INFOWATCH

InfoWatch Traffic Monitor 5.5

Руководство администратора

INFOWATCH TRAFFIC MONITOR 5.5

Руководство администратора

© ЗАО “ИнфоВотч”
Тел. +7 (495) 229-00-22 • Факс +7 (495) 229-00-22
http://www.infowatch.ru
Дата редакции: апрель 2015 года

СОДЕРЖАНИЕ

ВВЕДЕНИЕ ... 7
Аудитория ... 7
Структура руководства ... 7
Дополнительная документация ... 7
Условные обозначения ... 8
Техническая поддержка пользователей ... 8

ГЛАВА 1. ОБЗОР INFOWATCH TRAFFIC MONITOR ... 9
1.1. Функции InfoWatch Traffic Monitor ... 9
1.1.1. Перехват трафика в потоке/на шлюзе ... 9
1.1.1.1. SMTP-трафик ... 9
1.1.1.2. HTTP-траффик ... 12
1.1.1.3. HTTPS-трафик ... 15
1.1.1.4. ICQ-трафик ... 16
1.1.1.5. NRPC-трафик ... 17
1.1.1.6. FTP/Skype/Печать/Копирование на съемные носители/Jabber (XMPP)/Mail.ru (MMP) ... 18
1.1.2. Проверка файлов внутри корпоративной сети ... 19
1.1.3. Обработка трафика, полученного от сторонних систем ... 19
1.1.3.1. Обработка трафика, полученного от системы DeviceLock ... 19
1.1.3.2. Обработка трафика, полученного от системы MS Lync ... 19
1.2. Состав InfoWatch Traffic Monitor ... 20
1.3. Лицензирование ... 21

ГЛАВА 2. НАСТРОЙКА СИСТЕМЫ ПОСЛЕ УСТАНОВКИ ... 24
2.1. Предварительные настройки ... 24
2.1.1. Настройка синхронизации времени ... 24
2.1.2. Дополнительные настройки при установке с ключами IWDBX и IWTM ... 25
2.2. Настройка перехвата трафика ... 25
2.2.1. SMTP-трафик ... 26
2.2.1.1. SPAN, или Port Mirroring ... 26
2.2.1.2. Прием копий с почтового сервера ... 26
2.2.1.3. "В разрыв" ... 26
2.2.1.4. Общие настройки для SMTP-трафика ... 28
2.2.1.4.1. Настройка пересылки скрытых копий ... 28
2.2.1.4.2. Настройка сервера Postfix в системе Traffic Monitor ... 30
2.2.2. HTTP-траффик ... 32
2.2.2.1. SPAN, или Port Mirroring ... 32
2.2.2.2. "В разрыв" ... 32
2.2.3. HTTPS-трафик ... 32
2.2.3.1. "В разрыв" ... 32
2.2.4. ICQ-трафик ... 33
2.2.4.1. SPAN, или Port Mirroring ... 33
2.2.5. NRPC-трафик ... 33
2.2.5.1. SPAN, или Port Mirroring ... 33
2.2.6. Прием объектов, перехваченных InfoWatch Device Monitor ... 34
2.2.7. Проверка файлов, находящихся в корпоративной сети ... 34
2.3. Общие настройки ... 34

2.3.1. SPAN, или Port Mirroring ... 34
2.3.1.1. Настройка работы сервера Traffic Monitor в качестве Sniffer ... 35
2.3.1.2. Настройка сервера Traffic Monitor на прием копии трафика от Sniffer ... 36
2.3.1.3. Создание кластера Traffic Monitor ... 37
2.3.2. Перехват трафика, передаваемого по протоколу ICAP ... 38
2.3.2.1. Настройка ICAP ... 39
2.3.2.2. Рекомендации по настройке ICAP для Blue Coat SG Series ... 40
2.3.2.3. Рекомендации по настройке SQUID ... 40
2.3.3. Настройка работы "в разрыв" для нескольких переватчиков ... 41
2.4. Автозапуск процессов ... 42
2.4.1. Проверка автозапуска процессов ... 42
2.4.2. Включение и выключение автозапуска процессов ... 44
2.5. Модуль взаимодействия с удаленной базой данных ... 45
2.5.1. Установка клиентской части модуля взаимодействия с удаленной БД ... 45
2.5.2. Установка серверной части модуля взаимодействия с удаленной БД ... 46
2.6. Настройка OCR-библиотек ... 46
2.7. Настройка отправки уведомлений пользователям и сотрудникам ... 47
2.8. Ограничение количества найденных событий ... 48
2.9. Включение/отключение морфологической индексации ... 48

ГЛАВА 3. РАБОТА В КОНСОЛИ УПРАВЛЕНИЯ ... 50
3.1. Вход в веб-консоль и выход из нее ... 50
3.2. Управление интеграцией с LDAP каталогами ... 50
3.2.1. Создание подключения к серверу ... 52
3.2.2. Редактирование подключения к серверу ... 52
3.2.3. Удаление подключения к серверу ... 52
3.2.4. Запуск синхронизации с сервером вручную ... 53
3.3. Управление пользователями Системы и их ролями ... 53
3.3.1. Пользователи ... 53
3.3.1.1. Создание учетной записи пользователя ... 54
3.3.1.2. Редактирование учетной записи пользователя ... 55
3.3.1.3. Удаление учетной записи пользователя ... 55
3.3.1.4. Изменение пароля учетной записи пользователя ... 55
3.3.1.5. Изменение статуса учетной записи пользователя ... 55
3.3.1.6. Импорт учетной записи пользователя ... 56
3.3.1.7. Задание пользователю роли ... 56
3.3.1.8. Задание пользователю области видимости ... 56
3.3.2. Роли ... 57
3.3.2.1. Создание роли ... 57
3.3.2.2. Редактирование роли ... 58
3.3.2.3. Удаление роли ... 59
3.3.3. Области видимости ... 59
3.3.3.1. Создание области видимости ... 59
3.3.3.2. Редактирование области видимости ... 62
3.3.3.3. Удаление области видимости ... 62
3.4. Управление лицензиями ... 62
3.4.1. Проверка валидности лицензии ... 63
3.4.2. Установка лицензии ... 63
3.4.3. Удаление лицензии ... 64
3.4.4. Запрос лицензии ... 64
3.5. Состояние системы ... 64

ГЛАВА 4. КОНФИГУРИРОВАНИЕ ПЕРЕХВАТЧИКА CRAWLER 66
4.1. Настройка сетевых правил доступа 66
4.2. Конфигурационные файлы Crawler 68
4.2.1. Конфигурационный файл сервера Crawler 68
4.2.1.1. Изменение учетной записи, от имени которой запускается служба сервера Crawler 69
4.2.2. Конфигурационный файл сканера Crawler 69
4.3. Работа с журналами Crawler 70

ГЛАВА 5. КОНФИГУРИРОВАНИЕ INFOWATCH LYNC ADAPTER 71

ГЛАВА 6. МОНИТОРИНГ 72
6.1. Настройки подсистемы мониторинга 72
6.1.1. Настройка в случае раздельной установки Traffic Monitor Enterprise и базы данных 73
6.1.2. Настройка адреса сервера синхронизации времени для подсистемы мониторинга 74
6.1.3. Настройка соединения с серверами 75
6.1.4. Настройка порогов срабатывания для индикатора нагрузки 77
6.1.5. Настройка запуска служб 77
6.1.6. Настройка механизма уведомлений 77
6.1.6.1. Настройка отправки уведомлений о превышении порогового значения индикаторов 78
6.1.6.2. Настройка отправки писем-уведомлений с помощью Postfix 79

ГЛАВА 7. АДМИНИСТРИРОВАНИЕ БАЗЫ ДАННЫХ 80
7.1. Проведение регламентных работ на сервере базы данных 80
7.2. Табличные пространства в базе данных InfoWatch Traffic Monitor 81
7.3. Управление ежедневными табличными пространствами 82
7.3.1. Настройка размещения файлов на файловой системе 82
7.3.2. Индексирование данных в ежедневных табличных пространствах 84
7.3.3. Архивирование ежедневных табличных пространств 85
7.3.3.1. Автоматическое архивирование ежедневных табличных пространств 86
7.3.3.2. Архивирование ежедневных табличных пространств вручную 86
7.3.4. Восстановление ежедневных табличных пространств 88
7.3.5. Удаление ежедневных табличных пространств 88
7.4. Резервное копирование базы данных 90
7.4.1. Создание резервной копии базы данных 90
7.4.1.1. Определение размера резервной копии 91
7.4.1.2. Проверка хранилища резервной копии 91
7.4.1.3. Создание папок для резервной копии 91
7.4.1.4. Создание вспомогательных файлов на Linux 92
7.4.1.5. Создание списка файлов, подлежащих резервному копированию 93
7.4.1.6. Остановка системы IWTM 94
7.4.1.7. Остановка БД Oracle 94
7.4.1.8. Копирование файлов БД в хранилище резервных копий 94
7.4.2. Восстановление базы данных из резервной копии 95
7.4.2.1. Восстановление на той же базе данных 95
7.4.2.2. Восстановление на новой БД 95

