5C81F53F7C",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac673590@trafmon.iw",
    "IS_PRIMARY": 0,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.408071",
    "CHANGE_DATE": "2017-03-07 08:54:56.408071",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA3898A7620E0530100007F388100000000",
    "IDENTITY_ID": "D4B1F21E90098D4880ABAB5C81F53F7C",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "email",
    "VALUE": "lene.escher@acme.com",
```

```
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.407607",
            "CHANGE_DATE": "2017-03-07 08:54:56.407607",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA3898B7620E0530100007F388100000000",
            "IDENTITY_ID": "D4B1F21E90098D4880ABAB5C81F53F7C",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "phone",
            "VALUE": "+49-6131-340459",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.407817",
            "CHANGE_DATE": "2017-03-07 08:54:56.407817",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA3898F7620E0530100007F388100000000",
            "IDENTITY_ID": "D4B1F21E90098D4880ABAB5C81F53F7C",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "sid",
            "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156712",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.408198",
            "CHANGE_DATE": "2017-03-07 08:54:56.408198",
            "SOURCE": "ad"
        }],
        "status": []
    }, {
        "PERSON_ID": "7B238377335B7B48AFDC99851D8F4793",
        "WHENCHANGED": "20151229230305.0Z",
        "WHENCREATED": "20151229230305.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
        "DISTINGUISHEDNAME": "CN=Annett Schwanke,OU=Testou,DC=trafmon,DC=iw",
        "DISPLAY_NAME": "Annett Schwanke",
        "GIVENNAME": "Annett",
        "SN": "Schwanke",
        "OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156711",
        "SAMACCOUNTNAME": "AC275412",
        "NETBIOSNAME": "TRAFMON",
        "DNSROOT": "trafmon.iw",
        "USERPRINCIPALNAME": "AC275412@acme.com",
        "MAIL": "Annett.Schwanke@acme.com",
        "TELEPHONENUMBER": "+49-33633-744751",
        "SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
        "CREATE_DATE": "2017-03-07 08:54:56.408263",
        "CHANGE_DATE": "2017-03-10 08:40:35.742148",
        "SOURCE": "ad",
        "HAS_TM_THUMBNAILPHOTO": false,
```

```
"HAS_THUMBNAILPHOTO": false,
"TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
"contacts": [{
    "CONTACT_ID": "4A211BA389947620E0530100007F388100000000",
    "IDENTITY_ID": "7B238377335B7B48AFDC99851D8F4793",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac275412@acme.com",
    "IS_PRIMARY": 0,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.409108",
    "CHANGE_DATE": "2017-03-07 08:54:56.409108",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA389927620E0530100007F388100000000",
    "IDENTITY_ID": "7B238377335B7B48AFDC99851D8F4793",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac275412@trafmon",
    "IS_PRIMARY": 1,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.408985",
    "CHANGE_DATE": "2017-03-07 08:54:56.408985",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA389937620E0530100007F388100000000",
    "IDENTITY_ID": "7B238377335B7B48AFDC99851D8F4793",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "auth",
    "VALUE": "ac275412@trafmon.iw",
    "IS_PRIMARY": 0,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.409051",
    "CHANGE_DATE": "2017-03-07 08:54:56.409051",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA389907620E0530100007F388100000000",
    "IDENTITY_ID": "7B238377335B7B48AFDC99851D8F4793",
    "IDENTITY_TYPE": "person",
    "IDENTITY_SOURCE": "ad",
    "CONTACT_TYPE": "email",
    "VALUE": "annett.schwanke@acme.com",
    "IS_PRIMARY": 1,
    "IS_PERSONAL": 0,
    "CREATE_DATE": "2017-03-07 08:54:56.408589",
    "CHANGE_DATE": "2017-03-07 08:54:56.408589",
    "SOURCE": "ad"
}, {
    "CONTACT_ID": "4A211BA389917620E0530100007F388100000000",
    "IDENTITY_ID": "7B238377335B7B48AFDC99851D8F4793",
```

```
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "phone",
            "VALUE": "+49-33633-744751",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.408799",
            "CHANGE_DATE": "2017-03-07 08:54:56.408799",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA389957620E0530100007F388100000000",
            "IDENTITY_ID": "7B238377335B7B48AFDC99851D8F4793",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "sid",
            "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156711",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.409176",
            "CHANGE_DATE": "2017-03-07 08:54:56.409176",
            "SOURCE": "ad"
        }],
        "status": []
    }, {
        "PERSON_ID": "E277B624BC988C4C96590A8435F634ED",
        "WHENCHANGED": "20151229230305.0Z",
        "WHENCREATED": "20151229230305.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
        "DISTINGUISHEDNAME": "CN=Edgar Genz,OU=Testou,DC=trafmon,DC=iw",
        "DISPLAY_NAME": "Edgar Genz",
        "GIVENNAME": "Edgar",
        "SN": "Genz",
        "OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156714",
        "SAMACCOUNTNAME": "AC938446",
        "NETBIOSNAME": "TRAFMON",
        "DNSROOT": "trafmon.iw",
        "USERPRINCIPALNAME": "AC938446@acme.com",
        "MAIL": "Edgar.Genz@acme.com",
        "TELEPHONENUMBER": "+49-7191-731883",
        "SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
        "CREATE_DATE": "2017-03-07 08:54:56.409247",
        "CHANGE_DATE": "2017-03-10 08:40:35.742335",
        "SOURCE": "ad",
        "HAS_TM_THUMBNAILPHOTO": false,
        "HAS_THUMBNAILPHOTO": false,
        "TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
        "contacts": [{
            "CONTACT_ID": "4A211BA3899A7620E0530100007F388100000000",
            "IDENTITY_ID": "E277B624BC988C4C96590A8435F634ED",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "auth",
```

```
        "VALUE": "ac938446@acme.com",
        "IS_PRIMARY": 0,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.410087",
        "CHANGE_DATE": "2017-03-07 08:54:56.410087",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389987620E0530100007F388100000000",
        "IDENTITY_ID": "E277B624BC988C4C96590A8435F634ED",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac938446@trafmon",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.409967",
        "CHANGE_DATE": "2017-03-07 08:54:56.409967",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389997620E0530100007F388100000000",
        "IDENTITY_ID": "E277B624BC988C4C96590A8435F634ED",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac938446@trafmon.iw",
        "IS_PRIMARY": 0,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.410030",
        "CHANGE_DATE": "2017-03-07 08:54:56.410030",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389967620E0530100007F388100000000",
        "IDENTITY_ID": "E277B624BC988C4C96590A8435F634ED",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "email",
        "VALUE": "edgar.genz@acme.com",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.409572",
        "CHANGE_DATE": "2017-03-07 08:54:56.409572",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389977620E0530100007F388100000000",
        "IDENTITY_ID": "E277B624BC988C4C96590A8435F634ED",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "phone",
        "VALUE": "+49-7191-731883",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.409781",
        "CHANGE_DATE": "2017-03-07 08:54:56.409781",
```

```
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA3899B7620E0530100007F388100000000",
            "IDENTITY_ID": "E277B624BC988C4C96590A8435F634ED",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "sid",
            "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156714",
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.410155",
            "CHANGE_DATE": "2017-03-07 08:54:56.410155",
            "SOURCE": "ad"
        }],
        "status": []
    }, {
        "PERSON_ID": "DEF1CC1FA015CA428D5DE3CD5B804B69",
        "WHENCHANGED": "20151229230305.0Z",
        "WHENCREATED": "20151229230305.0Z",
        "DISABLED": 0,
        "IS_EMPLOYEE": 1,
        "DISTINGUISHEDNAME": "CN=Velten SchÃ¶ning,OU=Testou,DC=trafmon,DC=iw",
        "DISPLAY_NAME": "Velten SchÃ¶ning",
        "GIVENNAME": "Velten",
        "SN": "SchÃ¶ning",
        "OBJECTSID": "S-1-5-21-4236050433-3472386798-155597913-156713",
        "SAMACCOUNTNAME": "AC617874",
        "NETBIOSNAME": "TRAFMON",
        "DNSROOT": "trafmon.iw",
        "USERPRINCIPALNAME": "AC617874@acme.com",
        "MAIL": "Velten.SchÃ¶ning@acme.com",
        "TELEPHONENUMBER": "+49-9184-565860",
        "SERVER_ID": "65E2D37A643561E5E43C7E757BE121096253B4D6",
        "CREATE_DATE": "2017-03-07 08:54:56.410219",
        "CHANGE_DATE": "2017-03-10 08:40:35.742522",
        "SOURCE": "ad",
        "HAS_TM_THUMBNAILPHOTO": false,
        "HAS_THUMBNAILPHOTO": false,
        "TM_PHOTO": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
        "contacts": [{
            "CONTACT_ID": "4A211BA389A07620E0530100007F388100000000",
            "IDENTITY_ID": "DEF1CC1FA015CA428D5DE3CD5B804B69",
            "IDENTITY_TYPE": "person",
            "IDENTITY_SOURCE": "ad",
            "CONTACT_TYPE": "auth",
            "VALUE": "ac617874@acme.com",
            "IS_PRIMARY": 0,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.411056",
            "CHANGE_DATE": "2017-03-07 08:54:56.411056",
            "SOURCE": "ad"
        }, {
            "CONTACT_ID": "4A211BA3899E7620E0530100007F388100000000",
```

```
        "IDENTITY_ID": "DEF1CC1FA015CA428D5DE3CD5B804B69",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac617874@trafmon",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.410937",
        "CHANGE_DATE": "2017-03-07 08:54:56.410937",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA3899F7620E0530100007F388100000000",
        "IDENTITY_ID": "DEF1CC1FA015CA428D5DE3CD5B804B69",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "auth",
        "VALUE": "ac617874@trafmon.iw",
        "IS_PRIMARY": 0,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.411000",
        "CHANGE_DATE": "2017-03-07 08:54:56.411000",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA3899C7620E0530100007F388100000000",
        "IDENTITY_ID": "DEF1CC1FA015CA428D5DE3CD5B804B69",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "email",
        "VALUE": "velten.schÃ¶ning@acme.com",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.410541",
        "CHANGE_DATE": "2017-03-07 08:54:56.410541",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA3899D7620E0530100007F388100000000",
        "IDENTITY_ID": "DEF1CC1FA015CA428D5DE3CD5B804B69",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "phone",
        "VALUE": "+49-9184-565860",
        "IS_PRIMARY": 1,
        "IS_PERSONAL": 0,
        "CREATE_DATE": "2017-03-07 08:54:56.410750",
        "CHANGE_DATE": "2017-03-07 08:54:56.410750",
        "SOURCE": "ad"
    }, {
        "CONTACT_ID": "4A211BA389A17620E0530100007F388100000000",
        "IDENTITY_ID": "DEF1CC1FA015CA428D5DE3CD5B804B69",
        "IDENTITY_TYPE": "person",
        "IDENTITY_SOURCE": "ad",
        "CONTACT_TYPE": "sid",
        "VALUE": "s-1-5-21-4236050433-3472386798-155597913-156713",
```

