

INFOWATCH

InfoWatch Traffic Monitor 6.1

Руководство администратора

InfoWatch Traffic Monitor 6.1

Руководство администратора

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

Дата редакции: 2016-08-08

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ ... 8

1.1 Аудитория ... 8
1.2 Комплект документов ... 8
1.3 Техническая поддержка пользователей ... 8

2 ОБЗОР TRAFFIC MONITOR ... 10

2.1 Функции InfoWatch Traffic Monitor ... 10
2.1.1 Перехват трафика в потоке/на шлюзе ... 10
2.1.1.1 SMTP-трафик ... 11
2.1.1.2 POP3-трафик ... 14
2.1.1.3 HTTP-трафик ... 14
2.1.1.4 HTTPS-трафик ... 18
2.1.1.5 ICQ-трафик ... 20
2.1.1.6 NRPC-трафик ... 21
2.1.1.7 IMAP4-трафик ... 22
2.1.1.8 FTP/Skype/Печать/Копирование на съемные носители/Jabber (XMPP)/Yahoo/Mail.ru (MMP) ... 23
2.1.2 Анализ информации на файловых ресурсах внутрикорпоративной сети ... 23
2.1.3 Обработка трафика, полученного от сторонних Систем ... 23
2.2 Состав InfoWatch Traffic Monitor ... 24
2.3 Лицензирование ... 25

3 НАСТРОЙКА СИСТЕМЫ ПОСЛЕ УСТАНОВКИ ... 29

3.1 Настройка синхронизации времени ... 29
3.2 Конфигурирование работы Sphinx при распределенной установке ... 30
3.3 Общие настройки ... 30
3.3.1 SPAN, или Port Mirroring ... 31
3.3.1.1 Настройка работы сервера Traffic Monitor в качестве Sniffer ... 31
3.3.1.2 Настройка сервера Traffic Monitor на прием копии трафика от Sniffer ... 32
3.3.1.3 Создание кластера Traffic Monitor ... 33
3.3.2 Перехват трафика, передаваемого по протоколу ICAP ... 35
3.3.2.1 Настройка ICAP ... 36
3.3.2.2 Рекомендации по настройке Blue Coat SG Series ... 37
3.3.2.3 Рекомендации по настройке SQUID ... 38
3.3.2.3.1 Установка SQUID ... 38
3.3.2.3.2 Настройка ICAP ... 38
3.3.2.3.3 Настройка перехвата и раскрытия SSL ... 39
3.3.2.3.4 Настройка аутентификации пользователей ... 40
3.3.2.4 Рекомендации по настройке Cisco Iron Port ... 41
3.3.2.5 Рекомендации по настройке McAfee Web Gateway ... 43
3.3.2.6 Отключение ICAP ... 45
3.3.3 Настройка работы "в разрыв" для нескольких перехватчиков ... 45
3.4 Настройка перехвата трафика ... 46
3.4.1 SMTP-трафик ... 47
3.4.1.1 SPAN, или Port Mirroring ... 47
3.4.1.2 Прием копий с почтового сервера ... 47
3.4.1.3 "В разрыв" ... 48
3.4.1.4 Общие настройки для SMTP-трафика ... 51
3.4.1.4.1 Настройка пересылки скрытых копий Microsoft Exchange Server 2007 и 2010 ... 51
3.4.1.4.2 Настройка пересылки скрытых копий ZCS Zimbra ... 53
3.4.1.4.3 Настройка пересылки скрытых копий MDaemon ... 54
3.4.1.4.4 Настройка сервера Postfix в системе Traffic Monitor ... 55
3.4.2 POP3-трафик ... 58
3.4.3 HTTP-трафик ... 58
3.4.3.1 SPAN, или Port Mirroring ... 58
3.4.3.2 "В разрыв" ... 59

3.4.4 HTTPS-трафик ... 59
3.4.4.1 "В разрыв" ... 59
3.4.5 ICQ-трафик ... 60
3.4.5.1 SPAN, или Port Mirroring ... 60
3.4.6 NRPC-трафик ... 60
3.4.6.1 SPAN, или Port Mirroring ... 60
3.4.7 IMAP4-трафик ... 61
3.4.8 Прием объектов, перехваченных InfoWatch Device Monitor ... 61
3.4.9 Проверка файлов, находящихся в корпоративной сети ... 61
3.5 Автозапуск процессов ... 62
3.5.1 Проверка автозапуска процессов ... 62
3.5.2 Включение и выключение автозапуска процессов ... 64
3.6 Настройка OCR-экстракторов ... 65
3.7 Настройка отправки уведомлений пользователям и сотрудникам ... 66
3.8 Ограничение количества найденных событий ... 67

4 РАБОТА В КОНСОЛИ УПРАВЛЕНИЯ ... 68

4.1 Вход в веб-консоль и выход из нее ... 68
4.2 Управление интеграцией с LDAP каталогами ... 69
4.2.1 Создание подключения к серверу ... 70
4.2.2 Редактирование подключения к серверу ... 71
4.2.3 Удаление подключения к серверу ... 71
4.2.4 Запуск синхронизации с сервером вручную ... 71
4.3 Управление пользователями Системы и их ролями ... 72
4.3.1 Пользователи ... 72
4.3.1.1 Создание учетной записи пользователя ... 73
4.3.1.2 Редактирование учетной записи пользователя ... 74
4.3.1.3 Удаление учетной записи пользователя ... 74
4.3.1.4 Изменение пароля учетной записи пользователя ... 74
4.3.1.5 Изменение статуса учетной записи пользователя ... 75
4.3.1.6 Импорт учетной записи пользователя ... 75
4.3.1.7 Задание пользователю роли ... 76
4.3.1.8 Задание пользователю области видимости ... 76
4.3.2 Роли ... 76
4.3.2.1 Создание роли ... 77
4.3.2.2 Редактирование роли ... 78
4.3.2.3 Удаление роли ... 79
4.3.3 Области видимости ... 79
4.3.3.1 Создание области видимости ... 80
4.3.3.2 Редактирование области видимости ... 82
4.3.3.3 Удаление области видимости ... 82
4.4 Управление лицензиями ... 83
4.4.1 Проверка валидности лицензии ... 84
4.4.2 Установка лицензии ... 85
4.4.3 Удаление лицензии ... 85
4.4.4 Запрос лицензии ... 85
4.5 Состояние системы ... 86
4.5.1 Настройка параметров отправки уведомлений ... 87
4.6 Управление службами ... 88
4.6.1 Запуск службы ... 88
4.6.2 Остановка службы ... 88
4.6.3 Перезапуск службы ... 89
4.6.4 Сохранение логов службы ... 89
4.7 Сбор диагностических данных ... 89
4.7.1 Сбор диагностических данных в обычном режиме ... 91
4.7.2 Сбор диагностических данных в расширенном режиме ... 91
4.8 Аудит действий пользователя ... 91

4.8.1 События аудита ... *92*
4.8.1.1 Расширенная информация ... 93
4.8.2 Фильтрация по пользователю ... *93*
4.8.3 Фильтрация по действию ... *94*
4.8.4 Фильтрация по объекту ... *94*
4.8.5 Фильтрация по дате ... *94*
4.9 Контроль целостности ... 95
4.9.1 Ручная проверка целостности ... *95*
4.9.2 Автоматическая проверка целостности ... *95*
4.9.3 Принятие результата за эталонный ... *95*
4.10 Плагины ... 96
4.10.1 Добавление плагина ... *98*
4.10.2 Удаление плагина ... *98*
4.10.3 Работа с токенами ... *98*
4.10.3.1 Добавление токена ... 99
4.10.3.2 Удаление токена ... 99

5 КОНФИГУРИРОВАНИЕ ПЕРЕХВАТЧИКА CRAWLER ... 100

5.1 Настройка сетевых правил доступа ... 100
5.2 Конфигурационные файлы Краулер ... 102
5.2.1 Конфигурационный файл сервера Краулер ... *103*
5.2.1.1 Изменение учетной записи, от имени которой запускается служба сервера Краулер ... 103
5.2.1.2 Скрипты сканирования SharePoint ... 104
5.2.2 Конфигурационный файл сканера Краулер ... *104*
5.2.3 Выключение шифрования трафика между компонентами ... *105*
5.3 Работа с журналами Краулер ... 105
5.4 Автоматическое удаление событий Краулер ... 106

6 МОНИТОРИНГ ... 108

6.1 Настройки подсистемы мониторинга ... 108
6.1.1 Настройка подключения Device Monitor ... *109*
6.1.2 Ручная настройка индикаторов ... *109*
6.1.3 Настройка адреса сервера синхронизации времени для подсистемы мониторинга ... *109*
6.1.4 Настройка порогов срабатывания для индикатора нагрузки ... *110*
6.1.5 Настройка механизма уведомлений ... *110*
6.1.5.1 Настройка отправки уведомлений о превышении порогового значения индикаторов ... 110
6.1.5.2 Настройка отправки писем-уведомлений с помощью Postfix ... 112

7 АДМИНИСТРИРОВАНИЕ БАЗЫ ДАННЫХ ... 113

7.1 Oracle ... 113
7.1.1 Проведение регламентных работ на сервере базы данных ... *113*
7.1.2 Табличные пространства в базе данных InfoWatch Traffic Monitor ... *115*
7.1.3 Управление ежедневными табличными пространствами ... *115*
7.1.3.1 Настройка размещения файлов в файловой системе ... 116
7.1.3.2 Индексирование данных в ежедневных табличных пространствах ... 117
7.1.3.3 Архивирование ежедневных табличных пространств ... 119
7.1.3.3.1 Автоматическое архивирование ежедневных табличных пространств ... 119
7.1.3.3.2 Архивирование ежедневных табличных пространств вручную ... 120
7.1.3.4 Восстановление ежедневных табличных пространств ... 122
7.1.3.5 Удаление ежедневных табличных пространств ... 122
7.1.4 Резервное копирование базы данных ... *124*
7.1.4.1 Создание резервной копии базы данных ... 125
7.1.4.1.1 Определение размера резервной копии ... 125
7.1.4.1.2 Проверка хранилища резервной копии ... 126
7.1.4.1.3 Создание папок для резервной копии ... 126
7.1.4.1.4 Создание вспомогательных файлов на Linux ... 126
7.1.4.1.5 Создание списка файлов, подлежащих резервному копированию ... 128

7.1.4.1.6 Остановка системы IWTM 129
7.1.4.1.7 Остановка БД Oracle 129
7.1.4.1.8 Копирование файлов БД в хранилище резервных копий 129
7.1.4.2 Восстановление базы данных из резервной копии 130
7.1.4.2.1 Восстановление на той же БД 130
7.1.4.2.2 Восстановление на новой БД 130
7.2 POSTGRE SQL 131
7.2.1 Табличные пространства в базе данных InfoWatchTraffic Monitor 131
7.2.2 Управление ежедневными табличными пространствами 132
7.2.2.1 Архивирование ежедневных табличных пространств 132
7.2.2.1.1 Автоматическое архивирование ежедневных табличных пространств 133
7.2.2.1.2 Архивирование ежедневных табличных пространств вручную 134
7.2.2.2 Восстановление ежедневных табличных пространств 135
7.2.2.3 Настройка размещения файлов в файловой системе 136
7.2.2.4 Удаление ежедневных табличных пространств 137
7.2.3 Резервное копирование базы данных 139
7.2.3.1 Создание резервной копии базы данных 139
7.2.3.1.1 Определение размера резервной копии 140
7.2.3.1.2 Проверка хранилища резервной копии 140
7.2.3.1.3 Создание каталов для резервной копии 140
7.2.3.1.4 Остановка системы 141
7.2.3.1.5 Остановка Postgre SQL 141
7.2.3.1.6 Копирование файлов БД в хранилище резервных копий 141
7.2.3.2 Восстановление базы данных из резервной копии 142
7.2.3.2.1 Восстановление на той же базе данных 142
7.2.3.2.2 Восстановление на новой базе данных 142

8 АДМИНИСТРИРОВАНИЕ СЕРВЕРНОЙ ЧАСТИ INFOWATCH TRAFFIC MONITOR 143

8.1 ПРОЦЕССЫ СЕРВЕРНОЙ ЧАСТИ TRAFFIC MONITOR SERVER 143
8.1.1 Список процессов серверной части Traffic Monitor 143
8.1.2 Работа с процессами серверной части Traffic Monitor 150
8.2 НАСТРОЙКА КОНФИГУРАЦИОННЫХ ФАЙЛОВ СЕРВЕРНОЙ ЧАСТИ TRAFFIC MONITOR 152
8.2.1 Общие настраиваемые параметры конфигурационных файлов 152
8.2.1.1 Секция Logging 152
8.2.1.2 Секция Startup 153
8.2.1.3 Секция Nookdir 153
8.2.2 Специфичные настраиваемые параметры конфигурационных файлов 153
8.2.2.1 Конфигурационный файл serman_resolver.conf 154
8.2.2.2 Конфигурационный файл sniffer.conf 154
8.2.2.3 Конфигурационный файл proxy.conf 155
8.2.2.3.1 Секция Http 155
8.2.2.3.2 Секция Icq 157
8.2.2.3.3 Секция Smtp 158
8.2.2.4 Конфигурационный файл oracle.conf 158
8.2.2.5 Конфигурационный файл cas.conf 158
8.2.2.5.1 Секция Analysis 159
8.2.2.5.2 Секция ThriftServers 159
8.2.2.5.3 Секция Config 160
8.2.2.6 Конфигурационный файл expressd.conf 160
8.2.2.6.1 Секция Expressd 160
8.2.2.6.2 Секция Expressd, параметр Http 161
8.2.2.6.3 Секция Expressd, параметр Ocr 161
8.2.2.7 Конфигурационный файл messed.conf 162
8.2.2.8 Конфигурационный файл smtpd.conf 162
8.2.2.9 Конфигурационный файл capstack.conf 163
8.2.2.9.1 Секция UsedProcessors 163
8.2.2.9.2 Секция UsedSources 163
8.2.2.10 Конфигурационный файл indexer.conf 164
8.2.2.11 Конфигурационный файл web.conf 164
8.2.2.12 Конфигурационный файл analysis.conf 165

8.2.2.12.1 Секция Analysis 165
8.2.2.12.2 Секция Bookworm 165
8.2.2.13 Конфигурационный файл sample_compiler.conf 166
8.3 Настройка параметров работы с HTTP-запросами, передаваемыми по протоколу ICAP (файл icap.conf) 166
8.4 Настройка параметров обработки архивов вложений 168
8.4.1 Конфигурационный файл extractors.conf 168
8.4.2 Конфигурационный файл extractors.xml 168
8.5 Архивирование каталога очереди сообщений 170
8.6 Логирование работы Системы 171
8.7 Загрузка очередей объектов 172
8.8 Восстановление работоспособности системы в аварийных ситуациях 173
8.9 Управление языками морфологии 174
8.9.1 Добавление нового языка морфологии 174
8.9.2 Обновление установленного языка морфологии 175
8.9.3 Удаление языка морфологии 176
8.10 Настройка serman.conf при изменении адреса сервера БД 176
8.11 Настройка передачи информации в SIEM 177
8.11.1 Настройки на стороне SIEM 177
8.11.1.1 Табличное представление событий ТМ 178
8.11.1.2 Табличное представление аудита пользователей 186
8.11.2 Настройки на стороне ТМ 191
8.11.2.1 Передача логов в SIEM 192
8.11.2.2 Управление логированием сессий пользователей БД ТМ 193
8.11.2.3 Управление пользователем siem 193
8.11.2.3.1 Создание пользователя siem 193
8.11.2.3.2 Смена пароля пользователя siem 194
8.11.2.3.3 Удаление пользователя siem 194
8.11.3 Типы логов, передаваемых в SIEM 195
8.12 Удаление временных файлов 195

9 ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ИМЕН И ПАРОЛЕЙ 197

10 ПРИЛОЖЕНИЕ В. ИНДИКАТОРЫ МОНИТОРИНГА 199

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 пользователя*».

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

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

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

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

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

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: http://www.infowatch.ru/support.html.
Перед обращением в службу технической поддержки мы рекомендуем вам посетить раздел База

знаний на нашем сайте: https://kb.infowatch.com/. Возможно там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

2 ОБЗОР TRAFFIC MONITOR

В этой главе:

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

2.1 Функции InfoWatch Traffic Monitor

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

Основные функции InfoWatch Traffic Monitor:

- Перехват трафика в потоке/на шлюзе, передаваемого по протоколам SMTP, POP3, HTTP, HTTPS, OSCAR (ICQ), NRPC (IBM Notes);
- Анализ Skype-трафика, теневых копий файлов и заданий на печать, передачи трафика по протоколу FTP, контроль обмена данными через Jabber (протокол XMPP), Yahoo (YMSG), через Mail.Ru Агент (протокол MPP);
- Анализ информации, размещенной на файловых ресурсах;
- Обработка трафика, полученного от сторонних Систем;
- Анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности;
- Фильтрация перехваченного трафика путем выдачи разрешения/запрещения на доставку определенных данных.

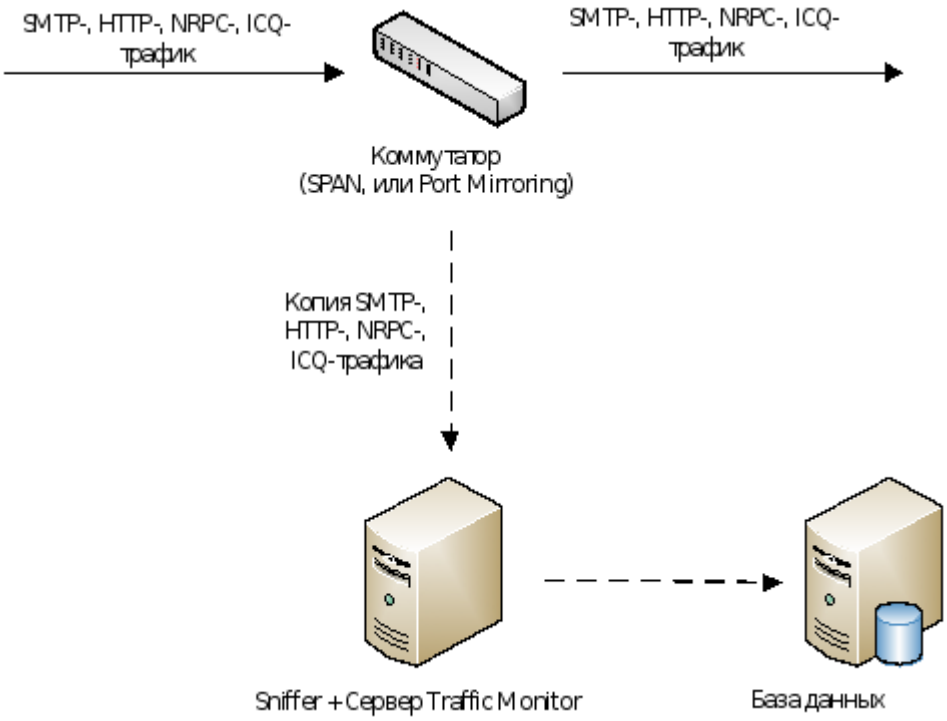
2.1.1 Перехват трафика в потоке/на шлюзе

Раздел содержит информацию о видах трафика и схемах его перехвата:

- SMTP-трафик;
- POP3-трафик;
- HTTP-трафик;
- HTTPS-трафик;
- ICQ-трафик;
- NRPC-трафик;
- IMAP4-трафик;
- FTP/Skype/Печать/Копирование на съемные носители/Jabber (XMPP)/Yahoo/Mail.ru (MMP).

2.1.1.1 SMTP-трафик

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:

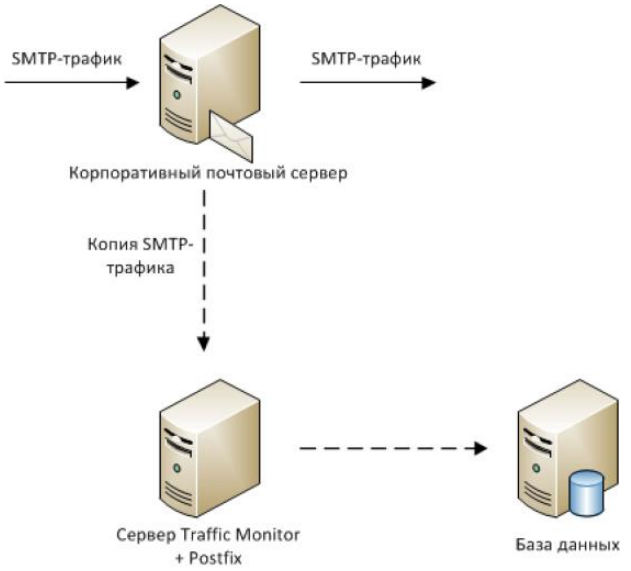
- Способ позволяет безопасно анализировать трафик даже в изолированном сегменте сети. Система никак не может повлиять на анализируемый трафик, независимо от состояния сервера.
- Анализируется также SMTP-трафик внешних серверов (к примеру, трафик Mail.ru, при условии, что используется SMTP-протокол)

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 мониторинга.
- Внутренняя переписка не котролируется.

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. "Примем копий с почтового сервера"

Преимущества:

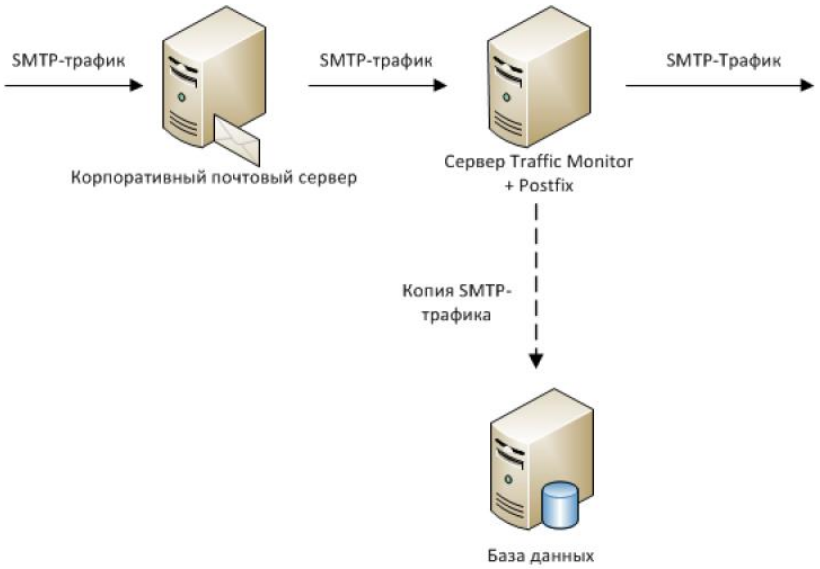
- Позволяет анализировать не только внешнюю, но и внутреннюю переписку компании;
- При использовании MS Exchange 2007 и более новых есть возможность анализировать переписку определенной группы пользователей;
- Гарантирует анализ всех писем.

Недостатки:

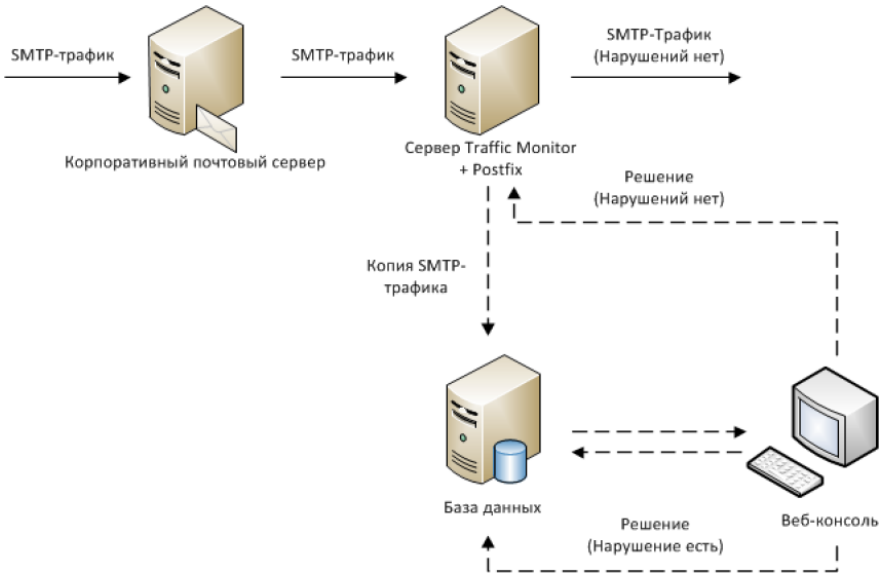
- Требует внесения изменений в настройки корпоративного почтового сервера;
- Никак не контролируются внешние почтовые серверы (если их использование разрешено);
- При недоступности сервера Traffic Monitor, пользователи получат сообщение об ошибке доставки скрытой копии;
- Дополнительная нагрузка на почтовый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

Способ №3

Сервер мониторинга используется как промежуточный почтовый сервер. В состав сервера мониторинга входит почтовый сервер Postfix.



Копия

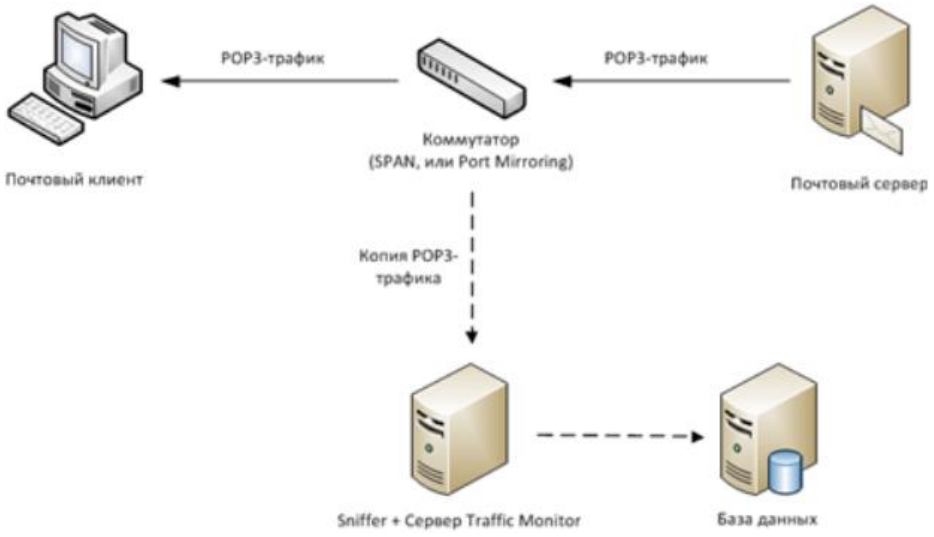


Блокировка
О настройке данного функционала "В разрыв"
Преимущества:
Позволяет включить функционал блокировки почтового трафика
Недостатки:

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

2.1.1.2 POP3-трафик

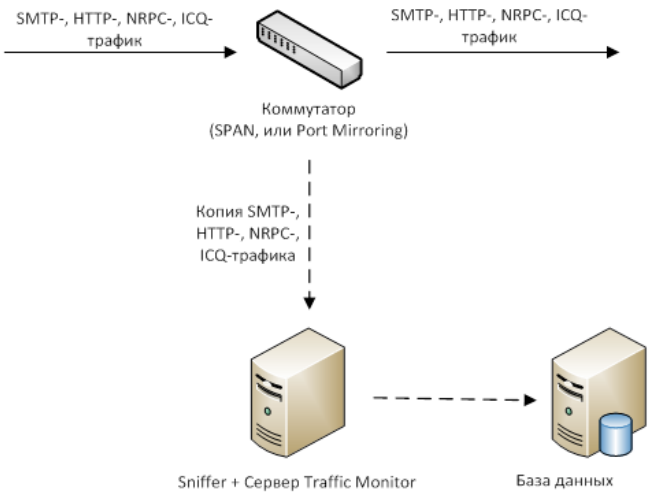
Трафик снимается с управляемого коммутатора по технологии SPAN Port, или Port Mirroring. Большое количество управляемых сетевых коммутаторов позволяют дублировать трафик от одного или нескольких портов или VLAN на отдельно взятый порт.
В данном случае настроенный порт коммутатора подключается к сетевому 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. "POP3-трафик".

2.1.1.3 HTTP-трафик

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 мониторинга.

Частный случай №1:
Если сервер мониторинга находится в виртуальной среде, то в дополнение к настройке порта коммутатора, для мониторинга трафика создаётся 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.

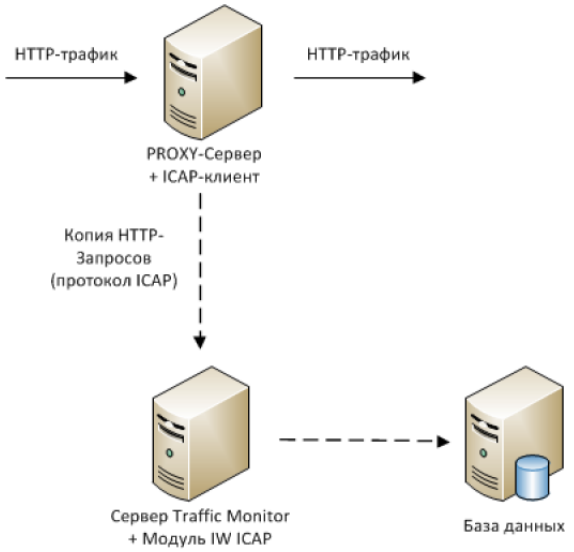
Способ №2:
Копия трафика, передаваемого по протоколу ICAP, снимается с корпоративного прокси-сервера. Сервер Traffic Monitor выступает в качестве ICAP-клиента. Если в компании работает прокси-сервер, поддерживающий ICAP протокол, то можно использовать данный функционал для анализа HTTP-трафика.
Данную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

- Cisco Ironport
- SQUID (при условии, что пакет собран с поддержкой ICAP)

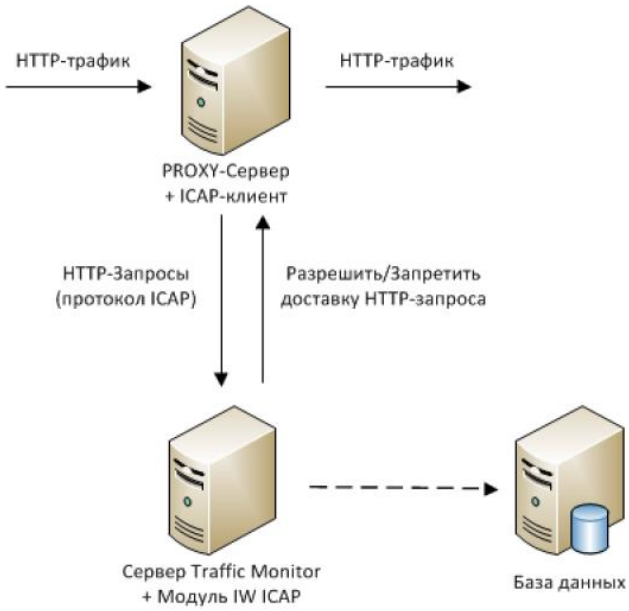
- Blue Coat SG
- MDaemon
- Zimbra ZCS
- Microsoft Forefront Threat Management Gateway 2010 SP2 (требуется установка веб-фильтра)

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.