ГЛАВА 8. АДМИНИСТРИРОВАНИЕ СЕРВЕРНОЙ ЧАСТИ INFOWATCH TRAFFIC MONITOR 97
8.1. Модули и процессы Traffic Monitor Server 97
8.1.1. Список модулей Traffic Monitor Server 97
8.1.2. Работа с процессами Traffic Monitor Server 101
8.2. Настройка параметров работы Traffic Monitor Server 102
8.2.1. Общие настраиваемые параметры конфигурационных файлов 102

8.2.1.1. Секция Logging ... 103
8.2.1.2. Секция Startup ... 103
8.2.1.3. Секция Nookdir ... 103
8.2.1.4. Секция Serman ... 104
8.2.2. Специфичные настраиваемые параметры конфигурационных файлов ... 104
8.2.2.1. Конфигурационный файл serman_resolver.conf ... 104
8.2.2.2. Конфигурационный файл sniffer.conf ... 105
8.2.2.3. Конфигурационный файл proxy.conf ... 105
8.2.2.3.1. Секция Icq ... 105
8.2.2.3.2. Секция Http ... 105
8.2.2.3.3. Секция Smtp ... 107
8.2.2.4. Конфигурационный файл oracle.conf ... 107
8.2.2.5. Конфигурационный файл cas.conf ... 108
8.2.2.5.1. Секция Analysis ... 108
8.2.2.5.2. Секция Classifier ... 108
8.2.2.5.3. Секция Tableanalysis ... 108
8.2.2.5.4. Секция Thrift ... 109
8.2.2.6. Конфигурационный файл expressd.conf ... 109
8.2.2.6.1. Секция Expressd ... 109
8.2.2.6.2. Секция Expressd, параметр Http ... 110
8.2.2.6.3. Секция Expressd, параметр Ocr ... 110
8.2.2.7. Конфигурационный файл messed.conf ... 111
8.2.2.8. Конфигурационный файл smtpd.conf ... 111
8.3. Настройка использования OCR для различных перехватчиков ... 112
8.4. Настройка параметров работы с HTTP-запросами, передаваемыми по протоколу ICAP (файл icap.conf) ... 112
8.5. Настройка параметров обработки архивов вложений (файл extractors.conf) ... 113
8.6. Архивирование каталога очереди сообщений ... 115
8.7. Протоколирование работы Системы ... 116
8.8. Перемещение объектов между очередями (утилита iw_qtool) ... 116
8.9. Загрузка очередей объектов ... 118
8.10. Восстановление работоспособности системы в аварийных ситуациях ... 119

ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ИМЕН И ПАРОЛЕЙ ... 120

ПРИЛОЖЕНИЕ В. ИНДИКАТОРЫ МОНИТОРИНГА ... 122

ГЛОССАРИЙ ... 126

ВВЕДЕНИЕ

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

Аудитория

Руководство предназначено для администраторов InfoWatch Traffic Monitor Server, знакомых с основами работы в среде операционных систем Microsoft Windows и Linux.

Руководство рассчитано на пользователей, обладающих следующими навыками:

- администрирование СУБД Oracle;
- эксплуатация Red Hat Enterprise Linux, а также управление конфигурационными файлами;
- работа в Microsoft Windows.

Структура руководства

В настоящем руководстве Вы можете найти следующую информацию:

- *Глава 1. Обзор InfoWatch Traffic Monitor (стр. 9)*

  Общие сведения об InfoWatch Traffic Monitor (назначение, основные функции).

- *Глава 2. Настройка Системы после установки (стр. 24)*

  Описание шагов, выполняемых администратором для настройки Системы.

- *Глава 3. Работа в Консоли управления (стр. 50)*

  Описание настроек Системы, выполняемых в Консоли управления.

- *Глава 4. Конфигурирование перехватчика Crawler (стр. 66)*

  Описание порядка настройки сетевых правил доступа для инфраструктуры с Crawler; описание работы с конфигурационными файлами и журналами перехватчика.

- *Глава 5. Конфигурирование Infowatch Lync Adapter (стр. 71)*

- *Глава 6. Мониторинг (стр. 72)*

  Описание настройки подсистемы мониторинга Nagios.

- *Глава 7. Администрирование базы данных (стр. 80)*

  Описание задач по управлению базой данных InfoWatch Traffic Monitor (проведение регламентных работ, управление сегментами данных).

- *Глава 8. Администрирование серверной части InfoWatch Traffic Monitor (стр. 97)*

  Сведения по управлению серверной частью после установки Системы: дополнительное конфигурирование серверной части.

Дополнительная документация

Сведения по некоторым дополнительным вопросам Вы можете найти в следующих документах:

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

  В документе описывается порядок установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.

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

В документе описывается работа с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, правила составления сценария обработки объектов).

- *«InfoWatch Device Monitor. Руководство пользователя»*

  Содержит описание принципов работы системы InfoWatch Device Monitor, а также инструкции по установке, настройке и эксплуатации системы.

- *«InfoWatch DeviceLock Adapter. Руководство по установке и конфигурированию».*

  В документе описывается установка и первоначальная настройка InfoWatch DeviceLock Adapter.

- *«InfoWatch DeviceLock Adapter. Руководство администратора».*

  В документе приводятся сведения по настройке и мониторингу работы InfoWatch DeviceLock Adapter.

Условные обозначения

Для наглядности в тексте документации используются различные стили оформления. Области применения стилей указаны в следующей таблице.

Стиль оформления	Область применения	Пример
Полужирный шрифт	Названия элементов графического пользовательского интерфейса (кнопки, команды меню и пр.), компоненты системы (при первом упоминании)	Для перемещения объектов из одной очереди в другую используется утилита **iw_qtool**
Курсив	При описании таблиц, в примерах, описаниях – названия и значения атрибутов объектов	База контентной фильтрации содержит термин *Договор*
`Шрифт Courier New`	Имена файлов, примеры текста программ; значения параметров конфигурационных файлов, примеры настройки	Проверка запуска Traffic Monitor Server осуществляется командой: `service iwtm status`
`ШРИФТ COURIER NEW (ВЕРХНИЙ РЕГИСТР)`	Названия секций конфигурационных файлов (в квадратных скобках), переменных, параметров. При описании базы данных – ключевые слова SQL, инструкции PL/SQL, типы данных, привилегии	Параметры автозапуска задаются в файле `/opt/iw/tm5/etc/sniffer.conf`, секция `Startup`

Техническая поддержка пользователей

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

- Если Вы приобрели продукт у партнера компании InfoWatch, обратитесь в службу технической поддержки партнера.
- Если продукт приобретен у компании InfoWatch напрямую, Вы можете обратиться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com. Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/support.

  Примечание: 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.

  Часы работы Службы технической поддержки – с 7-00 до 21-00 с понедельника по пятницу по московскому времени, исключая официальные выходные и праздничные дни в РФ.

ГЛАВА 1. ОБЗОР INFOWATCH TRAFFIC MONITOR

В этой главе:

- *Функции InfoWatch Traffic Monitor (п. 1.1 на стр. 9).*
- *Состав InfoWatch Traffic Monitor (п. 1.2 на стр. 20).*
- *Лицензирование (п. 1.3 на стр. 21).*

1.1. 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, HTTP, HTTPS, OSCAR (ICQ), NRPC (IBM Notes) – см. п. 1.1.1 на стр. 9;
- Проверка файлов, находящихся внутри корпоративной сети – см. п. 1.1.2 на стр. 19.
- Анализ Skype-трафика, теневых копий файлов и заданий на печать, передачи трафика по протоколу FTP, контроль обмена данными через Jabber (протокол XMPP) и через Mail.Ru Агент (протокол MPP) – см. п. 1.1.1.6 на стр. 18.
- Анализ теневых копий файлов, перехваченных системой DeviceLock ЗАО «Смарт Лайн Инк», – см. п. 1.1.3.1 на стр. 19.
- Анализ копий файлов, полученных от системы Microsoft Lync, – см. п. 1.1.3.2 на стр. 19.
- Анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности.
- Фильтрация перехваченного трафика путем выдачи разрешения/запрещения на доставку определенных данных.