```
            "IS_PRIMARY": 1,
            "IS_PERSONAL": 0,
            "CREATE_DATE": "2017-03-07 08:54:56.411129",
            "CHANGE_DATE": "2017-03-07 08:54:56.411129",
            "SOURCE": "ad"
        }],
        "status": []
    }],
    "meta": {
        "totalCount": 232525,
        "start": 0,
        "limit": 10
    }
}
```

Получение списка статусов персоны

**Описание** : Список всех возможных статусов персон

**Метод**: `GET`

**Ресурс**: `person/status`

**Параметры**:

- `start` — с какой позиции начать отдавать элементы, по-умолчанию 0
- `limit` — сколько элементов отдавать, по-умолчанию 100, не может быть больше 1000

**Ответ**: Список статусов, описанный следующей JSON-Schema:

**JSON схема отдачи списка статусов**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "object",
    "properties": {
        "data": {
            "description": "Массив статусов",
            "type": "array",
            "items": {
                "description": "Статус персоны",
                "type": "object",
                "required": [
                    "IDENTITY_STATUS_ID",
                    "CREATE_DATE",
                    "CHANGE_DATE",
                    "ASSIGNMENT_DATE",
                    "DISPLAY_NAME",
                    "COLOR",
                    "EDITABLE"
                ],
                "properties": {
                    "IDENTITY_STATUS_ID": {
                        "description": "Уникальный идентификатор статуса",
                        "type": "string"
```

```
                    },
                    "CREATE_DATE": {
                        "description": "Дата создания статуса",
                        "type": "string"
                    },
                    "CHANGE_DATE": {
                        "description": "Дата изменения статуса",
                        "type": "string"
                    },
                    "ASSIGNMENT_DATE": {
                        "description": "Дата проставления статуса персоне",
                        "type": "string"
                    },
                    "DISPLAY_NAME": {
                        "description": "Название статуса",
                        "type": "string"
                    },
                    "COLOR": {
                        "description": "Цвет статуса (например #ff0000)",
                        "type": "string"
                    },
                    "EDITABLE": {
                        "description": "Признак, что статус не является системным",
                        "type": "integer"
                    }
                }
            }
        },
        "meta": {
            "description": "Дополнительные данные",
            "type": "object",
            "required": [
                "totalCount",
                "start",
                "limit"
            ],
            "properties": {
                "totalCount": {
                    "description": "Общее количество",
                    "type": "integer"
                },
                "start": {
                    "description": "С какой позиции началось отдаваться",
                    "type": "integer"
                },
                "limit": {
                    "description": "Сколько всего отдалось",
                    "type": "integer"
                }
            }
        }
    }
}
```

**Пример**:

**Запрос**

```
GET /xapi/person/status?start=0&limit=10
```

Получение списка с типами контактов персоны

**Описание** : Список всех возможных типов контактов персоны

**Метод**: `GET`

**Ресурс**: `person/contact_type`

**Параметры**:

- `start` — с какой позиции начать отдавать элементы, по-умолчанию 0
- `limit` — сколько элементов отдавать, по-умолчанию 100, не может быть больше 1000

**Ответ**: Список типов, описанный следующей JSON-Schema:

**JSON схема отдачи списка контактов**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "object",
    "properties": {
        "data": {
            "description": "Массив типов контактов",
            "type": "array",
            "items": {
                "description": "Тип контакта",
                "type": "object",
                "properties": {
                    "CONTACT_TYPE_ID": {
                        "description": "Уникальный идентификатор типа контактов",
                        "type": "string"
                    },
                    "DISPLAY_NAME": {
                        "description": "Название типа контакта",
                        "type": "string"
                    },
                    "LANGUAGE": {
                        "description": "Язык перевода",
                        "type": "string"
                    },
                    "MNEMO": {
                        "description": "Мнемонический идентификатор (используется в
сущности контактов)",
                        "type": "string"
                    }
                }
            }
        },
        "meta": {
```

```
            "description": "Дополнительные данные",
            "type": "object",
            "required": [
                "totalCount",
                "start",
                "limit"
            ],
            "properties": {
                "totalCount": {
                    "description": "Общее количество",
                    "type": "integer"
                },
                "start": {
                    "description": "С какой позиции началось отдаваться",
                    "type": "integer"
                },
                "limit": {
                    "description": "Сколько всего отдалось",
                    "type": "integer"
                }
            }
        }
    }
}
```

**Пример**:

**Запрос**

```
GET /xapi/person/contact_type?start=0&limit=10
```

Получение статистики по персонам

**Описание**: Статистика по персонам

**Метод**: `GET`

**Ресурс**: `person/stat`

**Параметры**:

- `filter` — список фильтрации:
  - `change_date[from]` — от даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[to]`)
  - `change_date[to]` — до даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[from]`)

**Ответ**:

**JSON схема отдачи**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Статистика",
    "type": "object",
    "properties": {
```

```
        "data": {
            "description": "Не используется",
            "type": "array",
            "items": {}
        },
        "meta": {
            "description": "Статистика",
            "type": "object",
            "properties": {
                "CHANGE_DATE": {
                    "description": "Дата изменения",
                    "type": "object",
                    "properties": {
                        "from": {
                            "description": "Самая ранняя дата изменения",
                            "type": "string"
                        },
                        "to": {
                            "description": "Самая поздняя дата изменения",
                            "type": "string"
                        }
                    }
                },
                "totalCount": {
                    "description": "Общее количество элементов",
                    "type": "integer"
                }
            }
        }
    }
}
```

**Пример**:

```
GET /xapi/person/stat?filter[change_date][to]=1494951762&filter[change_date][from]=149
4951000
```

**Ответ**

```
{
  "data": [],
  "meta": {
    "CHANGE_DATE": {
      "from": "2017-03-24 10:40:03",
      "to": "2017-05-24 12:10:22"
    },
    "totalCount": 539693
  }
}
```

Получение информации по рабочим станциям

Получение списка рабочих станций

**Описание** : Список рабочих станций

**Метод**: `GET`

**Ресурс**: `workstation`

**Параметры**:

- `filter` — список фильтрации:
  - `change_date[from]` — от даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[to]` )
  - `change_date[to]` — до даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[from]` )
  - `create_date[from]` — от даты создания в формате UNIX-timestamp (можно использовать отдельно от `create_date[to]` )
  - `create_date[to]` — до даты создания в формате UNIX-timestamp (можно использовать отдельно от `create_date[from]`
  - is_deleted — флаг 1 или 0. Если параметр указан, то будут выдавать сущности с указанным значением
  - `disabled` — флаг 1 или 0, признак активности. Если выставлен, то сущность неактивна (признак берется из LDAP)

  - `contact_type[]` — фильтрация по типу контакта (можно передать несколько, например: `/xapi/workstation?filter[contact_type][]=webaccount&filter[contact_type][]=icq` )
  - `contact_value[]` — фильтрация по значению контакта (можно передавать несколько, например: `/xapi/workstation?filter[contact_value][]=user@ad&filter[contact_value][]=login@example.com` )
  - `group_id[]` — фильтрация по группам (можно передать несколько, например: `/xapi/workstation?filter[group_id][]=FCE1409680E5D6469E1F7998266CE9E9&filter[group_id][]=918462B6DC2C954BAAF8706F7DC53F14)`
- `with[]` — список дополнительных сущностей, которые должны быть добавлены к объекту:
  - `contacts` — контакты рабочей станции
  - `w2g` — связь рабочей станции с группами
  - `status` — статусы рабочей станции
- `sort` — параметр для сортировки
  - `change_date` — сортировать по дате изменения `asc` или `desc` (например: `/xapi/workstation?sort[change_date]=asc` ) может замедлить выдачу
- `start` — с какой позиции начать отдавать элементы, по умолчанию 0
- `limit` — сколько элементов отдавать, по умолчанию 100, не может быть больше 1000

**Ответ** : Список рабочих станций, описанный в следующей JSON-Schema :

**JSON схема отдачи**

```
{
```

```
"$schema": "http://json-schema.org/draft-04/schema#",
"type": "object",
"required": [
    "data",
    "meta"
],
"properties": {
    "data": {
        "description": "Массив Рабочих станций",
        "type": "array",
        "items": {
            "description": "Рабочая станция",
            "type": "object",
            "required": [
                "WORKSTATION_ID",
                "CREATE_DATE",
                "CHANGE_DATE",
                "DISPLAY_NAME",
                "DISTINGUISHEDNAME",
                "DNSHOSTNAME",
                "DISABLED",
                "TYPE",
                "IS_DELETED"
            ],
            "properties": {
                "WORKSTATION_ID": {
                    "description": "Уникальный идентификатор рабочей станции",
                    "type": "string"
                },
                "CREATE_DATE": {
                    "description": "Дата создания записи",
                    "type": "string"
                },
                "CHANGE_DATE": {
                    "description": "Дата изменения записи",
                    "type": "string"
                },
                "DISPLAY_NAME": {
                    "description": "Название рабочей станции",
                    "type": "string"
                },
                "DISTINGUISHEDNAME": {
                    "description": "Отличительное имя",
                    "type": "string"
                },
                "DNSHOSTNAME": {
                    "description": "Полное имя",
                    "type": "string"
                },
                "DISABLED": {
                    "description": "Состояние рабочей станции",
                    "type": "integer"
                },
```

```
                    "TYPE": {
                        "description": "Тип: computer – Рабочая станция, mobile –
Мобильное устройство, terminal – Терминальный сервер",
                        "type": "string"
                    },
                    "IS_DELETED": {
                        "description": "Удалена ли рабочая станция из ТМ",
                        "type": "integer"
                    },
                    "contacts": {
                        "description": "Массив контактов",
                        "type": "array",
                        "items": {
                            "description": "Контакт",
                            "type": "object",
                            "required": [
                                "CONTACT_ID",
                                "CREATE_DATE",
                                "CHANGE_DATE",
                                "CONTACT_TYPE",
                                "VALUE",
                                "IS_PERSONAL",
                                "IS_PRIMARY",
                                "SOURCE"
                            ],
                            "properties": {
                                "CONTACT_ID": {
                                    "description": "Уникальный идентификатор объекта",
                                    "type": "string"
                                },
                                "CREATE_DATE": {
                                    "description": "Дата создания",
                                    "type": "string"
                                },
                                "CHANGE_DATE": {
                                    "description": "Дата изменения",
                                    "type": "string"
                                },
                                "CONTACT_TYPE": {
                                    "description": "Тип",
                                    "type": "string"
                                },
                                "VALUE": {
                                    "description": "Значение",
                                    "type": "string"
                                },
                                "IS_PERSONAL": {
                                    "description": "Принадлежность (Рабочий, Личный)",
                                    "type": "integer"
                                },
                                "IS_PRIMARY": {
                                    "description": "Признак основной",
                                    "type": "integer"
```

```
                                },
                                "SOURCE": {
                                    "description": "Тип",
                                    "type": "string"
                                }
                            }
                        }
                    },
                    "w2g": {
                        "description": "Массив связи с группами",
                        "type": "array",
                        "items": {
                            "description": "Связь с группой",
                            "type": "object",
                            "required": [
                                "WORKSTATION_ID",
                                "PARENT_GROUP_ID",
                                "RELATION_TYPE"
                            ],
                            "properties": {
                                "WORKSTATION_ID": {
                                    "description": "Уникальный идентификатор рабочей
станции",
                                    "type": "string"
                                },
                                "PARENT_GROUP_ID": {
                                    "description": "Уникальный идентификатор группы",
                                    "type": "string"
                                },
                                "RELATION_TYPE": {
                                    "description": "Тип связи: 0 - tm, 1 - member, 2 -
distinguishedname, 3 - primarygroupsid",
                                    "type": "integer"
                                }
                            }
                        }
                    },
                    "status": {
                        "description": "Массив статусов",
                        "type": "array",
                        "items": {
                            "description": "Статус персоны",
                            "type": "object",
                            "required": [
                                "IDENTITY_STATUS_ID",
                                "CREATE_DATE",
                                "CHANGE_DATE",
                                "ASSIGNMENT_DATE",
                                "DISPLAY_NAME",
                                "COLOR",
                                "EDITABLE"
                            ],
                            "properties": {
```

```
                                "IDENTITY_STATUS_ID": {
                                    "description": "Уникальный идентификатор статуса",
                                    "type": "string"
                                },
                                "CREATE_DATE": {
                                    "description": "Дата создания статуса",
                                    "type": "string"
                                },
                                "CHANGE_DATE": {
                                    "description": "Дата изменения статуса",
                                    "type": "string"
                                },
                                "ASSIGNMENT_DATE": {
                                    "description": "Дата проставления статуса персоне",
                                    "type": "string"
                                },
                                "DISPLAY_NAME": {
                                    "description": "Название статуса",
                                    "type": "string"
                                },
                                "COLOR": {
                                    "description": "Цвет статуса (например #ff0000)",
                                    "type": "string"
                                },
                                "EDITABLE": {
                                    "description": "Признак, что статус не является
системным",
                                    "type": "integer"
                                }
                            }
                        }
                    }
                }
            }
        },
        "meta": {
            "description": "Дополнительные данные",
            "type": "object",
            "required": [
                "totalCount",
                "start",
                "limit"
            ],
            "properties": {
                "totalCount": {
                    "type": "integer",
                    "description": "Общее количество"
                },
                "start": {
                    "type": "integer",
                    "description": "С какой позиции началось отдаваться"
                },
                "limit": {
```

```
                    "type": "integer",
                    "description": "Сколько всего отдалось"
                }
            }
        }
    }
}
```