2.1.1.4 HTTPS-трафик

Важно!

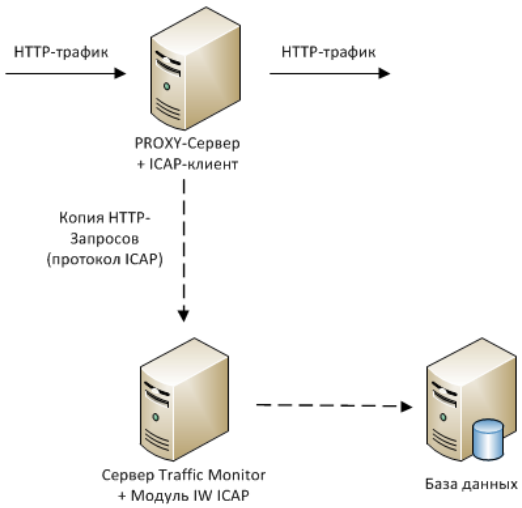
При использовании любого способа анализа HTTPS-трафика требуется соблюдать максимальную осторожность. Технология анализа HTTPS основана на подмене сертификата HTTPS-сессии на сертификат, выданный прокси-сервером (**man-in-the-middle attack**). На машине пользователя обязательно должно быть настроено 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.

Недостатки: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:

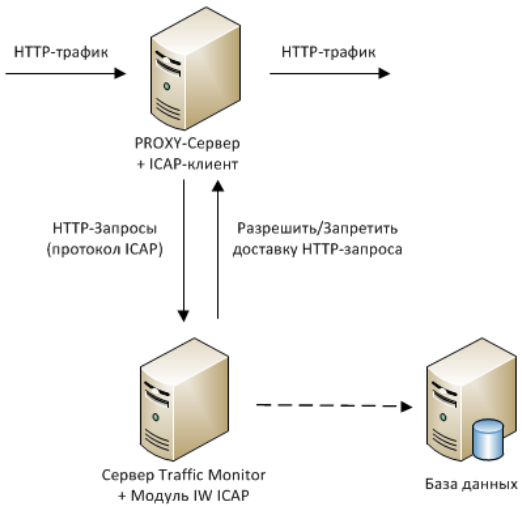
- Cisco Ironport
- SQUID (при условии, что пакет собран с поддержкой ICAP)
- Blue Coat SG
- MDaemon
- Zimbra ZCS
- Microsoft Forefront Threat Management Gateway 2010 SP2 (требуется установка веб-фильтра)

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.

- Нужно учесть потребности всех пользователей, которые пользуются данным прокси-сервером;
- Дополнительная нагрузка на прокси-сервер;

- Требуются серьёзные 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 Device Monitor. Руководство пользователя».
Преимущества:

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

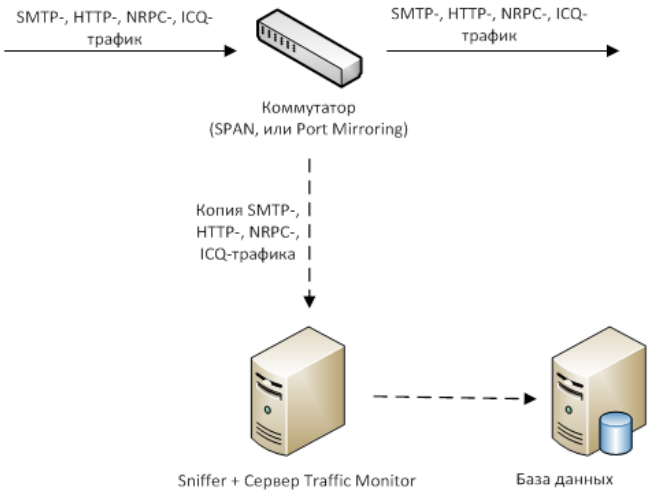
Недостатки:
Нужно предусмотреть потребности пользователя данной машины.

2.1.1.5 ICQ-трафик

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.

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:

- 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 мониторинга.

2.1.1.6 NRPC-трафик

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

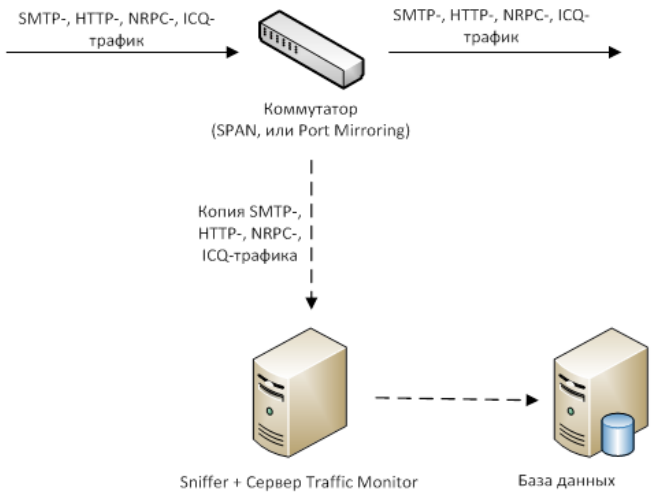
Способ №1:

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:

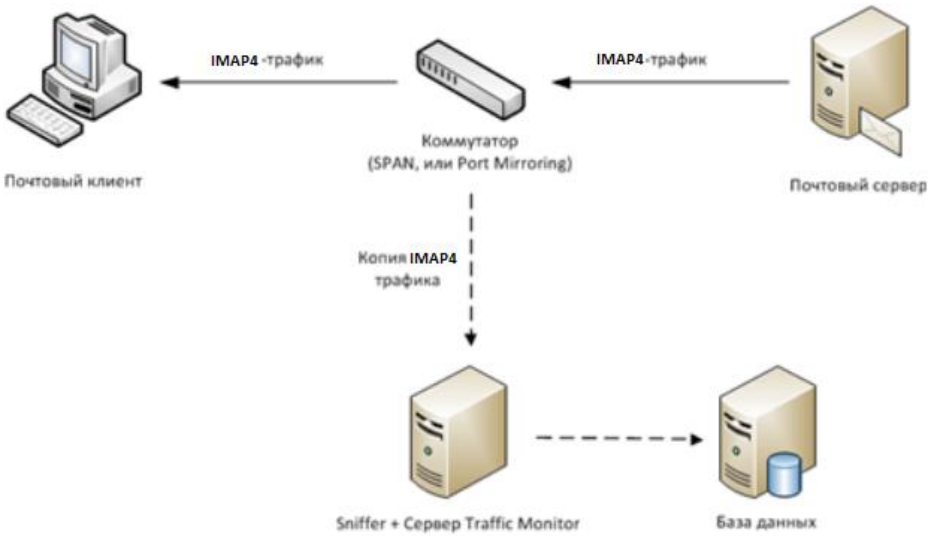
- При большой нагрузке на коммутатор часть пакетов может теряться, особенно если трафик с нескольких портов зеркалируется в один. Чтобы предотвратить потерю пакетов, требуются:

- коммутатор с соответствующим функционалом;

- дополнительный сетевой адаптер на сервере мониторинга.

2.1.1.7 IMAP4-трафик

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".

2.1.1.8 FTP/Skype/Печать/Копирование на съемные носители/Jabber (XMPP)/Yahoo/Mail.ru (MMP)

Перехват этих каналов обеспечивается агентами Device Monitor. Агент может быть установлен на клиентские ОС Microsoft Windows XP SP3 и более новые.



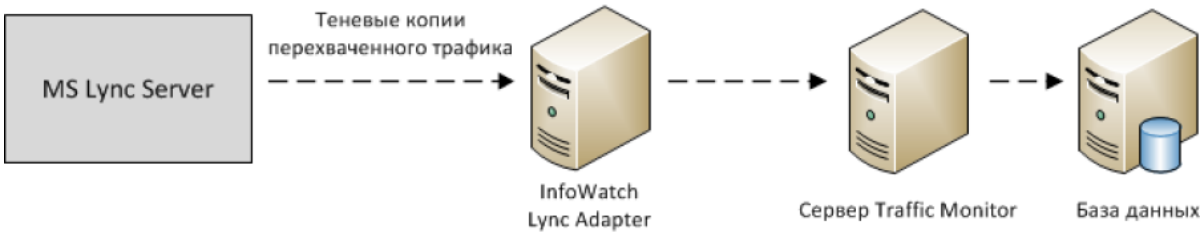
О настройке данного функционала см. документ «InfoWatch Device Monitor. Руководство пользователя».

2.1.2 Анализ информации на файловых ресурсах внутрикорпоративной сети

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

2.1.3 Обработка трафика, полученного от сторонних Систем

Анализ объектов, перехваченных с помощью InfoWatch Lync Adapter.



InfoWatch Lync Adapter должен быть установлен на каждом Microsoft Lync Server, который будет работать с IWTM. Рекомендации по установке приводятся в документе «InfoWatch MS Lync Adapter. Руководство по установке и конфигурированию».

2.2 Состав InfoWatch Traffic Monitor

Подсистема InfoWatch Traffic Monitor	**Назначение подсистемы**
Подсистема перехвата трафика	Перехват и передача на обработку трафика: объектов или их копий. Состоит из следующих модулей: • Модуль Sniffer; • Модуль ICAP; • Модуль Device Monitor.
Подсистема обработки	Извлечение из перехваченных объектов значимой информации и вложений, определение форматов вложений и передача извлеченных текстов в подсистему анализа. **Примечание:** при создании объекта составляется его XML-контекст – текстовый файл, включающий содержимое объекта и информацию о нем.
Подсистема анализа	Анализ текстовых данных, извлеченных из перехваченных объектов (текстов писем, сообщений, запросов, а также текстов, извлеченных из вложений). Состоит из следующих технологий: • Категории и термины; • Текстовые объекты; • Эталонные документы; • Бланки; • Печати; • Выгрузки из БД; • Графические объекты.

Подсистема InfoWatch Traffic Monitor	Назначение подсистемы
Подсистема применения политик	На основе результатов работы подсистемы анализа и подсистемы обработки выносит вердикт о факте нарушения или не нарушения перехваченным объектом политики информационной безопасности. Также обеспечивает привязку данных о получателе или отправителе объекта к записям справочника сотрудников и рабочих станций. Состоит из следующих модулей: Модуль интеграции с Active Directory 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 управления. Представляет собой базу данных. Состоит из следующих модулей: Модуль взаимодействия с удаленной БД, Модуль загрузки объектов в БД, Модуль хранения настроек системы, Модуль хранения объектов. **Примечание:** перед сохранением объектов в БД, они преобразуются из одного внутреннего формата (XML) в другой внутренний формат (LIRO)
Подсистема мониторинга	Возможность удаленного мониторинга состояния серверов, на которых установлены компоненты InfoWatch Traffic Monitor, и работающих на них служб. Также выполнение общих действий по управлению сервером. Работа с подсистемой осуществляется администратором через веб-интерфейс.
Подсистема «Консоль управления»	Обеспечение работы графического пользовательского интерфейса, с помощью которого производится администрирование, настройка и использование Traffic Monitor. Состоит из следующих модулей: • Модуль мониторинга; • Модуль контроля; • Модуль настройки.

2.3 Лицензирование

Ознакомительная лицензия на перехватчики действует в течение 30 дней со дня сборки устанавливаемого дистрибутива Traffic Monitor и допускает использование не более чем 100 пользователями.

Лицензия включает в себя все перехватчики и технологии анализа, использующиеся в продукте. Дата начала действия лицензии соответствует дате сборки продукта.

Чтобы продолжить эксплуатацию Системы, установите коммерческую лицензию на перехватчики, которые Вы планируете использовать.
Чтобы продолжить эксплуатацию Системы по истечении ознакомительного срока, установите коммерческую лицензию на перехватчики, которые Вы планируете использовать. Для этого запросите файл коммерческого лицензионного ключа (см. "Запрос лицензии").
Коммерческий лицензионный ключ представляет собой файл формата LIC.
При установке и использовании лицензионного ключа нужно учитывать следующее:

- Если период действия ознакомительной лицензии истек, работа перехватчиков будет остановлена. Установите коммерческую лицензию или удалите Систему.

- 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
Об управлении лицензиями

Ниже приведены списки модулей и технологий, которые используются в продукте.

Список модулей перехвата:

Подсистема	Типы событий	Протокол
TM	Email	POP3 IMAP4 SMTP NRPC
	Web-сообщение	HTTP
	Web-почта	HTTP
	ICQ	OSCAR
	Краулер	-
DM	Email	POP3 IMAP MAPI SMTP
	Email (mobile)	POP3 IMAP SMTP
	Web-сообщение	HTTP HTTPS
	Web-почта	HTTP HTTPS
	Web-сообщение (mobile)	HTTP HTTPS
	Web-почта (mobile)	HTTP HTTPS

Подсистема	Типы событий	Протокол
	Внешнее устройство	-
	Печать	-
	Skype	SKYPE
	XMPP	XMPP
	Mail.Ru Агент	MMP
	Yahoo!	YMSG
	FTP	FTP
	SMS	-
	Фотосъёмка	-
	WhatsApp	WhatsApp
Adapters	MS Lync	SIP
	Email (Lotus)	NRPC
	Внешнее устройство (Device Lock)	-
	Внешнее устройство (Lumension Device Control)	-
	Печать (Device Lock)	-
	Печать (Lumension Device Control)	-
	Web-сообщение (ICAP)	ICAP
	Web-почта (ICAP)	ICAP

Список технологий:

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

Ограничение:

Технология блокирования каналов утечки на рабочих станциях по результатам анализа не

лицензируется.

3 НАСТРОЙКА СИСТЕМЫ ПОСЛЕ УСТАНОВКИ

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

- 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, требуемые для поддержки почтовых уведомлений, отправляемых в результате срабатывания тех или иных правил в политиках (см. "InfoWatch Traffic Monitor. Руководство пользователя").
- Ограничение количества найденных событий - изменение максимального количества событий, выводимых в Консоли управления.

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:
   ```
   service ntpd stop
   ```
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:
   `service ntpd start`
8. Проверьте текущее состояние службы ntpd с помощью команды:
   `service ntpd status`
9. Включите автоматическую синхронизацию времени:
   `chkconfig --level 345 ntpd on`

3.2 Конфигурирование работы Sphinx при распределенной установке

Полнотекстовый поиск по запросам в Traffic Monitor осуществляется посредством поискового механизма Sphinx. Служба **sphinx** устанавливается в режиме установки **All-in-one** или **TME DB server** (см. "Infowatch Traffic Monitor. Руководство по установке", статья "Установка из дистрибутива TME").

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

При наличии второстепенных серверов, выполните следующие действия:

1. На сервере **TME Node server** в параметре `hostname` секции `search` конфигурационного файла **web.conf** укажите IP-адрес сервера, на котором запущена служба **sphinx** (сервер с базой данных);
2. На сервере **TME DB server** в конфигурационном файле **/opt/iw/tm5/etc/serman_resolver.conf** в параметре `Host` укажите `IP-адрес` основного сервера.

3.3 Общие настройки

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

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

3.3.1 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 (ключ установки **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 (ключ установки **Node server**):
    a. Настройте сервер на работу в качестве Sniffer (см. "Настройка работы сервера Traffic Monitor в качестве Sniffer", вариант 1).
2. На другом компьютере (ключ установки **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 (ключ установки **DB server**).
2. На компьютере, где будет работать Sniffer (ключ установки **Node server**):
    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 (ключ установки **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").

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

3.3.1.1 Настройка работы сервера Traffic Monitor в качестве Sniffer

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

1. Остановите серверные процессы Traffic Monitor:
   ```
   service 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):

i. Включите автозапуск процесса **iw_sniffer** (см. "Включение и выключение автозапуска процессов").

ii. Отключите автозапуск других процессов (см. "Включение и выключение автозапуска 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):

  i. Включите автозапуск процессов **iw_sniffer, iw_loader, iw_updater, iw_warpd и iw_adlibitum** (см. "Включение и выключение автозапуска процессов").

  ii. Отключите автозапуск других процессов (см. "Включение и выключение автозапуска процессов").

3. В конфигурационном файле **proxy.conf**, расположенном в директории `/opt/iw/tm5/etc`, в секции `Startup` включите автозапуск для нужных перехватчиков трафика (настройка для SMTP,HTTP(S), ICQ-трафика:
   - `"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}` – включение всех перехватчиков;
   - `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}` – включение перехватчика **iw_proxy_http**;
   - `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}` – выключение всех перехватчиков.

> **Примечание:**
>
> Описание настройки автозапуска для перехвата NRPC-трафика приведено в статье "SPAN, или Port Mirroring".

4. 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
5. Запустите процессы Traffic Monitor:
   ```
   service iwtm start
   ```

3.3.1.2 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. 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`

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 `Host` и `Port`.
   Например, 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
 }
```

3.3.1.3 Создание кластера Traffic Monitor

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

Важно!

Один кластер может содержать до двух экземпляров сервера Traffic Monitor. Не рекомендуется использовать более 3-х кластеров.
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 и `Host` и `Port`.
   Например,
   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
   }
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 двух экземпляров сервера Traffic Monitor
Система перехватывает копию SMTP- и HTTP-трафика через Sniffer. Для повышения производительности при анализе трафика создается кластер из двух экземпляров сервера Traffic Monitor (см. рис. 3).

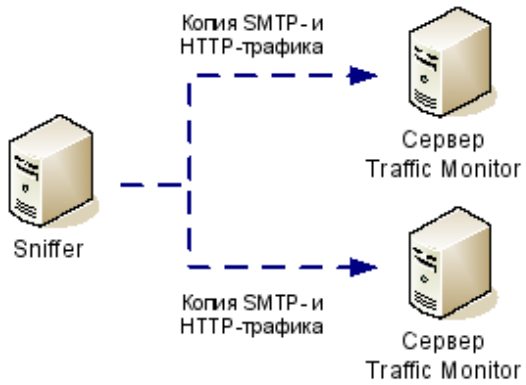


Рисунок 3. Создание кластера из двух серверов Traffic Monitor

3.3.2 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.

Прокси-сервер с поддержкой протокола ICAP перехватывает HTTP-трафик и передает его на сервер Traffic Monitor для анализа и загрузки в базу данных.В данной схеме на сервере Traffic Monitor используется автоматически устанавливаемый модуль IW ICAP.
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 используемый прокси-сервер (SQUID, Blue Coat, Cisco IronPort). 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 ТМ 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 Iron Port;*
- *Рекомендации по настройке McAfee Web Gateway.*

3.3.2.1 Настройка ICAP

Модуль IW ICAP автоматически устанавливается вместе с сервером Traffic Monitor (опции **IWTMX**, **IWALLX** или **IWTMSX**). Автозапуск процесса iw_icap на сервере TM по умолчанию включен.

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 получить из документации к используемому браузеру.

В конфигурационном файле **system.lua**, расположенном в директории `/opt/iw/tm5/etc/scripts`, приведите код к следующему виду:Настройте транспортный режим для трафика, передаваемого по ICAP.

Чтобы трафик передавался в режиме «Копия»:

1. `if not get_child(processing, 'transport_mode') then processing:add_child('transport_mode'):set_text('Copy');`
2. В конфигурационном файле **icap.conf**, расположенном в директории `/opt/iw/tm5/etc/`, укажите значение `true` для параметра `AsyncCheck` секции `Icap`.

Чтобы трафик передавался в режиме «Блокировка»:

1. В конфигурационном файле **system.lua**, расположенном в директории `/opt/iw/tm5/etc/scripts`, приведите код к следующему виду:
   `if not get_child(processing, 'transport_mode') then processing:add_child('transport_mode'):set_text('Normal');`
2. В конфигурационном файле **icap.conf**, расположенном в директории `/opt/iw/tm5/etc/`, укажите значение `false` для параметра `AsyncCheck` секции `Icap`.

Важно!

Транспортный режим, настроенный в конфигурационном файле **system.lua** 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")

3.3.2.2 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**.

3. Перейдите в раздел **Health Checks ► General**. Убедитесь, что включена проверка состояния для серверов – на вкладке **Health Checks** отображаются адреса: `icap.tm`
4. Проверьте доступность всех перечисленных серверов, нажав кнопку **Perform health check** .

3.3.2.3 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.*

3.3.2.3.1 Установка SQUID

Чтобы установить прокси-сервер SQUID из установочного пакета с диска kickstart Traffic Monitor, используйте следующую команду:

```
cd /opt/distr/infowatch/extras/squid-ssl/
rpm -i squid-3.4.0.2-2.el6.x86_64.rpm
cd /etc/squid/
vim squid.conf
```

3.3.2.3.2 Настройка ICAP

Чтобы настроить ICAP, добавьте в конец 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
```

3.3.2.3.3 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 создаёт 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 её 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** её 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.

3.3.2.3.4 Настройка аутентификации пользователей

Работа SUID 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]

3.3.2.4 Рекомендации по настройке Cisco Iron Port

Для настройки Cisco Iron Port 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): • **Server address and port**. Доменное имя машины и номер порта, на которой работает ICAP-сервер Traffic Monitor • **Reconnection attempts**. Количество попыток соединения с ICAP-сервером Traffic Monitor. Рекомендуется указать значение 5. • **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.

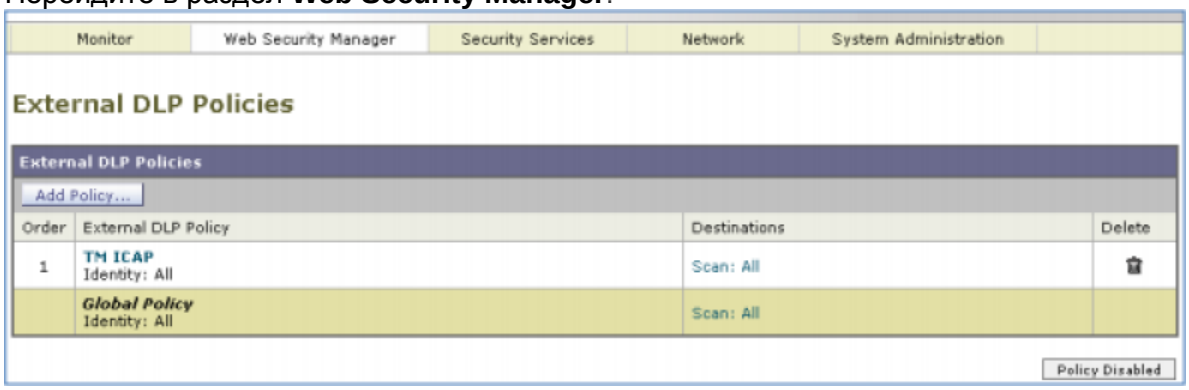
5. При необходимости задайте дополнительный ICAP-сервер, путем нажатия кнопки **Add Row**.
6. Проверьте связь с ICAP-сервером с помощью нажатия кнопки **Start Test**.
7. Нажмите **Submit** чтобы сохранить внесенные изменения.

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**:

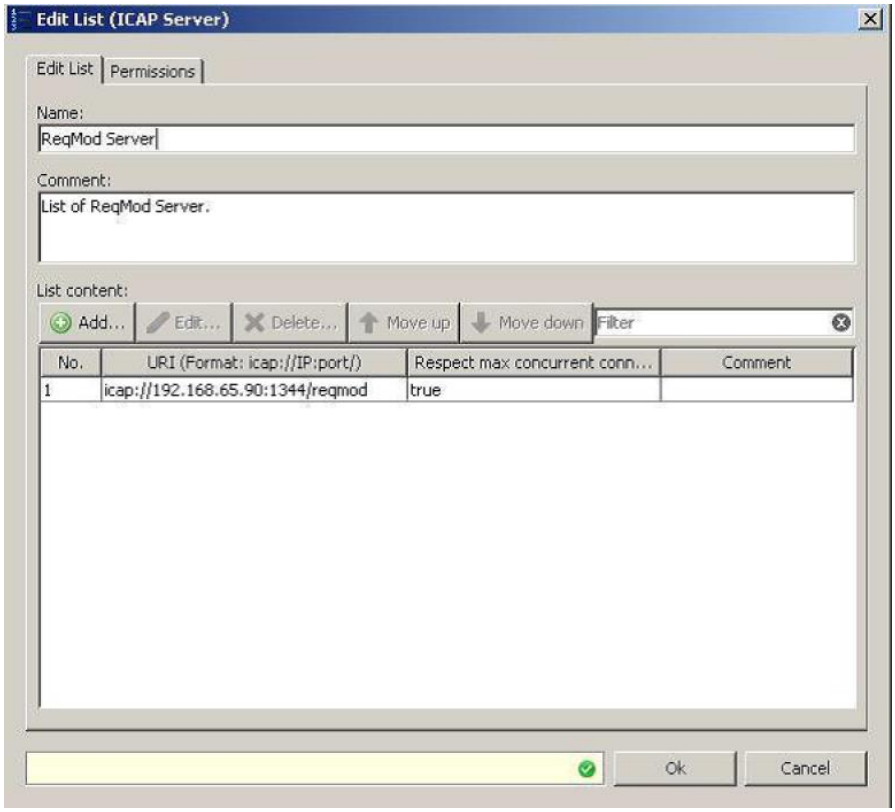


2. Выберите политику в колонке **Destinations**.
3. В выпадающем списке **Edit Destination Settings** выберите значение **Define Destinations Scanning Custom Settings**.
4. В разделе **Destinations to scan** выберите **Scan All Uploads**.
5. Нажмите **Submit** чтобы сохранить внесенные изменения.

	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»).

3.3.2.5 Рекомендации по настройке McAfee Web Gateway

1. Выполните вход в в веб-консоль McAfee Web Gateway.
2. Перейдите на вкладку **Rule Sets** раздела **Policy**.
3. Нажмите **Add** и выберите **Rule Set From Library**.
4. В появившемся окне выберите библиотеку **ICAP Client**, нажмите **OK**.
   В списке **Rule Sets Library** добавится набор правил **ICAP Client**.
5. Раскройте список **ICAP Client** и выделите правило **ReqMod**.
6. В рабочей области справа от списка правил нажмите кнопку **Show details**.
7. Установите флажок для атрибута **Enabled** в строке **DLP Solution: Skip Requests That Do Not Carry Information**.
8. Перейдите по ссылке **ReqMod** в строке **Call ReqMod Server**.
9. В появившемся окне, на вкладке **Edit Settings,** в разделе **Settings content** нажмите **Edit**.
10. Введите данные для сервера, чтобы получилось так, как показано на рисунке:



11. Нажмите **ОК**.
12. В открывшемся окне нажмите **ОК**.
13. Раскройте список **ICAP Client** и выделите правило **RespMod**.
14. Перейдите по ссылке **RespMode** в строке **Call RespMod Server**.
15. В появившемся окне, на вкладке **Edit Settings**, в разделе **Settings content** нажмите **Edit**.
16. Повторите шаг 10 с тем различием, что в поле **URI** значение **reqmod** замените на **respmod**.
17. Нажмите **ОК**.
18. В рабочей области справа от списка правил снимите флажок для атрибута **Enable.**

	Примечание: Последнее действие необходимо для того, чтобы пользовательские изменения не блокировались от сохранения сервером.

19. Нажмите кнопку  несколько раз для перемещения набора правил **ICAP Client** в верхнюю часть списка.
20. Нажмите кнопку  в верхнем правом углу браузера.

3.3.2.6 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:
   `service iwtm stop`
   Отключите автозапуск процесса `iw_icap` (см. "Включение и выключение автозапуска процессов").
2. Запустите процессы Traffic Monitor:
   `service iwtm start`
3. Проверьте состояние процессов Traffic Monitor:
   `service iwtm status`

После отключения модуля верните исходные настройки прокси-сервера.

3.3.3 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 требуется изменить конфигурационный файл **system.lua** следующим образом.

1. Войдите в систему от имени пользователя **root**:
   `su – root`
2. Откройте файл **system.lua**, расположенный в директори `/opt/iw/tm5/etc/scripts`, на редактирование.
3. Замените секцию кода
   ```
   if not get_child(processing, 'transport_mode') then
   processing:add_child('transport_mode'):set_text('Copy');
   end;
   ```
   на следующую:
   ```
   if not get_child(processing, 'transport_mode') then
   local monitor = get_monitor(root);
   if monitor == 'SMTP' then
   processing:add_child('transport_mode'):set_text('Normal');
   elseif monitor == 'HTTP' then
   processing:add_child('transport_mode'):set_text('Normal');
   else
   processing:add_child('transport_mode'):set_text('Copy');
   end
   end;
   ```
4. В зависимости от того, какой режим требуется включить для какого перехватчика, укажите:
   - для SMTP-перехватчика
     - для использования режима «Копия»:
       ```
       if monitor == 'SMTP' then
       processing:add_child('transport_mode'):set_text('Copy');
       ```

- для использования режима «Блокировка»:
```
if monitor == 'SMTP' then
processing:add_child('transport_mode'):set_text('Normal');
```

- для HTTP(S)-перехватчика
  - для использования режима «Копия»:
```
if monitor == 'HTTP' then
processing:add_child('transport_mode'):set_text('Copy');
```

- для использования режима «Блокировка»:
```
if monitor == 'HTTP' then
processing:add_child('transport_mode'):set_text('Normal');
```

5. Сохраните файл.

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

6. Перезагрузите Систему:
```
service iwtm restart
```

3.4 Настройка перехвата трафика

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

- *SMTP-трафик*
- *HTTP-трафик*
- *HTTPS-трафик*
- *ICQ-трафик*
- *NRPC-трафик*
- *IMAP4-трафик*

- *Прием объектов, перехваченных InfoWatch Device Monitor*
- Проверка файлов, находящихся в корпоративной сети

Важно!

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

Важно!

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

3.4.1 SMTP-трафик

Описание данного способа перехвата трафика см. в "SMTP-трафик".

3.4.1.1 SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. "SPAN, или Port Mirroring").
2. Убедитесь, что в конфигурационном файле proxy.conf, расположенном в директории `/opt/iw/tm5/etc`, в секции Startup включен автозапуск перехватчика SMTP-трафика:
```
"Startup": {
"Enabled": true,
"smtp": true
```
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_loader** (см. "Включение и выключение автозапуска процессов").
4. Чтобы избежать дублирования перехваченных данных, отключите процесс **iw_smtpd** (см. "Включение и выключение автозапуска процессов").

3.4.1.2 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_cas, iw_loader (см. "Автозапуск процессов").
5. Убедитесь, что в конфигурационном файле **system.lua**, расположенном в директории `/opt/iw/tm5/etc/scripts`, для параметра `set_text` указано значение `Copy`:

```
if not get_child(processing, 'transport_mode') then
 processing:add_child('transport_mode'):set_text('Copy');
```

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".

3.4.1.3 "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 с помощью Postfix предается адресату или следующему relay-серверу в почтовой системе организации.

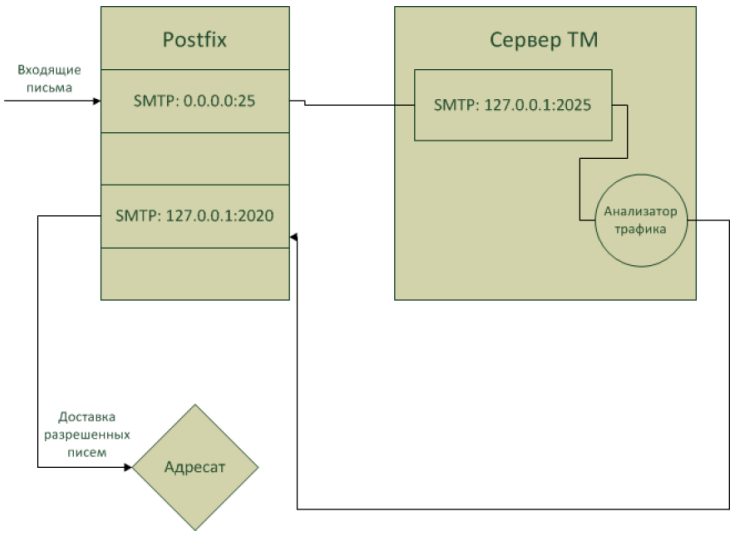


Рисунок 1. Интеграция с Postfix (Копия)

- 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, Система блокирует доставку письма. Письмо будет доставлено только в том случае, если Офицер безопасности разрешит доставку письма в Консоли управления (см. документ «InfoWatch Traffic Monitor. Руководство пользователя»). Доставка осуществляется следующим образом: процесс **iw_messed** 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.

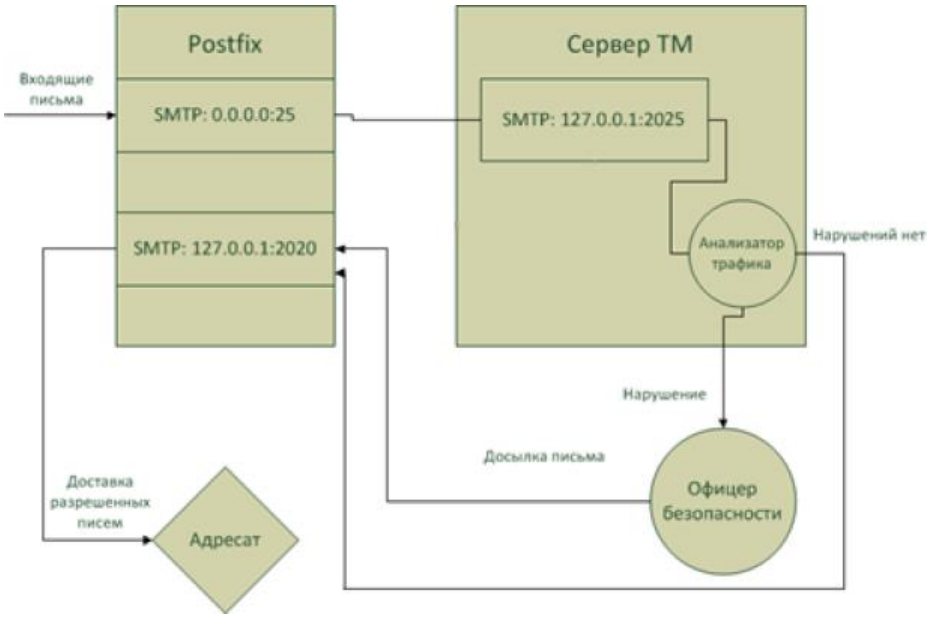


Рисунок 2. Интеграция с Postfix (Блокировка)

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 настроены 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. В конфигурационном файле system.lua, расположенном в директории `/opt/iw/tm5/etc/scripts`, в зависимости от используемой схемы, добавьте соответствующую секцию кода:

- в случае использования режима «Копия»:

```
if not get_child(processing, 'transport_mode') then
 processing:add_child('transport_mode'):set_text('Copy');
```

- в случае использования режима «Блокировка»:

```
if not get_child(processing, 'transport_mode') then
 processing:add_child('transport_mode'):set_text('Normal');
```

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".

3.4.1.4 Общие настройки для SMTP-трафика

3.4.1.4.1 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 ТМ

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**.

3.4.1.4.2 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`

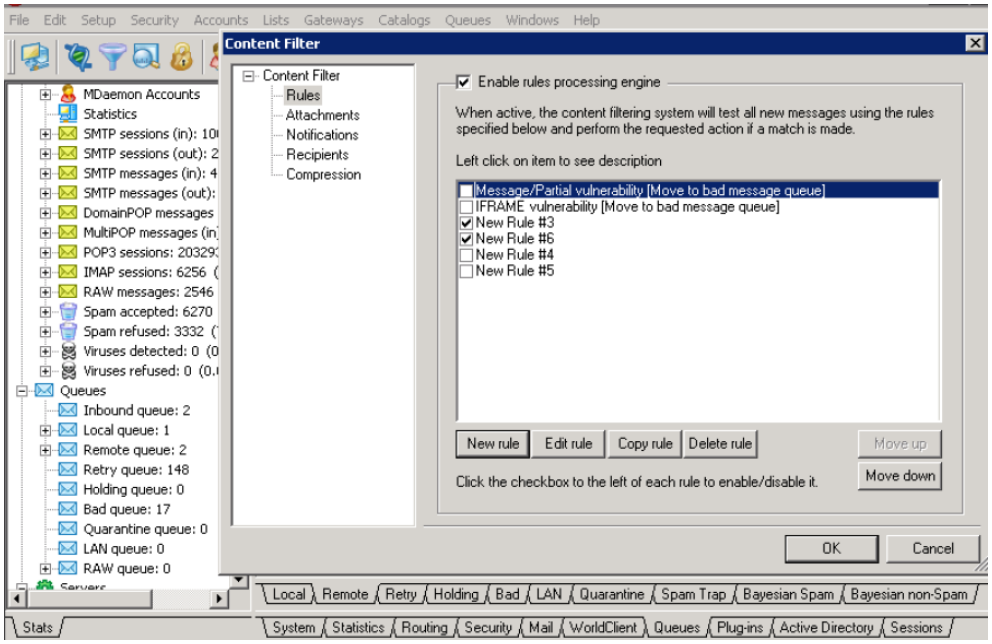
Настройка отправки BCC

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

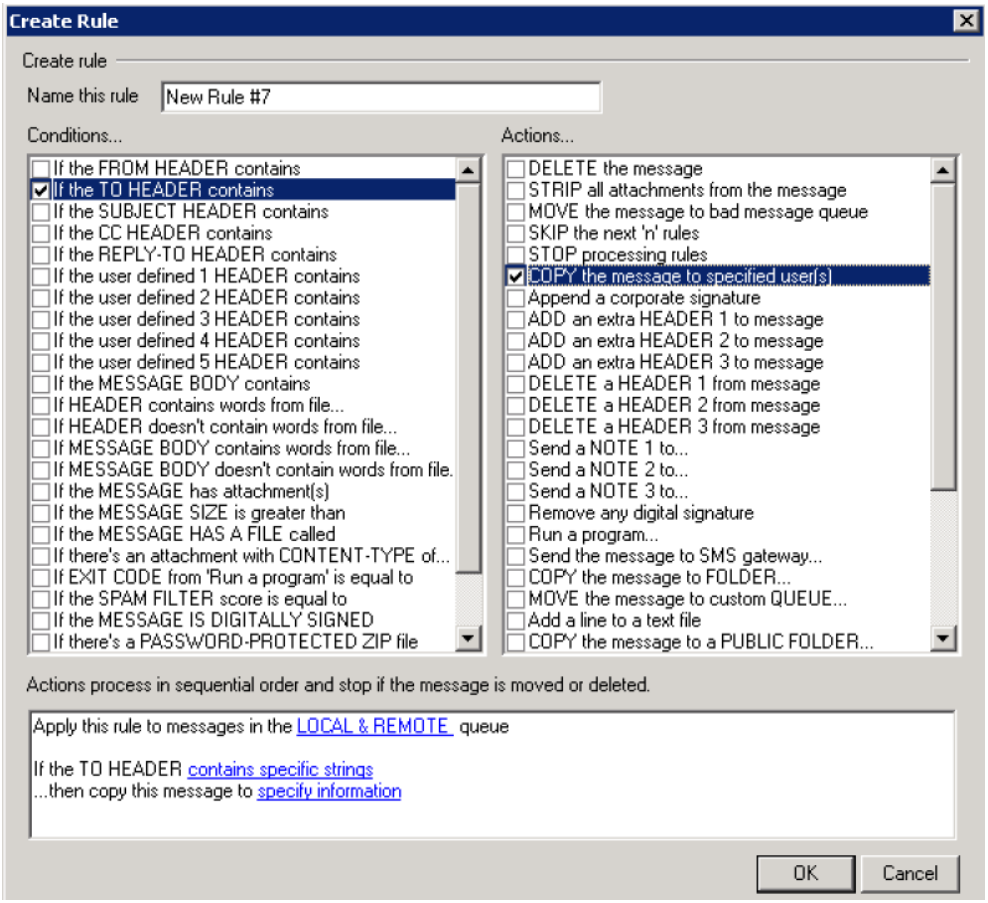
3.4.1.4.3 Настройка пересылки скрытых копий MDaemon

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**.

3.4.1.4.4 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 (ключ kickstart **IWTMX**)	Обязательна
	Все компоненты установлены на один сервер (ключ kickstart **IWALLX** или **IWTMSX**)	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 (ключ kickstart **IWTMX**)	Обязательна
	Все компоненты установлены на один сервер (ключ kickstart **IWALLX** или **IWTMSX**)	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.

> **Примечание:**
>
> 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.

> **Примечание:**
>
> 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.
   - 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=<$hostname>
```

5. В файле **main.cf** проверьте, что в параметре mynetworks корректно указана подсеть, где расположены почтовые серверы.
6. 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 программы-инсталлятора (**kickstart**) данная настройка устанавливается автоматически.

7. Проверьте корректность синтаксиса файлов конфигурации:
   `service postfix check`
8. Перезапустите Postfix:
   `service postfix restart`
9. 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

.

3.4.2 POP3-трафик

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 `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`.

3.4.3 HTTP-трафик

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

3.4.3.1 SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. "SPAN, или Port Mirroring").
2. Убедитесь, что в конфигурационном файле **proxy.conf**, расположенном в директории `/opt/iw/tm5/etc`, в секции Startup включен автозапуск перехватчика SMTP-трафика:
```
"Startup": {
"Enabled": true,
"http": true
```
3. Убедитесь, что включен автозапуск для процессов, участвующих в перехвате и обработке HTTP трафика:
iw_sniffer, **iw_proxy_HTTP**, **iw_warpd**, **iw_cas**, **iw_loader** (см. "Включение и выключение автозапуска процессов").

3.4.3.2 "В разрыв"

> **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").

3.4.4 HTTPS-трафик

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

3.4.4.1 "В разрыв"

> **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.

3.4.5 ICQ-трафик

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

3.4.5.1 SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. "SPAN, или Port Mirroring").
2. Убедитесь, что в конфигурационном файле **proxy.conf**, расположенном в директории `/opt/iw/tm5/etc`, в секции `Startup` включен автозапуск перехватчика SMTP-трафика:
```
"Startup": {
"Enabled": true,
"icq": true
```

3.4.6 NRPC-трафик

3.4.6.1 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. Убедитесь, что в секции Startup включен автозапуск:
```
"Startup": {
"Enabled": true
},
```
6. Сохраните файл **capstack.conf**.

7. Перезапустите процесс **capstack**:
   `service iwtm restart capstack`

3.4.7 IMAP4-трафик

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 `Hi Port` 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`.

3.4.8 Прием объектов, перехваченных InfoWatch Device Monitor

Описание данного способа перехвата трафика см. в статье "FTP/Skype/Печать/Копирование на съемные носители/Jabber (XMPP)/Yahoo/Mail.ru (MMP)".

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

3.4.9 Проверка файлов, находящихся в корпоративной сети

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

1. Установите и настройте сервер Traffic Monitor (см. "InfoWatch Traffic Monitor. Руководство по установке").
2. Установите и настройте Crawler (см. "InfoWatch Traffic Monitor. Руководство по установке").
3. Настройте общие параметры работы сканера Crawler.

Настройте параметры анализа объектов (см. "InfoWatch Traffic Monitor. Руководство пользователя").

3.5 Автозапуск процессов

В этом разделе:

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

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

3.5.1 Проверка автозапуска процессов

Важно!

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

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

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

Процесс	**По умолчанию автозапуск включен**
iw_adlibitum	Да **Примечание:** Процесс должен работать только на основном сервере
iw_agent	Да

Процесс	По умолчанию автозапуск включен

iw_kicker	Да
	Процесс объединяет сервисы:
	`selection`
	`blackboard`
	`systemcheck`
	`agent`
	`xapisamplecompiler`
	`export`
	`samplecompiler`
	`report`
	`import`
	`notifier`
	`crawler`
	Чтобы включить сервис, выставьте сервису значение `1` в секции `kickers` конфигурационного файла **web.conf**.
	Чтобы выключить сервис, выставьте сервису значение `0` в секции `kickers` конфигурационного файла **web.conf**.
	Примечание: Процесс должен работать только на сервере с веб-консолью

iw_blackboard	Да
iw_bookworm	Да
iw_capstack	Да
iw_cas	Да
iw_deliver	Да
iw_expressd	Да
iw_icap	Да
iw_indexer	Да **Примечание:** Процесс должен работать только на основном сервере
iw_licensed	Да **Примечание:** Процесс должен работать только на основном сервере
iw_loader	Да
iw_luaengined	Да
iw_messed	Да

Процесс	По умолчанию автозапуск включен
iw_proxy_http iw_proxy_icq iw_proxy_smtp	Да
iw_qmover_client	Нет
iw_qmover_server	Нет
iw_sample_compiler	Да
iw_selection_kicker	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью
iw_serman	Да
iw_smtpd	Да
iw_sniffer	Да
iw_system_check	Да
iw_updater	Да
iw_warpd	Да
iw_whiteboard	Да
iw_xml2liro	Да

Примечение:

Чтобы удалить с сервера все **iw_*_kicker** процессы, удалите пакет **iwtm-webgui**:

```
rpm -e iwtm-webgui
```

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

3.5.2 Включение и выключение автозапуска процессов

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

1. Для корректной смены параметров остановите серверные процессы Traffic Monitor:
   `service iwtm stop`
2. В файле `/opt/iw/tm5/etc/sniffer.conf` выполните настройки:
   Чтобы включить автозапуск для процесса, установите в блоке процесса:
   `"Startup" : {"Enabled" : true}`

Чтобы отключить автозапуск для процесса, установите в блоке процесса:
`"Startup" : {"Enabled" : false}`

Важно!

Для службы **iw_proxy** включение и выключение компонентов выполняется следующим образом:

- `"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}` – включение всех модулей;
- `"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}` – включение модуля **iw_proxy_http**;
- `"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}` – выключение всех модулей.

3. Запустите процессы Traffic Monitor:
`service iwtm start`

3.6 Настройка OCR-экстракторов

Настройка OCR для различных перехватчиков производится в следующих конфигурационных файлах:

- **expressd.conf** – требуется указать значение `true` каждому перехватчику, для которого нужно включить использование OCR (см. "Секция Expressd, параметр Ocr")
- **messed.conf** – требуется указать значение `true` параметру `OCR`, если нужно включить использование OCR для писем, проходящих через почтовый relay-сервер (см. "Конфигурационный файл messed.conf").
- **warpd.conf –** в секции `Warp` требуется указать параметру `EnableOCR` значение `true`.
- **proxy.conf –** в секции Http или Icq требуется указать параметру `OCR` значение `true` (см. "Конфигурационный файл proxy.conf")
- **analysis.conf** – в секции `Analysis` требуется указать параметру `OCR` значение `true` (см. "Конфигурационный файл analysis.conf")

Распознавание текста из извлеченных изображений производится с использованием одного из двух OCR-экстракторов: Tesseract 3.0 и ABBYY FineReader Engine 9.5.
При установке с помощью программы-инсталлятора (**kickstart**) на серверную часть Системы устанавливаются оба OCR-экстрактора. По умолчанию на работу настроен Tesseract 3.0.

Функциональные ограничения экстракторов приведены в таблице ниже:

Функциональность	Tesseract 3.0	ABBYY FineReader Engine 9.5
Распознавание углов поворота изображения	-	0(+/-20) , 90(+/-20), 180(+/-20) и 270(+/-20) градусов

Функциональность	Tesseract 3.0	ABBYY FineReader Engine 9.5
Распознавание цветного изображения	-	+
Коррекция изображения	-	+
Рекомендуемое разрешение изображения	300dpi для текста с размером шрифта от 10pt 400-600dpi для текста с размером шрифта 9pt и меньше	300dpi для текста с размером шрифта от 10pt 400-600dpi для текста с размером шрифта от 9pt и меньше

Чтобы настроить на работу экстрактор ABBYY FineReader Engine 9.5:

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 9.5 на Tesseract 3.0:

1. Удалите символьную ссылку **/opt/iw/tm5/bin/iw_image2text** .
2. Создайте символьную ссылку:
   ```
   ln -s /opt/iw/tm5/bin/iw_image2text_ts /opt/iw/tm5/bin/iw_image2text
   ```

3.7 Настройка отправки уведомлений пользователям и сотрудникам

Пользователь Консоли управления имеет возможность настроить отправку уведомлений из Системы пользователю или сотруднику. Уведомления отправляются в результате срабатывания тех или иных правил в политиках (подробнее см. документ "InfoWatch Traffic Monitor. Руководство пользователя"). 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 Postfix.

Чтобы настроить электронный адрес для отправки уведомлений:

1. Подключитесь к БД от имени владельца схемы.
2. В таблице *SETTING*, для атрибута `NOTIFY_SENDER` укажите требуемый e-mail адрес отправителя.

Чтобы проверить, отправляются ли письма через Postfix,
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).

3.8 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 РАБОТА В КОНСОЛИ УПРАВЛЕНИЯ

Ряд действий по настройке Системы может выполняться администратором упрощенно, с помощью веб-интерфейса управления (веб-консоли), доступного из браузера любой рабочей станции локальной сети.
Основные действия администратора по управлению Системой с помощью веб-консоли описаны в следующих разделах:

- Вход в веб-консоль и выход из нее;
- Управление интеграцией с LDAP каталогами;
- Управление пользователями Системы и их ролями;
- Управление лицензиями;
- Состояние системы;
- Управление службами;
- Сбор диагностических данных;
- Аудит действий пользователя;
- Контроль целостности;
- Плагины.

4.1 Вход в веб-консоль и выход из нее

Чтобы войти в веб-консоль:

1. Откройте интернет-браузер (рекомендуется использовать браузер Google Chrome. Если у Вас не установлен этот браузер, Вы можете загрузить его, перейдя по ссылке: http://www.google.com/intl/ru/chrome/browser/).
2. В адресной строке введите адрес сервера InfoWatch Traffic Monitor.
3. В поле **Логин** укажите имя пользователя.
4. В поле **Пароль** укажите пароль.
5. Нажмите **Войти**.

Важно!

Для обеспечения безопасности данных настоятельно рекомендуется по окончании работы с веб-консолью выполнить выход. Для этого в верхнем правом углу консоли нажмите **Выйти**.
В Системе настроен автоматический выход из Консоли управления, если в течение 30 минут не выполнялось никаких действий.

4.2 Управление интеграцией с LDAP каталогами

Настройка синхронизации с LDAP каталогами выполняется в разделе **Управление -> LDAP Синхронизация**.

Важно!

Если для интернет-браузера установлено расширение Adblock Plus, отключите его для обеспечения корректной работы в этом разделе веб-консоли.

В левой части рабочей области **LDAP сервера** расположена панель инструментов.
Список серверов, синхронизация с LDAP каталогами которых настроена, отображается под панелью инструментов.
Панель инструментов содержит набор инструментов для работы с подключениями.
В центральной части рабочей области отображаются параметры выбранного подключения:

Параметр	**Описание**
Название сервера	Идентификатор соединения, который используется в консоли управления
Тип сервера	Признак того, какой сервер используется – *Active Directory* или *Domino Directory*
Синхронизация	Признак того, что синхронизация выполняется по указанному расписанию
Период синхронизации	Тип периодичности выполнения синхронизации

Параметр	Описание
Повторение	Время повторения синхронизации ***Например*** , при заданных значениях • *Период синхронизации* – ежеминутно; • *Повторение* – 60 минут, синхронизация будет выполняться каждые 60 минут.
LDAP-сервер	Сетевой идентификатор сервера, с LDAP каталогами которого производится синхронизация
Глобальный LDAP-порт	Порт для подключения глобального LDAP каталога. **Примечание:** данная настройка доступна только для Active Directory
LDAP-порт	Порт для подключения доменного каталога
Глобальный каталог	Признак того, что для синхронизации используется глобальный LDAP каталог **Примечание:** данная настройка доступна только для Active Directory
LDAP-запрос	Домен (LDAP base), в котором ведется поиск данных AD. **Примечание:** данная настройка не обязательна для Domino Directory Для оптимизации поиска по AD Вы можете использовать отдельные уровни иерархии базы. ***Например*** , чтобы использовать в качестве базы поиска ветку `Users`, расположенную в домене компании, необходимо присвоить параметру **Атрибуты фильтрации** следующее значение: `cn=users,dc=company,dc=com`
Логин	Логин для доступа к серверу синхронизации
Пароль	Пароль для доступа к серверу синхронизации
Последняя синхронизация	Дата и время завершения последней синхронизации
Статус последней синхронизации	Результат последней синхронизации
Следующая синхронизация	Дата и время следующей синхронизации

Настройка интеграции с LDAP каталогами описана в разделах:

- Создание подключения к серверу;
- Редактирование подключения к серверу;
- Удаление подключения к серверу;
- Запуск синхронизации с сервером вручную.

4.2.1 Создание подключения к серверу

Чтобы создать подключение к серверу:

1. Перейдите в раздел **Управление -> LDAP Синхронизация**.
2. На панели инструментов нажмите  **Создать**.
3. Укажите параметры для нового подключения (см. "Управление интеграцией с LDAP каталогами").
4. Нажмите **Проверить соединение**, чтобы выполнить контрольную проверку подключения к серверу.
5. Нажмите **Сохранить**.

4.2.2 Редактирование подключения к серверу

Чтобы отредактировать подключение к серверу:

1. Перейдите в раздел **Управление -> LDAP Синхронизация**.
2. Щелчком левой кнопки мыши выберите требуемый сервер.
3. На панели инструментов нажмите  **Редактировать**.
4. Измените параметры подключения (см. "Управление интеграцией с LDAP каталогами").
5. Нажмите **Проверить соединение**, чтобы выполнить контрольную проверку подключения к серверу.
6. Нажмите **Сохранить**.

4.2.3 Удаление подключения к серверу

Чтобы удалить существующее подключение к серверу, выполните следующие шаги:

1. Перейдите в раздел **Управление -> LDAP Синхронизация**.
2. Щелчком левой кнопки мыши выберите требуемый сервер.
3. На панели инструментов нажмите  **Удалить**.

> **Примечание:**
>
> Чтобы удалить несколько подключений сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить**.

4. В появившемся окне нажмите **Да**.

4.2.4 Запуск синхронизации с сервером вручную

Чтобы запустить синхронизацию с сервером вручную, выполните следующие шаги:

1. Перейдите в раздел **Управление -> LDAP Синхронизация**.

2. Щелчком левой кнопки мыши выберите требуемый сервер.
3. На панели инструментов нажмите **Запустить синхронизацию**.

Информация о результатах синхронизации будет показана в строках *Дата последней синхронизации* и *Статус последней синхронизации*.

Примечание:

Если для подключения в качестве атрибута *Период синхронизации* выбраны значения Каждые N минут, Каждые N часов, Ежедневно или Еженедельно, автоматическая синхронизация будет выполняться с указанной периодичностью после последнего ручного запуска.

Важно!

Синхронизация будет запускаться по локальному времени сервера (поле)

4.3 Управление пользователями Системы и их ролями

Для работы пользователя в Системе используются следующие сущности:

- *Пользователь* – учетная запись (см. "Пользователи");
- *Роль* – набор прав, которые могут быть присвоены Пользователю (см. "Задание пользователю роли");
- *Область видимости* – группа конкретных атрибутов объектов перехвата, к которым могут иметь доступ только указанные пользователи (см. "Области видимости").

4.3.1 Пользователи

Настройка списка пользователей Системы выполняется в разделе **Управление -> Управление доступом**, на вкладке **Пользователи**.
В рабочей области расположен список пользователей Системы, панель инструментов и раскрывающееся меню.
В списке пользователей отображаются пользователи Системы.
Панель инструментов содержит набор инструментов для работы с пользователями.
Раскрывающееся меню определяет количество пользователей, отображаемых на странице.
Атрибуты учетной записи приведены в таблице:

Параметр	**Описание**
Логин	Имя учетной записи пользователя

Параметр	Описание
Полное имя	ФИО пользователя
Email	Адрес электронной почты пользователя
Роли	Список ролей пользователя
Области видимости	Список областей видимости пользователя
Описание	Примечание к учетной записи
Статус	Признак того, является ли учетная запись пользователя активной или выключенной

Вы можете выполнять следующие действия при управлении пользователями:

- Создание учетной записи пользователя;
- Редактирование учетной записи пользователя;
- Удаление учетной записи пользователя;
- Изменение пароля учетной записи пользователя;
- Изменение статуса учетной записи пользователя;
- Импорт учетной записи пользователя;
- Задание пользователю роли;
- Задание пользователю области видимости.

4.3.1.1 Создание учетной записи пользователя

Чтобы создать учетную запись:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. На панели инструментов нажмите  **Создать пользователя**.
4. В открывшемся окне укажите параметры учетной записи:

Параметр	Описание
Логин	Имя учетной записи пользователя
Статус	Признак того, является ли учетная запись пользователя активной или выключенной
Язык интерфейса	Язык, который будет присвоен интерфейсу выбранной учетной записи
Пароль	Пароль учетной записи **Примечание:** О правилах создания имен и паролей для пользователей читайте в Приложении А "Рекомендации по составлению имен и паролей".

Параметр	Описание
Подтверждение пароля	Пароль учетной записи
Email	Адрес электронной почты пользователя
Полное имя	ФИО пользователя
Описание	Примечание к учетной записи

5. Нажмите **Сохранить**.

4.3.1.2 Редактирование учетной записи пользователя

Чтобы изменить параметры существующей учетной записи:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите  **Редактировать пользователя**.
5. В открывшемся окне измените параметры учетной записи (см. "Пользователи").
6. Нажмите **Сохранить**.

4.3.1.3 Удаление учетной записи пользователя

Чтобы удалить учетную запись:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите  **Удалить пользователя**.

> **Примечание:**
>
> Чтобы удалить несколько учетных записей сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить пользователя**.

5. В появившемся окне нажмите **Да**.

4.3.1.4 Изменение пароля учетной записи пользователя

Чтобы изменить учетную запись:

1. Перейдите в раздел **Управление -> Управление доступом**.

2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите  **Сменить пароль**.
5. В открывшемся окне введите новый пароль в полях **Пароль** и **Подтверждение пароля**.

> **Примечание:**
>
> О правилах создания имен и паролей для пользователей читайте в Приложении А "Рекомендации по составлению имен и паролей".

6. Нажмите **Сохранить**.

4.3.1.5 Изменение статуса учетной записи пользователя

Чтобы изменить статус учетной записи:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите  **Активировать пользователя/**  **Деактивировать пользователя**.

> **Примечание:**
>
> Вы можете изменить статус любой учетной записи, кроме **Administrator**.

4.3.1.6 Импорт учетной записи пользователя

Для удобства создания пользователей Вы можете импортировать учетные записи из Active Directory или Domino Directory.

Чтобы импортировать учетную запись:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. На панели инструментов нажмите  **Добавить пользователя из LDAP**.

4. В открывшемся окне укажите LDAP сервер, на котором хранится требуемая учетная запись пользователя.

> **Примечание:**
>
> Для удобства поиска учетной записи введите часть названия учетной записи в поле **Строка поиска** и нажмите **Поиск**.

5. Установите флажок для требуемых пользователей.
6. Нажмите **Сохранить**.

4.3.1.7 Задание пользователю роли

Чтобы задать пользователю роль:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите  **Задать роль**.
5. В открывшемся окне установите флажок для требуемых ролей (см. "Роли").
6. Нажмите **Добавить**.

4.3.1.8 Задание пользователю области видимости

Чтобы задать пользователю область видимости:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Пользователи**.
3. В списке пользователей щелчком левой кнопки мыши выберите требуемую учетную запись.
4. На панели инструментов нажмите  **Задать область видимости**.
5. В открывшемся окне установите флажок для требуемых областей видимости (см. "Области видимости").
6. Нажмите **Добавить**.

4.3.2 Роли

Для контроля избыточности доступа к настройкам системы, политик разных структурных отделов, объектов перехвата и прочей важной информации, в InfoWatch Traffic Monitor предусмотрена ролевая система разграничения прав доступа с областью видимости.

Назначение ролей пользователям описано в статье "Задание пользователю роли".

Изначально в системе присутствуют две предустановленные роли и два предустановленных пользователя – роли **Администратор** и **Офицер безопасности**, которые назначены, соответственно, пользователям Administrator и Officer.

Роль **Администратор** предоставляет возможность проводить первичную настройку системы (Управление пользователями, ролями, областями видимости, лицензиями и синхронизацией с LDAP-каталогами).

Роль **Офицер безопасности** обладает всеми правами, кроме первичной настройки.

Настройка списка ролей выполняется в разделе **Управление -> Управление доступом**, на вкладке **Роли**.
В рабочей области расположен список ролей, панель инструментов и раскрывающееся меню.
Атрибуты роли приведены в таблице:

Параметр	**Описание**
Название	Имя роли
Пользователи	ФИО пользователя
Описание	Примечание к роли

Вы можете выполнять следующие действия при управлении ролями:

- *Создание роли;*
- *Редактирование роли;*
- *Удаление роли.*

4.3.2.1 Создание роли

Чтобы создать новую роль, выполните следующие действия:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Роли**.
3. На панели инструментов нажмите  **Создать роль**.
4. В открывшемся окне установите флажки на те действия, которые требуется разрешить выбранной роли.

Примечание:

Чтобы развернуть или свернуть список, нажмите кнопки ▶ или ◢ соответственно.