1.1.1. Перехват трафика в потоке/на шлюзе

1.1.1.1. SMTP-трафик

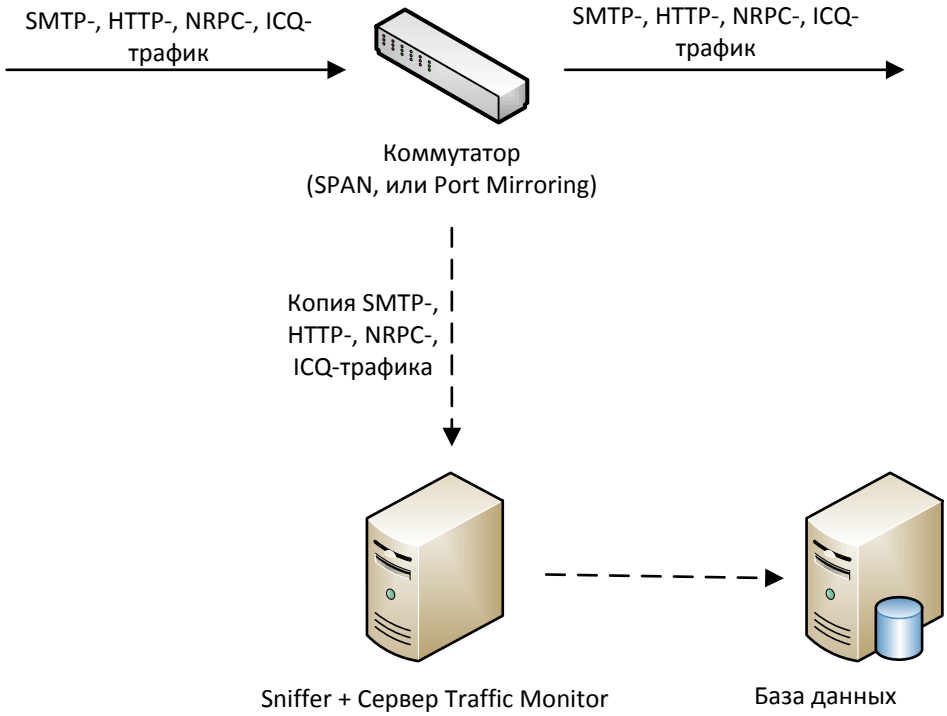
Способ №1:

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 при подключении к сетевому интерфейсу не требуется.

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



О настройке данного функционала *см. п. 2.2.1.1* на стр. *26.*

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:

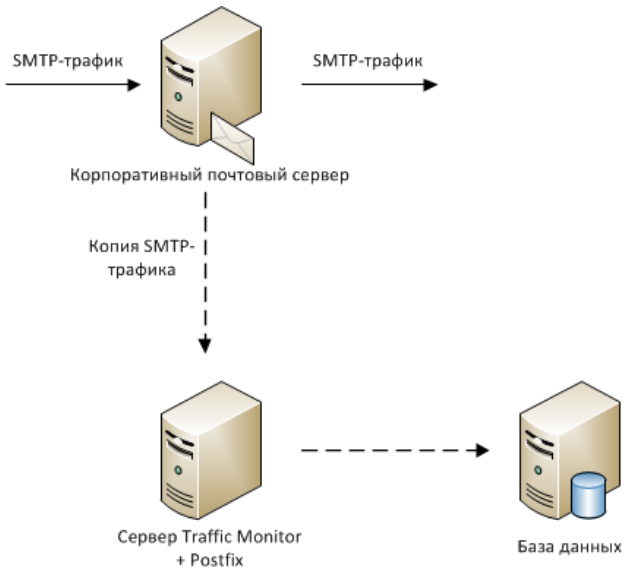
  - коммутатор с соответствующим функционалом;

  - дополнительный сетевой адаптер на сервере мониторинга.

- Внутренняя переписка не контролируется.

Способ №2:

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



О настройке данного функционала см. п. 2.2.1.2 на стр. 26.

Преимущества:

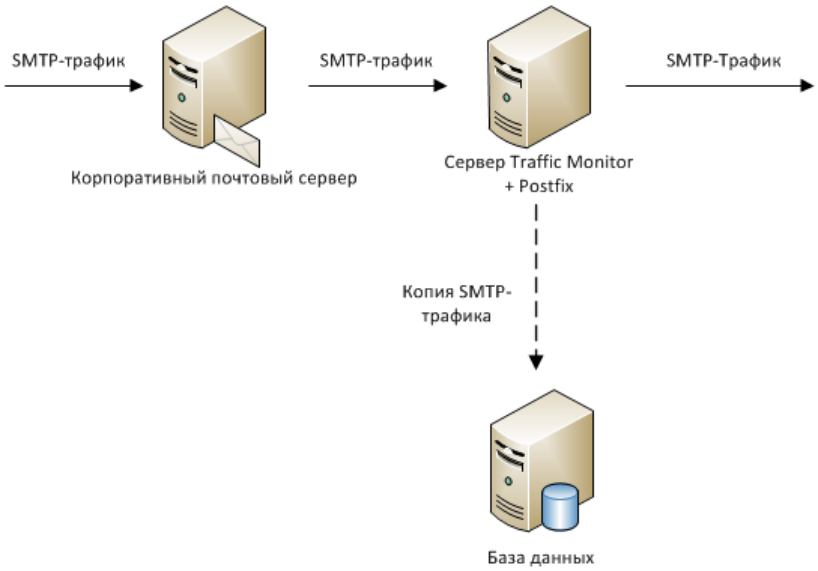
- Позволяет анализировать не только внешнюю, но и внутреннюю переписку компании;
- При использовании MS Exchange 2007 и более новых есть возможность анализировать переписку определенной группы пользователей;
- Гарантирует анализ всех писем.

Недостатки:

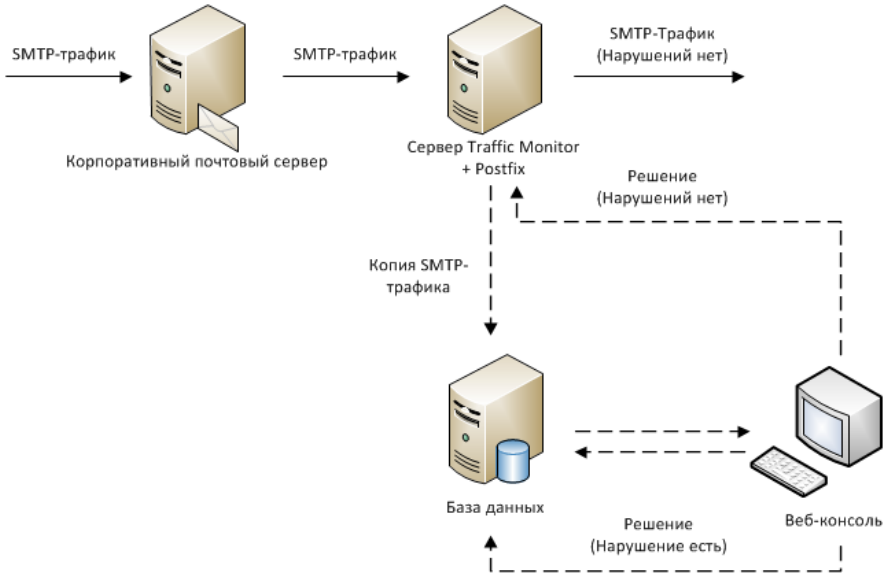
- Требует внесения изменений в настройки корпоративного почтового сервера;
- Никак не контролируются внешние почтовые серверы (если их использование вообще разрешено);
- При недоступности сервера Traffic Monitor, пользователи получат сообщение об ошибке доставки скрытой копии;
- Дополнительная нагрузка 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 см. п. 2.2.1.3 на стр. 26.

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 вообще разрешено);
- В случае недоступности сервера мониторинга, пользователи не смогут отправлять письма, если не предусмотрено резервирование сервиса (к примеру, через MX-записи).

1.1.1.2. HTTP-траффик

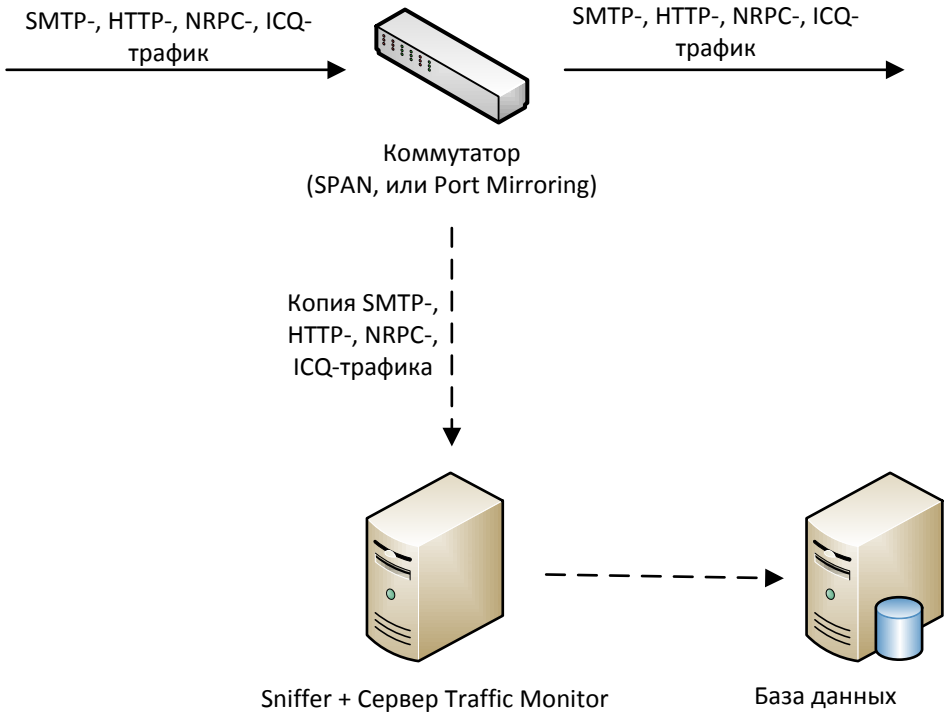
Способ №1:

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. *п. 2.2.2.1 на стр. 32.*

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.