**Пример**:

**Запрос**

```
/xapi/workstation?filter[change_date][from]=1&filter[change_date][to]=2&with[]=contact
s&with[]=w2g&limit=10&sort[change_date]=asc
```

Получение списка со статусами рабочих станций

**Описание** : Список всех возможных статусов рабочих станций

**Метод**: `GET`

Ресурс: `workstation/status`

- `start` — с какой позиции начать отдавать элементы, по-умолчанию 0
- `limit` — сколько элементов отдавать, по-умолчанию 100, не может быть больше 1000

**Пример**:

**Запрос**

```
GET /xapi/workstation/status?start=0&limit=10
```

Получение списка с типами контактов рабочих станций

**Описание** : Список всех возможных типов контактов рабочих станций

**Метод**: `GET`

**Ресурс**: `workstation/contact_type`

- `start` — с какой позиции начать отдавать элементы, по-умолчанию 0
- `limit` — сколько элементов отдавать, по-умолчанию 100, не может быть больше 1000

**Пример**:

**Запрос**

```
GET /xapi/workstation/contact_type?start=0&limit=10
```

Получение статистики по рабочим станциям

**Описание**: Статистика по рабочим станциям

**Метод**: `GET`

**Ресурс**: workstation `/stat`

**Параметры**:

- `filter` — список фильтрации:
  - `change_date[from]` — от даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[to]`)
  - `change_date[to]` — до даты последнего изменения в формате UNIX-timestamp (можно использовать отдельно от `change_date[from]`)

**Ответ**:

**JSON схема отдачи**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Статистика",
    "type": "object",
    "properties": {
        "data": {
            "description": "Не используется",
            "type": "array",
            "items": {}
        },
        "meta": {
            "description": "Статистика",
            "type": "object",
            "properties": {
                "CHANGE_DATE": {
                    "description": "Дата изменения",
                    "type": "object",
                    "properties": {
                        "from": {
                            "description": "Самая ранняя дата изменения",
                            "type": "string"
                        },
                        "to": {
                            "description": "Самая поздняя дата изменения",
                            "type": "string"
                        }
                    }
                },
                "totalCount": {
                    "description": "Общее количество элементов",
                    "type": "integer"
                }
            }
        }
    }
}
```

**Пример**:

```
GET /xapi/workstation/stat?filter[CAPTURE_DATE][to]=1494951762&filter[CAPTURE_DATE]
[from]=1494951000
```

**Ответ**

```
{
  "data": [],
  "meta": {
    "CHANGE_DATE": {
      "from": "2017-03-24 10:40:03",
      "to": "2017-05-24 12:10:22"
    },
    "totalCount": 539693
  }
}
```

## Получение событий

Получение извлеченного текста множества событий

**Метод**: `POST`

**Ресурс**: `event/texts`

**Параметры** (передаются в виде JSON):

- `response_type` — тип ответа:
  - `chunked` — используется `Transfer-Encoding: chunked`, где каждый текст отдаётся в своём блоке и в порядке, переданном в теле запроса, если текста нет, то вместо текста передаётся null символ "\0"
  - `multipart/mixed` — используется формат `multipart/mixed` rfc tech-ms, он не входит в стандарт HTTP, но используется в электронных письмах. Поэтому реализовать его не составляет труда. Также он очень похож на `multipart/form-data`. Каждый текст отдаётся в своём блоке и помечен отдельно заголовком X-Event-ID, к какому событию он принадлежит. Если текста нет, то он либо не передаётся, либо тело этого текста отсутствует
- `event` — массив объектов с полями:
  - `id` — ID события
  - `tbsId` — Табличное пространство, в котором событие

**Примеры**:

**`chunked`**:

**Запрос**

```
POST /xapi/event/texts
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
(пустая строка)
{"response_type": "chunked", "events": [{"id": 2, "tbsId": 4}, {"id": 4, "tbsId": 4}]}
```

**Ответ**

```
HTTP/1.1 200 OK
Content-Type: text/plain
Transfer-Encoding: chunked
(пустая строка)
1
\0 (символ отсутствия текста для события 2)
48AC
(содержимое текста для события 4)
0
```

`multipart/mixed` :

**Запрос**

```
POST /xapi/event/texts
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
(пустая строка)
{"response_type": "multipart/mixed", "events": [{"id": 2, "tbsId": 4}, {"id": 4, "tbsId": 4}]}
```

**Ответ**

```
HTTP/1.1 200 OK
Content-Type: multipart/mixed; boundary=Asrf456BGe4h
Content-Length: (суммарный объём, включая дочерние заголовки, может отсутствовать!)
(пустая строка)
(отсутствующая преамбула)
--Asrf456BGe4h
Content-Type: application/x-empty
Content-Disposition: attachment; filename="text-2.txt"
X-Event-ID: 2
(пустая строка и после нулевое содержимое)
--Asrf456BGe4h
Content-Disposition: attachment; filename="text-4.txt"
Content-Type: text/plain
X-Event-ID: 4
(пустая строка)
(содержимое текста для события 4)
--Asrf456BGe4h--
(отсутствующий эпилог - пустая строка)
```

Получение извлеченного текста события

**Метод**: `POST`

**Ресурс**: `event/texts`

**Параметры** (передаются в виде JSON):

- `response_type` — тип ответа:

    - `chunked` — используется `Transfer-Encoding: chunked`, где каждый текст отдаётся в своём блоке и в порядке, переданном в теле запроса, если текста нет, то вместо текста передаётся null символ "\0"
    - `multipart/mixed` — используется формат `multipart/mixed` rfc tech-ms, он не входит в стандарт HTTP, но используется в электронных письмах. Поэтому реализовать его не составляет труда. Так же он очень похож на `multipart/form-data`. Каждый текст отдаётся в своём блоке и помечен отдельно заголовком X-Event-ID, к какому событию он принадлежит. Если текста нет, то оно либо не передаётся, либо тело этого текста отсутствует
- `events` — массив объектов с полями:
    - `id` — ID события
    - `tbsId` — Табличное пространство события

**Примеры**:

**`chunked`**:

**Запрос**

```
 POST /xapi/event/texts
X-API-Version: 1.1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
(пустая строка)
{"response_type": "chunked", "events": [{"id": 2, "tbsId": 4}, {"id": 4, "tbsId": 4}]}
```

**Ответ**

```
HTTP/1.1 200 OK
Content-Type: text/plain
Transfer-Encoding: chunked
(пустая строка)
1
\0 (символ отсутствия текста для события 2)
48AC
(содержимое текста для события 4)
0
```

**`multipart/mixed`**:

**Запрос**

```
POST /xapi/event/texts
X-API-Version: 1.1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
(пустая строка)
{"response_type": "multipart/mixed", "events": [{"id": 2, "tbsId": 4}, {"id": 4, "tbsId": 4}]}
```

**Ответ**

```
HTTP/1.1 200 OK
Content-Type: multipart/mixed; boundary=Asrf456BGe4h
Content-Length: (суммарный объём, включая дочерние заголовки, может отсутствовать!)
(пустая строка)
(отсутствующая преамбула)
--Asrf456BGe4h
Content-Type: application/x-empty
Content-Disposition: attachment; filename="text-2.txt"
X-Event-ID: 2
(пустая строка и после нулевое содержимое)
--Asrf456BGe4h
Content-Disposition: attachment; filename="text-4.txt"
Content-Type: text/plain
X-Event-ID: 4
(пустая строка)
(содержимое текста для события 4)
--Asrf456BGe4h--
(отсутствующий эпилог - пустая строка)
```

Получение метаданных события

**Метод**: `GET`

**Ресурс**: `event/{id}`

**Параметры:**

- `{id}` - `OBJECT_ID` события
- `with[]` - список дополнительных сущностей, которые должны быть добавлены к объекту (например: отправители, получатели и т.д.)

**Ответ**: Событие

**Пример**:

**Получить событие с OBJECT_ID "1" с отправителями, получателями:**

```
GET /xapi/event/1?with[]=senders&with[]=recipients
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: aplab
X-API-Auth-Token: gla20dos1pcdbr69caxz
```

Получение множества контентов событий

**Метод**: `POST`

**Ресурс**: `event/raws`

**Параметры** (передаются в виде JSON):

- `response_type` — тип ответа:
  - `chunked` — используется `Transfer-Encoding: chunked`, где каждый контент отдаётся в своём блоке и в порядке, переданном в теле запроса, если контента нет, то вместо контента передаётся null символ "\0"

    - `multipart/mixed` — используется формат `multipart/mixed` rfc tech-ms, он не входит в стандарт HTTP, но используется в электронных письмах. Поэтому реализовать его не составляет труда. Так же он очень похож на `multipart/form-data`. Каждый контент отдаётся в своём блоке и помечен отдельно заголовками X-Event-ID и X-Content-ID, к какому событию и контенту он принадлежит. Если контента нет, то оно либо не передаётся, либо тело этого текста отсутствует
- `event` — массив объектов с полями:
    - `id` — ID события
    - `tbsId` — Табличное пространство, в котором событие
    - `contentId` — ID контента. Если не указан, то отдаётся главный узел

**Примеры**:

**`chunked`**:

**Запрос**

```
POST /xapi/event/raws
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
(пустая строка)
{"response_type": "chunked", "events": [{"id": 2, "tbsId": 4}, {"id": 3, "tbsId": 4}, {"id": 4, "tbsId": 4,
"contentId": 8}]}
```

**Ответ**

```
HTTP/1.1 200 OK
Content-Type: text/plain
Transfer-Encoding: chunked
(пустая строка)
1
\0 (символ отсутствия контента для события 2)
3E4
(содержимое корневого контента для события 3)
48AC
(содержимое контента 8 для события 4)
0
```

**`multipart/mixed`**:

**Запрос**

```
POST /xapi/event/raws
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
(пустая строка)
{"response_type": "multipart/mixed", "events": [{"id": 2, "tbsId": 4}, {"id": 3, "tbsId": 4}, {"id": 4,
"tbsId": 4, "contentId": 8}]}
```

**Ответ**

```
HTTP/1.1 200 OK
Content-Type: multipart/mixed; boundary=Asrf456BGe4h
Content-Length: (суммарный объём, включая дочерние заголовки, может отсутствовать!)
(пустая строка)
(отсутствующая преамбула)
--Asrf456BGe4h
Content-Type: application/x-empty
Content-Disposition: attachment; filename="content-2"
X-Event-ID: 2
(пустая строка и после нулевое содержимое)
--Asrf456BGe4h
Content-Disposition: attachment; filename="content-3-5.eml"
Content-Type: email
X-Event-ID: 3
X-Content-ID: 5
(пустая строка)
(содержимое корневого контента для события 3)
--Asrf456BGe4h
Content-Disposition: attachment; filename="my-project.jpg"
Content-Type: image/jpeg
X-Event-ID: 4
X-Content-ID: 8
(пустая строка)
(содержимое контента 8 для события 4)
--Asrf456BGe4h--