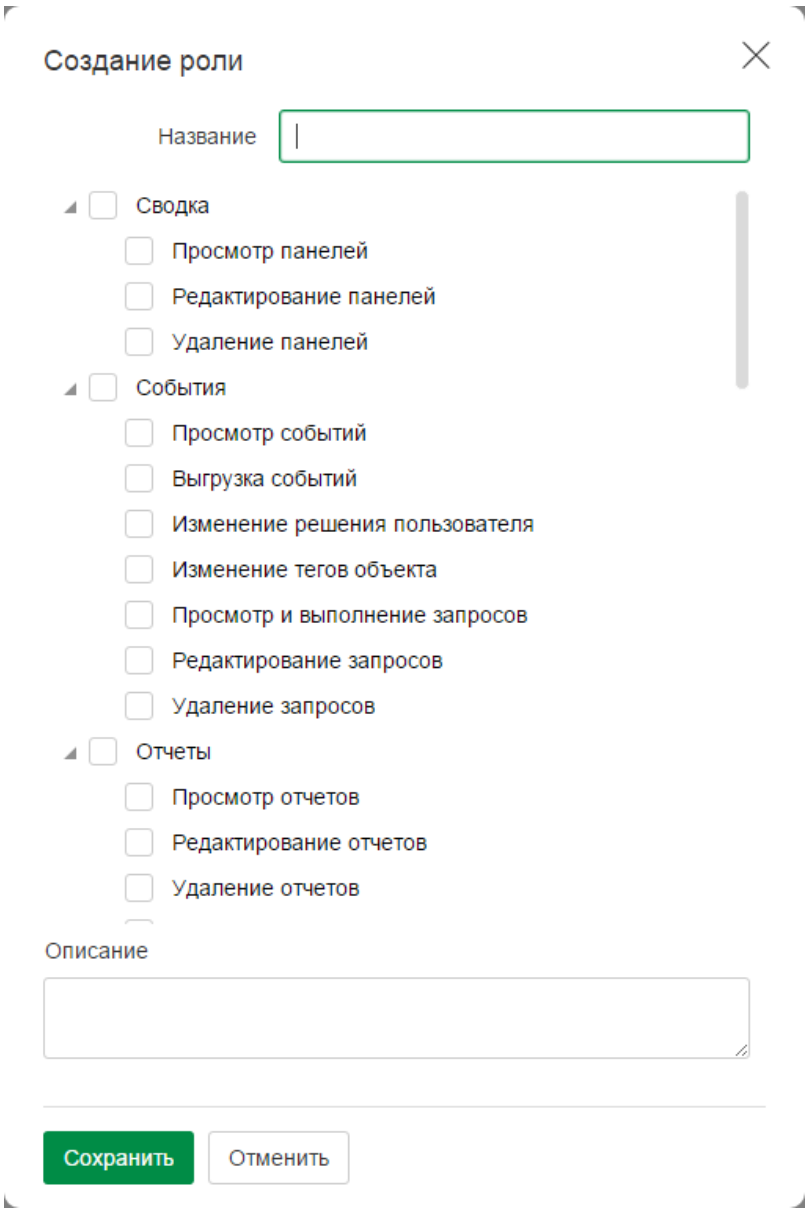


Рисунок 4. Создание роли

5. Нажмите **Сохранить**.

4.3.2.2 Редактирование роли

Чтобы изменить параметры существующей роли, выполните следующие действия:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Роли**.
3. В списке ролей щелчком левой кнопки мыши выберите требуемую роль.

4. На панели инструментов нажмите  **Редактировать роль**.
5. В открывшемся окне установите флажки на те действия, которые разрешены для выбранной роли.

> **Примечание:**
>
> Чтобы развернуть или свернуть список, нажмите кнопки ▶ или ◢ соответственно.

6. Нажмите **Сохранить**.

4.3.2.3 Удаление роли

Чтобы удалить роль:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Роли**.
3. В списке ролей щелчком левой кнопки мыши выберите требуемую роль.
4. Нажмите  **Удалить роль**.

> **Примечание:**
>
> Чтобы удалить несколько ролей сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить роль**.

5. В появившемся окне нажмите **Да**.

> **Примечание:**
>
> Вы можете изменить любую роль, кроме роли **Администратор** и **Офицер безопасности**.

4.3.3 Области видимости

Области видимости позволяют осуществлять дополнительный контроль доступа к перехваченным объектам. Область видимости создается из атрибутов объектов перехвата. Пользователю будут видны только те событий, атрибуты которых совпадают с атрибутами, заданными в области видимости.

Например,

Пользователю officer 1 присвоена область видимости с Персоной: Иванов и Тегом: 1. Пользователь officer 1 сможет просматривать только события с участием персоны Иванов и помеченные тегом 1.

Примечание:

Для одного пользователя может быть задано несколько областей видимости.

Назначение областей видимости пользователям описано в статье "Задание пользователю области видимости".

Настройка списка областей видимости выполняется в разделе **Управление -> Управление доступом** на вкладке **Области видимости**.

В рабочей области расположен список областей видимости, панель инструментов и раскрывающееся меню.

В списке областей видимости отображаются области видимости пользователей Системы.

Панель инструментов содержит набор инструментов для работы с областями видимости.

Раскрывающееся меню определяет количество областей видимости, отображаемых на странице.

Атрибуты области видимости приведены в таблице:

Параметр	**Описание**
Название	Имя области видимости
Описание	Примечание к области видимости

Вы можете выполнять следующие действия при управлении областями видимости:

- *Создание области видимости*;
- *Редактирование области видимости*;
- *Удаление области видимости*.

4.3.3.1 Создание области видимости

Чтобы создать область видимости:

1. Перейдите в раздел **Управление -> Управление доступом** .
2. Перейдите на вкладку **Области видимости**.
3. На панели инструментов нажмите  **Создать область видимости**.

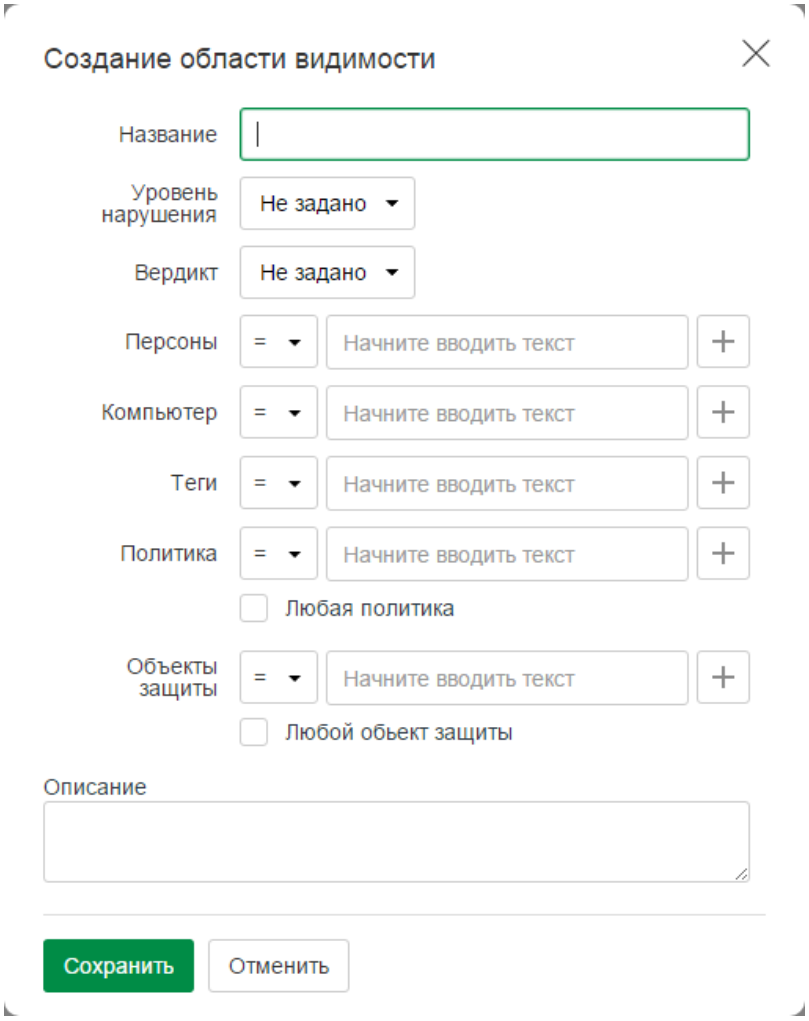


Рисунок 5. Создание области видимости

4. В открывшемся окне заполните требуемые поля следующим образом:
    a. *Название* - введите название в поле.
    b. *Уровень нарушения* - выберите из раскрывающегося списка.
    c. *Вердикт* - выберите из раскрывающегося списка.
    d. *Персоны* :
    введите первые символы наименования пользователя и выберите требуемое значение из выпадающего списка
    или
    нажмите + и в появившемся окне, в списке пользователей, установите флажки требуемым пользователям. Нажмите **Добавить**.
    e. *Компьютер* – аналогично пункту d.
    f. *Теги* - аналогично пункту d.
    g. *Политика* – аналогично пункту d.
    h. *Объект защиты* – аналогично пункту d.
    i. *Любой объект защиты* - выберите настройку.

j. *Описание* - введите текст описания в поле.

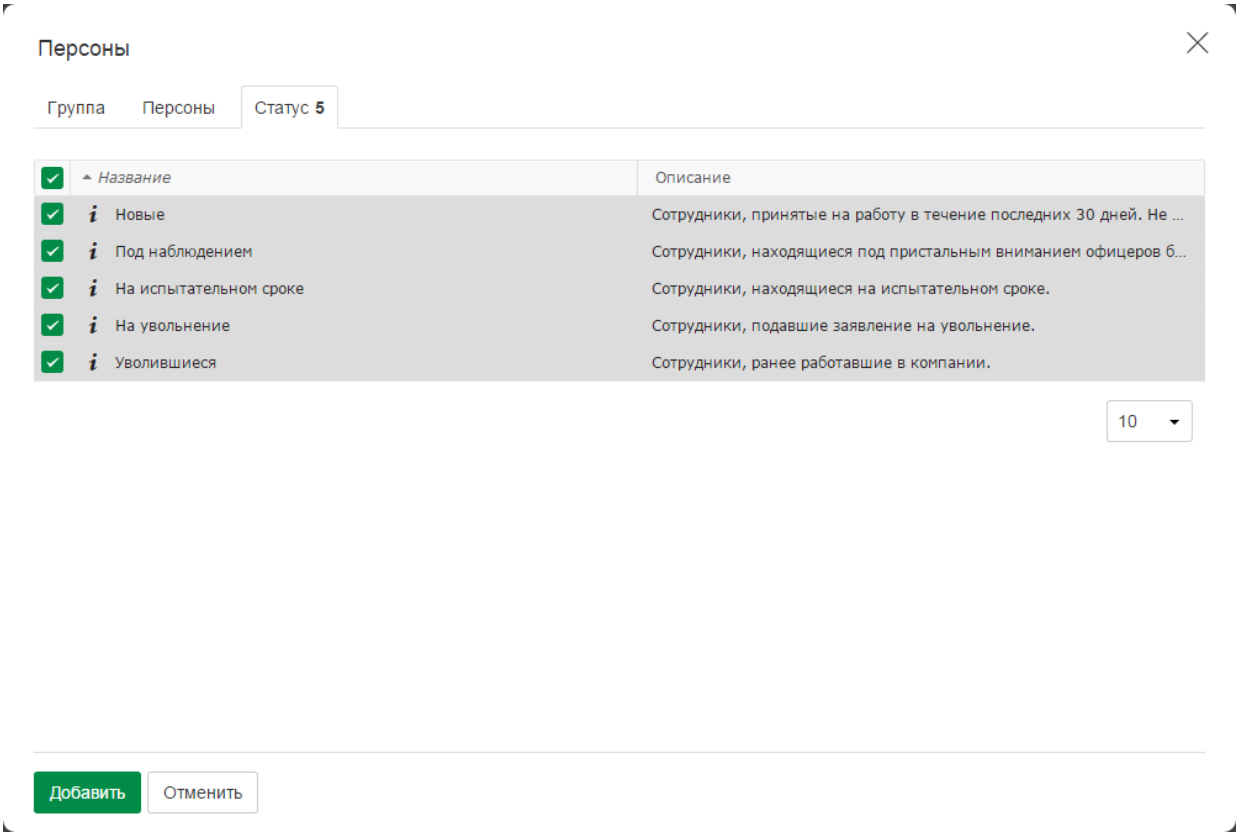


Рисунок 6. Добавление отправителей в область видимости

5. Нажмите **Добавить.**

4.3.3.2 Редактирование области видимости

Чтобы изменить параметры области видимости:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Области видимости**.
3. На панели инструментов нажмите  **Редактировать область видимости**.
4. В открывшемся окне измените параметры области видимости аналогично действиям по созданию области видимости (см. "Создание области видимости").
5. Нажмите **Сохранить**.

4.3.3.3 Удаление области видимости

Чтобы удалить область видимости:

1. Перейдите в раздел **Управление -> Управление доступом**.
2. Перейдите на вкладку **Области видимости**.

3. На панели инструментов нажмите  **Удалить область видимости**.

> **Примечание:**
>
> Чтобы удалить несколько областей видимости сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить**.

4. В появившемся окне нажмите **Да**.

4.4 Управление лицензиями

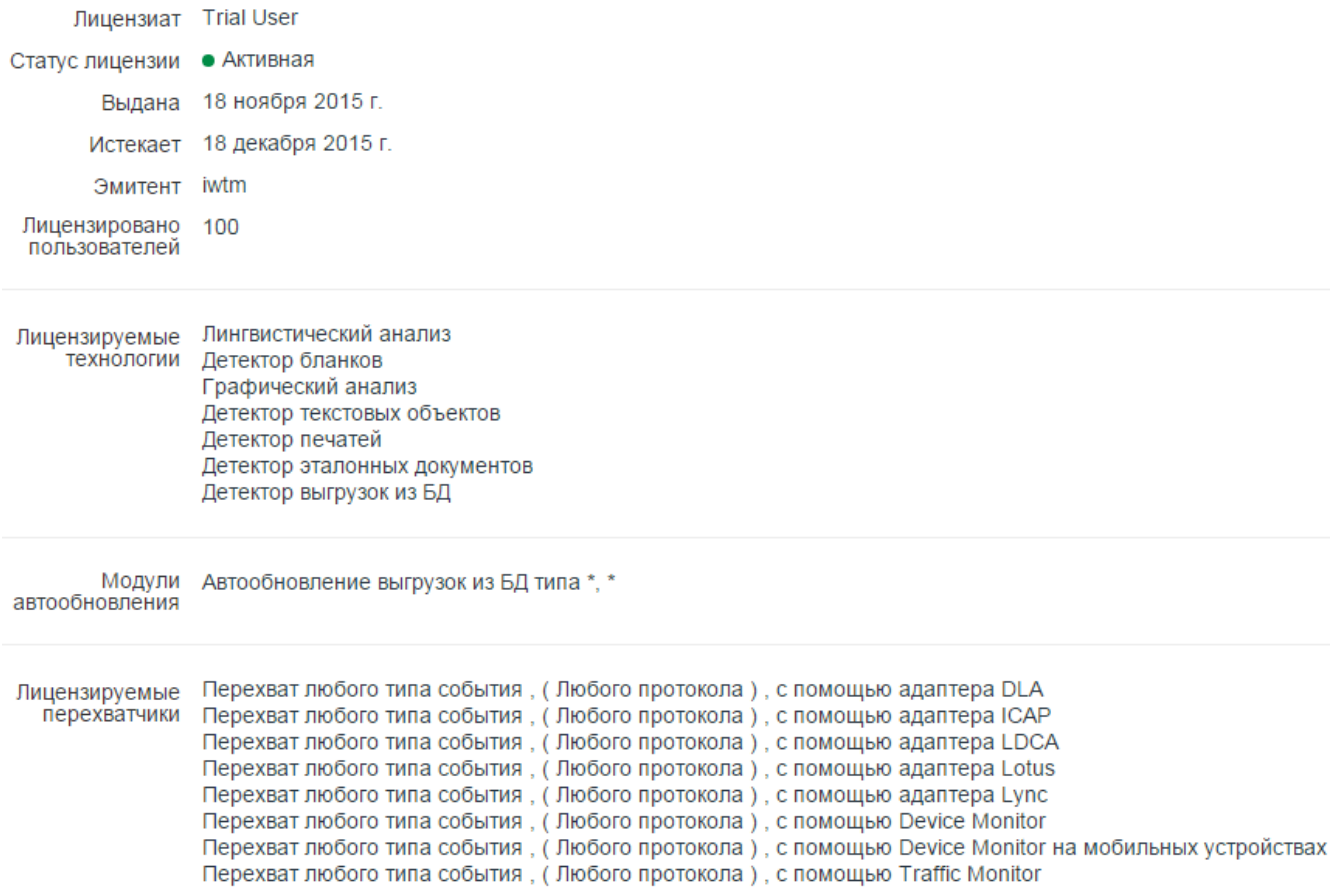
> **Важно!**
>
> Описание лицензирования Системы приведено в статье "Лицензирование".

Работа с лицензиями ведется в Консоли управления, в разделе **Управление –> Лицензии**:

- в левой части рабочей области Консоли управления расположены список лицензий и панель управления лицензиями.
- в центральной части рабочей области отображается информация о выбранной в списке лицензии.

Примечание:

Редактирование лицензии недоступно. Есть возможность только загрузить новую или удалить ранее созданную лицензию.



Доступны следующие действия с лицензиями:

- Установка лицензии;
- Удаление лицензии;
- Запрос лицензии.

4.4.1 Проверка валидности лицензии

Сведения о лицензируемых технологиях и перехватчиках, а также о статусе, сроке истечения и количестве лицензированных пользователей приведены в правой части рабочей области раздела **Управление –> Лицензии**.

Чтобы проверить валидность лицензии:

1. Перейдите в раздел **Управление -> Лицензии**.
2. Убедитесь, что значение поля **Истекает** содержит дату, которая еще не наступила.

3. Убедитесь, что значение поля **Лицензиат** соответствует значению параметра Licensee конфигурационного файла **license.conf**, расположенного в директории `/opt/iw/tm5/etc`.

4.4.2 Установка лицензии

Чтобы установить лицензионный ключ:

1. Перейдите в раздел **Управление -> Лицензии**.
2. На панели инструментов нажмите  **Добавить лицензию**.
3. В открывшемся окне нажмите **Загрузить**.
4. В открывшемся диалоговом окне выберите полученный по запросу файл **licence.lic** и нажмите **Открыть**.
   В открывшемся окне **Добавление лицензии** отобразятся сведения о лицензии и лицензируемых технологиях и перехватчиках.
5. Нажмите **Добавить**.
6. В открывшемся диалоговом окне нажмите **Да**.

Страница браузера перезагрузится, и новая лицензия будет добавлена в список установленных лицензий. Старую лицензию Вы можете оставить или удалить.

4.4.3 Удаление лицензии

Чтобы удалить лицензионный ключ:

1. В списке лицензий выделите целевую лицензию.
2. На панели инструментов нажмите  **Удалить**.

> **Примечание:**
>
> Чтобы удалить несколько лицензий сразу, выделите их в списке (например, удерживая нажатыми клавиши **<SHIFT>** или **<CTRL>**) и нажмите **Удалить**.

3. В открывшемся окне нажмите **Да**.

4.4.4 Запрос лицензии

Чтобы отправить запрос на получение лицензии:

1. Перейдите в раздел **Управление - Лицензии**;
2. В правом верхнем углу нажмите кнопку **Запросить лицензию**.

3. Отправьте автоматически сформированное письмо, при необходимости указав дополнительную информацию в теле письма.

4.5 Состояние системы

Просмотр состояний каждого из серверов, на которых развернута Система, ведется в Консоли управления, в разделе **Управление -> Состояние системы**.
Список индикаторов представлен в виде таблицы для каждого из используемых в Системе серверов:

	Параметр	Детальные данные
●	Общая нагрузка Системы	OK - load average: 0.21, 0.15, 0.19
●	Количество активных пользователей	USERS OK - 3 users currently logged in
●	Состояние локального почтового сервера	SMTP OK - 0.013 sec. response time
●	Отклонение системного времени	NTP OK: Offset -0.01090276241 secs
●	Ошибки в Alert-логе.	OK - no errors found in log
●	Размер Alert-лога базы данных.	OK - size of PostgresSQL system log is 9047 bytes
●	Состояние базы данных PostgreSQL.	OK - database postgres (0.003083 sec.)
●	Доступность сервера	PING OK - Packet loss = 0%, RTA = 0.06 ms
●	Свободное место в корневой партиции	DISK OK - free space: / 96362 MB (71% inode=98%):
●	Состояние службы синхронизации времени	OK - ntpd (pid 2491) is running...
●	Состояние службы Syslog	OK - 'rsyslogd' is running
●	Доступность сервера по SSH	SSH OK - OpenSSH_5.3 (protocol 2.0)
●	Использование файла подкачки	SWAP OK - 77% free (6145 MB out of 8015 MB)
●	Очередь обработки действий, указанных в примененных к событиям политиках.	OK - Blackboard queue: 0 item(s), 0.000 MBytes
●	Количество ошибок обработки действий из применённых к событиям политик.	OK - Blackboard-errors queue: 0 item(s), 0.000 MBytes
●	Наличие дампов памяти	OK
●	Состояние компонентов Системы	OK
●	Количество ошибок индексации событий службой INDEXER.	OK - index_error queue: 0 item(s)
●	TM_PG_INDEXER_QUEUE	OK - index_queue queue: 0 item(s)
●	Очередь загрузки в хранилище	OK - DB queue: 0 item(s), 0.000 MBytes
●	Очередь ошибок обработки	OK - Errors queue: 0 item(s), 0.000 MBytes
●	Очередь обработки почтового трафика	OK - SMTP queue: 0 item(s), 0.000 MBytes
●	Количество ошибок обработки событий службами IW_LOADER и IW_XML2LIRO	OK - XML2LIRO-errors queue: 0 item(s), 0.000 MBytes
●	Количество запущенных процессов	PROCS OK: 283 processes with STATE = RSZDT
●	Свободное место в партиции /var	DISK OK - free space: / 96361 MB (71% inode=98%):

Для каждого индикатора отображается следующая информация:

- **Статус** – текущее значение индикатора:
  - ● – CRITICAL, значение проверяемого параметра превышает критический порог;
  - ● – WARNING, значение проверяемого параметра находится в зоне предупреждения (если такая предусмотрена);
  - ● – OK, значение параметра находится в норме.
- **Параметр** – название индикатора.
- **Подробнее** – подробная информация о результатах проверки.

Важно!

Если значение индикатора получить не удалось, то считается, что текущее значение

индикатора превышает пороговое значение.

Показатели обновляются с периодичностью:

- каждые 5 минут – для параметров:
  - Ошибки в журнале предупреждений БД/DB Alert Log Errors
  - Использование файла подкачки/Swap usage
  - Размер журнала предупреждений БД/DB Alert log Size
- каждые 10 минут – для параметров:
  - Доступность сервера по SSH/SSH availability
  - Состояние базы данных/Database Status
  - Статус службы доступа к базе данных/Oracle TNS Status
- каждые 360 минут – для параметра Отклонение системного времени/NTP time deviation
- каждые 30 минут – для всех остальных параметров

Если требуется обновить показатели вручную, нажмите  **Обновить статус**.

4.5.1 Настройка параметров отправки уведомлений

Чтобы настроить параметры уведомлений о состоянии системы:

1. Перейдите в раздел **Управление** - **Состояние системы**;
2. Нажмите кнопку  **Параметры сервера мониторинга**;
3. Установите флажок в поле **Разрешить уведомления**.
4. Укажите значения для следующих параметров:

Параметр	**Описание**
Почтовый сервер	IP-адрес или DNS-имя почтового сервера, который будет использоваться для отправки уведомлений. Должен быть указан сервер, поддерживающий отправку писем без SMTP-аутентификации.
Порт почтового сервера	Порт почтового сервера. Значение по умолчанию: `25`
Почтовый префикс	Почтовый префикс используется для удобства сортировки почтовых сообщений из разных систем мониторинга. Введенное значение будет добавлено к началу строки поля «Тема» отправляемых почтовых сообщений. Значение по умолчанию: `IWTM`
Получатели	Почтовый адрес получателя/получателей. Значение по умолчанию: `nagios@localhost`

5. Нажмите *Отправить тестовое сообщение*, чтобы проверить работоспособность указанных настроек.
6. Нажмите **Сохранить**.

4.6 Управление службами

Администратору Системы предоставлена возможность управлять службами без использования командной строки Linux.

Доступны следующие действия со службами:

- Запуск службы;
- Остановка службы;
- Перезапуск службы;
- Сохранение логов службы.

4.6.1 Запуск службы

Чтобы запустить службу:

1. Перейдите в раздел **Управление - Службы**.
2. Установите флажок в поле службы, которую Вы хотите запустить.
3. Нажмите кнопку .
4. Выберите опцию **Запустить**.

> **Примечание:**
>
> Чтобы запустить несколько служб, необходимо установить флажок напротив каждой из них.

4.6.2 Остановка службы

Чтобы остановить службу:

1. Перейдите в раздел **Управление - Службы**.
2. Установите флажок в поле службы, которую Вы хотите остановить.

3. Нажмите кнопку .
4. Выберите опцию **Остановить**.

> **Примечание:**
>
> Чтобы остановить несколько служб, необходимо установить флажок напротив каждой из них.

4.6.3 Перезапуск службы

Чтобы перезапустить службу:

1. Перейдите в раздел **Управление - Службы**.
2. Установите флажок в поле службы, которую Вы хотите перезапустить.
3. Нажмите кнопку .
4. Выберите опцию **Перезапустить**.

> **Примечание:**
>
> Чтобы перезапустить несколько служб, необходимо установить флажок напротив каждой из них.

4.6.4 Сохранение логов службы

Чтобы сохранить логи службы:

1. Перейдите в раздел **Управление - Службы**.
2. Нажмите **Сохранить** в колонке **Логи** напротив службы, логи которой Вы хотите сохранить.

4.7 Сбор диагностических данных

Сбор диагностических данных выполняется в разделе **Управление - Сбор диагностических данных.**

Режим сбора данных	**Описание**

Режим сбора данных	Описание
Обычный	Информация о логах Системы, конфигурационная информация, данные о начальной установке
Расширенный	Информация о логах Системы, конфигурационная информация, данные о начальной установке, о ситуациях аварийного завершения процессов системы

Диагностическая информация будет собрана из следующих источников:

Тип данных	Путь к файлам

Логи	`/var/log/infowatch/*.log`
	`/var/log/nagios/nagios.log`
	`/root/iwsetup-install-logs/*`
	`/opt/distr/infowatch/appl-auto-update/appl_updater.log`
	`/home/oracle/addm/logs/*`
	`/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log`
	`/var/log/nagios/status.dat`

Конфигурационная информация	`/opt/iw/tm5/etc/*.conf`
	`/opt/iw/tm5/etc/scripts/*.lua`
	`/opt/iw/tm5/etc/config/vademecums/*.info`
	`/opt/iw/tm5/etc/config/vademecums/vademecum.list`
	`/etc/nagios/*`
	`/etc/nagios/objects/*`

Логи и скрипты начальной установки системы	`/root/iw*`

Чтобы скачать отчет по результатам последней диагностики:

1. Перейдите в раздел **Управление - Сбор диагностических данных**.
2. Нажмите на ссылку **Результаты последней диагностики доступны** в формате `dd-mm-yyyy_hh-mm-ss`.
3. Откройте архив.

Важно!

В случае, если диагностика ранее не проводилась, скачивание результатов последней диагностики доступно не будет.

Диагностические данные могут быть собраны следующими способами:

- Сбор диагностических данных в обычном режиме;
- Сбор диагностических данных в расширенном режиме.

4.7.1 Сбор диагностических данных в обычном режиме

Чтобы собрать диагностическую информацию в обычном режиме:

1. Перейдите в раздел **Управление - Сбор диагностических данных**.
2. Установите маркер в поле **Обычный**.
3. Нажмите кнопку Запустить диагностику.
4. Дождитесь завершения сборка диагностической информации.
5. В сплывающем окне нажмите **Загрузить**.

4.7.2 Сбор диагностических данных в расширенном режиме

Чтобы собрать диагностическую информацию в расширенном режиме:

1. Перейдите в раздел **Управление - Сбор диагностических данных**.
2. Установите маркер в поле **Расширенный**.
3. Нажмите кнопку Запустить диагностику.
4. Дождитесь завершения сборка диагностической информации.
5. В сплывающем окне нажмите **Загрузить**.

4.8 Аудит действий пользователя

Система предоставляет возможность отслеживать действия пользователя в Консоли управления.

Просмотр событий аудита и фильтры поиска по событиям выполняются в разделе **Управление - Аудит**.

Система фиксирует и отображает в разделе **События аудита** следующую информацию:

- вход в Систему и выход из Системы;
- управление объектами, отвечающими за разграничение доступа (пользователи, роли, области видимости);
- действия пользователя с объектами Системы (запросы, отчёты, политики, элементы классификатора и т. д.).

Примечание:

Изменения элементов вследствие отмены конфигурации не фиксируются в событиях аудита. В данном случае будет создано только событие отмены конфигурации.

Чтобы задать период хранения событий аудита:

1. Перейдите в раздел **Управление - Аудит**;
2. В области **Период хранения событий аудита (дни)** укажите количество дней хранения событий аудита;
3. Нажмите **Сохранить**.

Примечание:

События аудита в БД хранятся в формате UTC.
Если вы работает в другом часовом поясе, то события в день, подлежащий очистке, будут удалены по 23:59:59 UTC, что по вашему часовому поясу будет отличаться (UTC+ или UTC-) Например, для Москвы это будет означать 02:59:59 следующего дня (UTC+3:00).

Работа с событиями аудита описана в следующих разделах:

- События аудита;
- Фильтры поиска;
- Фильтрация по действию;
- Фильтрация по объекту;
- Фильтрация по дате.

4.8.1 События аудита

Область События аудита находится в разделе **Управление - Аудит**.

Область **События аудита** показывает результаты **Фильтров поиска** и представляет из себя список событий аудита в виде плашек со следующими атрибутами:

Атрибут	**Описание**
Пользователь	Имя пользователя, осуществившего действие
Объект	Имя объекта, над которым осуществлялось действие
Действие	Тип действия, которое было произведено пользователем
Дата и время действия	Дата/время зарегистрированного действия пользователя

Атрибут	Описание
Расширенная информация	Дополнительная информация о событии аудита

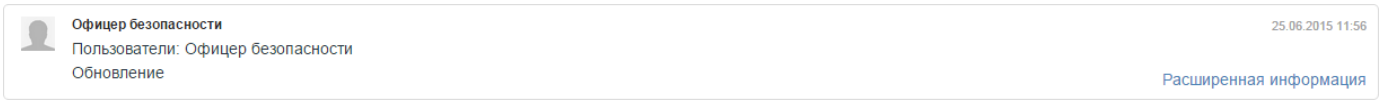
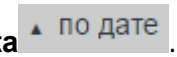


Рисунок 1. Плашка события аудита

Чтобы отсортировать события аудита по дате:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В левом верхнем углу нажмите **Сортировка** 

.