Частный случай №1:

Если сервер мониторинга находится в виртуальной среде, то в дополнение к настройке порта коммутатора, для мониторинга траффика 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.

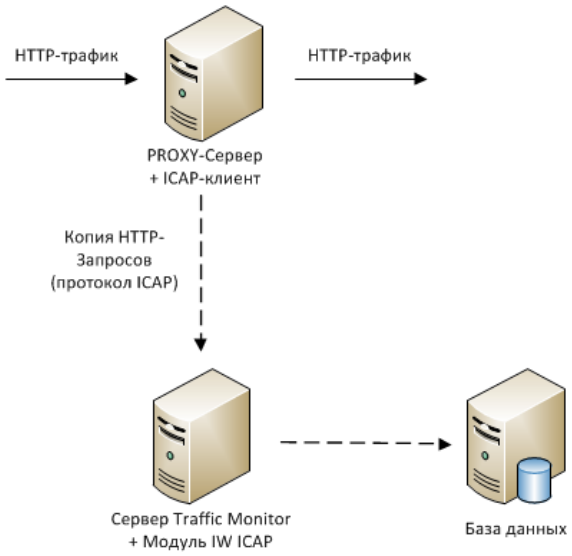
Сервер Traffic Monitor выступает в качестве ICAP-клиента. Если в компании работает прокси-сервер, поддерживающий ICAP протокол, то можно использовать данный функционал для анализа HTTP-трафика.

Данную функцию поддерживают следующие прокси-серверы:

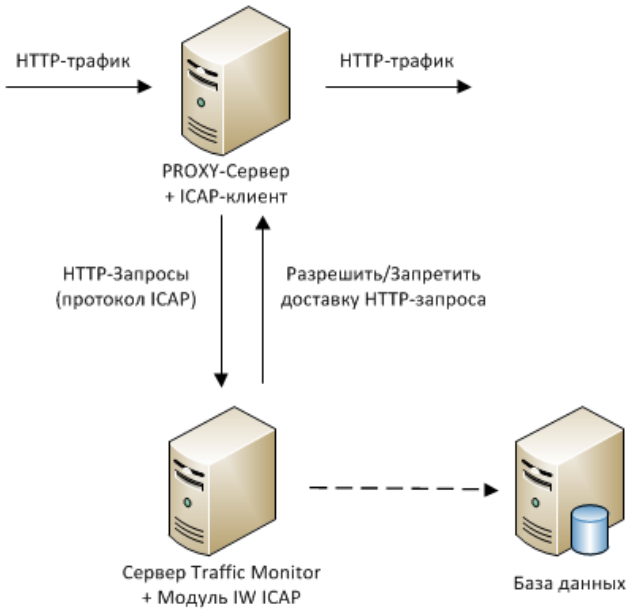
- Cisco Ironport
- SQUID (при условии, что пакет собран с поддержкой ICAP)
- Blue Coat SG

- 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. п. 2.2.2.2 на стр. 32.*

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.

1.1.1.3. HTTPS-трафик

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

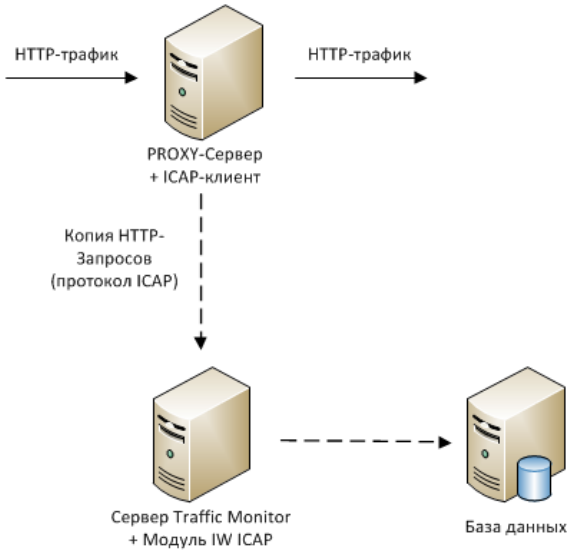
Способ №1:

Подмену сертификата и разбор HTTPS-трафика осуществляет корпоративный прокси-сервер. После разбора HTTPS-трафика прокси-сервер отправляет разобранный трафик в виде HTTP по ICAP протоколу на сервер Traffic Monitor.

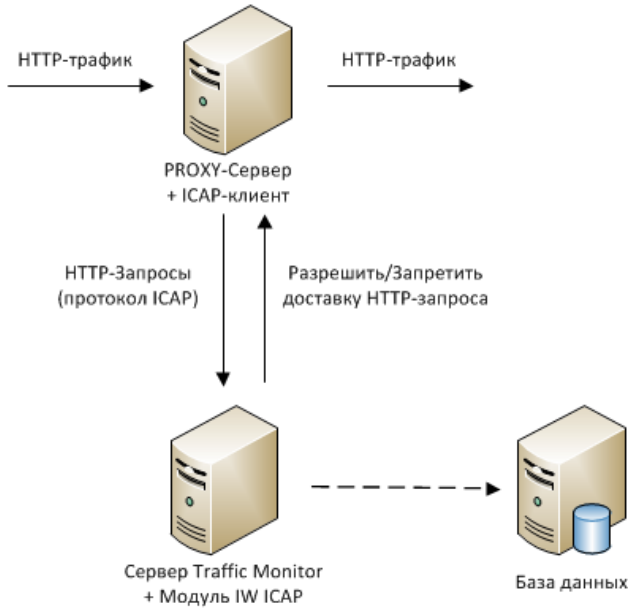
Данным функционалом обладают следующие прокси-серверы:

- Cisco Ironport
- SQUID (при условии, что пакет собран с поддержкой ICAP)
- Blue Coat SG
- 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. п. 2.2.3.1 на стр. 32.*

Преимущества:

- Анализируется весь HTTPS-трафик.

Недостатки:

- 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.

1.1.1.4. ICQ-трафик

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

Внимание!

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

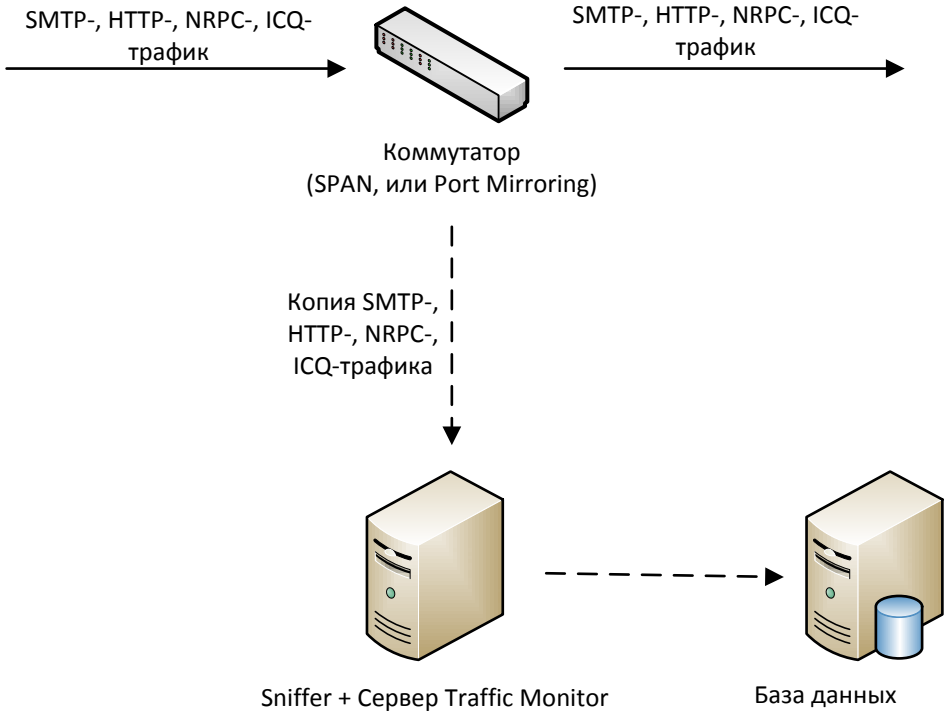
Способ №1:

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 при подключении к сетевому интерфейсу не требуется.

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



О настройке данного функционала *см. п. 2.2.4.1 на стр. 33.*

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.