(отсутствующий эпилог - пустая строка)
```

Получение информации о контентах события

**Метод**: `POST`

**Ресурс**: `event/contents`

**Параметры** (передаются в виде JSON):

- `response_type` – тип ответа:
  - `chunked` – используется `Transfer-Encoding: chunked`, где каждый контент отдаётся в своём блоке и в порядке, переданном в теле запроса, если контента нет, то вместо контента передаётся null символ "\0"
  - `multipart/mixed` – используется формат `multipart/mixed` rfc tech-ms, он не входит в стандарт HTTP, но используется в электронных письмах. Поэтому реализовать его не составляет труда. Так же он очень похож на `multipart/form-data`. Каждый контент отдаётся в своём блоке и помечен отдельно заголовками X-Event-ID и X-Content-ID, к какому событию и контенту он принадлежит. Если контента нет, то оно либо не передаётся, либо тело этого текста отсутствует
- `events` – массив объектов с полями:
  - `id` – ID одного или нескольких событий, по которым нужно получить контенты;
  - `tbsId` – ID табличных пространств для каждого события;
- `filter[mime]–` типы контентов с возможностью указать несколько значений (по точному совпадению или по маске) или сразу все
- `start` - с какой позиции начать отдавать контенты, по-умолчанию 0
- `limit` - сколько контентов отдавать. По умолчанию 100, не может быть больше 1000 в одном запросе.

**Пример**:

**Запрос**

```
curl -X POST "https://qa-2e55.infowatch.ru/xapi/event/contents?filter[mime][]=image%2Fjpeg&filter[mime][]=text%2F%2A&start=1&limit=10" -H "accept: application/json" -H "Content-Type: application/json" -H "X-Enable-OpenAPI: 1" -d "{\"events\":[{\"id\":2,\"tbsId\":4}]}"
```

По запросу будут предоставлены ID контентов, соответствующих условиям запроса, с указанием следующих атрибутов:

**Ответ**

```
{
  "data": [
    {
      "OBJECT_CONTENT_ID": 15,
      "MIME": "string",
      "OBJECT_ID": 2,
      "TBS_ID": 4,
      "CONTENT_SIZE": 1500,
      "is_filename": 0           // признак, что контент является или не является именем файла
    }
  ],
  "meta": {
    "totalCount": 1,
    "start": 1,
    "limit": 10
  }
}
```

Получение перехваченного файла события

**Метод**: `GET`

**Ресурс**: `event/{id}/raw?download=0`

**Параметры**:

- `{id}` - OBJECT_ID события, обязательный
- `download` - добавляет HTTP-заголовки для скачивания файла ( `Content-Disposition` , `Content-Transfer-Encoding` и прочие), обязательный, значения 1 или 0 (по умолчанию 0)

Поддерживается HTTP-заголовок `Range`

**Ответ**: Файл перехваченного события. Например: eml (для писем) или сам файл для событий копирования файла.

Получение списка ОЗ

**Описание** : Список ОЗ, отсортированный по имени.

**Метод**: `GET`

**Ресурс**: `event/protectedDocument`

**Параметры**:

- `start` - с какой позиции начать отдавать ОЗ, по-умолчанию 0
- `limit` - сколько ОЗ отдавать, по-умолчанию 100, не может быть больше 1000
- `with[]` — список дополнительных сущностей, которые должны быть добавлены к ОЗ:
  - `pd2pc` — связь объекта защиты к каталогу объекта защиты

**Ответ**: Список ОЗ, описанный следующей **JSON схемой отдачи списка ОЗ:**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "object",
    "properties": {
        "data": {
            "type": "array",
            "description": "Массив ОЗ",
            "items": {
                "type": "object",
                "description": "ОЗ",
                "properties": {
                    "DOCUMENT_ID": {
                        "type": "string",
                        "description": "Идентификатор"
                    },
                    "DISPLAY_NAME": {
                        "type": "string",
                        "description": "Имя"
                    },
                    "CREATE_DATE": {
                        "type": "string",
                        "description": "Дата создания"
                    },
                    "IS_DELETED": {
                        "type": "integer",
                        "description": "Удален ли из активной конфигурации",
                        "enum": [
```

```
                            0,
                            1
                        ]
                    },
                    "pd2pc": {
                        "description": "Массив связи с каталогами ОЗ",
                        "type": "array",
                        "items": {
                            "description": "Связь с каталогом ОЗ",
                            "type": "object",
                            "required": [
                                "CATALOG_ID",
                                "DOCUMENT_ID"
                            ],
                            "properties": {
                                "CATALOG_ID": {
                                    "description": "Уникальный идентификатор каталога
ОЗ",
                                    "type": "string"
                                },
                                "DOCUMENT_ID": {
                                    "description": "Уникальный идентификатор ОЗ",
                                    "type": "string"
                                }
                            }
                        }
                    }
                },
                "required": [
                    "DOCUMENT_ID",
                    "DISPLAY_NAME",
                    "CREATE_DATE",
                    "IS_DELETED"
                ]
            }
        },
        "meta": {
            "description": "Дополнительные данные",
            "type": "object",
            "properties": {
                "totalCount": {
                    "type": "integer",
                    "description": "Общее количество ОЗ"
                },
                "start": {
                    "type": "integer",
                    "description": "С какой позиции началось отдаваться"
                },
                "limit": {
                    "type": "integer",
                    "description": "Сколько всего отдалось"
                }
            },
```

```
            "required": [
                "totalCount",
                "start",
                "limit"
            ]
        }
    },
    "required": [
        "data",
        "meta"
    ]
}
```

**Пример**:

**Запрос**

```
GET /xapi/event/protectedDocument?start=0&limit=10
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
```

**Ответ**

```
{
    "data": [{
        "DOCUMENT_ID": "C78E821A67C7F34A1B1D63A4151CEF6300000000",
        "DISPLAY_NAME": "Грифованная информация",
        "CREATE_DATE": "2016-05-12 10:24:41.342554",
        "IS_DELETED": 0
    }],
    "meta": {
        "totalCount": 1,
        "start": 0,
        "limit": 10
    }
}
```

Получение списка заголовков

**Описание:** Получение списка дополнительных полей события.

**Метод**: `GET`

**Ресурс**: `event/header`

**Параметры**:

- `start` - с какой позиции начать отдавать заголовки, по-умолчанию 0
- `limit` - сколько заголовков отдавать, по-умолчанию 100, не может быть больше 1000

**Ответ:** Список дополнительный полей, описанных следующей **JSON схемой отдачи:**

```
{
```

```
    "$id": "http://infowatch.com/iwtm/xapi/event/header.json",
    "type": "object",
    "$schema": "http://json-schema.org/draft-07/schema#",
    "properties": {
        "data": {
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "NAME": {
                        "type": "string",
                        "title": "Код атрибута, который будет использоваться в заголовках события и для идентификации в xAPI/PushAPI",
                        "examples": [
                            "mac_level"
                        ]
                    },
                    "NOTE": {
                        "type": "string",
                        "title": "Отображаемое в консоли ТМ название атрибута",
                        "examples": [
                            "Уровень мандатного доступа"
                        ]
                    },
                    "TYPE": {
                        "type": "string",
                        "title": "Одно из следующих значений: число (целое, дробное, строка), дата и время в UTC + указание смещение часового пояса, длительность, гиперссылка",
                        "enum": [
                            "integer",
                            "float",
                            "string",
                            "date",
                            "UTC",
                            "duration",
                            "link"
                        ]
```

```
                    },
                    "IS_DELETED": {
                        "type": "integer",
                        "title": "Является ли заголовок удаленным из системы (у старых объектов он остаётся)",
                        "default": 0,
                        "enum": [
                            0,
                            1
                        ]
                    },
                    "FORMAT": {
                        "type": "string",
                        "title": "Тип значения (с версии 1.2)",
                        "enum": [
                            "string",
                            "date",
                            "number"
                        ]
                    },
                    "IS_SYSTEM": {
                        "type": "integer",
                        "title": "Является ли заголовок системным (с версии 1.1)",
                        "default": 1,
                        "enum": [
                            0,
                            1
                        ]
                    },
                    "IS_MULTIPLE_VALUE": {
                        "type": "integer",
                        "title": "Может ли заголовок содержать несколько значений (с версии 1.1)",
                        "default": 0,
                        "enum": [
                            0,
                            1
```

```
                        ]
                    },
                    "locale": {
                        "type": "array",
                        "title": "Локализация для заголовков (с версии 1.2)",
                        "items": {
                            "type": "object",
                            "title": "Локализация для заголовка",
                            "properties": {
                                "NAME": {
                                    "type": "string",
                                    "title": "Код атрибута, который будет использоваться в заголовках события и для идентификации в xAPI/PushAPI"
                                },
                                "LANGUAGE": {
                                    "type": "string",
                                    "title": "Название языка",
                                    "enum": [
                                        "rus",
                                        "eng"
                                    ]
                                },
                                "DISPLAY_NAME": {
                                    "type": "string",
                                    "title": "Отображаемое в консоли ТМ название атрибута"
                                }
                            }
                        }
                    }
                }
            },
            "meta": {
                "description": "Дополнительные данные",
                "type": "object",
                "properties": {
```

```
                "totalCount": {
                    "type": "integer",
                    "description": "Общее количество ОЗ"
                },
                "start": {
                    "type": "integer",
                    "description": "С какой позиции началось отдаваться"
                },
                "limit": {
                    "type": "integer",
                    "description": "Сколько всего отдалось"
                }
            },
            "required": [
                "totalCount",
                "start",
                "limit"
            ]
        }
    },
    "required": [
        "data",
        "meta"
    ]
}
```

**Пример**:

**Запрос**

```
GET /xapi/event/header
X-API-Version: 1.1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
```

**Ответ**

```
{
    "data": [
        {
```

```
            "NAME": "device_type",
            "NOTE": "Тип устройства",
            "TYPE": "enum",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "destination_type",
            "NOTE": "Тип источника сканирования",
            "TYPE": "enum",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "destination_url",
            "NOTE": "URL",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "print_server",
            "NOTE": "Имя сервера печати",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "location",
            "NOTE": "Расположение принтера",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
```

```
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "comment",
            "NOTE": "Комментарий к принтеру",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "port_name",
            "NOTE": "Имя порта принтера",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "copies",
            "NOTE": "Количество копий",
            "TYPE": "number",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "task_name",
            "NOTE": "Имя задания",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "print_task_name",
            "NOTE": "Имя задания на печать",
```

```
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "task_run_date",
            "NOTE": "Дата запуска задания",
            "TYPE": "date",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "create_date",
            "NOTE": "Дата создания файла",
            "TYPE": "date",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "modify_date",
            "NOTE": "Дата модификации файла",
            "TYPE": "date",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "source_ip",
            "NOTE": "IP адрес источника",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
```

```
        {
            "NAME": "workstation_type",
            "NOTE": "Тип рабочей станции",
            "TYPE": "enum",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "application_path_from",
            "NOTE": "Путь к приложению из которого скопировано событие",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "application_path_to",
            "NOTE": "Путь к приложению в которое скопировано событие",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "terminal_session",
            "NOTE": "Признак терминальной сессии",
            "TYPE": "number",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "emitter",
            "NOTE": "Источник события",
            "TYPE": "enum",
            "IS_DELETED": 0,
```

```
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        },
        {
            "NAME": "charset",
            "NOTE": "Кодировка текста вложения",
            "TYPE": "string",
            "IS_DELETED": 0,
            "IS_SYSTEM": 1,
            "IS_MULTIPLE_VALUE": 0
        }
    ],
    "meta": {
        "totalCount": 20,
        "start": 0,
        "limit": 100
    }
}
```