4.8.1.1 Расширенная информация

Расширенная информация будет отображена в зависимости от *Объекта* и *Действия* зарегистрированных в Системе.

Например, при выходе пользователя из Системы, параметры события аудита будут следующими:

- **DNS-имя** - имя компьютера, с которого происходит выход в Системы;
- **IP** - IP-адрес компьютера, с которого происходит выход в Системы;
- **Логин** - имя пользователя, который произвел выход из Системы.

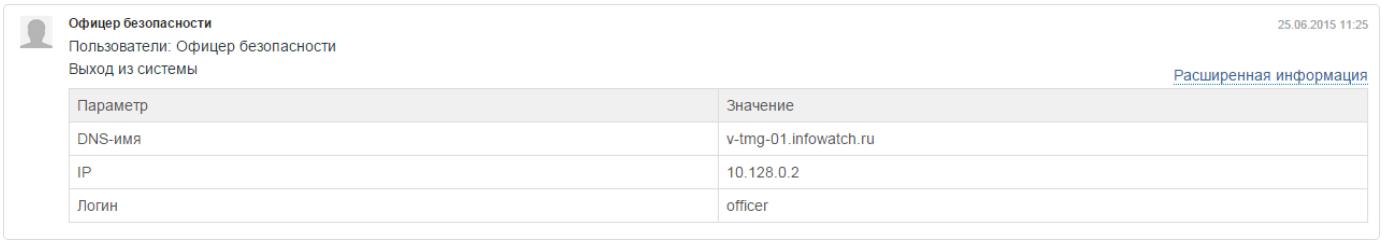


Рисунок 2. Расширенная информация

> **Важно!**
>
> Параметры события аудита могут варьироваться в зависимости от *Объекта* и *Действия*.

Чтобы посмотреть расширенную информацию о событии аудита:

1. Перейдите в раздел **Управление - Аудит**.
2. На плашке событий аудита нажмите **Расширенная информация**.

4.8.2 Фильтрация по пользователю

Чтобы отфильтровать события аудита по пользователю:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В области **Фильтры поиска** выберите имя пользователя из выпадающего списка **Пользователь** (см. "Управление пользователями Системы и их ролями").

Чтобы добавить дополнительные условия фильтрации, используйте параметры *Действие*, *Объект*, *Дата*.

4.8.3 Фильтрация по действию

Чтобы отфильтровать события по совершенному действию:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В области **Фильтры поиска** выберите действие из выпадающего списка **Действие**.

Чтобы добавить дополнительные условия фильтрации, используйте параметры *Пользователь*, *Объект*, *Дата*.

4.8.4 Фильтрация по объекту

Чтобы отфильтровать события по объекту:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В области **Фильтры поиска** выберите объект из выпадающего списка **Объект**.

Чтобы добавить дополнительные условия фильтрации, используйте параметры *Пользователь*, *Действие*, *Дата*.

4.8.5 Фильтрация по дате

Чтобы отфильтровать события по дате:

1. Перейдите в раздел **Управление** - **Аудит**;
2. В области **Фильтры поиска** нажмите на поле **Дата**.
3. В календаре укажите даты начала и конца периода, за который будут показаны события аудита.
4. Нажмите **Применить**.
5. Чтобы отменить фильтрацию по дате, нажмите **Очистить**.

Чтобы добавить дополнительные условия фильтрации, используйте параметры *Пользователь*, *Действие*, *Объект*.

4.9 Контроль целостности

Контроль целостности предназначен для отслеживания состояния системных файлов. Первичные эталонные суммы формируются Системой автоматически.

Контроль целостности системных файлов описан в следующих разделах:

- Ручная проверка целостности;
- Автоматическая проверка целостности;
- Принятие результата за эталонный.

4.9.1 Ручная проверка целостности

Чтобы проверить целостность системных файлов:

1. Перейдите в раздел **Управление** - **Контроль целостности**;
2. В центральной части рабочей области нажмите **Проверить целостность**.

> **Примечание:**
>
> В процессе проверки целостности будет отображаться сообщение **Выполняется проверка целостности**. По окончании проверки будет выведено сообщение с датой и временем последней проверки.

4.9.2 Автоматическая проверка целостности

Чтобы настроить автоматическую проверку целостности системных файлов:

1. Перейдите в раздел **Управление** - **Контроль целостности**;
2. В центральной части рабочей области включите настройку **Автоматическая проверка**.
3. В поле **Проверять ежедневно в** установите время проверки целостности при помощи стрелок **вверх** и **вниз**.
4. Нажмите **Сохранить**.

4.9.3 Принятие результата за эталонный

Чтобы принять результат проверки целостности как эталонный:

1. Перейдите в раздел **Управление** - **Контроль целостности**;
2. В центральной части рабочей области нажмите **Принять результат как эталонный**.

4.10 Плагины

Система использует плагины для подключения дополнительных перехватчиков. Расширение позволяет принимать события от внешних перехватчиков, а также автоматически обновлять эталонные выгрузки.

Любые Push API/Public API коннекторы внешних систем, должны быть зарегистрированы в ТМ путем добавления нового плагина.

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 контактов и типов событий (необязательно);
- файл **manifest.json**, содержащий информацию о плагине. Для плагинов, используемых для получения событий, и плагинов, используемых для обновления эталонных выгрузок, состав файла будет различаться.

Примечание:

Имена файлов, входящих в плагин должны содержать только символы латинского алфавита и/или цифры.

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

Название	**Является обязательным**	**Описание**
Версия	Да	Версия плагина
Идентификатор компании-разработчика	Да	Соответствует названию компании в лицензии
Используемые предустановленные типы событий, контакты и протоколы	Нет	Список предустановленных в Системе типов событий и протоколов, которые перехватываются с помощью данного плагина
Название	Да	Название плагина
Описание	Нет	Описание плагина
Признак "Предустановленный"	Нет	Входит ли в состав Системы

Название	Является обязательным	Описание
Регистрируемые типы событий, контакты и протоколы	Нет	Содержит следующие данные: • Тип регистрируемых событий с указанием типа сервиса, к которому он относится; • Протоколы; • Действия; • Код типа перехватчика для плагинов InfoWatch; • Локализации наименований типов событий минимум на одном языке; • Типы регистрируемых контактов и их локализация минимум на одном языке; • Файлы с иконками регистрируемых контактов и типов событий.
Уникальный идентификатор	Да	Уникальный 128-битный идентификатор (UUID) плагина

Для внешних систем – источников эталонных выгрузок файл **manifest.json** должен содержать следующую информацию:

Название	Является обязательным	Описание
Версия	Да	Версия плагина
Идентификатор компании-разработчика	Да	Соответствует названию компании в лицензии
Название	Да	Название плагина
Обновляемые типы данных	Да	Список эталонных выгрузок, которые обновляются с помощью данного плагина, с указанием систем-источников данных.
Описание	Да	Описание плагина.
Признак "Предустановленный"	Нет	Входит ли в состав Системы.
Уникальный идентификатор	Да	Уникальный 128-битный идентификатор (UUID) плагина.

В разделе **Плагины** можно осуществлять следующие действия:

- Добавление плагина;
- Удаление плагина;
- Работа с токенами.

Важно!

Плагины и токены удаляются из Системы при удалении схемы БД (см. "Infowatch Traffic Monitor 6.0. Руководство по установке", статья "Удаление схемы базы данных"). Для восстановления плагина Device Monitor:

1. Создайте файл **/opt/iw/tm5/www/backend/protected/runtime/first_run** от имени пользователя **iwtm**;
2. Перезапустите процесс **iw_kicker**:
   `service iwtm restart kicker`

Остальные плагины необходимо добавить вручную (см. "Добавление плагина").

4.10.1 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.

4.10.2 Удаление плагина

Чтобы удалить плагин:

1. Перейдите в раздел **Управление - Плагины**;
2. В области **Плагины** нажмите .
3. Нажмите **Да**, чтобы подтвердить удаление.

4.10.3 Работа с токенами

Токен предназначен для авторизации внешней Системы, использующей Push API/Public API. После добавления плагина, токен генерируется автоматически (см. "Добавление плагина").

Токен для InfoWatch Device Monitor создается автоматически и доступен в разделе **Управление -> Плагины -> Токены** Консоли управления.

Система предоставляет возможность следующих действий с токенами:

- Добавление токена;
- Удаление токена.

4.10.3.1 Добавление токена

Чтобы добавить токен:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите .

4.10.3.2 Удаление токена

Чтобы удалить токен:

1. Перейдите в раздел **Управление - Плагины**;
2. Выберите плагин в области **Плагины**;
3. Перейдите в закладку **Токены**;
4. Нажмите .

5 КОНФИГУРИРОВАНИЕ ПЕРЕХВАТЧИКА CRAWLER

Подсистема Crawler системы InfoWatch Traffic Monitor позволяет выполнять проверку файлов, находящихся в корпоративной сети, на предмет нарушения корпоративных политик безопасности. Таким образом, подсистема Crawler позволяет контролировать файловые ресурсы компании для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.
Подсистема Crawler работает как один из перехватчиков Traffic Monitor.
В работе Crawler участвуют следующие компоненты системы InfoWatch Traffic Monitor:

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

Важно!

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

Более подробная информация о настройке Crawler изложена в следующих разделах:

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

5.1 Настройка сетевых правил доступа

Если сегменты сети, где развернута система InfoWatch Traffic Monitor с Краулер, разделены между собой межсетевыми экранами, для корректной работы Краулер должны быть открыты TCP порты

6556 (подключение сканера Краулер к серверу Краулер) и **1337** (подключение Веб-сервера InfoWatch Traffic Monitor к серверу Краулер).
Более подробно информацию о сетевых портах, доступность которых необходима для эффективной работы системы, смотрите на следующей схеме и в таблице с пояснениями.

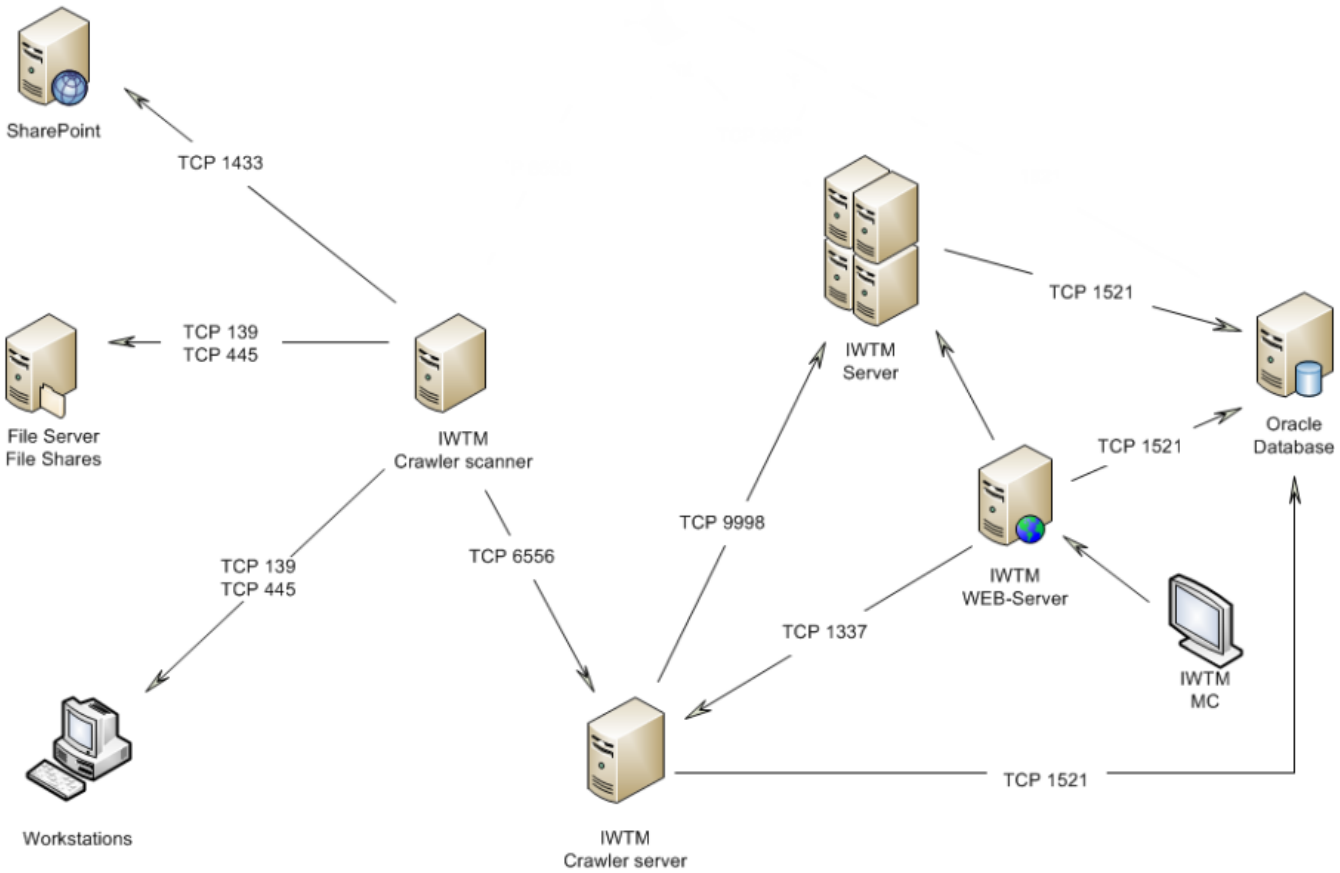
Примечание:

На схеме не указаны порты подключения:

- веб-консоли управления к веб-серверу IWTM;
- веб-сервера IWTM к серверу IWTM.

Порты не указаны, поскольку при установке с использованием kickstart указанные компоненты Системы устанавливаются на один компьютер.

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



Подключение	Порт
Сканер Краулер – сервер Краулер	TCP 6556

Подключение	Порт
Сервер Краулер – БД IWTM	TCP 1521
Сервер Краулер – IWTM	TCP 9998
Веб-сервер IWTM – сервер Краулер	TCP 1337
Сканер Краулер – рабочие станции и файловые сервера	TCP 139 TCP 445
Сканер Краулер – файловое хранилище SharePoint (сервер MS SQL)	TCP 1443

Важно!

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

Чтобы отключить брандмауэр в профиле домена:

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

Прмиечание:

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

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

5.2 Конфигурационные файлы Краулер

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

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

Files\InfoWatch\Crawler\Scanner для 32-битных систем и C:\Program Files (x86)\InfoWatch\Crawler\Scanner для 64-битных). Подробнее см. "Конфигурационный файл сканера Краулер".

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

5.2.1 Конфигурационный файл сервера Краулер

Администратор, обслуживающий систему, может выполнить некоторые низкоуровневые настройки сервера Краулер с помощью конфигурационного файла InfoWatch.Crawler.Server.exe.config. Конфигурационный файл размещается в том же каталоге, что и исполняемый файл InfoWatch.Crawler.Server.exe (по умолчанию - C:\Program Files\InfoWatch\Crawler\Server для 32-битных систем и C:\Program Files (x86)\InfoWatch\Crawler\Server для 64-битных).
Конфигурационный файл можно просматривать и редактировать при помощи любого текстового или XML-редактора. Кодировка файла - UTF-8.
Первоначальная настройка параметров выполняется во время установки Краулер (см. документ "InfoWatch Traffic Monitor. Руководство по установке").
Далее описаны параметры, которые может потребоваться изменять. Изменять остальные параметры настоятельно не рекомендуется.

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

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

Примечание:

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

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

5.2.1.1 Изменение учетной записи, от имени которой запускается служба сервера Краулер

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

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

5.2.1.2 Скрипты сканирования SharePoint

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

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

Чтобы обновить скрипты:

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

Примечание:

Если в процессе эксплуатации в скрипты сканирования были внесены изменения и при последующем обновлении Краулера их необходимо перенести в новую версию:

1. Сохраните измененные скрипты.
2. Произведите обновление Системы.
3. В папке `C:\Program Files (x86)\InfoWatch\Crawler\Server\SharePoint_scripts` замените скрипты на сохраненные ранее.
4. Перезапустите службу **InfoWatch Crawler Server Service**.

5.2.2 Конфигурационный файл сканера Краулер

Конфигурационный файл службы сканирования Crawler `InfoWatch.Crawler.Scanner.exe.config` размещается в том же каталоге, что и исполняемый файл `InfoWatch.Crawler.Scanner.exe` (по умолчанию - `C:\Program Files\InfoWatch\Crawler\Scanner` для 32-битных систем и `C:\Program Files (x86)\InfoWatch\Crawler\Scanner` для 64-битных).
Конфигурационный файл можно просматривать и редактировать при помощи любого текстового

или XML-редактора. Кодировка файла UTF-8.
При необходимости администратор Системы может изменить следующие параметры:

- Строка соединения с сервером Краулер. Данный параметр указывается в следующем блоке:

  ```
  <client>
  <endpoint name="ScannerEndpoint" binding="netTcpBinding"
  bindingConfiguration="EncryptedBinding" address="net.tcp://localhost:6556/Scanner"
  contract="InfoWatch.Crawler.Contracts.Server.IScannerDispatcher"/>
  </client>
  ```

  При изменении расположения сервера Краулер Вы можете в параметре address вместо указанного в примере значения localhost указать необходимый **IP-адрес или имя сервера**.

- Передача файлов в базу данных. Данный параметр указывается в следующем блоке:

  ```
  <setting name="SendEmptyFileToTm" serializeAs="String">
   <value>False</value>
   </setting>
  ```

  Если требуется, чтобы Краулер передавал в Traffic Monitor только результаты анализа файлов и не передавал теневые копии файлов, измените параметр `value` на **True**. В этом случае в Traffic Monitor будут передаваться файлы нулевой длины.

Изменять остальные параметры настоятельно не рекомендуется.

5.2.3 Выключение шифрования трафика между компонентами

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

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

5.3 Работа с журналами Краулер

Администратор системы может получить информацию о работе сканера и сервера Краулер из файлов журналов, расположенных в домашней директории пользователя, от имени которого

запускается сервис, в поддиректории %appdata%\InfoWatch\TM\Logs. Так, например, если сканер Краулер установлен с параметрами по умолчанию, то он запускается от имени Local System Account и для Windows 7 журналы сканера Краулер располагаются в директории: C:\Windows\System32\config\systemprofile\AppData\Roaming\InfoWatch\TM\Logs

Примечание:

При установке на ОС Windows 7 журналы сервера Краулер по умолчанию располагаются в директории C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\InfoWatch\TM\Logs.

Изменение расположения файлов журнала

Расположение файлов журнала определяется в конфигурационных файлах (InfoWatch.Crawler.Server.exe.config и InfoWatch.Crawler.Scanner.exe.config: см. "Конфигурационные файлы Краулер"), в секции <configuration>, значение для <listeners>, например:

```
<configuration>
 …
 <loggingConfiguration>
 <listeners>
 …
 <add name="Rolling Flat File Trace Listener" fileName="путь_к_файлу_журнала" …>
 …
```

Настройка уровня логирования Краулер

Настройка уровня логирования выполняется в конфигурационных файлах (InfoWatch.Crawler.Server.exe.config и InfoWatch.Crawler.Scanner.exe.config: см. "Конфигурационные файлы Краулер").

Уровень логирования настраивается в разделе <specialSources>, параметр <allEvents switchValue="All" name="All Events">. По умолчанию задано значение **All**: ведется запись обо всех событиях. Вы можете изменить это значение на одно из следующих (перечислено в порядке уменьшения подробности): **All**, **Verbose**, **Information**, **Warning**, **Error**, **Critical**, **Off**.

5.4 Автоматическое удаление событий Краулер

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

1. Подключитесь к серверу ТМ.
2. В каталоге /opt/iw/tm5/etc/scripts/ откройте конфигурационный файл **system.lua**.
3. Закомментируйте следующие строчки кода:

```
if get_monitor(root) == 'CRAWLER' and
root:xFind('/root/processing[count(postanalysis/*|policies/policy)>0]').count == 0
then – RM: Не удаляем объекты с ошибками анализа
if root:xFind('//object/processing/messages/message[@module="cas"][@severity="fatal"
or @severity="error"]').count == 0 then
processing:find_or_add_child('delete_content'):set_text('true');
```

```
end
end
```

4. Сохраните изменения.

6 МОНИТОРИНГ

Подсистема мониторинга выполняет следующие функции:

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

Подсистема мониторинга автоматически устанавливается при установке серверных компонентов системы InfoWatch Traffic Monitor с помощью программы-инсталлятора (**kickstart**). О порядке установки см. документ «InfoWatch Traffic Monitor. Руководство по установке и конфигурированию».

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

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

Просмотр индикаторов мониторинга осуществляется также администратором Системы (см. "Состояние системы").

6.1 Настройки подсистемы мониторинга

Важно!

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

Настройка подсистемы мониторинга включает следующие задачи:

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

- Настройка порогов срабатывания для индикатора нагрузки;
- Настройка механизма уведомлений.

6.1.1 Настройка подключения Device Monitor

Чтобы настроить мониторинг для сервера Device Monitor:

1. Отредактируйте файл **/etc/nagios/iwmon/iwmon-hosts-dm.cfg**:
    - Раскомментируйте секции `host` и `hostgroup`.
    - В параметре `address` секции `host` определите имя хоста или IP-адрес сервера Device Monitor.
2. В файле `/etc/nagios/iwmon/iwmon-services-dm.cfg` раскомментируйте секцию `service`.
3. В файле `/etc/nagios/iwmon/iwmon-commands.cfg` раскомментируйте секцию `Check Dm server`.
4. Перезапустите процесс nagios:
   `service nagios restart`

6.1.2 Ручная настройка индикаторов

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

- iwmon-services-db-psql.cfg – настройка индикаторов для базы данных Postgre SQL;
- iwmon-services-db.cfg – настройка индикаторов для базы данных Oracle;
- iwmon-services-dm.cfg – настройка индикаторов для Device Monitor;
- iwmon-services-loadavg.cfg – настройка параметров нагрузки на серверы (индикатор Общая нагрузка системы);
- iwmon-services.cfg – настройка основных индикаторов;
- iwmon-services-queue.cfg – настройка индикаторов очередей;
- iwmon-services-traffic.cfg – настройка индикатора трафика из подсетей.

Параметр `service_description` отображает назначение каждого индикатора.

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

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

Чтобы применить изменения, перезапустите процесс nagios:

`nagios service restart`

6.1.3 Настройка адреса сервера синхронизации времени для подсистемы мониторинга

Для корректной синхронизации времени, на всех серверах системы необходимо указать IP-адрес NTP-сервера. Вы можете использовать любую службу точного времени, работающую по протоколу

NTP и доступную из вашей сети: как сетевое оборудование, так и контроллеры домена Windows.
Чтобы настроить синхронизацию времени на сервере:

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

6.1.4 Настройка порогов срабатывания для индикатора нагрузки

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

6.1.5 Настройка механизма уведомлений

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

- Настройка отправки уведомлений о превышении порогового значения индикаторов;
- Настройка отправки писем-уведомлений с помощью Postfix.

6.1.5.1 Настройка отправки уведомлений о превышении порогового значения индикаторов

Чтобы настроить отправку почтовых уведомлений:

1. В конфигурационном файле **/etc/nagios/private/resource-notify-iw.cfg** в качестве значения параметра `$USER10$` укажите сервер Postfix, встроенный в систему Traffic Monitor, и используемый порт. Например:
   `$USER10$=localhost:25`
2. В конфигурационном **файле /etc/nagios/iwmon/iwmon-contacts.cfg** добавьте контакты, на которые будут отправляться уведомления. Для этого нужно для каждого контакта добавить секцию вида:

```
define contact{
        contact_name                    <название контакта>
        use                             generic-contact
        alias                           Recipient Notification
        service_notification_commands   iw-notify-service-by-email
        host_notification_commands      iw-notify-host-by-email
        email                           <адрес>
        register                        1
}
```

Примечание:

Также в этой секции можно указать дополнительные настройки отправки уведомлений, например, время отправки и события, при которых будут отправляться уведомления. Подробную информацию Вы можете найти в документации Nagios.

3. В этом же файле, в поле `members`, укажите названия контактов, на которые будут отсылаться уведомления. Контакты указываются через запятую:
```
define contactgroup{
        contactgroup_name            admins
        alias                        IW Nagios Notification Recipient
        members                      <название контакта>, <название контакта1>
}
```
4. Перезапустите Nagios, выполнив следующую команду:
```
service nagios restart
```

Уведомления будут содержать следующую информацию:

- Название индикатора;
- Имя сервера, на котором контролируемый индикатор превысил пороговое значение;
- IP адрес этого сервера;
- Текущее состояние индикатора;
- Дата и время превышения порогового значения индикатора;
- Системное сообщение от источника.

Чтобы настроить отправку почтовых уведомлений для выбранных индикаторов:

1. Зайдите в каталог подсистемы Nagios:
```
cd /etc/nagios/iwmon
```
2. Откройте файл iwmon-services.cfg:
```
 nano /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
5. Сохраните изменения.

Примечание:

В случае если в конфигурационном файле отсутствует параметр `notifications_enabled`, добавьте его вручную.

6.1.5.2 Настройка отправки писем-уведомлений с помощью Postfix

Если Система установлена так, что:

- отправка SMTP-писем выполняется с использованием Postfix (см. «*InfoWatch Traffic Monitor. Руководство по установке*», раздел «Схемы развертывания Системы и выбор типа установки»),

и

- подсистема мониторинга установлена на тот же сервер, что и Postfix,

то для корректной отправки писем с уведомлениями:

1. В файле `/etc/postfix/transport` добавьте строчки вида:
   `example@example.com smtp:[mailserver]`
   где `example@example.com` - адрес, на который должны отправляться почтовые сообщения, а `mailserver` – имя почтового сервера компании.
   Для каждого адресата должна быть указана отдельная строчка.

Важно!

Для проектов, находящихся на поддержке InfoWatch, в списке должен присутствовать адрес monitoring@infowatch.com.

2. Выполните команду:

   ```
   postmap /etc/postfix/transport
   ```

3. В файл /etc/postfix/main.cf добавьте параметр transport_maps:
   `transport_maps = hash:/etc/postfix/transport`
4. Перезагрузите Postfix:
   `service postfix restart`

7 АДМИНИСТРИРОВАНИЕ БАЗЫ ДАННЫХ

Этот раздел содержит информацию по администрированию:

- Oracle;
- Postgre SQL.

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

7.1 Oracle

Раздел содержит инструкции по администрированию Oracle:

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

7.1.1 Проведение регламентных работ на сервере базы данных

Важно!

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

При выполнении регламентных работ на сервере базы данных придерживайтесь такого порядка:

1. Закройте все окна браузера, отображающие Консоль управления. Убедитесь, что отсутствуют соединения со схемой БД Traffic Monitor из других программ. Если такие соединения есть, отключите их.
2. На сервере Traffic Monitor остановите процессы ТМ:
   ```
   service iwtm stop
   service 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. Выполните необходимые работы с базой данных.

7. 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>
```

8. Запустите процессы Traffic Monitor Server:
```
service iwtm start
service 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
dbms_scheduler.enable('JOB_1');
…
dbms_scheduler.enable('JOB_N');
COMMIT;
END;
/
```
где JOB_1… JOB_N – имена ранее остановленных заданий.

7.1.2 Табличные пространства в базе данных InfoWatch Traffic Monitor

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

Тип табличного пространства	Назначение
Основное	Хранение настроек, которые нужны для анализа и обработки объектов (конфигурация, теги, цвета и пр.). Управление системой через Консоль управления (роли, учетные записи пользователей и др.)
Ежедневное	Хранение объектов, перехваченных в течение одних суток. Хранение информации о результатах анализа и обработки объектов (разобранный объект, категории, термины и др.). Состоит из двух табличных пространств: для хранения объектов со статусами *Нарушение* и *Нет нарушений*. 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:

- <*SchemaOwner*>_*YYYY_MM_DD_N* – табличное пространство за день, которое содержит объекты без нарушений.
- <*SchemaOwner*>_*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. Для удержания определенных событий в Базе Данных возможно назначать событию тег *Защита от удаления*. В этом случае событие не будет удалено автоматически (см. "InfoWatch Traffic Monitor. Руководство пользователя").

7.1.3 Управление ежедневными табличными пространствами

В этом разделе:

- Настройка размещения файлов в файловой системе;
- Индексирование данных в ежедневных табличных пространствах;
- Архивирование ежедневных табличных пространств;
- Восстановление ежедневных табличных пространств;
- Удаление ежедневных табличных пространств.

7.1.3.1 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.

7.1.3.2 Индексирование данных в ежедневных табличных пространствах

Контекстный поиск по тексту перехваченных объектов возможен при условии, что в базе данных регулярно выполняется индексация поступающих данных. По умолчанию задание на индексацию запускается каждые 20 минут.

Примечание:

При необходимости Вы можете останавливать и запускать задание вручную (см. "Проведение регламентных работ на сервере базы данных").

Корректность работы задания на индексацию данных (отсутствие зависаний) можно проверить, выполнив следующий запрос от имени владельца схемы базы данных:

```
select t.REQ_START_DATE, t.actual_start_date, t.RUN_DURATION
from sys.user_scheduler_job_run_details t
```

```
where t.job_name='IWTM_SYNC_INDEXES' and t.LOG_DATE > sysdate - 3/24
```

По результатам запроса выводится информация о работе задания на индексацию данных за последние 3 часа. Если интервал индексации не менялся, то задание должно запускаться каждые 20 минут и выполняться менее чем за 20 минут. При сильной загрузке базы данных следует выполнять эту проверку периодически, с интервалами в несколько часов.

Изменение интервала индексации

> **Примечание:**
>
> Контекстный поиск по объектам, загруженным в базу данных, становится возможен только после того, как эти объекты будут проиндексированы. Это необходимо учитывать при изменении интервала между процедурами индексации.

Далее показано несколько примеров использования сценария.Чтобы изменить интервал индексации, запустите сценарий:

```
DECLARE
 v_start_date date;
 v_repeat_interval VARCHAR2(100);
 BEGIN
 v_start_date := SYSDATE;
 v_repeat_interval := 'FREQ=MINUTELY; INTERVAL=10';
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
 COMMIT;
 END;
 /
```

где:

- v_start_date – дата и время запуска задания. Указывается в любом из форматов даты, поддерживаемых СУБД Oracle.
- v_repeat_interval – частота выполнения задания. Определяется параметрами:
    - FREQ. Размерность частоты, с которой будет выполняться задание. Допустимы следующие значения: DAILY, WEEKLY, MONTHLY, HOURLY, MINUTELY.
    - INTERVAL. Значение частоты с выбранной размерностью. Допустимы целые значения от 1 до 99.

Пример 1. Запуск индексации 1 раз в минуту

```
DECLARE
 v_start_date date;
 v_repeat_interval VARCHAR2(100);
 BEGIN
 v_start_date := SYSDATE;
 v_repeat_interval := 'FREQ=MINUTELY; INTERVAL=1';
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
 COMMIT;
 END;
 /
```

Пример 2. Запуск индексации 1 раз в 2 часа

```
DECLARE
 v_start_date DATE;
 v_repeat_interval VARCHAR2(100);
 BEGIN
 v_start_date := SYSDATE;
 v_repeat_interval := 'FREQ= HOURLY; INTERVAL=2';
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
 COMMIT;
 END;
 /
```

Пример 3. Запуск индексации ежесуточно в 00 ч 00 мин 00 с, начиная со следующего дня

```
DECLARE
 v_start_date DATE;
 v_repeat_interval VARCHAR2(100);
 BEGIN
 v_start_date := trunc(SYSDATE + 1);
 v_repeat_interval := 'FREQ= DAILY; INTERVAL=1';
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','START_DATE', v_start_date);
 dbms_scheduler.set_attribute('IWTM_SYNC_INDEXES','REPEAT_INTERVAL', v_repeat_interval);
 COMMIT;
 END;
 /
```

7.1.3.3 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").

7.1.3.3.1 Автоматическое архивирование ежедневных табличных пространств

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

```
select value
```

120

```
from setting

where setting = 'archive_path'
```

Пользователь `oracle` должен являться владельцем каталога.

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

```
begin;

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

commit;
```

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

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

```
begin
 sp_setting_set('violation_archive_enabled', 1);
 sp_setting_set('violation_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 архивироваться Системой.