1.1.1.5. NRPC-трафик

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

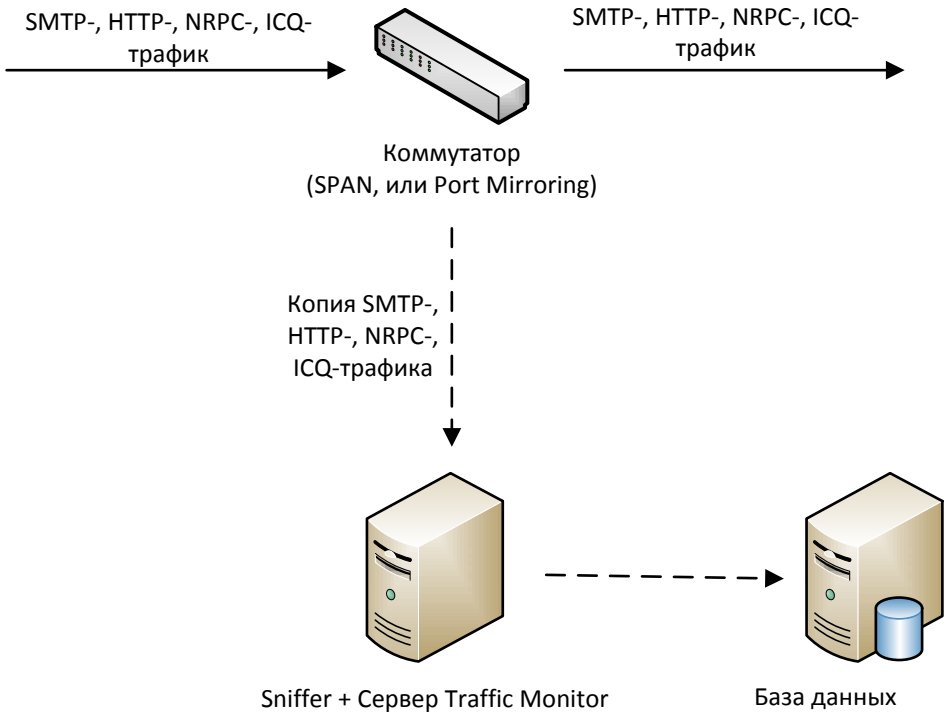
Способ №1:

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. п. 2.2.5 на стр. 33.*

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.

1.1.1.6. FTP/Skype/Печать/Копирование на съемные носители/Jabber (XMPP)/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».

1.1.2. Проверка файлов внутри корпоративной сети

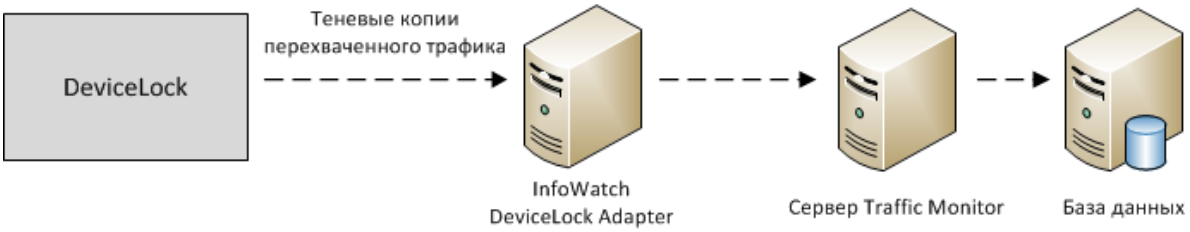
Анализ содержания файловых серверов и сетевых ресурсов возможен после установки специального модуля на сервер под управление MS Windows Server ОС.

О настройке данного функционала см. Глава 4 на стр. 66.

1.1.3. Обработка трафика, полученного от сторонних систем

1.1.3.1. Обработка трафика, полученного от системы DeviceLock

Анализ теневых копий файлов, перехваченных системой DeviceLock ЗАО «Смарт Лайн Инк» (версии 6.3 и более новых).

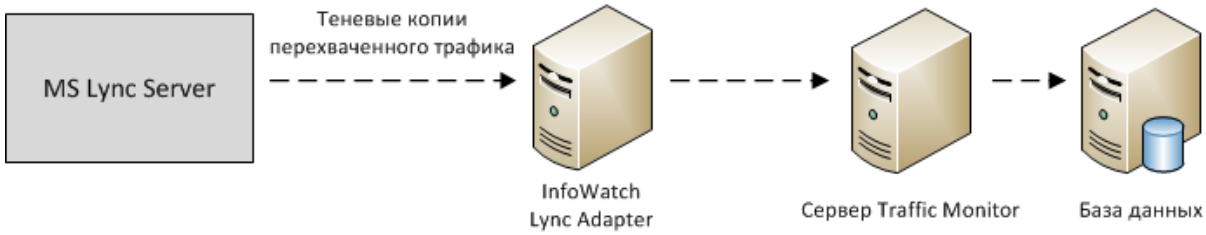


На каждый сервер, который должен выполнять прием объектов, установите InfoWatch DeviceLock Adapter и выполните его настройку. Рекомендации приводятся в документах:

- «*InfoWatch DeviceLock Adapter. Руководство по установке и конфигурированию*».
- «*InfoWatch DeviceLock Adapter. Руководство администратора*».

1.1.3.2. Обработка трафика, полученного от системы MS Lync

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 Traffic Monitor. Руководство по установке*».

1.2. 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; • Модуль DeviceLock Adapter (поставляется отдельно)
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, извлеченные из вложений). Состоит из следующих модулей: • Модуль лингвистического анализа; • Модуль графического анализа; • Модуль детектирования форм; • Модуль детектирования печатей; • Модуль детектирования текстовых объектов; • Модуль детектирования цифровых отпечатков; • Модуль детектирования выгрузок из БД.
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 InfoWatch Traffic Monitor	Назначение подсистемы
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.

1.3. 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. Чтобы продолжить эксплуатацию Системы, установите коммерческую лицензию на перехватчики, которые Вы планируете использовать.

При необходимости лицензию для устанавливаемой Системы генерирует инженер внедрения.

Чтобы продолжить эксплуатацию Системы по истечении ознакомительного срока, установите коммерческую лицензию на перехватчики, которые Вы планируете использовать (см. п. 3.4.1 на стр. 63). Для этого запросите файл коммерческого лицензионного ключа (см. п. 3.4.4 на стр. 64).

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.

Внимание!

О проверке валидности лицензии см. п. 3.4.1 на стр. 63.

Об управлении лицензиями см. п. 3.4 на стр. 62.

О лицензировании второстепенных серверов см. п. 2.3.3 на стр. 41.

Ниже приведены списки устанавливаемых в ознакомительной версии модулей и технологий.

Список модулей перехвата:

Канал	Кем перехватывается	Комментарий
SMTP	TM	
SMTP/endpoint	DM	В том числе трафик в канале TLS
POP3	TM	
POP3/endpoint	DM	В том числе трафик в канале TLS
IMAP4	TM	
MAPI	DM	
HTTP	TM	
HTTPS/endpoint	DM	
ICQ	TM	
Storage	DM	Перехват копирования на съемные носители
Print	DM	Перехват печати
FTP	DM	
Skype	DM	
Jabber	DM	Перехват переписки по протоколу XMPP
Mail.Ru	DM	
HTTP/endpoint	DM	
Yahoo	DM	
Lync	TM	
Lotus Domino	TM	
Crawler	Crawler	
Lotus Domino Adapter	TM	
Device Lock Adapter	TM	
ICAP	TM	

Список модулей анализа:

Название технологии	Комментарий
Classifier	Классификация текста на основе набора терминов. Для настройки классификации возможно: • самостоятельно сформировать наборы терминов; • приобрести разные БКФ; • приобрести Auto-linguist – для формирования набора терминов на основе коллекций документов
Fingerprints	Цифровые отпечатки
Templates Analyser	Текстовые шаблоны
Database Table Detector	Детектор выгрузок БД
Text Form Detector	Детектор форм
Graphic Analysis	Классификация графических изображений
Stamp Detector	Детектор печатей

ГЛАВА 2. НАСТРОЙКА СИСТЕМЫ ПОСЛЕ УСТАНОВКИ

2.1. Предварительные настройки

После установки системы необходимо выполнить следующие настройки:

- *Настройка синхронизации времени (п. 2.1.1 на стр. 24)*
- *Дополнительные настройки при установке с ключами IWDBX и IWTM (п. 2.1.2 на стр. 25)*

2.1.1. Настройка синхронизации времени

1. Установите системное время с помощью команды `date`. Например, для установки 11 сентября 2013 13:30 запустите команду со следующими параметрами:

   ```
   date 09111330
   ```

2. Скопируйте системное время для настройки аппаратных часов с помощью команды:

   ```
   hwclock --systohc
   ```

3. Проверьте, что системное и аппаратное время настроены корректно:

   ```
   hwclock ; date
   ```

   Время должно быть одинаковым, допустимы небольшие отклонения.