Получение списка каталогов ОЗ

**Описание** : Список каталогов ОЗ, отсортированных по имени.

**Метод**: `GET`

**Ресурс**: `event/protectedCatalog`

**Параметры**:

- `start` - с какой позиции начать отдавать каталоги (по умолчанию 0)
- `limit` - сколько каталогов отдавать (по умолчанию 100, не может быть больше 1000)

**Ответ**: Список каталогов ОЗ, описанный следующей JSON-Schema:

**JSON схема отдачи списка каталогов.**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "object",
    "properties": {
        "data": {
            "type": "array",
            "description": "Массив каталогов ОЗ",
            "items": {
                "type": "object",
                "description": "Каталог ОЗ",
                "properties": {
                    "CATALOG_ID": {
                        "type": "string",
```

```
                        "description": "Идентификатор"
                    },
                    "DISPLAY_NAME": {
                        "type": "string",
                        "description": "Имя"
                    },
                    "CREATE_DATE": {
                        "type": "string",
                        "description": "Дата создания"
                    },
                    "IS_DELETED": {
                        "type": "integer",
                        "description": "Удален ли из активной конфигурации",
                        "enum": [
                            0,
                            1
                        ]
                    }
                },
                "required": [
                    "CATALOG_ID",
                    "DISPLAY_NAME",
                    "CREATE_DATE",
                    "IS_DELETED"
                ]
            }
        },
        "meta": {
            "description": "Дополнительные данные",
            "type": "object",
            "properties": {
                "totalCount": {
                    "type": "integer",
                    "description": "Общее количество ОЗ"
                },
                "start": {
                    "type": "integer",
                    "description": "С какой позиции началось отдаваться"
                },
                "limit": {
                    "type": "integer",
                    "description": "Сколько всего отдалось"
                }
            },
            "required": [
                "totalCount",
                "start",
                "limit"
            ]
        }
    },
    "required": [
        "data",
        "meta"
    ]
}
```


**Пример:**

**Запрос**

```
GET /xapi/event/protectedCatalog?start=0&limit=10
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: aplab
X-API-Auth-Token: gla20dos1pcdbr69caxz
```

**Ответ**

```
{
    "data": [{
        "CATALOG_ID": "3D0F8CDAF9E74F82AC85EB32D12727A700000000",
        "DISPLAY_NAME": "Грифованная информация",
        "CREATE_DATE": "2016-05-12 10:24:41.342554",
        "IS_DELETED": 0
    }],
    "meta": {
        "totalCount": 1,
        "start": 0,
        "limit": 10
    }
}
```

Получение списка политик

**Описание**: Список политик отсортированный по имени.

**Метод**: `GET`

**Ресурс**: `event/policy`

**Параметры**:

- `start` — с какой позиции начать отдавать политики, по-умолчанию 0
- `limit` — сколько политик отдавать, по-умолчанию 100, не может быть больше 1000

**Ответ**: Список политик, описанный следующей **JSON схемой отдачи списка каталогов:**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "object",
    "properties": {
        "data": {
            "type": "array",
            "description": "Массив политик",
            "items": {
                "type": "object",
                "description": "Политика",
                "properties": {
                    "POLICY_ID": {
                        "type": "string",
                        "description": "Идентификатор"
                    },
                    "DISPLAY_NAME": {
```

```
                        "type": "string",
                        "description": "Имя"
                    },
                    "CREATE_DATE": {
                        "type": "string",
                        "description": "Дата создания"
                    },
                    "IS_DELETED": {
                        "type": "integer",
                        "description": "Удалена ли из активной конфигурации",
                        "enum": [
                            0,
                            1
                        ]
                    }
                },
                "required": [
                    "POLICY_ID",
                    "DISPLAY_NAME",
                    "CREATE_DATE",
                    "IS_DELETED"
                ]
            }
        },
        "meta": {
            "description": "Дополнительные данные",
            "type": "object",
            "properties": {
                "totalCount": {
                    "type": "integer",
                    "description": "Общее количество политик"
                },
                "start": {
                    "type": "integer",
                    "description": "С какой позиции началось отдаваться"
                },
                "limit": {
                    "type": "integer",
                    "description": "Сколько всего отдалось"
                }
            },
            "required": [
                "totalCount",
                "start",
                "limit"
            ]
        }
    },
    "required": [
        "data",
        "meta"
    ]
}
```

**Пример**:

**Запрос**

```
GET /xapi/event/policy?start=0&limit=10
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
```

**Ответ**

```
{
    "data": [{
        "POLICY_ID": "3D0F8CDAF9E74F82AC85EB32D12727A700000000",
        "DISPLAY_NAME": "Грифованная информация",
        "CREATE_DATE": "2016-05-12 10:24:41.342554",
        "IS_DELETED": 0
    }],
    "meta": {
        "totalCount": 1,
        "start": 0,
        "limit": 10
    }
}
```

Получение списка событий

**Описание**: Список событий, отсортированных по времени перехвата (от новых к старым).

**Метод**: `GET`

**Ресурс**: `event`

**Параметры**:

- `filter` - список фильтрации:
  - `date[from]` — дата начала в формате UNIX-timestamp (можно использовать отдельно от `date[to]` )
  - `date[to]` — дата окончания в формате UNIX-timestamp (можно использовать отдельно от `date[from]` )
  - `insert_date[>]` — дата вставки начала в формате UNIX-timestamp и через точку microtime, например `filter[insert_date][>]=1234.123312`
  - `insert_date[<]` — дата вставки окончания в формате UNIX-timestamp и через точку microtime, например `filter[insert_date][<]=1234.123312`
  - `insert_date[>=]` — дата вставки начала в формате UNIX-timestamp и через точку microtime, например `filter[insert_date][>=]=1234.123312` (включительно) (с версии API 1.1)
  - `insert_date[<=]` — дата вставки окончания в формате UNIX-timestamp и через точку microtime, например `filter[insert_date][<=]=1234.123312` ( включительно) (с версии API 1.1)
  - `rule_group_type[]` — группа правил (с версии API 1.1)
  - `violation_level[]` — уровень нарушения (с версии API 1.1)
  - `verdict[]` — вердикт (с версии API 1.1)

    - `object_type_code[]` — тип события (возможно несколько значений)
    - `protocol[]` — протокол (возможно несколько значений)
    - `user_decision[]` — решение пользователя (возможно несколько значений)
    - `document_id[]` — идентификатор документа идентификатор
    - `object_size[from]` — от скольки байт искать событие (можно использовать отдельно от `object_size [to]` )
    - `object_size[to]` — до скольки байт искать событие (можно использовать отдельно от `object_size [from]` )
    - `protected_catalog_id[]` — идентификатор каталога ОЗ (возможно несколько значений)
    - `tag_id[]` — идентификатор тега (возможно несколько значений)
- `with[]` - список дополнительных сущностей, которые должны быть добавлены к объекту (например: отправители, получатели и т.д.):
    - `protected_catalogs`
    - `protected_documents`
    - `policies`
    - `senders_keys`
    - `senders`
    - `recipients_keys`
    - `recipients`
    - `workstations_keys`
    - `workstations`
    - `tags`
    - `perimeters` (с версии API 1.1)
    - `attachments` (с версии API 1.1)
    - `files` (с версии API 1.1) — недокументированный параметр, отдающий все контенты, в которых непустое поле FILE_NAME
    - `contents_renderer` (с версии API 1.8) - прикрепить контенты рендерера различного типа
- `without[] – дополнительные флаги`
    - `count` — не считать `totalCount` (расчет `totalCount` может занимать больше половины времени запроса, поэтому лучше воспользоваться методом `event/stat` )
- `headers[]` — список дополнительных полей (заголовков) события (можно написать *, если нужны все). Список можно получить с помощью метода `event/header (с версии API 1.1)`
- `sort[]` — недокументированное поле, позволяющее сортировать результат (получение событий замедляется существенно, для получения последнего/первого события лучше использовать метод `event/stat` . Возможные ключи:
    - `capture_date — asc` (с версии API 1.1) `/desc` , например: `?sort[capture_date]=desc`
    - `insert_date — asc/desc` , например: `?sort[insert_date]=asc (с версии API 1.1)`
- `start` - с какой позиции начать отдавать события (по умолчанию 0)
- `limit` - сколько событий отдавать (по умолчанию 100, не может быть больше 1000)

**Алгоритм при первом получении событий:**

1. Определить, с какого времени нужно получать события. Например, получить из статистики событий (GET /xapi/event/stat) интервал INSERT_DATE.
2. Разделить интервал на меньшее из значений: количество потоков (но не более 32) **или** количество ядер на сервере.
3. В каждом потоке составить и запустить первый запрос на получение списка события вида:
   GET /xapi/event?without[]=count&filter[insert_date][>=]={минимум_интервала}&filter[insert_date][<=]={максимум_интервала}&sort[insert_date]=asc&limit=1000
4. В полученном списке запомнить все OBJECT_ID.
5. В полученном списке найти последнюю INSERT_DATE и использовать её в запросе из пункта 3, в качестве `минимум_интервала.`
6. В полученном новом списке исключить события, которые запомнили в предыдущей итерации.
7. Если не дошли до `максимум_интервала`, снова начать с пункта 4.
8. Сохранить в персистентное хранилище:
   a. максимальное значение INSERT_DATE, полученное из пункта 1.
   b. список OBJECT_ID из интервала, в который входит максимальное значение INSERT_DATE.

**Примеры**:

**Получить первые 100 событий с за январь 2015 года:**

```
GET /xapi/event?filter[date][from]=1420059600&filter[date][to]=1422737999&start=0&limit=100
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: aplab
X-API-Auth-Token: gla20dos1pcdbr69caxz
```

**Получить 1000 событий с письмами, содержащими контент:**

```
GET /xapi/event?with=contents_renderer&limit=1000
X-API-Version: 1.8
X-API-CompanyId: IW
X-API-productName: Vision
X-API-Auth-Token: 1eja07v23vs9k1s5ij5k
```

Ответ содержит список событий, отсортированный по времени перехвата от новых к старым. Для разных типов событий структура ответа будет отличаться.