- 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;
```

где:
1 – показатель того, что автоматическое архивирование включено (чтобы выключить, вместо 1 используйте значение 0);
D – количество дней, по истечении которого ежедневное табличное пространство будет архивироваться Системой.

7.1.3.3.2 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:
   `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 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'`

7.1.3.4 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
   .

7.1.3.5 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. После удаления табличных пространств, которые отключены от базы данных (имеют статус *Offline*), остаются файлы данных. Чтобы освободить пространство на жестком диске, удалите эти файлы вручную.
3. Процедура IWTM_DELETE_TABLESPACES не работает с теми табличными пространствами, которые были отключены/подключены вручную.

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

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

Примечание:

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

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

Важно!

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

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

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

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

где:
1 – показатель того, что автоматическое удаление включено (чтобы выключить, вместо 1 используйте значение 0);

D – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

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

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

где:
1 – показатель того, что автоматическое удаление включено (чтобы выключить, вместо 1 используйте значение 0);
D – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

Включение запуска процедуры 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;
 /
```

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

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

7.1.4 Резервное копирование базы данных

Для снижения рисков потери данных рекомендуется ежемесячно выполнять создание резервной копии (бэкапа) базы данных. Для хранения бэкапов рекомендуется использовать специально выделенные системы хранения.
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.

7.1.4.1 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.

7.1.4.1.1 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 программы-инсталлятора (kickstart), 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
   ```

7.1.4.1.2 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.

7.1.4.1.3 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
   ```

7.1.4.1.4 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 kickstart IWTM, 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 kickstart IWTM 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`

7.1.4.1.5 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
   ```

7.1.4.1.6 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:
   `OS> service iwtm stop`
   По окончании процедуры резервного копирования сервисы можно запустить с помощью следующих команд:
   `OS> service iwtm start`

7.1.4.1.7 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`

7.1.4.1.8 Копирование файлов БД в хранилище резервных копий

1. Убедитесь, что все сервисы Oracle остановлены. 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 программы-инсталлятора (**kickstart**) и были оставлены параметры по умолчанию, то пути будут такими:
   скопируйте содержимое директории **/u01/app/oracle/oradata/iwtm/** - в директорию **/opt/IWTM_Backup_Files/IWTM**,
   а директорию **/u02/oradata/** - в директорию **/opt/IWTM_Backup_Files/Oradata**
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.

7.1.4.2 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".

7.1.4.2.1 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. Установите БД Oracle согласно инструкции, приведенной в документе «*InfoWatch Traffic Monitor. Руководство по установке*».
3. Выполните следующие шаги:
    a. Удалите все содержимое папок **/u02/oradata/** и **/u01/app/oracle/oradata/iwtm/**
    b. Скопируйте содержимое директории **/opt/IWTM_Backup_Files/Oradata/** в директорию **/u02/oradata/**
    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/Oradata/**, в **control02.ctl** и скопируйте его в директорию **/u01/app/oracle/fast_recovery_area/iwtm/**
    e. Проверьте права.
4. При необходимости, измените их:
```
OS> chown oracle:oinstall /u02/oradata –R
OS> chown oracle:oinstall /u01/app/oracle/oradata/iwtm/ -R
OS> chown oracle:oinstall /u01/app/oracle/fast_recovery_area/iwtm/ -R
```
5. Запустите БД
```
OS> dbstart $ORACLE_HOME
```

7.1.4.2.2 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.

7.2 Postgre SQL

Чтобы подключиться к серверу БД из терминала сервера Traffic Monitor, используйте следующую команду:

```
psql postgre iwtm
```

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/postgresql/database.conf**.

Раздел содержит инструкции по администрированию Postgre SQL:

- Табличные пространства в базе данных InfoWatchTraffic Monitor;
- Управление ежедневными табличными пространствами;
- Резервное копирование базы данных.

7.2.1 Табличные пространства в базе данных InfoWatchTraffic Monitor

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

Тип табличного пространства	Назначение

Тип табличного пространства	Назначение
Основное	Хранение настроек, которые нужны для анализа и обработки объектов (конфигурация, теги, цвета и пр.). Управление системой через Консоль управления (роли, учетные записи пользователей и др.)
Ежедневное	Хранение объектов, перехваченных в течение одних суток. Хранение информации о результатах анализа и обработки объектов (разобранный объект, категории, термины и др.). Состоит из двух табличных пространств: для хранения объектов со статусами *Нарушение* и *Нет нарушений*. Таким образом, достигается возможность раздельного архивирования, восстановления и удаления.

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

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

Параметры, предназначенные для управления сегментами данных, задаются при настройке схемы базы данных, но могут быть переопределены после создания схемы (см. "Управление ежедневными табличными пространствами").
При использовании типа установки **TM Standard**, события хранятся в едином табличном пространстве. Автоматический расчет свободного места для будущих событий с освобождением пространства происходит еженедельно. Для удержания определенных событий в Базе Данных возможно назначать событию тег *Защита от удаления*. В этом случае событие не будет удалено автоматически (подробнее см. "Infowatch Traffic Monitor 6.0. Руководство пользователя", статья "Работа с тегами").

7.2.2 Управление ежедневными табличными пространствами

В этом разделе:

- Настройка размещения файлов в файловой системе;
- Архивирование ежедневных табличных пространств;
- Восстановление ежедневных табличных пространств;
- Удаление ежедневных табличных пространств.

7.2.2.1 Архивирование ежедневных табличных пространств

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

Важно!

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

Архивирование может выполняться:

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

7.2.2.1.1 Автоматическое архивирование ежедневных табличных пространств

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

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

Пользователь postgre должен являться владельцем каталога.

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

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

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

- Для ежедневного табличного пространства, хранящего объекты со статусом *Нарушение*:
  ```
  begin;
  select sp_setting_set('violation_archive_enabled', '1');
  select sp_setting_set('violation_archive_period', 'D');
  commit;
  ```

1 – показатель того, что автоматическое архивирование включено (чтобы выключить, вместо 1 используйте значение 0);
D – количество дней, по истечении которого ежедневное табличное пространство будет архивироваться Системой.

- Для ежедневного табличного пространства, хранящего объекты со статусом *Нет нарушений*:
  ```
  begin;
  select sp_setting_set('noviolation_archive_enabled', '1');
  select sp_setting_set('noviolation_archive_period', 'D');
  ```

```
commit;
```

где:
1 – показатель того, что автоматическое архивирование включено (чтобы выключить, вместо 1 используйте значение 0);
D – количество дней, по истечении которого ежедневное табличное пространство будет архивироваться Системой.

7.2.2.1.2 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 <= date_trunc('day', current_date) - '100 days'::interval  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.

Архивное табличное пространство расположено в отдельных каталогах.
Чтобы получить имена этих каталогов, выполните следующий запрос:

```
select s.value || t.tbs_name archive_path

from tbs_list t

inner join setting s on s.setting  = 'archive_path'

where t.part_date <= date_trunc('day', current_date) - '100 days'::interval  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 <*SchemaOwner*>_iwtm_add_parts, <*SchemaOwner*>_iwtm_delete_tablespaces, <*SchemaOwner*>_iwtm_archive_tablespaces так как это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:
   `select pkg_part_archive_tablespace(N);`
   где `N` – это значение атрибута `tbs_id` целевого ТП из таблицы `tbs_list`.
   После выполнения этого сценария статус ежедневного ТП изменится на *Отключено от базы данных*.
2. Повторите вызов процедуры для каждого ежедневного ТП, которое нужно отключить.

Перенос файлов данных

Перенесите каталоги с заархивированными табличными пространствами, принадлежащие отключенным ежедневным ТП, на другой носитель информации.
Для получения списка отключенных табличных пространств используйте команду:
`select 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'`

7.2.2.2 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 <*SchemaOwner*>_iwtm_add_parts, <*SchemaOwner*>_iwtm_delete_tablespaces и <*SchemaOwner*>_iwtm_archive_tablespaces. Это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:
   `select pkg_part_restore_tablespace(N);`

где N – ID табличного пространства (указывается в tbs_list).
После выполнения процедуры статус ежедневного ТП изменится на *Восстановлено*.

2. Повторите вызов процедуры для каждого ежедневного ТП, которое нужно подключить.

7.2.2.3 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. "InfoWatch Traffic Monitor. Руководство по установке") задается использование одного ежедневного табличного пространства, расположенного в `/u02/pgdata`.

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.

7.2.2.4 Удаление ежедневных табличных пространств

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

Важно!

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

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

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

Примечание:

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

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

Важно!

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

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

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

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

где:
1 – показатель того, что автоматическое удаление включено (чтобы выключить, вместо 1 используйте значение 0);

D – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

- Для ЕТП, хранящего объекты со статусом *Нет нарушений*:
  ```
  begin;
  select sp_setting_set('noviolation_delete_enabled', '1');
  select sp_setting_set('noviolation_delete_period', 'D');commit;
  ```

где:
1 – показатель того, что автоматическое удаление включено (чтобы выключить, вместо 1 используйте значение 0);
D – количество дней, по истечении которого ежедневное табличное пространство будет удаляться Системой.

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

```
select pkg_part_delete_tablespaces()
```

7.2.3 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 Postgre, 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.

7.2.3.1 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 каталов для резервной копии;
- Остановка системы;
- Копирование файлов БД в хранилище резервных копий;
- Остановка Postgre SQL.

7.2.3.1.1 Определение размера резервной копии

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

1. Войдите в систему от имени пользователя **root**;
2. Получите суммарный размер каталогов:
   ```
   du -sx -BM /u01/postgres/ /u01/iwtm_main/ /u01/iwtm_data/
   ```

7.2.3.1.2 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.

7.2.3.1.3 Создание каталов 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/Pgdata
   mkdir /opt/IWTM_Backup_Files/IWTM_main
   mkdir/opt/IWTM_Backup_Files/IWTM_data
   ```

7.2.3.1.4 Остановка системы

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

Чтобы остановить систему:

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

7.2.3.1.5 Остановка Postgre SQL

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

Чтобы остановить Postgre SQL БД:

1. На компьютере, где работает база данных, зайдите в систему от имени пользователя **root**.
2. В командной строке введите:
   ```
   service pgagent-9.4 stop
   service postrgesql-9.4 stop
   ```
   По окончании процедуры резервного копирования сервисы можно запустить с помощью следующей команды:
   ```
   service pgagent-9.4 start
   service postrgesql-9.4 start
   ```

7.2.3.1.6 Копирование файлов БД в хранилище резервных копий

1. Убедитесь, что все сервисы Postgre SQL остановлены. Если сервисы Postgre SQL не остановлены, файлы резервной копии могут быть повреждены и оказаться непригодными для восстановления.
2. На компьютере, где установлена БД, скопируйте директории (со всем содержимым) с помощью ранее созданного списка директорий.
   Если система была установлена с помощью программы-инсталлятора (kickstart) и были оставлены параметры по умолчанию, то пути будут такими:
   скопируйте содержимое директории **/u01/iwtm_main/** и **/u01/iwtm_data/** - в директории **/opt/IWTM_Backup_Files/IWTM_main** и **/opt/IWTM_Backup_Files/IWTM_data** соответственно, а директорию **/u01/postgres/** - в директорию **/opt/IWTM_Backup_Files/Pgdata**

7.2.3.2 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").

7.2.3.2.1 Восстановление на той же базе данных

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

Чтобы восстановить базу данных с помощью создания новой базы данных:

1. Убедитесь в работоспособности БД. Проверьте существующую схему БД, сервер БД, где размещена эта схема, и компьютер, на котором работает сервер БД;
2. Остановите сервисы Postgre SQL:
   `service pgagent-9.4 stopservice postrgesql-9.4 stop`
3. Установите БД Postgre SQL согласно инструкции, приведенной в документе «InfoWatch Traffic Monitor. Руководство по установке».
4. Выполните следующие шаги:
   Удалите все содержимое каталогов **/u01/iwtm_main/**, **/u01/iwtm_data/** и **/u01/postgres/**
   Скопируйте содержимое директории **/opt/IWTM_Backup_Files/Pgdata** в директорию **/u01/postgres/**
   Скопируйте содержимое директории **/opt/IWTM_Backup_Files/IWTM_main/** в директорию **/u01/iwtm_main/**
   Скопируйте содержимое директории **/opt/IWTM_Backup_Files/IWTM_data/** в директорию **/u01/iwtm_data/**
5. Проверьте права.
   При необходимости, измените их:`chown postgres /u01/iwtm_main/ –R`
   `chown postgres /u01/iwtm_data/ –R`
   `chown postgres /u01/postgres/ –R`
6. Запустите базу данных:`service postrgesql-9.4 start`
   `service pgagent-9.4 start`

7.2.3.2.2 Восстановление на новой базе данных

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

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

8 АДМИНИСТРИРОВАНИЕ СЕРВЕРНОЙ ЧАСТИ INFOWATCH TRAFFIC MONITOR

В этой главе:

- Процессы серверной части Traffic Monitor Server;
- Настройка конфигурационных файлов серверной части Traffic Monitor;
- Настройка параметров работы с HTTP-запросами, передаваемыми по протоколу ICAP (файл icap.conf);
- Настройка параметров обработки архивов вложений;
- Архивирование каталога очереди сообщений;
- Логирование работы Системы;
- Загрузка очередей объектов;
- Восстановление работоспособности системы в аварийных ситуациях;
- Настройка передачи информации в SIEM;
- Удаление временных файлов.

8.1 Процессы серверной части Traffic Monitor Server

В этом разделе:

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

8.1.1 Список процессов серверной части Traffic Monitor

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

Назначение	Имя процесса	Описание процесса	Конфигурационный файл

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_loader** для сохранения в базу данных	/opt/iw/tm5/etc/icap.conf
	iw_sniffer	Процесс, перехватывающий трафик, который передается по протоколам SMTP, HTTP, ICQ, POP3 и IMAP	/opt/iw/tm5/etc/sniffer.conf

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
	iw_proxy	Принимает копию трафика и передает ее модулю iw_messed, разбив на http-, icq- и smtp-трафик. Включает следующие процессы: • iw_proxy_http - процесс, принимающий копию HTTP-трафика. Принимает HTTP-запрос, формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа и принятия решения. По окончании анализа копия объекта передается процессу **iw_loader** для укладки в базу данных. • 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. По окончании анализа копия объекта передается процессу **iw_loader** для укладки в базу данных • iw_proxy_smtp - процесс, принимающий копию SMTP-трафика. Принимает SMTP-письмо, формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа и принятия решения. По окончании анализа копия объекта передается процессу **iw_loader** для укладки в базу данных	/opt/iw/tm5/etc/proxy.conf

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
	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 и IMAP	/opt/iw/tm5/etc/capstack.conf
	iw_messed	Процесс обработки SMTP-писем. Извлекает данные из SMTP-, POP3- и IMAP-объектов. Затем извлеченные данные добавляются в полученный XML-контекст. Готовый XML-контекст, содержащий данные конверта и письма, передается подсистеме анализа и принятия решения для проверки. По окончании анализа **iw_messed** передает SMTP-письма, доставка которых разрешена, компоненту почтовой системы, ответственному за доставку почты (только в нормальном и прозрачном транспортном режиме). В случае интеграции с почтовым сервером Postfix, таким компонентом является Postfix. Если интеграция с Postfix отсутствует, то, в зависимости от настроек вашей почтовой системы, таким компонентом может быть корпоративный почтовый сервер или почтовый клиент. Кроме того, копия проверенного SMTP-письма передается процессу **iw_loader** для сохранения в базу данных	/opt/iw/tm5/etc/messed.conf

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
	iw_xapi	Получает объекты от Device Monitor через thrift-интерфейс и 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**. По очереди отправляет на обработку процессами **iw_warpd**, **iw_cas**, **iw_pas**, **iw_luaengined**. Далее объекты складываются в файловую очередь для отправки в базу данных	/opt/iw/tm5/etc/analysis.conf
	iw_expressd	Обрабатывает объекты, полученные от систем InfoWatch Device Monitor и DeviceLock. При получении данных (теневой копии файла, задания на печать) от InfoWatch Device Monitor или теневой копии файла от DeviceLock Adapter формирует XML-контекст из полученного объекта. Затем передает XML-контекст подсистеме анализа и принятия решения. По окончании анализа передает теневую копию файла процессу xml2liro. Затем обработаныые данные направляются процессу **iw_loader** для сохранения в базу данных	/opt/iw/tm5/etc/expressd.conf
Обработка данных	iw_warpd	Управляет процессами извлечения данных из контейнеров, вложенных в перехваченные объекты	/opt/iw/tm5/etc/warpd.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_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	/opt/iw/tm5/etc/luaengined.conf
	iw_xml2liro	Процесс, преобразовывающий xml-контекст, полученный из трафика, в бинарный формат liro	/opt/iw/tm5/etc/xml2liro.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 клиента, установленного в филиале. Передает объекты процессу **iw_loader** для сохранения в базу данных	/opt/iw/tm5/etc/qmover_server.conf
	iw_loader	Процесс, загружающий объекты в базу данных. Принимает объекты (проверенные подсистемой анализа и принятия решения) от процессов **iw_messed**, **iw_expressd**, **iw_proxy**. Загружает полученные объекты в базу данных	/opt/iw/tm5/etc/loader.conf
Инфраструктура	iw_adlibitum	Управляет процессами получения актуальных данных с сервера Active Directory	/opt/iw/tm5/etc/adlibitum.conf
	iw_agent	Требуется для управления конфигурацией Системы	/opt/iw/tm5/etc/agent.conf
	iw_blackboard	Осуществляет взаимодействие применяемых политик и базы данных	/opt/iw/tm5/etc/blackboard.conf
	iw_bookworm	Выполняет роль справочника в Системе	/opt/iw/tm5/etc/bookworm.conf
	iw_config_compiler	Переводит конфигурационный файл сервера контентного анализа в бинарный вид для возможности использования конфигурации в контентном анализе	/opt/iw/tm5/etc/config_compiler.conf
	iw_crawler	Процесс для подсистемы Crawler (сама подсистема работает на сервере, отличном от Traffic Monitor Server)	/opt/iw/tm5/etc/web.conf

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
	iw_deliver	Выполняет доставку писем. Отправляет SMTP-письма получателям в случае, если доставка письма разрешена из Management Console (только в нормальном и прозрачном транспортных режимах). Также этот процесс доставляет SMTP-письма, которые по той или иной причине (например, ввиду отсутствия связи с почтовым relay-сервером или почтовым клиентом) не смог доставить процесс **iw_messed**	/opt/iw/tm5/etc/deliver.conf
	iw_indexer	Служит для индексации текста объектов из БД. Получает доступ к базе данных для ее индексации и складывает индексы в файловое хранилище. При выполнении поискового запроса **sphinx** получает из файлового хранилища индексов id объектов	/opt/iw/tm5/etc/indexer.conf
	iw_kicker	Служит для быстрого запуска процессов на сервере с веб-консолью: iw_agent, iw_blackboard, iw_crawler, iw_report, iw_notifier, iw_selection, iw_systemcheck, iw_xapisamplecompiler, iw_export, iw_samplecompiler, iw_import.	/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_notifier	Процесс для отправки уведомлений из Системы	
	iw_report	Процесс для создания отчетов	
	iw_sample_compiler	Процесс, создающий цифровые отпечатки из загруженных эталонных файлов	/opt/iw/tm5/etc/sample_compiler.conf
	iw_selection	Процесс для работы с фильтрами (запросами)	
	iw_serman	Регистрирует и хранит регистрационную информацию сервисов, взаимодействующих с интерфейсом пользователя	/opt/iw/tm5/etc/serman.conf

Назначение	Имя процесса	Описание процесса	Конфигурационный файл
	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
	iw_whiteboard	Позволяет серверным процессам публиковать сообщения в интерфейсе пользователя	/opt/iw/tm5/etc/whiteboard.conf

8.1.2 Работа с процессами серверной части Traffic Monitor

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

Все процессы Traffic Monitor Server (за исключением **iw_warpd**) запускаются от имени пользователя **iwtm**. Процесс **iw_warpd** запускается от имени пользователя **root**.

Пользователи создаются в процессе установки Traffic Monitor Server автоматически (подробнее о учетных записях см. документ «InfoWatch Traffic Monitor. Руководство по установке»).

Примечание:

Имя пользователя прописывается в конфигурационных файлах процессов в параметре `User` секции `Permissions`.

Для стабильной работы Системы рекомендуется оставить значение этого параметра без изменений.

Во время работы состояние процессов Traffic Monitor Server проверяется сценарием **pguard**, который в ходе установки создается в директории `/opt/iw/tm5/bin`. 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 **iwtm**, находящегося в каталоге `/etc/rc.d/init.d`. Файл **iwtm** 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**).

Ключи запуска для сценария **iwtm**:

Ключ запуска	**Назначение**
start	запуск процессов
stop	остановка процессов
restart	перезапуск процессов
reload	перезагрузка конфигурации
status	вывод на экран информации о состоянии процессов

Примеры команд

Действие	**Команда**
Перезапустить сервер контентного анализа	`service iwtm restart cas`
Проверить состояние процессов Traffic Monitor Server	`service iwtm status`
Проверить состояние сервера контентного анализа	`service iwtm status 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 сценарием **iwtm** можно задать параметры автозапуска в конфигурационном файле.

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

1. Для корректной смены параметров остановите серверные процессы Traffic Monitor:
   `service iwtm stop`
2. В файле `/opt/iw/tm5/etc/sniffer.conf`, выполните настройки:
   - Чтобы включить автозапуск для процесса, установите в блоке процесса:
     `"Startup" : {"Enabled" : true}`
   - Чтобы отключить автозапуск для процесса, установите в блоке процесса:
     `"Startup" : {"Enabled" : false}`

3. Запустите процессы Traffic Monitor:
   ```
   service iwtm start
   ```

8.2 Настройка конфигурационных файлов серверной части Traffic Monitor

В данном разделе описаны настройки конфигурационных файлов Системы, которые вы можете изменять для отражения специфики работы Системы в вашей инфраструктуре. Файлы, не описанные в данном подразделе, изменять не рекомендуется.

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

Названия конфигурационных файлов соответствуют названиям тех компонентов, для настройки которых они используются. Например, для конфигурирования компонента **iw_loader** используется конфигурационный файл **loader.conf** (Полный перечень конфигурационных файлов перечислен в разделе "Специфичные настраиваемые параметры конфигурационных файлов").

Различают общие настраиваемые параметры (см. "Общие настраиваемые параметры конфигурационных файлов") и параметры, специфичные для каждого из конфигурационных файлов (см. "Специфичные настраиваемые параметры конфигурационных файлов").

8.2.1 Общие настраиваемые параметры конфигурационных файлов

Для конфигурирования работы Системы используются файлы формата JSON. В разделе описаны наиболее используемые секции и параметры.

Важно!

Настоятельно не рекомендуется изменять параметры, описание которых в настоящем документе не приведено.

Общие настраиваемые параметры содержатся в следующих секциях конфигурационных файлов:

- Секция Logging;
- Секция Startup;
- Секция Nookdir.

8.2.1.1 Секция Logging

Параметр	Описание процесса и путь к файлу

Параметр	Описание процесса и путь к файлу
ActiveBackends	Настройка вывода лог-файлов. Возможные варианты: • Console - вывод в консоль (если процесс запущен не как демон, иначе логи будут сохраняться в директорию /dev/null) • Syslog - вывод в системный лог (/var/log/messages) • File - вывод в отдельный файл (директория для создания файла указана в параметре DefaultDirectory) • Whiteboard - вывод логов в компонент **iw_whiteboard** (для последующей передачи информации в веб-консоль)
DefaultDirectory	Директория, содержащая лог-файлы
Descriptions	Описание формата для каждого типа логирования и специфичных настроек
GlobalLevel	Глобальный уровень логирования. Рекомендуемое значение при внедрении – *error*. Такая настройка позволит записывать в лог только сообщения уровня *error* и выше (*critical*). Значение по умолчанию - *warning*
DisableLogging	Возможность полного отключения логирования в компоненте

8.2.1.2 Секция Startup

В секции Startup включается (значение true) и выключается (значение false) автозапуск модуля.

Важно!

Для службы iw_proxy включение и выключение компонентов выполняется следующим образом:
"Startup" : {"Enabled" : true, "http" : true, "icq" : true, "smtp" : true}
– включение всех модулей;
"Startup" : {"Enabled" : true, "http" : true, "icq" : false, "smtp" : false}
– включение модуля **iw_proxy_http**;
"Startup" : {"Enabled" : false, "http" : true, "icq" : false, "smtp" : false}
– выключение всех модулей.

8.2.1.3 Секция Nookdir

В секции Nookdir указывается рабочий каталог модуля. По умолчанию – /opt/iw/tm5.

8.2.2 Специфичные настраиваемые параметры конфигурационных файлов

Для конфигурирования работы Системы используются файлы формата JSON.

Важно!

Настоятельно не рекомендуется изменять параметры, описание которых в настоящем документе не приведено.

В разделе описаны наиболее используемые секции и параметры следующих конфигурационных файлов:

- Конфигурационный файл serman_resolver.conf;
- Конфигурационный файл sniffer.conf;
- Конфигурационный файл proxy.conf;
- Конфигурационный файл oracle.conf;
- Конфигурационный файл cas.conf;
- Конфигурационный файл expressd.conf;
- Конфигурационный файл messed.conf;
- Конфигурационный файл smtpd.conf;
- Конфигурационный файл capstack.conf;
- Конфигурационный файл indexer.conf;
- Конфигурационный файл web.conf.

8.2.2.1 Конфигурационный файл serman_resolver.conf

В файле хранятся вспомогательные данные для работы модуля **iw_serman**: регистрационные данные компонентов, которые могут быть запрошены другими зарегистрированными сервисами.

Параметр	Описание
`Host`	IP-адрес, на котором работает служба **iw_serman**
`Password`	Пароль пользователя. Используется для подключения к Serman
`Port`	Порт для подключения к Serman
`Username`	Имя пользователя. Используется для подключения к Serman

8.2.2.2 Конфигурационный файл sniffer.conf

Если веб-консоль управления Traffic Monitor и компонент Sniffer установлены на одном компьютере, необходимо внести следующий фрагмент кода в секцию `Listenareas`, параметр `http`, подпараметр `Rules`:

```
{
 "HiPort": 80,
 "IP": "[Server_IP]",
 "LoPort": 80,
```

```
 "Mask": "0.0.0.0",
 "Policy": "DROP"
 }
```

где `[Server_IP]` – IP-адрес сервера, на котором установлена служба sniffer.

8.2.2.3 Конфигурационный файл proxy.conf

Конфигурационный файл **proxy.conf** содержит следующие секции, которые описывают обработку копий различного объектов, полученных от Sniffer:

- Секция Http;
- Секция Icq;
- Секция Smtp.

8.2.2.3.1 Секция Http

В секции `Http` заданы параметры, необходимые для обработки HTTP-запросов, а также ICQ-сообщений (при перехвате ICQ поверх HTTP), полученных от Sniffer:

Параметр	**Описание**
`AuthContext`	Отключает сохранение в очередь HTTP-запросов без аутентификации. Возможные значения: • `0` – производится сохранение запросов без аутентификации; • `1` – не сохраняются запросы с ответом прокси-сервера "*407*", • `2` – не сохраняются запросы с NTLM Type 1, либо без заголовка *Proxy-Authorization.* При этом значении значение параметра SkipNegotiate не имеет значения: Система работает так, как если бы он имел значение On. Значение по умолчанию `0`
`CharsetDetection`	Метод определения кодировки текста. Значение по умолчанию 0. При этом кодировка определяется обычным методом. После извлечения в контекст, тексты некоторых POST-запросов могут отображаться некорректно. Для исправления проблемы можно установить значение 1
`DataPoolSize`	Максимальный объем выделенной памяти для обработки соединений, в Мб. Значение по умолчанию `1024`
`DecodeHttpContent`	Включение распаковки содержимого запроса в случае наличия заголовка Content-Encoding со значением gzip, deflate или compress. Значение по умолчанию `true`
`DefaultCodepage`	Кодировка входящего ICQ-трафика. Значение по умолчанию `cp1251`
`DialogBytesCount`	Размер диалога (в байтах), по достижении которого ICQ-диалог (при перехвате ICQ поверх HTTP) сохраняется в файловую очередь. Значение по умолчанию `500`
`DialogTimeout`	Временной интервал (в минутах), по истечении которого с момента перехвата последнего сообщения происходит сохранение ICQ-диалога (при перехвате ICQ поверх HTTP) в файловую очередь. Значение по умолчанию `5`

Параметр	Описание
ExtractHttpEntity	Включение процедуры извлечения текста из кодированного содержимого запроса с помощью внешних распаковщиков. Эта процедура применяется при сбоях внутренней процедуры декодирования с использованием zlib. Значение по умолчанию false
FakeFileTransferPort	Порт, с помощью перенаправления на который блокируются попытки передачи файлов. Значение по умолчанию 62225
FormatXmlContext	Форматирование XML. Используется для отладки. Значение по умолчанию false
HttpDumpPath	Путь к файлу дампа для HTTP-трафика.
IcqDumpPath	Путь к файлу дампа для ICQ-трафика.
IcqFilter	Возможность перехвата ICQ-сообщений (если установлено значение true), передаваемых через прокси-сервер (поверх HTTP). По умолчанию возможность включена
IcqIgnoreHosts	Отключение перехвата ICQ-сессий определенных хостов.
IcqKnownServers	Диапазоны IP для ICQ серверов при перехвате ICQ поверх HTTP. Несколько диапазонов перечисляются через запятую, например: "205.188.251.0/24:443, 64.12.30.0/24:443, 205.188.8.8:443"
IcqSessionTimeOut	Время неактивности ICQ-сессии, после которого перехват трафика прекращается в секундах. Значение по умолчанию 10800
LogAuth	Запись в лог информации о привязке логина пользователя к его POST-запросам. Значение по умолчанию false
LogBlock	Запись в системный журнал сообщений о блокировке перехваченных HTTP-запросов. Запись ведется, если установлено значение true. По умолчанию запись отключена – значение false
MaxMemoryBlock	Максимальный объем данных POST-запроса (в килобайтах), которые могут храниться в оперативной памяти. Блоки большего размера будут выгружаться во временные файлы. Значение по умолчанию 4096 Кб
MessageWindow	Количество сообщений диалога, по достижении которого ICQ-диалог (при перехвате ICQ поверх HTTP) сохраняется в файловую очередь. Значение по умолчанию 10
MinHeader	Минимальный объем текста (в байтах) для одного блока переменной в кодировке URL, который будет передан на сервер контентного анализа. Значение по умолчанию 10.
MinText	Минимальный размер текстового блока для отправки в iw_cas. Значение по умолчанию 0
OCR	Использование технологии OCR. Значение по умолчанию false
OnlyPost	Перехват только POST-запросов. Значение по умолчанию true

Параметр	Описание
SetCp1251	Использование кодовой таблицы windows-1251 вместо mac-cyrillic при автоматическом определении кодировки текста в HTTP-запросе. Значение по умолчанию false. Если в вашей организации применяется программное обеспечение, использующее кодировку windows-1251, то рекомендуется включить этот параметр (значение true). Автоматическое определение кодовой таблицы в ряде случаев может происходить некорректно. В частности, при недостаточно большом объеме русскоязычного текста возможен выбор кодировки mac-cyrillic вместо windows-1251
SkipNegotiate	Отключает сохранение в очередь HTTP-запросов с NTLM Type 1 (необходимо для исключения дубликатов запросов). Значение по умолчанию false. При реализации схемы внедрения, когда перехват копии HTTP-трафика выполняется через Sniffer, должен принимать значение false.
SkipStat4XX	Отключает сохранение в очередь HTTP-запросов с ответом прокси-сервера вида "*4XX*", где *XX* – любые цифры. Значение по умолчанию false.
StatusCheck	Установка состояния доставки HTTP-запроса в зависимости от статус-кода, возвращенного веб- или прокси-сервером. Если установлено значение true, то анализ кода выполняется, что позволяет более точно показывать состояние доставки HTTP-запроса. Значение по умолчанию false
UnsafeMode	Режим, в котором при возникновении ошибки перехвата, работа процесса останавливается и создается дамп файл. Значение по умолчанию false
WCGAuthCache	Признак того, включена ли функция кэширования авторизационной информации, необходимая для интеграции с WebSense WSG. Чтобы включить кэширование, установите значение true. Значение по умолчанию false
WCGAuthTTL	Время кэширования авторизационной информации, если включен параметр WCGAuthCache, в секундах. Значение по умолчанию 900
ZimbraMail	Перехват почты Zimbra. Значение по умолчанию false

8.2.2.3.2 Секция Icq

В секции Icq заданы параметры, необходимые для обработки копий ICQ-сообщений, полученных от Sniffer:

Параметр	Описание
DefaultCodepage	Кодировка входящего ICQ-трафика. Значение по умолчанию cp1251
DialogBytesCount	Размер диалога (в байтах), по достижении которого ICQ-диалог сохраняется в файловую очередь. Значение по умолчанию 500
DialogTimeout	Интервал времени (в минутах), по истечению которого с момента перехвата последнего ICQ-сообщения необходимо сохранить диалог в файловую очередь. Значение по умолчанию 5
FakeFileTransferPort	Порт, с помощью перенаправления на который блокируются попытки передачи файлов. Значение по умолчанию 62225

Параметр	Описание
FormatXmlContext	Форматирование XML. Используется для отладки. Значение по умолчанию false
MessageWindow	Количество сообщений диалога, по достижении которого ICQ-диалог сохраняется в файловую очередь. Значение по умолчанию 10
OCR	Использование технологии OCR. Значение по умолчанию false

8.2.2.3.3 Секция Smtp

В секции Smtp задаются параметры, необходимые для обработки SMTP-сообщений, полученных от Sniffer:

Параметр	Описание
DumpMode	Регулирует количество данных, которое попадает в дамп. Значение по умолчанию false
DumpPath	Путь к файлу дампа. Значение по умолчанию dump.smtp
FormatXmlContext	Форматирование XML. Используется для отладки. Значение по умолчанию false
MaxMsgSize	Размер SMTP-сообщения (в байтах), при превышении которого сообщение не обрабатывается Системой. Значение по умолчанию – 52428800.
ReadBufferSize	Размер данных, получаемых от Sniffer за один раз. Значение по умолчанию 32768

8.2.2.4 Конфигурационный файл oracle.conf

Параметры соединения с сервером базы данных:

Параметр	Описание
ConnString	Строка соединения с сервером базы данных (псевдоним сервера из файла **tnsnames.ora**)
NLS_LANG	Кодировка, определяющая локализацию БД
ORACLE_HOME	Значение переменной окружения ORACLE_HOME
Password	Пароль учетной записи пользователя Linux части
Username	Имя учетной записи пользователя Linux части

8.2.2.5 Конфигурационный файл cas.conf

Конфигурационный файл **cas.conf** содержит следующие секции, описывающие настройки подсистемы контентного анализа:

- Секция Analysis;
- Секция ThriftServers;
- Секция Config.

8.2.2.5.1 Секция Analysis

Включение (значение on) и выключение (значение off) технологий анализа

Параметр	**Описание**	Примечание
Autoling	Автоматический лингвистический анализ	По умолчанию технология выключена – значение off
`Classifier`	Контентный анализ	RelevanceThreshold – порог срабатывания терминов. Значение по умолчанию – 0.10000000000000001 Spelling – технология опечаток. По умолчанию технология выключена – значение off Translit – технология транслитерации. По умолчанию технология выключена – значение off
Exclusions	Исключения	
`FormAnalysis`	Детектор форм	
Images	Детектор изображений	Barcode – технолигия распознавания штрих- и баркодов. Выдает текст ImageClassifier – технология классификатора изображений, работающая с паспортами, чертежами, географическими картами KeypointMatcher – технология поиска малых изображений на большом. Работает на кредитных картах MatcherConfig – путь к файлу с точными настройками анализа (image-matcher.yml) StampDetector – детектор печатей
`Researcher`	Детектор текстовых объектов	
`Stamper`	Детектор эталонных документов	
`TableAnalysis`	Детектор выгрузок из БД	MinWords – минимальное количество слов в файле эталонной выгрузки из БД, достаточное для детектирования эталонной выгрузки. В данное количество входят все названия полей и все содержащиеся в таблице данные. Требуется, чтобы слова были отделены друг от друга пробелом или иным отступом. Значение по умолчанию – `10`

8.2.2.5.2 Секция ThriftServers

Параметр	**Описание**
`Port`	Порт, на котором сервер контентного анализа принимает входящие соединения. Значение по умолчанию – `9987`
ServerType	Тип сервера
TransportType	Тип обмена данными. Значение по умолчанию – socket

8.2.2.5.3 Секция Config

Параметр	Описание
`CacheMaxSize`	Количество результатов анализа контентов, которое хранится в кэше. Количество элементов кэша. Значение по умолчанию – `10000`
`Path`	Путь, к конфигурационному файлу cas. Значение по умолчанию – `etc/config/cas`
`SchemaPath`	Путь до xsd файла, по которому проверяется валидность xml конфигурации. Значение по умолчанию – `etc/cas_config.xsd`

8.2.2.6 Конфигурационный файл expressd.conf

Конфигурационный файл **expressd.conf** описан в следующих разделах:

- Секция Expressd;
- Секция Expressd, параметр Http;
- Секция Expressd, параметр Ocr.

8.2.2.6.1 Секция Expressd

Параметр	**Описание**
`DumpDir`	Директория, в которую будет сохраняться очередь приходящих объектов (должен быть включен параметр DumpObjects). Значение по умолчанию – `/tmp/dump`
`DumpObjects`	Включение (true) или отключение (false) возможности сохранения приходящих объектов в очереди. Значение по умолчанию `false`. **Примечание:** значение данного параметра изменять не рекомендуется.
`FormatXmlContext`	Включение (true) или отключение (false) форматирования XML-контекста. Применяется для удобства восприятия контекста. Значение по умолчанию `false`.
`HTTP`	Настройка перехвата HTTP-объектов (см. "Секция Expressd, параметр Http")
`ListenAddr`	Адрес сетевого интерфейса сервера, на котором запущен процесс прослушивания объектов, поступающих от систем InfoWatch Device Monitor и DeviceLock. Значение по умолчанию `0.0.0.0`
`ListenPort`	Порт сервера, на котором запущен процесс прослушивания. Значение по умолчанию `4101`
`MaxBinarySize`	Максимальный размер графического файла в байтах, который будет проверяться Системой на соответствие установленным цифровым отпечаткам. Значение по умолчанию – `1048576`
`MaxLoadAvg`	Максимальная нагрузка на систему, в которой запущен процесс **iw_expressd** (пороговое значение, выраженное в условных единицах). Если загрузка системы равна указанному пороговому значению или превышает его, процесс **iw_expressd** прекращает прием объектов. Когда нагрузка на систему будет снижена, прием объектов возобновляется. Значение по умолчанию `10`

Параметр	Описание
OCR	Настройка использования технологии OCR (см. "Секция Expressd, параметр Ocr")
TempDir	Директория для хранения временных файлов. Значение по умолчанию – /tmp
ThreadsNumber	Максимальное количество потоков для параллельного выполнения процесса **iw_expressd**. Значение по умолчанию 4. Увеличение числа потоков повысит производительность процесса, но увеличит использование памяти. **Внимание!** Для корректного приема объектов от системы InfoWatch Device Monitor, укажите то же число обрабатывающих потоков, которое задано на сервере InfoWatch Device Monitor. За настройку числа обрабатывающих потоков InfoWatch Device Monitor отвечает параметр NumberOfConnections в конфигурационном файле InfoWatch.DeviceMonitor.Server.exe.config (подробнее см. «*InfoWatch Device Monitor. Руководство по установке и конфигурированию*»).

8.2.2.6.2 Секция Expressd, параметр Http

Параметр	Описание
CharsetDetection	Метод определения кодировки текста. Значение по умолчанию 0. При этом кодировка определяется обычным методом. После извлечения в контекст, тексты некоторых POST-запросов могут отображаться некорректно. Для исправления проблемы можно установить значение 1
DecodeHttpContent	Включение распаковки содержимого запроса в случае наличия заголовка Content-Encoding со значением gzip, deflate или compress. Значение по умолчанию true
ExtractHttpEntity	Включение процедуры извлечения текста из кодированного содержимого запроса с помощью внешних распаковщиков. Эта процедура применяется при сбоях внутренней процедуры декодирования с использованием zlib. Значение по умолчанию false
MaxMemoryBlock	Максимальный объем данных POST-запроса (в килобайтах), которые могут храниться в оперативной памяти. Блоки большего размера будут выгружаться во временные файлы. Значение по умолчанию 4096 Кб
MinHeader	Минимальный объем текста (в байтах) для одного блока переменной в кодировке URL, который будет передан на сервер контентного анализа. Значение по умолчанию 10.
MinText	Минимальный объем текста (в байтах), для которого будет проводиться контентный анализ. Значение по умолчанию 0 байт. Настройка данного параметра позволяет снизить нагрузку на сервер контентного анализа. Это может быть достигнуто путем отказа от контентного анализа текста, размер которого настолько мал, что не позволяет передавать значимые сообщения

8.2.2.6.3 Секция Expressd, параметр Ocr

Параметр	Описание
Crawler	Использование OCR для файлов, полученных от перехватчика Краулер
DM	Использование OCR для файлов, полученных от Device Monitor

Параметр	Описание
FTP	Использование OCR для файлов, полученных от FTP Monitor
HTTP	Использование OCR для файлов, полученных от HTTP Monitor
IMAP4	Использование OCR для IMAP4 трафика (Mail Monitor)
MAPI	Использование OCR для MAPI трафика (Mail Monitor)
MMP	Использование OCR для MMP трафика (IM Monitor)
NRPC	Использование OCR для файлов, полученных от Lotus Adapter
POP3	Использование OCR для POP3 трафика (Mail Monitor)
Photo	Использование OCR для файлов, полученных от Photo Monitor
Print	Использование OCR для файлов, полученных от Print Monitor
SMTP	Использование OCR для SMTP трафика (Mail Monitor)
Skype	Использование OCR для Skype трафика (IM Monitor)
XMPP	Использование OCR для XMPP трафика (IM Monitor)
Yahoo	Использование OCR для Yahoo трафика (IM Monitor)

8.2.2.7 Конфигурационный файл messed.conf

Параметр	Описание
HeloDomain	Значение команды HELLO SMTP-диалога. Значение по умолчанию smtp.company.com
OCR	Значение по умолчанию – false
Relay	Полное доменное имя почтового relay-сервера, которому перенаправляется письмо, используется для идентификации внутри почтового протокола. Задается при установке.
RelayPort	Порт почтового relay-сервера, которому перенаправляется письмо. Задается при установке.
Timeout	Время, в течение которого предпринимаются попытки доставки SMTP-писем, в секундах. По истечении указанного времени письмо передается в базу данных. Значение по умолчанию 1200
WorkerThreads	Максимальное количество потоков для параллельного выполнения процесса **iw_messed**. Значение по умолчанию 8. Увеличение числа потоков повысит производительность процесса, но увеличит использование памяти

8.2.2.8 Конфигурационный файл smtpd.conf

Параметр	Описание

Параметр	Описание
MaxThreads	Максимальное количество потоков для параллельного выполнения процесса **iw_smtpd**. Значение по умолчанию 8. Увеличение числа потоков увеличит производительность процесса, но повысит использование памяти.
MaxMsgSize	Максимальный размер письма (в байтах). Значение по умолчанию 104857600
Domain	Полное доменное имя принимающего SMTP-сервера, использующееся для идентификации внутри почтового протокола. Рекомендуется использовать имя сервера ТМ, на котором работает процесс **iw_smtpd**.
ListenAddr	Адрес сетевого интерфейса сервера, на котором запущен процесс прослушивания. Задается при установке.
ListenPort	Порт сервера, на котором запущен процесс прослушивания. Задается при установке.

8.2.2.9 Конфигурационный файл capstack.conf

Конфигурационный файл **capstack.conf** описан в следующих разделах:

- Секция UsedProcessors;
- Секция UsedSources.

8.2.2.9.1 Секция UsedProcessors

В секции UsedProcesses задаются протоколы, которые будет разбирать **iw_capstack**. Процесс разбирает протокол и преобразовывает его в расширение. Далее трафик передается процессу **iw_messed** (см. "Конфигурационный файл messed.conf").

Параметр	Описание
imap4	Разбор imap4. Возможные значения: true, false. Значение по умолчанию: true
nrpc	Разбор nrpc. Возможные значения: true, false. Значение по умолчанию: false
pop3	Разбор pop3. Возможные значения: true, false. Значение по умолчанию: true

8.2.2.9.2 Секция UsedSources

В секции UsedSources задаются параметры источника данных для **iw_capstack**.

Параметр	Описание
iscp	Использование в качестве получения трафика от компонента **iw_sniffer**. Значение по умолчанию: true. Возможные значения true, false

8.2.2.10 Конфигурационный файл indexer.conf

В файле хранится конфигурация модуля индексации. Параметры индексации применяются к модулю **iw_indexer**.В секции `Indexer` заданы параметры работы модуля с Базой Данных и методы индексации:

Параметр	Описание
`ArchiveDir`	Путь к каталогу архивированных индексов. Значение по умолчанию: `sphinx_archive`
`BuildIndexByContent`	Расширенная индексация. Возможные значения: `true, false`. Значение по умолчанию: true
`FetchSize`	Количество объектов, запрашиваемых службой из БД для последующей индексации. Значение по умолчанию: `100`
`IndexExactWords`	Точное совпадение. Возможные значения: `true, false`. Значение по умолчанию: `false`
`ProcessSizeInBytes`	Максимальный размер объектов в цикл индексации. Значение по умолчанию: `67108864`
`TarPath`	Путь к утилите архивации. Значение по умолчанию: /bin/tar
`WaitTimeInSects`	Время ожидания между попытками получить объекты из БД

8.2.2.11 Конфигурационный файл web.conf

В файле хранятся параметры взаимодействия Консоли управления с другими компонентами системы. В секции `Search` заданы параметры взаимодействия Консоли управления с сервисом полнотекстового поиска:

Параметр	Описание
`driver`	Название движка полнотекстового поиска. Значение по умолчанию: `sphinx`
`hostname`	Адрес сервера с БД. Значение в случае использования типа установки All-in-one: `127.0.0.1`
`max_matches_common`	Максимальное количество возвращаемых результатов при первичном запросе. Значение по умолчанию: `100000`
`max_matches_maximum`	Максимальное количество возвращаемых результатов при вторичном запросе. Значение по умолчанию: `10000000`
`page_size`	Количество результатов, возвращаемых при однократном обращении к службе **sphinx**: `10000`
`port`	Порт, через который Консоль управления подсоединяется к службе sphinx. Значение по умолчанию: `9306`

8.2.2.12 Конфигурационный файл analysis.conf

Файл содержит вспомогательную информацию для модуля **iw_analysis**. Конфигурационный файл **analysis.conf** содержит следующие секции:

- Секция Analysis;
- Секция Bookworm.

8.2.2.12.1 Секция Analysis

Параметр	Описание
`CharsetDetection`	Метод определения кодировки текста. Значение по умолчанию `0`. При этом кодировка определяется обычным методом. После извлечения в контекст, тексты некоторых POST-запросов могут отображаться некорректно. Для исправления проблемы можно установить значение 1
`DecodeHttpContent`	Включение распаковки содержимого запроса в случае наличия заголовка Content-Encoding со значением gzip, deflate или compress. Значение по умолчанию `true`
`ExtractHttpEntity`	Включение процедуры извлечения текста из кодированного содержимого запроса с помощью внешних распаковщиков. Эта процедура применяется при сбоях внутренней процедуры декодирования с использованием zlib. Значение по умолчанию `false`
`MaxMemoryBlock`	Максимальный объем данных POST-запроса (в килобайтах), которые могут храниться в оперативной памяти. Блоки большего размера будут выгружаться во временные файлы. Значение по умолчанию `4096` Кб
`MaxReadBuf`	Ограничение для размера буфера. Значение по умолчанию 131072.
`MinHeader`	Минимальный объем текста (в байтах) для одного блока переменной в кодировке URL, который будет передан на сервер контентного анализа. Значение по умолчанию `10`.
`MinText`	Минимальный объем текста (в байтах), для которого будет проводиться контентный анализ. Значение по умолчанию `0` байт. Настройка данного параметра позволяет снизить нагрузку на сервер контентного анализа. Это может быть достигнуто путем отказа от контентного анализа текста, размер которого настолько мал, что не позволяет передавать значимые сообщения
`OnlyPost`	Перехват только POST-запросов. Значение по умолчанию `true`
`ZimbraMail`	Перехват почты Zimbra. Значение по умолчанию `false`
`OCR`	Включение OCR. Значение по умолчанию `false`
`TempDir`	Директория для хранения временных файлов. Значение по умолчанию tmp
`WorkThreads`	Количество обрабатывающих потоков. Значение по умолчанию 12

8.2.2.12.2 Секция Bookworm

Параметр	Описание

Параметр	Описание
ConnectTryCount	Количество попыток соединения. Значение по умолчанию 5
CacheDuration	Время валидности справочных данных, которые возвращает **iw_bookworm**. Значение по умолчанию 15

8.2.2.13 Конфигурационный файл sample_compiler.conf

Секция/Параметр	Описание
Bookworm	Секция определяет параметры работы с процессом **iw_bookworm**
DebugBreak	Отладочный параметр. Значение по умолчанию false
EnableOCR	Включение использования OCR. Значение по умолчанию false
Logging	см. статью "Секция Logging"
NookDir	см. статью "Секция Nookdir"
OutChunckSizeLimit	Максимальный размер чанка, в который возаращаются результаты компиляции. Значение по умолчанию 1048576
ResourceLimits	Различные ограничения системных ресурсов, которые может использовать программа
Stratup	см. статью "Секция Startup "
Technologies	Секция конфигурирования отдельных технологий
ThreadsCount	Количество потоков обработки. Значение по умолчанию 5
ThriftServers	Настройки трифт-сервера, через который **sample_compiler** получает задачи на компиляцию данных

8.3 Настройка параметров работы с HTTP-запросами, передаваемыми по протоколу ICAP (файл icap.conf)

Примечание:

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

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

Параметр	Описание и примеры настройки
AllMethods	Включает анализ всех типов http-запросов. Значение по умолчанию false.
AsyncCheck	Сначала пропускает данные, затем включает процесс их анализа. Значение по умолчанию false.
DisableIPv6	Отключение (DisableIPv6 = true) и включение (DisableIPv6 = false) поддержки подключений по протоколу IPv6. По умолчанию поддержка выключена. Если на сервере ICAP поддержка IPv6 отключена, то служба **iw_icap** будет запускаться и работать в штатном режиме только при включенной опции, то есть когда DisableIPv6 = true.
ErrorHTML	Путь к HTML-файлу, в котором содержится сообщение, выводимое в окне интернет-обозревателя, если запрос пользователя был заблокирован Системой. Значение по умолчанию etc/error.html. (путь указан относительно текущего каталога, которым является корневой каталог Системы)
ForceKeepAlive	Использование одного TCP-соединения для отправки и получения множественных HTTP-запросов и ответов вместо открытия нового соединения для каждой пары запрос-ответ
ListenPort	Порт, на котором ICAP-сервер прослушивает HTTP-запросы, поступающие от прокси-сервера с ICAP-клиентом. Допускается использование портов с номерами от 1025. Значение по умолчанию 1344
LogBlock	Запись в системный журнал сообщений о блокировке перехваченных HTTP-запросов. Значение по умолчанию - false: запись не ведется
LogTimer	Запись в системный журнал сообщений о времени обработки HTTP-запросов. Запись ведется, если установлено значение true. По умолчанию имеет значение false – запись не ведется
MaxConnections	Максимальное количество соединений. По умолчанию имеет значение 100.
MaxMemoryBlock	Максимальный объём в килобайтах, который может занимать один объект в памяти. Значение по умолчанию: 4096
MinDataLength	Минимальный объем (в байтах) URL-переменной, который будет включен в текстовый блок для передачи на контентный анализ. Значение по умолчанию 10 байт.
MinTextLength	Минимальный объем текста (в байтах), для которого будет проводиться контентный анализ. Значение по умолчанию 5 байт. Настройка данного параметра позволяет снизить нагрузку на сервер контентного анализа. Это может быть достигнуто путем отказа от контентного анализа текста, размер которого настолько мал, что не позволяет передавать значимые сообщения
OCR	Использование технологии OCR (кроме трафика от почтового сервера Zimbra). Значение по умолчанию false
PathTemporary	Путь к хранилищу временных файлов ICAP-сервера (по умолчанию /opt/iw/tm5/tmp/icap)
SessionTimeout	Время простоя в секундах, по истечении которого сессия прерывается. Значение по умолчанию: 330
ZimbraMail	Параметр для работы с почтовым сервером Zimbra. Значение по умолчанию: false

Параметр	Описание и примеры настройки
ZimbraOCR	Использование технологии OCR для трафика от почтового сервера Zimbra. Значение по умолчанию false

8.4 Настройка параметров обработки архивов вложений

Обработка вложений настраивается в двух конфигурационных файлах: **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml** и **/opt/iw/tm5/etc/extractors.conf**.

В этом разделе:

- Конфигурационный файл extractors.conf;
- Конфигурационный файл extractors.xml.

8.4.1 Конфигурационный файл extractors.conf

Файл **/opt/iw/tm5/etc/extractors.conf** содержит локальные настройки экстракторов.

Параметр	Описание и примеры настройки
Dreamcatcher	Директория, в которой хранятся файлы, которые не удалось распаковать
MaxRecursiveLevel	Максимальный уровень вложенности файлов. Значение по умолчанию – 100
TempDir	Временная директория для результатов распаковки. Значение по умолчанию – tmp

8.4.2 Конфигурационный файл extractors.xml

Файл **/opt/iw/tm5/etc/config-perm/bookworm/extractors.xml** содержит настройки справочника и базу сигнатур, с помощью которых определяется тип файлов при распаковке архивов и вложений.

Параметр	Описание и примеры настройки
FilenameCharsets	Если кодировка имени файла отличается от стандартной (ANSI, UTF), то файл будет обрабатываться как соответствующий кодировкам, указанным в данном параметре. Несколько значений перечисляются через запятую; Система будет последовательно пытаться обработать файл в перечисленных кодировках, пока не найдет похожую. Значения по умолчанию – UTF-8,cp1251,cp866
MinFileSizeInBytes	Минимальный размер файла (в байтах), подлежащего распаковке. Это ограничение позволяет увеличить производительность Системы, за счет отказа от распаковки небольших файлов. Значение по умолчанию – 10

MaxTextPlainSizeInKb	Верхняя граница размера файла, сигнатура которого не определена. При превышении порогового значения файл автоматически считается бинарным и не отправляется на анализ в **iw_cas**. Значение по умолчанию – 25600
SpeedInKBs	Предположительная скорость работы экстрактора, в Кб/с, в расчете на 1 ГГц частоты процессора. Значение по умолчанию – 100
TimeoutInSec	Время ожидания (в секундах) до завершения обработки файла. Значение по умолчанию – 1800
UseLog	Логирование экстрактора. Значение по умолчанию – false

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

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

Параметр	**Описание и примеры настройки**
Extension	Расширение файла архива. Необязательный параметр, необходим для корректной работы некоторых архиваторов, которые требуют наличия правильного расширения входных файлов **Пример** Ext = arj
Name	Имя формата. Используется для точного определения имени формата при распаковке файла. Для определения/уточнения формата может включать также список имен: "defaultname, name1(code1), name2(code2)" В этом случае формат определяется на основании кода (*codeN*), присвоенного файлу при распаковке. Например, если распаковка завершается с кодом *code1*, то считается, что файл имеет формат *name1*. Список имен может также включать имя по умолчанию (*defaultname*), которое будет присваиваться в случаях, когда код не присвоен: **Пример 1 (одно имя формата)** text/xml **Пример 2 (список имен формата)** "application/arj, UNKNOWN(9), text/encrypted(4)" По умолчанию формат файла определяется как application/arj. Если формат архива не удается определить, ему присваивается имя UNKNOWN. Для зашифрованного архива используется имя форматаtext/encrypted

Signature	Сигнатура формата, которая представляет собой «образцовую» последовательность значений (байтов) с начальным смещением и масками. Эта последовательность необходима для однозначного определения формата файлов по их содержимому Сигнатура может включать до 16 триад вида: [OFFSET]:BYTE_VALUE/[MASK] Допускается также и строковая сигнатура, например, "BZh", для BZIP2. Эта сигнатура означает указанную последовательность байтов от смещения 0. Поиск строковых сигнатур выполняется без учета регистра символов. Параметр OFFSET является необязательным. Для первого байта этот параметр по умолчанию равен 0, для всех последующих – увеличивается на единицу. Смещение можно задать с символом «?» – поиск образца в первых N байтах файла. Например, для поиска образца в первых 500 байтах файла, нужно задать смещение '500?'. Параметр MASK, также является необязательным и равен 0xFF по умолчанию. **Пример** (сигнатура заголовка WAV-формата): Sign = "'RIFF', 0x8: 'WAVEfmt'" Начиная от смещения 0, расположена последовательность 'R', 'I', 'F', 'F', далее от смещения 8 должно следовать 'W', 'A', 'V', 'E', 'f', 'm', 't'
Comment	Комментарий с пояснениями. Например, указание используемой версии архиватора: Comment = "bzip2 v. 1.0.x"
Command	Строка команды для извлечения файлов. Например, Extract = "/usr/bin/bzip2 -f -dc ${SRC} > ${OUTDIR}/${SRC}" где ${OUTDIR} – каталог, в который будет распакован архив, а ${SRC} – имя файла, который нужно распаковать
ExcludeFromContext	Если параметр включен (On), то распаковка объекта выполняется, но информация об архиваторе не добавляется в XML-контекст объекта. Это позволяет не отображать в контексте объекта фиктивные контейнеры типа MS-TNEF. По умолчанию параметр отключен (Off)
CaseInsensitive	Учет регистра символов при обработке файла. Значение по умолчанию – false
CreateTags	Извлечение метаинформации из файла. Значение по умолчанию – true
Archive	Регламентирует вид извлеченной информации. При значении true - файлы. При значении false - данные.

8.5 Архивирование каталога очереди сообщений

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

8.6 Логирование работы Системы

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

Название уровня	**Описание**
`fatal`	Показывает ошибки, которые препятствуют дальнейшей работе процесса
`error`	Показывает сообщения об ошибках, которые не являются критическими для работоспособности процесса
`warning`	Выводит сведения о потенциально опасных ситуациях
`info`	Общая полезная информация о процессе (старт/стоп, применение конфигураций и т.д.)
`debug`	Выводит информацию, которая чаще всего используется для диагностики работы сервиса (IT, системные администраторы и т.д.)
`trace`	Чаще всего используется для отслеживания кода разработчиками

Настройка уровней протоколирования

> **Важно!**
>
> Следует учитывать, что изменение уровня протоколирования на более подробный может значительно снизить производительность Системы.

Конфигурационные файлы хранятся в директории `/opt/iw/tm5/etc`. По умолчанию все процессы имеют уровень протоколирования `warning`.

Чтобы изменить уровень протоколирования для процессов Traffic Monitor Server:

1. В конфигурационном файле нужного процесса, в секции `Logging` установите для параметра `GlobalLevel` необходимое значение.
2. Сохраните измененный файл.
3. После внесения изменений в системный журнал, перезапустите процесс:
   `service 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/extractors.conf**:

1. Откройте конфигурационный файл;
2. Для параметра `text-extractor` добавьте значение `-l <level>`
   Где <level> - уровень протоколирования.
   Например:

```
},
      "docx": {
```

```
            "Command": [
                "bin/text-extractor –l error -t ooxml -i
${SRC} -d ${OUTDIR}"
```

Примечание:

Данный тип настройки протоколирования доступен для экстракторов следующих форматов: docx, html, msoffice_xml, msole, odp, odt, pptx, xlsx, xml.

8.7 Загрузка очередей объектов

Чтобы обеспечить загрузку имеющихся очередей объектов:

1. Остановите службы **icap**, **smtp**, **expressd, sniffer, xapi.**
2. Переместите объекты из очереди ошибок в нужную очередь.
3. Дождитесь, пока будут обработаны все объекты в файловой очереди
4. Запустите службы **icap**, **smtp**, **expressd, sniffer, xapi.**

Примечание:

По окончании процесса убедитесь, что перехватчики запущены, и включен автозапуск процессов.

Traffic Monitor имеет следующие очереди:

Путь к директории очереди	**Формат файлов в очереди**
queue/analysis	.xml & .dat
queue/blackboard	.dat
queue/blackboard_errors	.dat
queue/whiteboard	.dat
queue/errors	.xml & .dat
queue/xml2liro-errors	.xml & .dat
queue/db	.xml & .dat
queue/smtp	.xml & .dat

Каждая из очередей содержит дополнительные технические очереди для отслеживания процесса обработки объектов:

-
    - .db
    - .out

- `.in`

Например:
`queue/db/.out`

`queue/db/.in`

`queue/db/.db`

Для очереди `smtp` процесс обработки разделен на следующие этапы:

1. `queue/smtp/.in` – файл формируется в данной очереди в процессе получения объектов от Postfix модулем `smtpd`. Если объект по какой-то причине задерживается в этой очереди, необходимо проверить модули `smtpd` или `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 **xapi**
3. `queue/smtp/.out` - в эту очередь объект перемещается следующим модулем в цепочке (в случае с очередью `smtp` - модулем `messed`).

Объекты в очередь помещаются посредством следующих модулей:

- ВХОД – модуль, который помещает события в очередь.
- ВЫХОД – модуль, который забирает события из очереди.

Имя очереди	**ВХОД**	**ВЫХОД**
queue/analysis	xapi	analysis
queue/smtp	xapi, smtpd и proxy_smtp	messed
queue/db	messed, icap, expressd, proxy_icq, proxy_http	xml2liro
queue/errors	все компоненты, если произошла ошибка обработки	нет
queue/blackboard	luaengined	blackboard
queue/blackboard_errors	ошибка при обработке blackboard	нет
queue/whiteboard	luaengined	whiteboard
queue/xml2liro-errors	ошибки обработки xml2liro	нет

8.8 Восстановление работоспособности системы в аварийных ситуациях

При серьезных сбоях в работе серверов или сети восстановить работоспособность Системы можно, выполнив следующие действия:

1. Остановите процессы Traffic Monitor Server, выполнив команду:
   `service iwtm stop`

2. Переместите объекты из ошибочных очередей в обычные. Процедура выполняется при помощи утилиты iw_qtool (см. интернет-статью "Перемещение объектов между очередями (утилита iw_qtool)").
3. По окончании работ проверьте соединение с СУБД Oracle, выполнив 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 процессов Traffic Monitor Server, выполнив команду:
   `service iwtm start`

После запуска Traffic Monitor Server, проверьте системный журнал на наличие ошибок. Путь к файлу журнала:

`/var/log/messages`

Если в системном журнале содержится информация об ошибках, обратитесь в службу технической поддержки.

8.9 Управление языками морфологии

Управление языками морфологии в Traffic Monitor осуществляется посредством изменения конфигурационного файла и установки пакета с словарём языка.

По умолчанию в Системе будет установлен Русский словарь морфологии.

Чтобы добавить к предустановленным словарям Английский словарь морфологии, выберите значение English в параметре **CFDb** на шаге выбора параметров локализации в процессе установки Системы (см. "InfoWatch Traffic Monitor 6.0. Руководство по установке").

После установки Системы у пользователя также есть возможность:

- Добавить новый язык морфологии;
- Обновить установленный язык морфологии;
- Удалить язык морфологии.

8.9.1 Добавление нового языка морфологии

Конфигурирование языка морфологии и языка Категорий и терминов производится в параметре `cfdb_language` конфигурационного файла **database.conf**.

Чтобы добавить в Систему новый словарь:

1. Остановите процесс **searchd**:
   `service searchd stop`
2. Остановите процесс **iw_indexer**:
   `service iwtm stop indexer`

3. Откройте файл **database.conf**:
    - `vim /opt/iw/tm5/csw/oracle/database.conf` при использовании базы данных Oracle.
    - `vim /opt/iw/tm5/csw/postgresql/database.conf` при использовании базы данных Postgre SQL.
4. Добавьте значение `'язык морфологии'` для параметра `cfdb_language.`
   Например, при добавлении немецкого словаря, конфигурационный файл будет выглядеть следующим образом:
   define cfdb_language = 'rus deu'
5. Перейдите в каталог с пакетами словарей:
   `cd opt/disrt/infowatch/traffic-monitor/Linux`
6. Выполните установку пакета:
   rpm -i название пакета
   Например:
   `rpm -i iwtm-sphinx_dict-deu-6.x-yz.x86_64.rpm`
7. Запустите процесс **iw_indexer**:
   `service iwtm start indexer`

Примечание:

Чтобы выставить приоритет языка, установите параметр с языком последним в списке параметров `define cfdb_language` файла **database.conf**

Примечание:

При установке нового словаря происходит полная переиндексация Базы Данных.

8.9.2 Обновление установленного языка морфологии

Чтобы обновить существующий в Системе словарь:

1. Перейдите в каталог с пакетами словарей:
   `cd opt/disrt/infowatch/traffic-monitor/Linux`
2. Выполните установку пакета:
   `rpm -i название пакета`
   Например:
   `rpm -i iwtm-sphinx_dict-deu-6.x-yz.x86_64.rpm`

Примечание:

При обновлении словаря, повторная индексация Базы Данных производиться не будет.

Поддержка языков будет производиться только для новых событий.

8.9.3 Удаление языка морфологии

Конфигурирование языка морфологии и языка БКФ производится в параметре `cfdb_language` конфигурационного файла **database.conf**.

Чтобы удалить словарь из Системы:

1. Остановите процесс **searchd**:
   `service searchd stop`
2. Остановите процесс **iw_indexer**:
   `service iwtm stop indexer`
3. Откройте файл **database.conf**:
   - `vim /opt/iw/tm5/csw/oracle/database.conf` при использовании базы данных Oracle.
   - `vim /opt/iw/tm5/csw/postgresql/database.conf` при использовании базы данных Postgre SQL.
4. Удалите значение `'язык морфологии'` из параметра `define cfdb_language`.
5. Удалите файлы индексации из директории:
   `/var/lib/sphinx/`
6. Запустите процесс **iw_indexer**.
   `service iwtm start indexer`

Примечание:

После удаления словаря происходит полная переиндексация Базы Данных.

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

Чтобы сохранить язык БКФ, добавьте значение `'язык морфологии'` в параметр `cfdb_language` конфигурационного файла **database.conf** непосредственно перед обновлением Системы. При этом язык морфологии также будет восстановлен.

Чтобы удалить язык морфологии после обновления Системы, повторно удалите значение `'язык морфологии'` из параметра `cfdb_language` конфигурационного файла **database.conf** .

8.10 Настройка serman.conf при изменении адреса сервера БД

В случае изменения IP-адреса сервера базы данных, укажите новый адрес БД в параметре `DefaultInterface` секции `Serman` конфигурационного файла **serman.conf**.

8.11 Настройка передачи информации в SIEM

Интеграция Traffic Monitor с SIEM системами (ArcSight, Tivoli) происходит посредством встроенных возможностей программы. Настройка данного функционала возможна при помощи утилиты **setup**, которая доступна на сервере Traffic Monitor.

Под интеграцией подразумевается поступление в SIEM систему консолидированной информации со всех установленных в компании заказчика компонент системы ТМ.

Информация из ТМ доступна для SIEM системы:

1. Посредством табличного представления:
    - События, зарегистрированные в ТМ;
    - Аудит сессий пользователей консоли ТМ;
2. Посредством rsyslog:
    - Вход/выход пользователей Linux-сервера ТМ;
    - События, зафиксированные в системном журнале Linux-сервера ТМ, включая информацию о входе/выходе пользователей Базы Данных Oracle или Postgre;
    - Состояние служб Linux-сервера ТМ или группы серверов.

В этом разделе:

- Настройки на стороне SIEM;
- Настройки на стороне ТМ;
- Типы логов, передаваемых в SIEM.

8.11.1 Настройки на стороне SIEM

Чтобы подготовить SIEM к получению данных от ТМ:

1. В SIEM укажите таблицы, из которых необходимо забирать информацию:
    - `IWTM.ARC_VIEW_OBJECTS`
      События ТМ
    - `IWTM.ARC_VIEW_AUDIT_LOG`
      Аудит пользователей ТМ
2. Создайте учетную запись SIEM для доступа к таблицам БД.
3. Настройте обработку данных, извлеченных из БД ТМ.

Чтобы проанализировать табличные представления событий ТМ и аудита пользователей см. "Представление событий ТМ" и "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.

8.11.1.1 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_OBJECTS`.

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
`object_id`	Number(20)	Атрибут события Идентификатор события.	ID события в БД TM. Всегда присутсвует.	110

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
monitorcode	Varchar2(4000)	Атрибут события Тип события.	Возможны значения: • Email • ICQ, • GTalk, • Ya.online, • Mail.Ru Agent, • Skype, • MSN, • SMS, • Jabber, • Web message (Web-сообщение), • File exchange (Обмен файлами), • Copying to an external device (Копирование на внешнее устройство), • Print (Печать), • Crawler (хранение на локальных дисках рабочих станций, Share Point, сетевых ресурсах), • MS Lync, • Yahoo! • Photo (фотография на мобильном устройстве),	Crawler
verdict	varchar2(12)	Атрибут события Вердикт.	Возможны значения: • Quarantined (Карантин), • Forbidden (Заблокировано), • Allowed (Пропущено).	Forbidden

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
date_of_capture	Varchar2(50)	Атрибут события дата перехвата в UTC и Часовой пояс даты перехвата.		2014-06-19T18:56:26+04:00
device	varchar2(256)	Атрибут события Имя устройства.	Наименование устройства, с которого или на которое происходило копирование. Либо наименование принтера, которому была осуществлена отправка на печать документа из перехваченного события. Может быть не заполнено.	Kingston USB Drive 5.0
Web-source	varchar2(256)	Атрибут события Ресурс.	Адрес посещенного веб-ресурса или адрес облачного хранилища. Может быть не заполнено.	Yahoo.com

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
recipientscontacts	clob	Атрибут события Получатели.	Список контактов получателей через запятую, указанные в формате <тип контакта>:<значение контакта>. Могут быть следующие типы контактов: - auth - email - icq - skype - mobile (Телефон мобильный) - phone (Телефон стационарный) - sid - webaccount - lotus Поле может быть не заполнено.	email:ivanov@infowatch.ru, email:petr.petrov@infowatch.ru
recipientsfullname	clob	Атрибут события Получатели.	Список полных имен получателей через запятую. Указаны в том же порядке, что и в recipients. Указаны только в том случае, если в получателей удалось проидентифицировать. Поле может быть не заполнено.	Ivanov Ivan Ivanovich, Petrov Petr Petrovich
recipientsdomainaccountname	clob	Атрибут события Получатели.	Список ключей идентификации типа auth всех получателей через запятую. Указаны в том же порядке, что и в recipients. Поле может быть не заполнено.	Ivanov@iw, Petrov@iw

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
senderdomainaccountname	clob	Атрибут события Отправители.	Ключ идентификации типа auth отправителя. Поле может быть не заполнено.	Petrov@iw
senderfullname	clob	Атрибут события Отправители.	Полное имя отправителя. Поле может быть не заполнено.	Petrov Petr Petrovich
sendercontact	clob	Атрибут события Отправители.	Контакт отправителя, указанный в формате <тип контакта>:<значение контакта>. Могут быть следующие типы контактов: - auth - email - icq - skype - mobile (Телефон мобильный) - phone (Телефон стационарный) - sid - webaccount - lotus Поле может быть не заполнено.	email:petr.petrov@infowatch.ru
sendermachinedomainname	clob	Атрибут события Рабочая станция.	Доменное имя рабочей dnshostname станции отправителя. Поле может быть не заполнено.	XP-PETROV

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
sendermachineip	clob	Атрибут события Рабочая станция.	IP-адрес рабочей станции отправителя. Поле может быть не заполнено.	10.60.20.184
perimetersin	clob	Наименование периметра, в которое вошло событие.	Список наименований периметров через запятую, в которые вошло событие. Поле может быть не заполнено.	Периметр компании
perimetersout	clob	Наименование периметра, из которых ушло событие.	Список наименований периметров через запятую, из которых ушло событие. Поле может быть не заполнено.	Периметр компании
tags	clob	Атрибут события Тег.	Список тегов через запятую. Поле может быть не заполнено.	New
categories	clob	Атрибут события Категория.	Список категорий через запятую. Поле может быть не заполнено.	Confidentially
text_objects	clob	Атрибут события Текстовый объект.	Список текстовых объектов, обнаруженных в перехваченном событии, через запятую. Поле может быть не заполнено.	special control

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
fingerprint	clob	Атрибуты события Эталонная форма, Эталонный документ, Эталонная печать, Эталонная выгрузка из БД.	Список наименований эталонных форм, эталонных документов, эталонных печатей, эталонных выгрузок из БД, обнаруженных в перехваченном объекте, через запятую. Поле может быть не заполнено.	Бланк заявки.doc
policy	clob	Атрибут события Политика.	Список наименований политик, сработавших на перехваченном объекте, через запятую. Поле может быть не заполнено.	Политика контроля новых сотрудников
violationtype	varchar2(40)	Атрибут события Группа правил.	Может принимать следующие значения: - Copy (Нарушение копирования) - Placement (Нарушение размещения) - Transfer (Нарушение передачи) Поле может быть не заполнено.	Copy

Наименование атрибута	Тип данных	Описание	Возможные значения	Пример заполнения
userdecision	varchar2(27)	Атрибут события Решение пользователя.	Решение пользователя консоли DLP. Может принимать следующие значения: - Violation (Нарушение), - NoViolation (Нет нарушения), - NotProcessed (Решение не принято), - AdditionalProcessingNeeded (Требует дополнительной обработки). Поле может быть не заполнено.	Violation
filepath	clob	Атрибут события Путь к файлу.	Список путей к файлам через запятую. Поле может быть не заполнено.	\\xp-petrov\C$\666.txt
url	varchar2(4000)	Атрибут события URL.	Полный адрес, с которого осуществлялась передача данных. Поле может быть не заполнено.	10.60.21.34/3.jpg
capture_server_ip	varchar2(256)	Атрибут события Сервер перехвата IP.	IP сервер, на котором были перехвачены данные. Поле может быть не заполнено.	10.60.21.34
capture_server_hostname	varchar2(256)	Атрибут события Сервер перехвата Имя.	Имя сервера, на котором были перехвачены данные. Поле может быть не заполнено.	iwtm.infowatch.ru

8.11.1.2 Табличное представление аудита пользователей

При подключении к БД ТМ 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 ТМ.	12345
`change_date`	Varchar2(50)	Дата и время зарегистрированного действия пользователя	2014-06-19T18:56:26+04:00
`user_login`	varchar2(256)	Логин пользователя, осуществившего действие.	Admin
`user_fullname`	varchar2(256)	Полное имя пользователя, совершившего действие.	Petrov Petr Petrovich
`user_email`	varchar2(256)	E-mail пользователя, совершившего действие.	petr.petrov@infowatch.ru

Атрибут	Тип данных	Описание	Пример заполнения
operation	varchar2(40)	Тип действия, которое было произведено пользователем. Возможны значения:[VK1] • Run (выполнение запроса) • Start (запуск) • Stop (остановка) • view (просмотр) • create (создание) • update (редактирование) • delete (удаление) • login_failure (неуспешная попытка входа) • login (успешный вход) • logout (выход) • change_password (изменение пароля) • decision_update (изменение пользовательского решения) • remove_tag (изменение тегов	Edit

Атрибут	Тип данных	Описание	Пример заполнения
entity_type	varchar2(40)	Тип объекта, над которым осуществлялось действие. Возможны значения:[VK2] • Category (категория) • Dashboard (дашборд) • Dashboard Widget (виджет) • EtForm (эталонные формы) • EtStamp (эталонные печати) • EtTable (эталонные выгрузки) • Fingerprint (эталонные документы) • LdapContact (LDAP контакт) • LdapGroup (LDAP группа) • LdapPerson (LDAP персона) • LdapStatus (LDAP статус персоны) • LdapWorkstation (LDAP рабочая станция) • Perimeter (периметр) • Policy (политика)	Dashboard

Атрибут	Тип данных	Описание	Пример заполнения
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 и при осуществлении входа в консоль управления. Возможны три формата заполнения поля.	
		Формат №1. Актуален только для событий управления ролями и областями видимости.	

Атрибут	Тип данных	Описание	Пример заполнения

		{
		“old”: {
		“<ТИП ОБЪЕКТА>”:{
		{
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”
		}
		}
		}
		{
		“new”: {
		“<ТИП ОБЪЕКТА>”:{
		{
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”
		}
		}
		}
		}
			{
			"old":{
			"visibilityareas":{
			}
			},
			"new":{
			"visibilityareas":[
			{
			"VISIBILITY_AREA_ID":"F00207A1E7E7743EE0433D003C0A5DD400000000",
			"DISPLAY_NAME":"<idclip>",
			"NOTE":"<idclip>",
			"VISIBILITY_AREA_CONDITION":"{"data":{"link_operator":"and","children":[]}}",
			"IS_SYSTEM":1
			}
			}
			}

		Формат №2. Актуален только для событий управления пользователями.	

Атрибут	Тип данных	Описание	Пример заполнения

		{
		“old”:{
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”
		}
		“new”:{
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”,
		“<ПОЛЕ>”: “<ЗНАЧЕНИЕ>”
		}
		}
			{
			"old":{
			"EMAIL":"asdasd@asdasd.ru",
			"CHANGE_DATE":"01-07-2014 09:46:29.000000"
			},
			"new":{
			"EMAIL":"asdasd11@asdasd.ru",
			"CHANGE_DATE":"01-07-2014 09:46:44.000000"
			}
			}

		Формат №3. Актуален только для событий входа пользователя в систему.	

		{
		"request":{
		"hostname": “<ИМЯ ХОСТА>”,
		"ip":"<IP-АДРЕС>",
		"login":"<ЛОГИН ПОЛЬЗОВАТЕЛЯ>"
		}
		}
			{
			"request":{
			"hostname":null,
			"ip":"127.0.0.1",
			"login":"officer"
			}
			}

8.11.2 Настройки на стороне ТМ

Чтобы настроить передачу консолидированной информации из ТМ:

1. Запустите меню утилиты **setup**.
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.

8.11.2.1 Передача логов в SIEM

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

1. Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup`.
2. Выберите опцию **IW Services configuration**.
3. Выберите опцию **iwtm-siem**
4. Выберите опцию **Log messages forwarding configuration**.
5. Задайте параметры передачи логов:

Параметр	**Описание**
`Enable forwarding`	Включение/выключение пересылки логов в siem. (Возможные значения: `Yes/No`)
`Forwarding server`	IP-адрес или dns-имя сервера SIEM
`Forwarding server port`	Порт сервера SIEM, на котором работает **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`)

6. Нажмите **Ok**.

Важно!

В БД не логируется отключение от БД пользователей с правами администратора, соответственно в SIEM данная информация попадать не будет.

8.11.2.2 Управление логированием сессий пользователей БД ТМ

Включение и выключение логирования сессий пользователей БД ТМ в системный журнал ОС осуществляется через **rsyslog**.

Чтобы включить логирование сессий пользователей Базы Данных ТМ:

1. Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup.`
2. Выберите опцию **IW Services configuration**.
3. Выберите опцию **iwtm-siem**
4. Выберите опцию **DB audit logging management**.
5. Задайте параметры:

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

6. Нажмите **Check logging status**.
7. 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.

8.11.2.3 Управление пользователем siem

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

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

8.11.2.3.1 Создание пользователя siem

Чтобы создать пользователя siem:

1. Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup.`
2. Выберите опцию **IW Services configuration**.
3. Выберите опцию **iwtm-siem**
4. Выберите опцию **DB siem user**.
5. В появившемся меню выберите опцию **Create DB siem user**.
6. Задайте параметры:

Параметр	Описание
`Enter login for DB administrative account`	Логин для учетной записи администратора Oracle/Postgre
`Enter password for DB administrative account`	Пароль для учетной записи администратора Oracle/Postgre
`Enter password DB siem user`	Пароль для новой учетной записи siem

7. Нажмите **Create**.

8.11.2.3.2 Смена пароля пользователя siem

Чтобы сменить пароль пользователю siem:

1. Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup.`
2. Выберите опцию **IW Services configuration**.
3. Выберите опцию **iwtm-siem**.
4. Выберите опцию **DB siem user**.
5. Выберите опцию **Change password for DB siem user**.
6. Задайте параметры:

Параметр	Описание
`Enter login for DB administrative account`	Логин для учетной записи администратора Oracle/Postgre
`Enter password for DB administrative account`	Пароль для учетной записи администратора Oracle/Postgre
`Enter new password user siem`	Новый пароль для учетной записи **siem**

7. Нажмите **Change password**.

8.11.2.3.3 Удаление пользователя siem

Чтобы удалить пользователя siem:

1. Зайдите в **setup** утилиту из терминала ТМ, используя команду `setup.`
2. Выберите опцию **IW Services configuration**.
3. Выберите опцию **iwtm-siem**.
4. Выберите опцию **DB siem user**.
5. Выберите опцию **Delete DB siem user**.
6. Задайте параметры:

Параметр	Описание
`Enter login for DB administrative account`	Логин для учетной записи администратора Oracle/Postgre

Параметр	Описание
`Enter password for DB administrative account`	Пароль для учетной записи администратора Oracle/Postgre

7. Нажмите **Delete**.

8.11.3 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_expressd: 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] : expressd
   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)
   ```

8.12 Удаление временных файлов

Возможность удаления временных файлов реализована в продукте в виде сценария **clean_temporary_files.sh**.

Сценарий удаляет следующую информацию:

1. Файлы из директории временных файлов операционной системы (директория `/opt/iw/tm5/tmp/`).
2. Данные из директорий файловых очередей Traffic Monitor (директория `/opt/iw/tm5/queue/`).

Примечание:

Во время удаления временных файлов обработка поступающих в Систему событий будет остановлена. Данные обо всех необработанных на момент начала удаления событиях будут удалены.

Чтобы удалить временные файлы:

1. Запустите сценарий **clean_temporary_files.sh**:
   `/opt/iw/tm5/bin/clean_temporary_files.sh`
2. Согласитесь на удаление временных файлов:
   `yes`

9 ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ИМЕН И ПАРОЛЕЙ

Требования к именам пользователей

- Длина имени пользователя может составлять от 1 до 20 символов.
- Имя пользователя может состоять из букв латинского алфавита, цифр и символа подчеркивания «_». Должно начинаться с буквы.

Требования к паролям пользователей

- Длина пароля может составлять до 30 символов.
- Пароль пользователя может состоять только из букв латинского алфавита, цифр и символов:

«#», «$» или «_».
Может начинаться только с буквы.

- Пароль чувствителен к регистру символов.

Рекомендации по составлению надежных паролей

- Рекомендуемая длина пароля: от 10 до 30 символов.
- 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	

10 ПРИЛОЖЕНИЕ В. ИНДИКАТОРЫ МОНИТОРИНГА

В приведенной ниже таблице перечислены все индикаторы, используемые подсистемой мониторинга для проверки состояния компонентов Системы. Под проверкой подразумевается периодическое получение значения индикатора и сравнение значения индикатора с пороговым значением.

Важно!

Если производились изменения конфигурационных файлов, то пороговые значения и период проверки могут отличаться от указанных.

Если все индикаторы указывают на критические значения, это может свидетельствовать о физической недоступности проверяемых серверов. Проверьте их работоспособность.

Управление сервисами (например, проверка статуса) выполняется из-под учетной записи root.

Важно!

Если действия, рекомендованные в таблице, не привели к решению проблемы, обратитесь в службу технической поддержки InfoWatch по адресу support@infowatch.com .

Название индикатора	Проверка	Значения	Период опроса
Общая нагрузка системы	Загрузка серверов IW-Linux-servers, TMcap-servers, DB-servers за последние 15, 5, 1 минут	🔴 – хотя бы одна цифра превышает соответствующее значение 20.0,16.0,12.0 за 15, 5, 1 🟡 – хотя бы одна цифра превышает соответствующее значение 10.0,8.0,6.0 за 15, 5, 1 🟢 – ни одна цифра не превышает соответствующее значение 10.0,8.0,6.0 за 15, 5, 1	30 мин.
Количество активных пользователей	Количество пользователей, зарегистрированных на хосте	🔴 – > 50 пользователей 🟡 – от 20 до 50 🟢 – < 20 пользователей	30 мин.

Название индикатора	Проверка	Значения	Период опроса
Доступность сервера Postfix	Доступность Postfix сервера	– не доступен – доступен	30 мин.
Отклонение системного времени	Лаг времени на серверах Системы и сервере NTP **Примечание:** Данная ошибка возникает, если Системе не удалось установить соединение с NTP-серверами или в конфигурации Системы не указано ни одного NTP-сервера, 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.	– > 40 секунд – от 20 до 40 секунд – < 20 секунд	360 мин.
Ошибки в журнале предупреждений БД	Наличие ошибок в журнале предупреждений БД	– есть ошибки – нет ошибок	5 мин.
Размер журнала предупреждений БД	Проверяет размер журнала предупреждений: • Для СУБД Oracle Alert Log • Для СУБД PostgreSQL System Log	– > 100 Мб – от 50 до 100 Мб – < 50 Мб	5 мин.
Состояние базы данных	Состояние указанного экземпляра базы данных Oracle или PostgreSQL (в зависимости от используемой в системе СУБД).	– ok – <> ok	10 мин.
Свободное место в основном каталоге БД	Свободное место на партиции хранения основной информации (По умолчанию: `/u01`)	– < 10 000 Мб – от 10000 до 20 000 Мб – > 20 000 Мб	30 мин.
Доступность сервера	Доступность Linux серверов	– > 500 мл с – от 100 до 500 мл с – < 100 мл с	5 мин.
Свободное место в корневой партиции	Наличие свободного места в корневой файловой системе	– < 10 000 Мб – от 10 000 МБ до 20 000 Мб – > 20 000 Мб	30 мин.

Название индикатора	**Проверка**	**Значения**	**Период опроса**
Состояние службы синхронизации времени	Доступность службы синхронизации времени	🟢 – NTP сервер доступен 🔴 – NTP сервер не доступен	30 мин.
Состояние сервиса syslog	Проверяет, запущен или нет сервис syslog	🔴 – не запущен 🟢 – запущен	30 мин.
Доступность сервера по SSH	Проверяет наличие ssh-сервиса на заданной группе серверов	🔴 – >= 10 секунд 🟢 – < 10 секунд	10 мин.
Использование файла подкачки	Наличие свободного места в swap (виртуальная память)	🔴 – свободно < 10% 🟡 – свободно от 10 % до 20% 🟢 – свободно > 20%	5 мин.
Очередь обработки действий от примененных политик	Очередь обработки действий, указанных в примененных к событиям политиках	🔴 – > 1000 объектов 🟡 – от 200 до 1000 объектов 🟢< 200 объектов	30 мин.
Очередь ошибок обработки действий примененных политик	Количество ошибок обработки действий из применённых к событиям политик	🔴 – > 50 объектов 🟡 – от 1 до 50 объектов 🟢 = 0	30 мин.
Наличие дампов памяти	Работоспособность служб	🟢 – нет дампов 🔴 – есть дамп	30 мин.
Состояние компонентов Системы	Проверяет статусы служб системы	🔴 – хотя бы один сервис не запущен 🟢 – все сервисы запущены	30 мин.
Количество ошибок индексации	Количество ошибок индексации событий процессом **iw_indexer**	🔴 – > 50 🟡 – от 1 до 50 🟢 – 0	30 мин.
Очередь индексации	Очередь объектов на индексацию в Sphinx для полнотекстового поиска	🔴 – > 10000 🟡 – от 1000 до 10000 🟢 – < 1000	30 мин.
Очередь загрузки в хранилище	Скорость загрузки событий в базу данных (скорость обработки службой IW_LOADER объектов, которые помещает в очередь служба IW_XML2LIRO). Количество объектов в очереди	🔴 – > 10000 объектов 🟡 – от 1000 до 10000 объектов 🟢 – < 1000 объектов	30 мин.

Название индикатора	Проверка	Значения	Период опроса
Очередь ошибок обработки событий	Количество объектов, обработанных с ошибкой службами IW_EXPRESSD, IW_MESSED, IW_PROXY (http, icq), IW_ICAP. Количество объектов в очереди ошибок	– > 1000 объектов – от 200 до 1000 объектов – < 200 объектов	30 мин.
Очередь обработки почтового трафика	Характеризует скорость обработки объектов сервисом IW_MESSED. Объекты помещаются в очередь сервисами IW_SMTPD и IW_PROXY (smtp). Возвращает количество объектов в очереди	– > 10000 объектов – от 1000 до 10000 объектов – < 1000 объектов	30 мин.
Очередь ошибок в работе сервисов **iw_xml2liro** и **iw_loader**	Количество ошибок обработки событий службами IW_LOADER и IW_XML2LIRO	– > 50 объектов – от 1 до 50 объектов = 0	30 мин.
Количество запущенных процессов	Проверяет количество запущенных процессов	– > 600 процессов – от 450 до 600 процессов – < 450 процессов	30 мин.
Свободное место в партиции /var	Наличие свободного места в файловой системе `/var`	– < 10 000 Мб – от 10 000 Мб до 20 000 Мб – > 20 000 Мб	30 мин.
Свободное место в каталоге событий БД	Свободное место на партициях хранения событий. (По умолчанию: `/u02`)	– < 7% – от 7 до 15% – > 15%	30 мин.
Доступность сервера Device Monitor (должно отображаться, если в системе установлена активная лицензия на Device Monitor)	Доступность сервера DM	– нет соединения – есть соединение	30 мин.
Статус службы доступа к базе данных	Состояние службы доступа к базе данных. **Примечание:** Индикатор включен и отображаться в списке, только если в Системе используется СУБД Oracle	– TNS listener не запущен – TNS listener запущен	10 мин.

Название индикатора	Проверка	Значения	Период опроса
Наличие патчей БД	Наличие установленных патчей Oracle (17402822, 12919564), необходимых для корректной работы Системы **Примечание:** Индикатор включен и отображаться в списке, только если в Системе используется СУБД Oracle	– не установлен – установлен	30 мин.
Наличие ошибок в журнале базы данных	Проверяет syslog базы данных на наличие ошибок для схемы iwtm	– нет ошибок – есть ошибки	30 мин.