4. 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
   ```

2.1.2. Дополнительные настройки при установке с ключами IWDBX и IWTM

При использовании двух и более серверов для их корректного функционирования необходимо логически разделить их на основной и второстепенный (второстепенные).

Чтобы ознакомиться со списком сервисов, которые должны быть запущены только на одном из серверов см. Автозапуск процессов (п. 2.4 на стр. 42).

Чтобы выполнить настройку на перехват основного и второстепенного сервера (серверов):

1. Остановите сервисы IWTM:

   ```
   service iwtm stop
   ```

2. В конфигурационном файле `/opt/iw/tm5/etc/serman_resolver.conf` каждого сервера в параметре `Host` укажите IP-адрес основного сервера.
3. В секции `Serman` конфигурационных файлов всех используемых сервисов укажите:
   - для второстепенного сервера (серверов):
     - `Host` - IP-адрес основного сервера
     - `ServiceHost` – внешний IP-адрес сервера.
   - для основного сервера
     - `Host` – 127.0.0.1
     - `ServiceHost` – IP-адрес основного сервера.
4. Убедитесь, что в конфигурационном файле `/opt/iw/tm5/etc/license.conf` второстепенного сервера (серверов) значение параметра `Licensee` совпадает с аналогичным параметром на основном сервере.

2.2. Настройка перехвата трафика

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

- *SMTP-трафик (см. п. 2.2.1 на стр. 26)*
- *HTTP-траффик (см. п. 2.2.2 на стр. 32)*
- *HTTPS-трафик (см. п. 2.2.3 на стр. 32)*
- *ICQ-трафик (см. п. 2.2.4 на стр. 33)*
- *NRPC-трафик (см. п. 2.2.5 на стр. 33)*
- *Прием объектов, перехваченных InfoWatch Device Monitor (см. п. 2.2.6 на стр. 34)*
- *Проверка файлов, находящихся в корпоративной сети (см. п. 2.2.7 на стр. 34)*

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»).*

2.2.1. SMTP-трафик

Описание данного способа перехвата трафика см. в п. 1.1.1.1 на стр. 9.

2.2.1.1. SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. п. 2.3.1 на стр. 34).
2. Убедитесь, что в конфигурационном файле `proxy.conf`, расположенном в директории `/ort/iw/tm5/etc`, в секции `Startup` включен автозапуск перехватчика SMTP-трафика:

```
"Startup": {
    "Enabled": true,
    "smtp": true
```

2.2.1.2. Прием копий с почтового сервера

На корпоративном почтовом сервере требуется настроить правило, отправляющее скрытую копию (BCC) для каждого отправленного письма. Копия должна отравляться на почтовый адрес с почтовым доменом, 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` (п. 2.4 на стр. 42).
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 п. 2.2.1.4.1 на стр. 28.
3. Настройте встроенный в Систему Postfix (п. 2.2.1.4.2 на стр. 30).
4. 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 п. 2.3.3 на стр. 41.

2.2.1.3. "В разрыв"

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

Интеграция сервера Traffic Monitor с почтовым сервером Postfix в данном случае реализуется следующим образом. Почтовый сервер Postfix, встроенный в систему Traffic Monitor, принимает входящие SMTP-письма на на `25`-й порт. Затем 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.

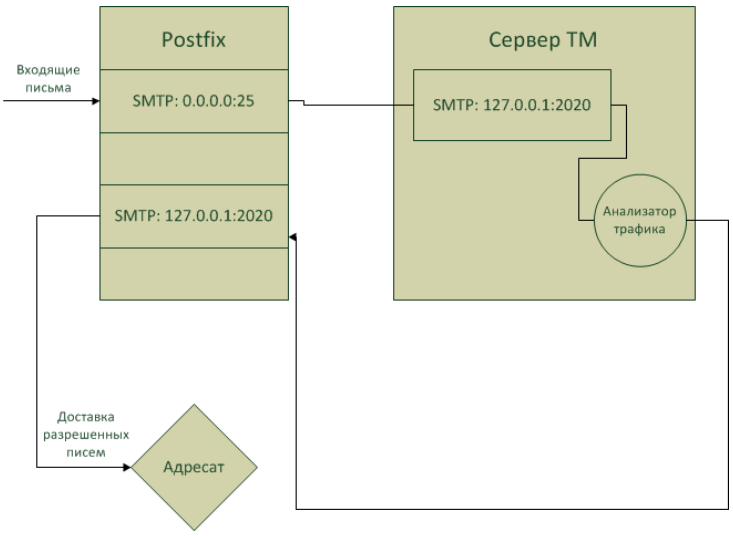


Рисунок 1. Интеграция с Postfix (Копия)

- Режим Блокировка – SMTP-трафик анализируется системой Traffic Monitor. В зависимости от наличия нарушений возможны следующие варианты движения трафика:
  - если нарушение отсутствует, SMTP-трафик с помощью Postfix предается адресату или следующему relay-серверу в почтовой системе организации.
  - 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 писем в режиме Блокировка 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.

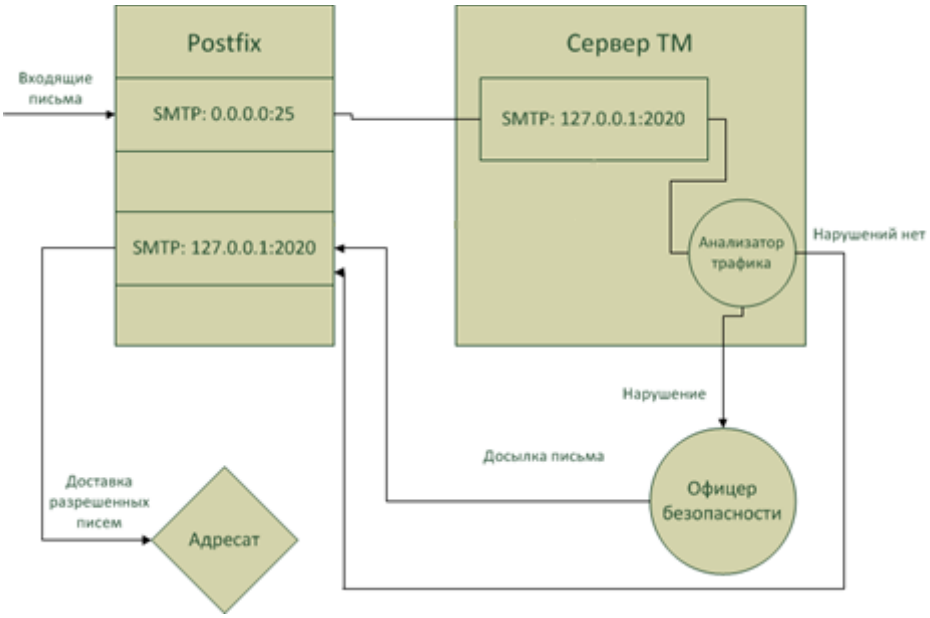


Рисунок 2. Интеграция с Postfix (Блокировка)

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 сервер Postfix
>
> Способ настройки зависит от того, какой почтовый сервер используется в компании.

В результате 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` (п. 2.4 на стр. 42).
3. Настройте встроенный в Postfix (п. 2.2.1.4.2 на стр. 30).
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. Чтобы выполнить более гибкую настройку, см. п. 2.3.3 на стр. 41.

2.2.1.4. Общие настройки для SMTP-трафика

2.2.1.4.1. Настройка пересылки скрытых копий

> **Внимание!**
>
> В данном разделе приведена инструкция по настройке пересылки скрытых копий SMTP-сообщений (BCC – Blind Carbon Copy) на сервер Traffic Monitor на примере Microsoft Exchange Server 2007 и 2010. При использовании других типов почтовых серверов порядок настройки будет отличаться.

Чтобы обеспечить отправку скрытых копий SMTP-сообщений, в Exchange Management Console необходимо создать и настроить коннектор, который будет пересылать почту на сервер Traffic Monitor.

1. Создание SMTP-коннектора, который будет пересылать почту 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 ТМ, 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 ТМ не требует авторизации. Нажмите **Next**.

6. На шаге **Source Server** 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.

2. 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 **Mail Contact** и нажмите **Next**.
3. На шаге **Configure smart host authentication settings** введите общую информацию о контакте. В строке **External e-mail address** нажмите **Edit**. В открывшемся диалоговом окне **SMTP Address** укажите почтовый адрес, на который будут перенаправляться копии почтовых сообщений.

   Внимание!

   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.

   Внимание!

   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
   ```

3. Создание транспортного правила для копирования писем

1. Выберите узел **Organization Configuration -> Hub Transport** и нажмите **New Transport Rule**.
2. В открывшемся окне мастера создания транспортного правила введите имя создаваемого правила и установите флажок в поле **Enable Rule**. 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 **ОК**. 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**.

4. Блокирование отправки сообщений при недоступности сервера TM

1. Выберите узел **Organization Configuration -> Hub Transport** и нажмите **New remote Domain**.
2. Укажите такое же имя, как у домена, использованного в п. 3 шага 2 данного раздела (при создании контакта, на который будут перенаправляться копии 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**.