**Пример ответа**

```
[
 OBJECT_ID: 1
 VIOLATION_LEVEL: 'High'
 CAPTURE_DATE: '12-03-2022 15:02:25'
 contents_renderer:
 [
    SUBJECT: [
       CONTENT_ID: 1
```

```
      OBJECT_ID: 1
      CONTENT_SIZE: 26
   ]
   BODY: [
      CONTENT_ID: 2
      OBJECT_ID: 1
      CONTENT_SIZE:5125
   ]
 ]
]
```

Получение списка тегов

**Описание**: Список тегов, отсортированных по имени.

**Метод**: `GET`

**Ресурс**: `event/tag`

**Параметры**:

- `start` - с какой позиции начать отдавать теги (по умолчанию 0)
- `limit` - сколько тегов отдавать (по умолчанию 100, не может быть больше 1000)

**Ответ**: Список тегов, описанный следующей JSON-Schema:

**JSON схема отдачи списка тэгов**

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "properties": {
       "data": {
           "type": "array",
           "description": "Массив тегов",
           "items": {
               "type": "object",
               "description": "Тег",
               "properties": {
                   "TAG_ID": {
                       "type": "string",
                       "description": "Идентификатор"
                   },
                   "DISPLAY_NAME": {
                       "type": "string",
                       "description": "Имя"
                   },
                   "COLOR": {
                       "type": "string",
                       "description": "Цвет тега в HEX RGP, например #ffffff"
                   },
                   "CREATE_DATE": {
                       "type": "string",
                       "description": "Дата создания"
                   },
                   "IS_DELETED": {
                       "type": "integer",
                       "description": "Удален ли из активной конфигурации"
```

```
                    },
                    "IS_SYSTEM": {
                        "type": "integer",
                        "description": "Является ли тег системным"
                    }
                },
                "required": [
                    "TAG_ID",
                    "DISPLAY_NAME",
                    "COLOR",
                    "CREATE_DATE",
                    "IS_DELETED",
                    "IS_SYSTEM"
                ]
            }
        },
        "meta": {
            "description": "Дополнительные данные",
            "type": "object",
            "properties": {
                "totalCount": {
                    "type": "integer",
                    "description": "Общее количество ОЗ"
                },
                "start": {
                    "type": "integer",
                    "description": "С какой позиции началось отдаваться"
                },
                "limit": {
                    "type": "integer",
                    "description": "Сколько всего отдалось"
                }
            },
            "required": [
                "totalCount",
                "start",
                "limit"
            ]
        }
    },
    "required": [
        "data",
        "meta"
    ]
}
```


**Пример:**

**Запрос**

```
GET /xapi/event/tag?start=0&limit=10
X-API-Version: 1
X-API-CompanyId: iw
X-API-ImporterName: aplab
X-API-Auth-Token: gla20dos1pcdbr69caxz
```

**Ответ**


```
{
    "data": [{
        "TAG_ID": "0AF69DD5742E6977E0530100007F2BB700000000",
        "DISPLAY_NAME": "VIP",
        "COLOR": "#4e954e",
        "CREATE_DATE": "2016-05-12 10:24:40.002673",
        "IS_DELETED": 0,
        "IS_SYSTEM": 1
    }],
    "meta": {
        "totalCount": 1,
        "start": 0,
        "limit": 10
    }
}
```


Получение статистики по событиям

**Описание**: Недокументированный метод получения статистики по событиям, отдаёт только статистику по дате перехвата.

**Метод**: `GET`

**Ресурс**: `event/stat`

**Параметры**:

- fields — список полей, которые нужно выбрать: CAPTURE_DATE , INSERT_DATE , totalCount (с версии API 1.2)
- `filter` — список фильтрации:
  - `date[from]` — дата начала в формате UNIX-timestamp (можно использовать отдельно от `date[to]` )
  - `date[to]` — дата окончания в формате UNIX-timestamp (можно использовать отдельно от `date[from]` )
  - `insert_date[>]` — дата вставки начала в формате UNIX-timestamp и через точку microtime, например `filter[insert_date][>]=1234.123312` (с версии API 1.1)
  - `insert_date[<]` — дата вставки окончания в формате UNIX-timestamp и через точку microtime, например `filter[insert_date][<]=1234.123312` (с версии API 1.1)
  - `insert_date[>=]` — дата вставки начала в формате UNIX-timestamp и через точку microtime, например `filter[insert_date][>=]=1234.123312` (включительно) (с версии API 1.1)
  - `insert_date[<=]` — дата вставки окончания в формате UNIX-timestamp и через точку microtime, например `filter[insert_date][<=]=1234.123312` ( включительно) (с версии API 1.1)
  - `object_type_code[]` — тип события (возможно несколько значений) (с версии API 1.1)
  - `violation_level[]` — уровень нарушения (с версии API 1.1)

**Ответ**: Статистика по событиям, описанная следующей JSON-Schema:

**JSON схема отдачи:**

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "object",
    "properties": {
        "data": {
            "description": "Пустая секция",
            "items": {},
            "type": "array"
        },
        "meta": {
            "description": "Дополнительные данные",
            "type": "object",
            "properties": {
                "CAPTURE_DATE": {
                    "description": "Статистика по полю CAPTURE_DATE",
                    "type": "object",
                    "properties": {
                        "from": {
                            "type": "string",
                            "description": "Дата перехвата первого события в выборке"
                        },
                        "to": {
                            "type": "string",
                            "description": "Дата перехвата последнего события в
выборке"
                        }
                    }
                },
                "INSERT_DATE": {
                    "description": "Статистика по полю INSERT_DATE (с версии API 1.1)",
                    "type": "object",
                    "properties": {
                        "from": {
                            "type": "string",
                            "description": "Дата вставки первого события в выборке"
                        },
                        "to": {
                            "type": "string",
                            "description": "Дата вставки последнего события в выборке"
                        }
                    }
                },
                "totalCount": {
                    "type": "integer",
                    "description": "Общее количество событий"
                }
            }
        }
    }
}
```

**Пример**:

**Запрос**

```
GET /xapi/event/stat?filter[data][from]=0
X-API-Version: 1.3
X-API-CompanyId: iw
X-API-ImporterName: dome
X-API-Auth-Token: brse99dugp1cdbr69axz
```

**Ответ**

```
{
    "data": [],
    "meta": {
        "CAPTURE_DATE": {
            "from": "2017-04-16 00:00:04",
            "to": "2017-05-16 16:20:36"
        },
        "INSERT_DATE": {
            "from": "2017-04-16 00:01:07",
            "to": "2017-05-16 16:20:40"
        },
        "totalCount": 225075
    }
}
```

Изменение атрибутов событий

Назначение вердикта пользователя
**Версия API**: ≥ 1.2

**Метод**: PATCH

**Ресурс**: event/{id}/userDecision?tbsId={tbsId}

**Описание:**

Метод назначает решение пользователя. Поля:

- `{id}` — ID события ( `OBJECT_ID` )
- `{tbsId}` — Табличное пространство события ( `TBS_ID` )
- `USER_DECISION` — Решение пользователя. Возможные значения:
    - `NotProcessed - Решение не принято`
    - `Violation - Нарушение`
    - `NoViolation - Нет нарушения`
    - `AdditionalProcessingNeeded - Требует дополнительной обработки`
- `NOTE –` комментарий, который сохраняется в разделе Аудит. Может быть заполнено, например, именем пользователя сторонней системы, который изменил значение атрибута. Длина поля не должна превышать 1000 символов.

Вызов данного API записывается в раздел Аудит. При назначении решения пользователя в событии могут автоматически поменяться следующие поля:

- `TBS_ID`

- `VERDICT`
- `FORWARD_STATE_CODE`

Поэтому в ответе API отдаются значения, которые можно будет обновить у вашей копии события.

**Тело запроса:JSON схема назначения вердикта пользователя**

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "type": "object",
  "title": "Set user decision schema",
  "required": [
    "USER_DECISION"
  ],
  "properties": {
    "USER_DECISION": {
      "$id": "#/properties/USER_DECISION",
      "type": "string",
      "title": "User decision",
      "enum": [
        "NotProcessed",
        "Violation",
        "NoViolation",
        "AdditionalProcessingNeeded"
      ]
    },
    "NOTE": {
      "$id": "#/properties/NOTE",
      "type": "string",
      "title": "Note",
      "maxLength": 1000
    }
  }
}
```

**Тело ответа: JSON схема ответа на назначение вердикта пользователя**

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "type": "object",
  "title": "Result setting user decision schema",
  "required": [
    "OBJECT_ID",
    "TBS_ID",
    "VERDICT",
    "USER_DECISION",
    "FORWARD_STATE_CODE"
  ],
  "properties": {
    "OBJECT_ID": {
      "$id": "#/properties/OBJECT_ID",
      "type": "integer",
      "title": "ID События"
    },
```

```
    "TBS_ID": {
      "$id": "#/properties/TBS_ID",
      "type": "integer",
      "title": "ID табличного пространства"
    },
    "VERDICT": {
      "$id": "#/properties/VERDICT",
      "type": "string",
      "title": "Вердикт",
      "enum": [
        "Allowed",
        "Quarantined",
        "Forbidden"
      ]
    },
    "USER_DECISION": {
      "$id": "#/properties/USER_DECISION",
      "type": "string",
      "title": "Проставленное решение пользователя",
      "enum": [
        "NotProcessed",
        "NoViolation",
        "Violation",
        "AdditionalProcessingNeeded"
      ]
    },
    "FORWARD_STATE_CODE": {
      "$id": "#/properties/FORWARD_STATE_CODE",
      "type": "string",
      "title": "Статус отправки",
      "examples": [
        "Sent",
        "NotSent",
        "Pending"
      ]
    }
  }
}
```


**Пример:** Назначение вердикта "Нарушение" с комментарием событию ID 194 в TBS 1 с помощью cUrl:

```
curl 'https://example.com/xapi/event/195/userDecision?tbsId=1' \
  -X PATCH \
  -H 'X-API-Auth-Token: 1792jmclf7fer1ikuhby' \
  -H 'X-API-Version: 1' \
  -H 'X-API-CompanyId: IW' \
  -H 'X-API-ImporterName: dome' \
  -H 'Content-Type: application/json' \
  --data-binary '{"USER_DECISION":"Violation","NOTE":"Назначение вердикта через Dome.
Сотрудник Иванов Виктор Павлович."}'
```

Назначение вердикта пользователя множеству событий
**Версия API**: ≥ 1.2

**Метод**: PATCH

**Ресурс**: event/userDecision

**Описание:**

Метод позволяет массово назначать решения пользователя (принимает не более **1000** решений пользователя, иначе возвращается сообщение об ошибке с кодом **413**). ID события и ID табличного пространства передаются в теле запроса с решением пользователя и комментарием.

**Тело запроса: JSON схема для множественного назначения вердиктов**

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "type": "array",
  "title": "Set batch user decision schema",
  "items": {
    "$id": "#/items",
    "type": "object",
    "required": [
      "OBJECT_ID",
      "TBS_ID",
      "USER_DECISION"
    ],
    "properties": {
      "OBJECT_ID": {
        "$id": "#/items/properties/OBJECT_ID",
        "type": "integer",
        "title": "ID События"
      },
      "TBS_ID": {
        "$id": "#/items/properties/TBS_ID",
        "type": "integer",
        "title": "ID табличного пространства"
      },
      "USER_DECISION": {
        "$id": "#/items/properties/USER_DECISION",
        "type": "string",
        "title": "User decision",
        "enum": [
          "NotProcessed",
          "Violation",
          "NoViolation",
          "AdditionalProcessingNeeded"
        ]
      },
      "NOTE": {
        "$id": "#/items/properties/NOTE",
        "type": "string",
        "title": "Note",
        "maxLength": 1000
      }
    }
  }
}
```

**Тело ответа: JSON схема для множественного назначения вердиктов**


```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
 "type": "array",
 "title": "Array result",
 "items": {
   "$id": "#/items",
   "type": "object",
   "title": "Result setting user decision schema",
   "required": [
     "OBJECT_ID",
     "TBS_ID",
     "VERDICT",
     "USER_DECISION",
     "FORWARD_STATE_CODE"
   ],
   "properties": {
     "OBJECT_ID": {
       "$id": "#/items/properties/OBJECT_ID",
       "type": "integer",
       "title": "ID События"
     },
     "TBS_ID": {
       "$id": "#/items/properties/TBS_ID",
       "type": "integer",
       "title": "ID табличного пространства"
     },
     "VERDICT": {
       "$id": "#/items/properties/VERDICT",
       "type": "string",
       "title": "Вердикт",
       "enum": [
         "Allowed",
         "Quarantined",
         "Forbidden"
       ]
     },
     "USER_DECISION": {
       "$id": "#/items/properties/USER_DECISION",
       "type": "string",
       "title": "Проставленное решение пользователя",
       "enum": [
         "NotProcessed",
         "NoViolation",
         "Violation",
         "AdditionalProcessingNeeded"
       ]
     },
     "FORWARD_STATE_CODE": {
       "$id": "#/items/properties/FORWARD_STATE_CODE",
       "type": "string",
       "title": "Статус отправки",
       "examples": [
         "Sent",
         "NotSent",
         "Pending"
```