2.2.1.4.2. 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 TM 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 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 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 (п. 2.2.1.3 на стр. 26 2.2.1.3 - подключение "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:

```
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 серверы Exchange.

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.

2.2.2. HTTP-траффик

Описание данного способа перехвата трафика см. в п. 1.1.1.2 на стр. 12.

2.2.2.1. SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. п. 2.3.1 на стр. 34).
2. Убедитесь, что в конфигурационном файле **proxy.conf**, расположенном в директории `/ort/iw/tm5/etc`, в секции `Startup` включен автозапуск перехватчика SMTP-трафика:

```
"Startup": {
    "Enabled": true,
    "http": true
```

2.2.2.2. "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. п. 2.3.2 на стр. 38).
2. Настройте параметры перехвата HTTP-запросов на прокси-сервере (см. п. 2.3.2.1 на стр. 39).

2.2.3. HTTPS-трафик

Описание данного способа перехвата трафика см. в п. 1.1.1.3 на стр. 15.

2.2.3.1. "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. п. 2.3.2 на стр. 38).
2. Настройте параметры перехвата HTTPS-запросов на прокси-сервере (см. п. 2.3.2.1 на стр. 39).
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, исходящий HTTPS-трафик с которой Вы планируете контролировать.

   > **Примечание:**
   >
   > Информацию по настройке Вы можете получить из документации к браузеру.

2.2.4. ICQ-трафик

Описание данного способа перехвата трафика см. в п. 1.1.1.4 на стр. 16.

2.2.4.1. SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. п. 2.3.1 на стр. 34).
2. Убедитесь, что в конфигурационном файле **proxy.conf**, расположенном в директории `/ort/iw/tm5/etc`, в секции `Startup` включен автозапуск перехватчика SMTP-трафика:

```
"Startup": {
    "Enabled": true,
    "icq": true
```

2.2.5. NRPC-трафик

2.2.5.1. SPAN, или Port Mirroring

1. Настройте сервер (серверы) на работу по технологии SPAN, или Port Mirroring (см. п. 2.3.1 на стр. 34).
2. Откройте на редактирование конфигурационный файл `capstack.conf`, расположенный в директории `/ort/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 start capstack
```

2.2.6. Прием объектов, перехваченных InfoWatch Device Monitor

Описание данного способа перехвата трафика см. в п. 1.1.1.6 на стр. 18.

1. Установите и настройте серверную часть Traffic Monitor (см. документ «InfoWatch Traffic Monitor. Руководство по установке»).
2. Настройте передачу событий из Device Monitor на сервер Traffic Monitor (см. документ «InfoWatch Device Monitor. Руководство пользователя»).
3. Настройте параметры анализа объектов (см. документ «InfoWatch Traffic Monitor. Руководство пользователя»).

2.2.7. Проверка файлов, находящихся в корпоративной сети

Описание данного способа перехвата трафика см. в п. 1.1.2 на стр. 19.

Анализ содержания файловых серверов и сетевых ресурсов возможен после установки специального модуля на сервер под управление MS Windows Server ОС.

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

Настройте параметры анализа объектов (см. документ «InfoWatch Traffic Monitor. Руководство пользователя»).

2.3. Общие настройки

2.3.1. 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 **IWALLX**). Кластер не создается:

1. Настройте сервер на работу в качестве Sniffer (п. 2.3.1.1 на стр. 35, вариант 2)
2. Настройте параметры приема копии трафика от Sniffer (п. 2.3.1.2 на стр. 36).

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

1. На одном компьютере (ключ установки **IWTMX**):
    a. Настройте сервер на работу в качестве Sniffer (п. 2.3.1.1 на стр. 35, вариант 1).
2. На другом компьютере (ключ установки **IWALLX**):
    a. Настройте параметры приема копии трафика от Sniffer (п. 2.3.1.2 на стр. 36).

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 Oracle со схемой БД Traffic Monitor с использованием типа установки *База данных* (ключ установки **IWDBX**).

2. На компьютере, где будет работать Sniffer (ключ установки **IWTMX**):
    a. Настройте его на работу в качестве Sniffer (п. 2.3.1.1 на стр. 35, вариант 1).
3. На компьютере, где будет работать экземпляр кластера Traffic Monitor (ключ установки **IWALLX**):
    a. Настройте параметры приема копии трафика от Sniffer (п. 2.3.1.2 на стр. 36).
    b. Укажите параметры кластеризации (п. 2.3.1.3 на стр. 37).

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

2.3.1.1. 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):

        a. Включите автозапуск процесса `iw_sniffer`.

        b. Отключите автозапуск других процессов.

        > **Примечание:**
        >
        > Подробнее о включении и выключении автозапуска процессов см. п. Включение и выключение автозапуска процессов на стр. 44.

    - Вариант 2. Перехват и анализ копии трафика будет выполняться на одном компьютере. Сервер Traffic Monitor будет принимать копию трафика от коммутатора (функция Sniffer), анализировать полученные данные и загружать их в базу данных (функции сервера Traffic Monitor):

        a. Включите автозапуск процессов `iw_sniffer`, `iw_loader`, `iw_updater`, `iw_warpd` и `iw_adlibitum`.

        b. Отключите автозапуск других процессов.

        > **Примечание:**
        >
        > Подробнее о включении и выключении автозапуска процессов см. п. Включение и выключение автозапуска процессов на стр. 44.

3. В конфигурационном файле **proxy.conf**, расположенном в директории `/ort/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 п. 2.2.5.1 на стр. 33.

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
   ```

2.3.1.2. 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 `Timneouts`)	Время сохранения соединения (в сек) при отсутствии пакетов. Рекомендуемое значение – `600`
`LiveInSec` (подсекция `Timneouts`)	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 `Timneouts`)	Время сохранения соединения (в сек) при переходе в состояние *TIME_WAIT*. Рекомендуемое значение – `300`
`TailInSec` (подсекция `Timneouts`)	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`.

   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
   }
   ```

2.3.1.3. Создание кластера Traffic Monitor

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

> **Внимание!**
>
> 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, превышающую в два раза 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` задайте параметры кластеризации:

1. Убедитесь, что в конфигурационном файле sniffer.conf секция `Usedareas` имеет следующий вид:

   ```
   "UsedAreas": [
   "capstack",
   "http",
   "icq",
   "smtp"
   ]
   ```

   По умолчанию данная настройка выполнена.

2. В конфигурационном файле proxy.conf, в разделе `Iscp` секций `Smtp`, `Icq`, `Http` укажите значение параметров `Host` и `Port`.

   Например,

   Для настройки взаимодействия с компьютером, имеющим IP-адрес `10.20.30.40` и порт `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).

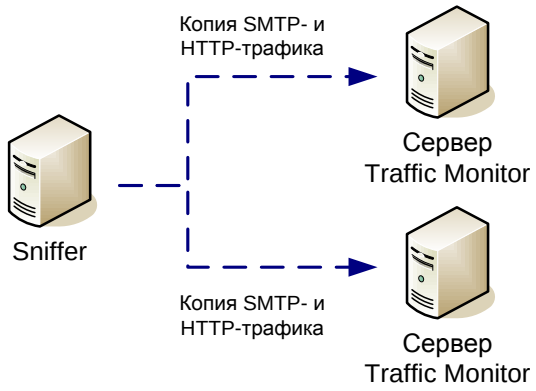


Рисунок 3. Создание кластера из двух серверов Traffic Monitor

2.3.2. 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.

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.

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

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

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

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

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

В этом разделе:

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

2.3.2.1. Настройка ICAP

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

> **Внимание!**
>
> 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 браузеру.

Настройте транспортный режим для трафика, передаваемого по ICAP.

Чтобы трафик передавался в режиме «Копия»:

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('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. п. 2.3.3 на стр. 41.

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. п. 2.3.2.2 на стр. 40) и SQUID (см. п. 2.3.2.3 на стр. 40).

2.3.2.2. Рекомендации по настройке ICAP для 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.

> **Примечания:**
>
> Процедура настройки, описанная ниже, может отличаться в зависимости от версии и модели прокси-сервера. Актуальную информацию по настройке Вы можете получить из документации к прокси-серверу.
>
> Если вам необходимо перехватывать HTTPS-трафик, то настройте Blue Coat так, чтобы HTTPS-трафик обрабатывался как HTTP-трафик. 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**.

     > **Внимание!**
     >
     > 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**.

2.3.2.3. Рекомендации по настройке SQUID

В настройках прокси-сервера задайте следующие параметры:

- разрешите использование ICAP;
- обязательно установите режим работы ICAP-сервера равным `Request Mode`;

- укажите IP-адрес ICAP-сервера, на который будут передаваться HTTP-запросы. ICAP-сервер входит в состав модуля IW ICAP. Поэтому нужно указывать IP-адрес компьютера, на который установлен модуль IW ICAP.

Пример настройки ICAP для SQUID 3.2.1

В файле `squid.conf` задайте параметры:

```
icap_enable on
icap_send_client_ip on
icap_send_client_username on
icap_service service_req reqmod_precache bypass=1 icap://IP_TM_Server:Port_TM_Server/reqmod
adaptation_access service_req allow all,
```

где `IP_TM_Server` - IP-адрес сервера Traffic Monitor, а `Port_TM_Server` – порт, на котором Traffic Monitor слушает ICAP (значение по умолчанию – 1344).