```
        ]
      }
    }
  }
}
```

**Пример:**

```
curl 'https://example.com/xapi/event/userDecision' \
  -X PATCH \
  -H 'X-API-Auth-Token: 1792jmclf7fer1ikuhby' \
  -H 'X-API-Version: 1' \
  -H 'X-API-CompanyId: IW' \
  -H 'X-API-ImporterName: dome' \
  -H 'Content-Type: application/json' \
  --data-binary '[{"OBJECT_ID": 1, "TBS_ID": 1,
"USER_DECISION":"Violation","NOTE":"Проставление вердикта через Dome. Сотрудник Иванов
Виктор Павлович."},{"OBJECT_ID": 24, "TBS_ID": 2,
"USER_DECISION":"AdditionalProcessingNeeded"}]'
```

## Получение списка пользователей консоли

**Описание**: Список пользователей консоли Traffic Monitor (включая бывших сотрудников)

**Метод**: `GET`

**Ресурс**: `user`

**Параметры** (передаются в виде JSON):

- `start` - с какой позиции начать отдавать данные пользователей (по умолчанию 0)
- `limit` - сколько комплектов данных пользователей отдавать (по умолчанию 100, не может быть больше 1000)

**JSON-схема отдачи списка пользователей**

```
schemas:
    user:
      type: object
      additionalProperties: false
      properties:
        USER_ID:
          type: integer
          description: User ID
        USERNAME:
          type: string
          description: Login
        DISPLAY_NAME:
          type: string
          description: Full name
        STATUS:
          type: integer
          description: Status (0 - active, 1 - disabled, 2 - deleted)
          enum: [0, 1, 2]
```

```
        CREATE_DATE:
          type: string
          description: Create Date with format "Y-m-d H:i:s.u" in UTC
        EMAIL:
          type: string
          description: E-mail
        NOTE:
          type: string
          description: Note
```

**Пример:**

**Запрос**

```
curl -X GET "https://qa-b2a1.infowatch.ru/xapi/user?start=1&limit=100" -H "accept: application/json" -H "X-Enable-OpenAPI: 1"
```

**Ответ**


```
{
  "data": [
    {
      "USER_ID": 0,
      "USERNAME": "string",
      "DISPLAY_NAME": "string",
      "STATUS": 0,
      "CREATE_DATE": "string",
      "EMAIL": "string",
      "NOTE": "string"
    }
  ],
  "meta": {
    "totalCount": 0,
    "start": 0,
    "limit": 0
  }
}
```


## Получение результатов выполнения запроса Traffic Monitor

Получение списка запросов

**Описание**: Список запросов Traffic Monitor

**Метод**: `GET`

**Ресурс**: `query`

**Параметры** (передаются в виде JSON):

- `userId` - id пользователя, список запросов которого требуется получить
- `start` - с какой позиции начать отдавать запросы (по умолчанию 0)
- `limit` - сколько запросов отдавать (по умолчанию 100, не может быть больше 1000)

По запросу будет предоставлен список уже существующих в TM запросов с указанием ID запроса и его текстовым именем.

**JSON-схема отдачи списка запросов:**

```
  "data": [
   {
     "QUERY_ID": 0,
     "DISPLAY_NAME": "string"
   }
 ],
 "meta": {
   "totalCount": 0,
   "start": 0,
   "limit": 0
 }
```

**Пример запроса:**

```
curl -X GET "https://server.company.ru/xapi/query?userId=5&start=0&limit=10" -H "accept: application/json"
 -H "X-Enable-OpenAPI: 1"
```

Запуск запроса на выполнение

**Описание**: Запуск запроса на выполнение в Traffic Monitor

**Метод**: `POST`

**Ресурс**: `query/{queryId}/exec`

**Параметры**:

- `queryId` - id запроса, который требуется запустить

**JSON-схема ответа на запуск запроса:**

```
{
 "data": {
   "QUERY_ID": 0,
   "QUERY_TYPE": "query",
   "DISPLAY_NAME": "string",
   "CREATE_DATE": "string",
   "CHANGE_DATE": "string"
 }
}
```

**Пример запроса:**

```
curl -X POST "https://server.conpany.ru/xapi/query/0/exec" -H "accept: application/json" -H "X-Enable-OpenAPI: 1"
```

Получение статуса запроса

**Описание**: Получение статуса запроса

**Метод**: `GET`

**Ресурс**: `query/{queryId}/status`

**Параметры**:

- `queryId` - id запроса, статус которого требуется получить

**JSON-схема ответа:**

```
{
  "data": {
    "QUERY_ID": 0,
    "USER_ID": 0,
    "STATUS": 0,
    "RUN_DATE": "string",
    "COMPLETE_DATE": "string",
    "PERCENT_COMPLETE": 0,
    "OBJECT_COUNT": 0
  }
}
```

**Пример запроса:**

```
curl -X GET "https://server.company.ru/xapi/query/0/status" -H "accept: application/json" -H "X-Enable-OpenAPI: 1"
```

Получение результатов запроса

**Описание**: Список с результатами запросов Traffic Monitor

**Метод**: `GET`

**Ресурс**: `query/{queryId}/result`

**Параметры** (передаются в виде JSON):

- `queryId` - id запроса;
- `start` - с какой позиции начать отдавать запросы (по умолчанию 0)
- `limit` - сколько запросов отдавать (по умолчанию 100, не может быть больше 1000)

- `fields:`
  - `OBJECT_ID –` идентификатор события в ТМ (положительное целое число);
  - `TBS_ID –` идентификатор табличного пространства (положительное целое число).

В ответ на ранее инициированный запрос (см. "Запуск запроса на выполнение") будет предоставлен список событий с указанием их ID.

**JSON-схема ответа:**

```
{
  "data": [
    {
      "OBJECT_ID": 0,
      "TBS_ID": 0
    }
  ],
  "meta": {
    "totalCount": 0,
    "start": 0,
    "limit": 0
  }
}
```

**Пример запроса:**

```
curl -X GET "https://server.company.ru/xapi/query/5/result?start=0&limit=10" -H "accept: application/json"
 -H "X-Enable-OpenAPI: 1"
```

# 10 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.

**Общие рекомендации**
Не рекомендуется начинать имена и пароли пользователей с последовательностей: SYS_ и ORA_.
В составе имени и пароля пользователя не рекомендуется использовать зарезервированные слова СУБД Oracle:

| | | | | |
|---|---|---|---|---|
| ACCESS | DELETE | INTERSECT | OPTION | SUCCESSFUL |
| ADD | DESC | INTO | OR | SYNONYM |
| ALL | DISTINCT | IS | ORDER | SYSDATE |
| ALTER | DROP | LEVEL | PCTFREE | TABLE |
| AND | ELSE | LIKE | PRIOR | THEN |
| ANY | EXCLUSIVE | LOCK | PRIVILEGES | TO |
| AS | EXISTS | LONG | PUBLIC | TRIGGER |
| ASC | FILE | MAXEXTENTS | RAW | UID |
| AUDITBETWEEN | FLOAT | MINUS | RENAME | UNION |

| | | | | |
|---|---|---|---|---|
| BY | FOR | MLSLABEL | RESOURCE | UNIQUE |
| CHAR | FROM | MODE | REVOKE | UPDATE |
| CHECK | GRANT | MODIFY | ROW | USER |
| CLUSTER | GROUP | NOAUDIT | ROWID | VALIDATE |
| COLUMN | HAVING | NOCOMPRESS | ROWNUM | VALUES |
| COMMENT | IDENTIFIED | NOT | ROWS | VARCHAR |
| COMPRESS | IMMEDIATE | NOWAIT | SELECT | VARCHAR2 |
| CONNECT | IN | NULL | SESSION | VIEW |
| CREATE | INCREMENT | NUMBER | SET | WHENEVER |
| CURRENT | INDEX | OF | SHARE | WHERE |
| DATE | INITIAL | OFFLINE | SIZE | WITH |
| DECIMAL | INSERT | ON | SMALLINT | |
| DEFAULT | INTEGER | ONLINE | START | |

# 11 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<br>🟡 – хотя бы одна цифра превышает соответствующее значение 10.0,8.0,6.0 за 15, 5, 1<br>🟢 – 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:<br>1. Выполните: `top`<br>2. Отсортируйте результаты:<br>a. Shift+m - по загрузке ОЗУ;<br>b. Shift+p - по загрузке ЦП. |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| Состояние компонентов Системы | Статусы служб системы | 30 мин. | 🔴 – хотя бы один сервис не запущен<br>🟢 – 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<br>🟢 – запущен | Проверьте запуск службы rsyslog: `systemctl status rsyslog`<br>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<br>🟡 – от 20 до 50<br>🟢 – < 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<br>🟢 – нет ошибок | Необходимо снизить количество ошибок с SEVERITY=HIGH.<br>**Поиск в Alert Log должен осуществляться по наличию слов:**<br>• ORA-<br>• Failed to archive<br>• ORACLE Instance .* - Archival Error<br>• ARC[0-9]: I/O error<br>• ARC[0-9]: RFS network |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | connection lost at host<br>• ARC[0-9]: Error 3113 creating<br>• Media Recovery failed with error<br>• Corrupt block<br>• Fractured block<br>• Bad header<br>• Data in bad block<br>• Reread of rdba<br>• log corruption<br>• RESETLOGS<br>**Поиск в pg_log должен осуществляться по наличию слов:**<br>• FATAL<br>• PANIC<br>• ERROR |
| Доступность сервера | Время ответа на посылаемые пакеты и количество потерянных пакетов (Linux-серверы) | 5 мин. | 🔴 – > 500 мс<br>🟡 – от 100 до 500 мс<br>🟢 – < 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 Postfix | 30 мин. | 🔴 – не доступен<br>🟢 – доступен | 1. Проверьте состояние сервера Postfix: `systemctl status postfix`<br>2. Запустите проверку конфигурационного файла */etc/postfix/main.cf* на |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | правильность: `postfix check` |
| Доступность сервера по SSH | Время ответа на запрос | 10 мин. | 🔴 – >= 10 с<br>🟢 – < 10 с | Проверьте состояние демона sshd: `systemctl status sshd` |
| Доступность сервера Device Monitor | Ответа на запрос | 30 мин. | 🔴 – нет соединения<br>🟢 – 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%<br>🟡 – свободно от 50% до 10%<br>🟢 – свободно > 50% | 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<br>🟡 – от 10 000 МБ до 20 000 Мб<br>🟢 – > 20 000 Мб | |
| Свободное место в партиции /var | Количество свободного места в файловой системе `/var.(` Linux-серверы) | 30 мин. | 🔴 – < 10 000 Мб<br>🟡 – от 10 000 Мб до 20 000 Мб<br>🟢 – > 20 000 Мб | |

| **Название индикатора** | **Что проверяется и где проверяется** | **Периодичность опроса** | **Значения индикатора** | Подробности и рекомендации |
|---|---|---|---|---|
| Состояние службы синхронизации времени | Статус сервиса ntpd. (NTPD) | 30 мин. | 🔴 – NTP сервер не доступен<br>🟢 – 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<br>🟡 – от 20 до 40 с<br>🟢 – < 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<br>🟢 – нет дампов | Обратитесь в службу технической поддержки InfoWatch по адресу<br><br>support@infowatch.com |
| Очередь ошибок обработки событий | Количество объектов в очереди **queue/final-errors** (iw_rammer) | 1 мин. | 🔴 – > 1<br>🟢 – 0 | **Вариант 1:** Очистите очереди, используя команды:<br>`su - iwtm`<br>`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/final-errors`<br>`exit`<br>**Вариант 2:** |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | 1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`<br>2. Уменьшите период очистки файлов в папках файловой очереди в штатном задании cron (значение по умолчанию - 30 дней).<br>3. Сохраните изменения и закройте файл.<br><br>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<br>🟢 – ok | Проверьте, доступна ли БД:<br>1. Зайдите в БД: `sqlplus iwtm@iwtm`<br>2. Введите пароль: xxXX1234<br>3. Наблюдайте: `SQL>` |
| Статус службы доступа к базе данных | Статус TNS listener'а oracle. | 10 мин. | 🔴 – TNS listener не запущен<br>🟢 – TNS listener запущен | Индикатор включен и отображается в списке, только если в Системе используется СУБД Oracle |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| Количество файлов данных Oracle | Превышение количества файлов в 90% от настроенного максимального количества файлов данных | 60 мин. | 🔴 – если текущее значение количества файлов равно максимальному<br>🟡 – если это значение составляет более 90% от максимального<br>🟢 – если это значение составляет менее 90% от максимального | Если количество файлов данных достигнет максимального значения, следует увеличить параметр Oracle db_files |
| Свободное место в основном каталоге БД | Свободное место на партиции хранения основной информации (По умолчанию: `/u01`) | 30 мин. | 🔴 – < 10 000 Мб<br>🟡 – от 10000 до 20 000 Мб<br>🟢 – > 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%<br>🟡 – от 7 до 15% (если для хранения ежедневных ТП используются несколько разделов, то при значении < 7% хотя бы в одном разделе)<br>🟢 – > 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<br>Подробнее см. "Рекомендации по разбиению дискового пространства серверов при |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | 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%<br>🟡 – от 7 до 15%<br>🟢 – > 15% | Индикатор добавляется, если при установке был выбран режим хранения данных *Быстрые и медленные диски*<br>Подробнее см. "Рекомендации по разбиению дискового пространства серверов при установке в разных режимах" |
| Наличие патчей БД | Наличие установленных патчей Oracle, необходимых для корректной работы Системы | 1 раз в сутки | 🔴 – не установлен<br>🟢 – установлен | Индикатор включен и отображается в списке, только если в Системе используется СУБД Oracle. Скачайте и установите требуемый патч. |
| Размер журнала предупреждений БД | Размер журнала предупреждений для СУБД PostgreSQL: System LogРазмер журнала предупреждений для СУБД Oracle: Alert Log | 5 мин. | 🔴 – > 3 Гб<br>🟡 – от 1 Гб до 3 Гб<br>🟢 – < 1 Гб | Обратитесь в службу технической поддержки InfoWatch по адресу<br>support@infowatch.com |
| Наличие ошибок в журнале базы данных | Наличие ошибок | 30 мин. | 🔴 – > 1<br>🟡 – 1<br>🟢 – нет ошибок | Необходимо снизить количество ошибок с SEVERITY=Error |
| Очередь обработки почтового трафика | Количество объектов в очереди **queue/smtp** (iw_messed) | 30 мин. | 🔴 – > 10000 объектов | 1. Проверьте статус службы: `systemctl` |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | 🟡 – от 1000 до 10000 объектов<br>🟢 – < 1000 объектов | `status iw_messed`<br>2. Просмотрите логи службы в `opt/iw/tm5/log/messed_app.log`<br>3. Проверьте нагрузку на оперативную память и swap:<br>a. для краткого вывода выполните: `free -m`<br>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<br>🟡 – от 1000 до 10000 объектов<br>🟢 – < 1000 объектов | 1. Проверьте статус службы: `systemctl status iw_analysis`<br>2. Просмотрите логи службы в `opt/iw/tm5/log/analysis.log`<br>3. Проверьте нагрузку на оперативную память и swap:<br>a. для краткого вывода выполните: `free -m`<br>b. для расширенного вывода выполните: |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | `cat /proc/meminfo` |
| Очередь загрузки объектов от перехватчиков в сервис **iw_x2x** | Количество объектов от перехватчиков для **iw_x2x** в очереди **queue/db** (iw_x2x) | 30 мин. | 🔴 – > 10000 объектов<br>🟡 – от 1000 до 10000 объектов<br>🟢 – < 1000 объектов | 1. Проверьте статус службы: `systemctl status iw_x2x`<br>2. Просмотрите логи службы в `opt/iw/tm5/log/x2x.log`<br>3. Проверьте нагрузку на оперативную память и swap:<br>a. для краткого вывода выполните: `free -m`<br>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<br>🟡 – от 1000 до 10000 объектов<br>🟢 – < 1000 объектов | 1. Проверьте статус службы: `systemctl status iw_x2db`<br>2. Просмотрите логи службы в `opt/iw/tm5/log/x2db.log`<br>3. Проверьте нагрузку на оперативную память и swap:<br>a. для краткого вывода выполните: `free -m`<br>b. для расширенного вывода |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | выполните: `cat /proc/meminfo` |
| Очередь обработки действий от примененных политик | Количество объектов в очереди **queue/blackboard** (Linux-серверы) | 30 мин. | 🔴 – > 1000 объектов<br>🟡 – от 200 до 1000 объектов<br>🟢 – < 200 объектов | 1. Проверьте статус службы: `systemctl status iw_analysis`<br>2. Просмотрите логи службы в `opt/iw/tm5/log/analysis.log`<br>3. Проверьте нагрузку на оперативную память и swap:<br>a. для краткого вывода выполните: `free -m`<br>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<br>🟡 – от 1000 до 10000 объектов<br>🟢 – < 1000 объектов | 1. Проверьте статус службы: `searchd --status -c /etc/infowatch/sphinx.conf`<br>2. Просмотрите логи службы в `opt/iw/tm5/log/sphinx/`<br>3. Проверьте нагрузку на |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | оперативную память и swap:<br>a. для краткого вывода выполните: `free -m`<br>b. для расширенного вывода выполните: `cat /proc/meminfo`<br>4. Вычислите количество запущенных экземпляров searchd:<br>a. если на ноде запущен iw_is, то: 1 (сам iw_is)+ 4 (grep max_children /opt/iw/tm5/etc/is.conf)=5<br>b. если на ноде запущен iw_indexer, то: 1 (сам iw_ndexer)+ 8 (grep max_children /opt/iw/tm5/etc/sphinx.conf )=9<br>c. Итого: a+b=14 экземпляров searchd. Чем больше процессов, тем меньше вероятность длительного |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | 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<br>🟡 – от 1000 до 10000 объектов<br>🟢 – < 1000 объектов | 1. Проверьте статус службы: `searchd --status -c /etc/infowatch/sphinx.conf`<br>2. Просмотрите логи службы в `opt/iw/tm5/log/sphinx/`<br>3. Проверьте нагрузку на оперативную память и swap:<br>a. для краткого вывода выполните: `free -m`<br>b. для расширенного вывода выполните: `cat /proc/meminfo` |
| Количество ошибок индексации событий службой **iw_indexer** | Количество ошибок индексации (iw_indexer) | 30 мин. | 🔴 – > 100 ошибок<br>🟡 – от 10 до 100<br>🟢 – 10 | 1. Проверьте статус службы: `systemctl status iw_indexer`<br>2. Просмотрите логи службы в `opt/iw/tm5/log/indexer.log`<br>3. Проверьте нагрузку на |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | оперативную память и swap:<br>a. для краткого вывода выполните: `free -m`<br>b. для расширенного вывода выполните: `cat /proc/meminfo` |
| Количество ошибок индексации метаинформации службой **iw_is** | Количество ошибок индексации метаинформации службой **iw_is** | 30 мин. | 🔴 – > 100 ошибок<br>🟡 – от 10 до 100 ошибок<br>🟢 – 10 ошибок | 1. Проверьте статус службы: `systemctl status iw_is`<br>2. Просмотрите логи службы в `opt/iw/tm5/log/is.log`<br>3. Проверьте нагрузку на оперативную память и swap:<br>a. для краткого вывода выполните: `free -m`<br>b. для расширенного вывода выполните: `cat /proc/meminfo` |
| Очередь команд **iw_is** | Количество команд в очереди службы **iw_is** | 30 мин. | 🔴 – > 100 команд<br>🟡 – от 50 до 100 команд<br>🟢 – < 50 команд | |
| Очереди выборки данных | Количество объектов в очереди службы **iw_is** | 30 мин. | 🔴 – > 100 объектов<br>🟡 – от 50 до 100 объектов<br>🟢 – < 50 объектов | |
| Очередь индексации **iw_is** | Количество объектов в очереди службы **iw_is** | 30 мин. | 🔴 – > 100 объектов<br>🟡 – от 50 до 100 объектов<br>🟢 – < 50 объектов | |
| Очередь ошибок **iw_is** | Наличие ошибок сервиса **iw_is** | 5 мин. | 🔴 – > 500<br>🟡 от 50 до 500<br>🟢 – < 50 | |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| Очередь команд для табличного пространства текста | Количество команд в очереди табличного пространства текста | 30 мин. | 🔴 – > 50 команд<br>🟡 – от 20 до 50 команд<br>🟢 – < 20 команд | 1. Включите логирование работы службы **iw_indexer** на `debug` (см. "Логирование работы Системы")<br>2. Просмотрите лог-файл **iw_indexer** на ошибки в `opt/iw/tm5/log/indexer.log`<br>3. Обратитесь в службу технической поддержки InfoWatch |
| Очередь команд для табличного пространства метаинформации | Количество команд в очереди табличного пространства метаинформации | 30 мин. | 🔴 – > 50 команд<br>🟡 – от 20 до 50 команд<br>🟢 – < 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. | 🔴 – > 500 объектов<br>🟡 – от 50 до 500 объектов<br>🟢 – < 50 объектов | **Вариант 1:** Очистите очередь, используя команды:<br>`su - iwtm`<br>`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/errors`<br>`exit`<br>**Вариант 2:**<br>1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`<br>2. Уменьшите период очистки файлов в папках файловой очереди в штатном задании cron (значение по |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | умолчанию - 30 дней).<br>3. Сохраните изменения и закройте файл. |
| Очередь ошибок обработки событий сервисом **iw_x2x** | Количество объектов в очереди **queue/x2x-errors** (iw_x2x) | 30 мин. | 🔴 – > 500 объектов<br>🟡 – от 50 до 500 объектов<br>🟢 – 50 | **Вариант 1:** Очистите очередь, используя команды:<br>`su - iwtm`<br>`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/x2x-errors`<br>`exit`<br>**Вариант 2:**<br>1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`<br>2. Уменьшите период очистки файлов в папках файловой очереди в штатном задании cron (значение по умолчанию - 30 дней).<br>3. Сохраните изменения и закройте файл. |
| Очередь ошибок обработки событий сервисом **iw_x2db** | Количество объектов в очереди **queue/x2db-errors** (iw_x2db) | 30 мин. | 🔴 – > 500 объектов<br>🟡 – от 50 до 500 объектов<br>🟢 – 50 | **Вариант 1:** Очистите очередь, используя команды:<br>`su - iwtm`<br>`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/x2db-errors` |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | `exit`<br>**Вариант 2:**<br>1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`<br>2. Уменьшите период очистки файлов в папках файловой очереди в штатном задании cron (значение по умолчанию - 30 дней).<br>3. Сохраните изменения и закройте файл. |
| Очередь ошибок обработки действий примененных политик | Количество объектов в очереди **queue/blackboard_errors** (Linux-серверы) | 30 мин. | 🔴 – > 500 объектов<br>🟡 – от 50 до 500 объектов<br>🟢 – 50 | **Вариант 1:** Очистите очередь, используя команды:<br>`su - iwtm`<br>`/opt/iw/tm5/bin/iw_qtool erase /opt/iw/tm5/queue/blackboard-errors`<br>`exit`<br>**Вариант 2:**<br>1. Откройте на редактирование файл `/etc/cron.d/iwtm_cleanup.`<br>2. Уменьшите период очистки файлов в папках файловой очереди в штатном задании cron (значение по |

| Название индикатора | Что проверяется и где проверяется | Периодичность опроса | Значения индикатора | Подробности и рекомендации |
|---|---|---|---|---|
| | | | | умолчанию - 30 дней).<br>3. Сохраните изменения и закройте файл. |