2.3.3. Настройка работы "в разрыв" для нескольких переватчиков

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');
         end
         if 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.

> **Внимание!**
>
> При конфигурировании HTTP перехватчика, необходимо также отредактировать конфигурационный файл `icap.conf` в соответствии с выбранной схемой (см. п. 2.3.2.1 на стр. 39)

6. Перезагрузите Систему:

   ```
   service iwtm restart
   ```

2.4. Автозапуск процессов

В этом разделе:

- Проверка автозапуска процессов (п. 2.4.1 на стр. 42);
- Включение и выключение автозапуска процессов (п. 2.4.2 на стр. 44).

2.4.1. Проверка автозапуска процессов

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

Процесс	По умолчанию автозапуск включен
iw_adlibitum	Да **Примечание:** Процесс должен работать только на основном сервере
iw_agent	Да
iw_agent_kicker	Да
iw_blackboard	Да
iw_blackboard_kicker	Да **Примечание:** Процесс должен работать только на основном сервере
iw_bookworm	Да
iw_capstack	Да
iw_cas	Да
iw_crawler_kicker	Да

Процесс	По умолчанию автозапуск включен
iw_deliver	Да
iw_expressd	Да
iw_icap	Да
iw_licensed	Да **Примечание:** Процесс должен работать только на основном сервере
iw_loader	Да
iw_luaengined	Да
iw_messed	Да
iw_notifier_kicker	Да
iw_proxy_http iw_proxy_icq iw_proxy_smtp	Да
iw_qmover_client	Нет
iw_qmover_server	Нет
iw_report_kicker	Да
iw_sample_compiler	Да
iw_selection_kicker	Да
iw_serman	Да **Примечание:** Процесс должен работать только на основном сервере
iw_smtpd	Да
iw_sniffer	Да
iw_system_check	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью
iw_systemcheck_kicker	Да **Примечание:** Процесс должен работать только на сервере с веб-консолью
iw_updater	Да
iw_warpd	Да
iw_whiteboard	Да
iw_xml2liro	Да

Внимание!

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

Подробнее о включении автозапуска процессов см. п. 2.4.2 на стр. 44.

2.4.2. 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}`

   Внимание!

   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`

2.5. Модуль взаимодействия с удаленной базой данных

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

2.5.1. Установка клиентской части модуля взаимодействия с удаленной БД

1. Установка и настройка общих параметров

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

Параметр	Описание	Требуемое значение
ListenerIP	IP-адрес сервера	IP-адрес сервера, на котором работает служба `qmover_server`
Port	Порт сервера (центральный офис)	16888
NookDir	Домашняя директория модуля	Произвольно
ChannelWidth	Ширина канала	От 10 до 4096 Кбит/с

2. Перезапустите Traffic Monitor:

   ```
   service iwtm restart
   ```

2. Настройка автозапуска процессов

- Включите автозапуск для процесса `iw_qmover_client`.
- Отключите автозапуск для процессов `iw_loader`, `iw_xml2liro`, `iw_deliverd` и `iw_adlibitum`.

  Подробнее о включении и выключении автозапуска процессов см. п. Включение и выключение автозапуска процессов на стр. 44.

3. Изменение ширины полосы пропускания для канала передачи данных

По умолчанию полоса пропускания имеет ширину 256 Кбит/с. Но Вы можете настроить автоматическое изменение полосы пропускания в различные периоды времени. Для этого используется утилита `iw_qmover_channel_width_setter`.

Допускается изменение ширины полосы пропускания. Минимальная ширина – 10 Кбит/с. Максимальная ширина не установлена, но рекомендуемое максимальное значение – 2 Мбит/с.

Чтобы настроить ограничения на ширину полосы пропускания,

Запустите утилиту с обязательными параметрами:

```
iw_qmover_channel_width_setter <unix_socket_name> <полоса_пропускания>,
```

где

- `unix_socket_name` – имя сокета (автоматически создается при запуске на время выполнения службы; при завершении службы удаляется автоматически); значение по умолчанию - `/opt/iw/tm5/run/.channel_socket;`

- полоса_пропускания – ширина полосы пропускания в кбит/с, которую нужно установить.

Пример

Имеется канал с полосой пропускания 256 кбит/с. Необходимо, чтобы в период с 9.00 до 18.00 канал был занят на 50 %. А с 18.00 до 9.00 - на 100%.

Рассчитайте ширину полосы пропускания, исходя из загрузки вашего канала. В этом примере ширина полосы пропускания для разных интервалов времени составляет:

Интервал	Ширина полосы пропускания	
	Процент от величины канала	В пересчете на кбит/с
9.00 до 18.00	50%	128
18.00 до 9.00	100%	256

Добавьте в etc/crontab команды:

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

2.5.2. Установка серверной части модуля взаимодействия с удаленной БД

1. Настройка конфигурации

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

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

Внимание!

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

2. Настройка автозапуска

Включите автозапуск для процесса iw_qmover_server (подробнее о включении и выключении автозапуска процессов см. п. Включение и выключение автозапуска процессов на стр. 44.).

2.6. Настройка OCR-библиотек

Распознавание текста из извлеченных изображений производится с использованием одной из двух OCR-библиотек: либо Tesseract 3.0, либо ABBYY FineReader Engine 9.5.

По умолчанию при установке с помощью программы-инсталлятора (**kickstart**) на серверную часть Системы устанавливаются обе OCR-библиотеки.

Чтобы изменить используемую библиотеку ABBYY FineReader Engine 9.5 на Tesseract 3.0:

1. Удалите установленную OCR-библиотеку с помощью команды:

   `rpm -e iwtm-image2text_fre`

2. Перейдите в директорию, в которой хранятся пакеты OCR-библиотек. По умолчанию это директория `/opt/distr/infowatch/traffic-monitor/Linux.`

3. Установите требуемую OCR-библиотеку с помощью команды:

   `rpm -i iwtm-image2text_ts*.rpm`

Чтобы изменить используемую библиотеку Tesseract 3.0 на ABBYY FineReader Engine 9.5:

1. Удалите установленную OCR-библиотеку с помощью команды:

   `rpm -e iwtm-image2text_ts*.rpm`

2. Перейдите в директорию, в которой хранятся пакеты OCR-библиотек. По умолчанию это директория `/opt/distr/infowatch/traffic-monitor/Linux`

3. Установите требуемую OCR-библиотеку с помощью команды:

   `rpm -i iwtm-image2text_fre*.rpm`

2.7. 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).

2.8. 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.

2.9. Включение/отключение морфологической индексации

Пользователь Консоли имеет возможность использовать расширенный поиск по событиям с учетом морфологии слова (подробнее см. документ «*InfoWatch Traffic Monitor. Руководство пользователя*»).

Для того чтобы данная опция стала доступна в Консоли, необходимо предварительно включить морфологическое индексирование в настройках БД Oracle.

Примечание:

Подготовьте БД к внесению изменений (п. Проведение регламентных работ на сервере базы данных на стр. 80).

1. Подключитесь к БД от имени владельца схемы.
2. Выполните следующую команду:
   - для включения морфологической индексации:

```
begin
CTX_DDL.SET_ATTRIBUTE('iwtm_lexer', 'index_stems', 'russian');
execute immediate 'ALTER INDEX TIX_OBJECT_TEXT PARAMETERS (''REPLACE METADATA LEXER
IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OC_FILENAME_TEXT PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OBJ_COMMENT_NOTE PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OBJECT_TASK_QUERY PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
end;
/
```

- для выключения морфологической индексации:

```
begin
CTX_DDL.UNSET_ATTRIBUTE('iwtm_lexer', 'index_stems');
execute immediate 'ALTER INDEX TIX_OBJECT_TEXT PARAMETERS (''REPLACE METADATA LEXER
IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OC_FILENAME_TEXT PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OBJ_COMMENT_NOTE PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
execute immediate 'ALTER INDEX TIX_OBJECT_TASK_QUERY PARAMETERS (''REPLACE METADATA
LEXER IWTM_LEXER'')';
end;
/
```

Важная информация!

На данный момент морфологическая индексация не поддерживается Oracle. Работоспособность данной функции не гарантируется. При возникновении проблем рекомендуется её отключить.

ГЛАВА 3. РАБОТА В КОНСОЛИ УПРАВЛЕНИЯ

Настройка Системы выполняется администратором с помощью упрощенного управления через веб-интерфейс управления (веб-консоль), доступный 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 (п. 3.1 на стр. 50);*
- *Управление интеграцией с LDAP каталогами (п. 3.2 на стр. 50);*
- *Управление пользователями Системы и их ролями (п. 3.3 на стр. 53);*
- *Управление лицензиями (п. 3.4 на стр. 62);*
- *Состояние системы (п. 3.5 на стр. 64);*

3.1. 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**.

> **Внимание!**
>
> 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.

3.2. Управление интеграцией с LDAP каталогами

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

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

В левой части рабочей области **Управление интеграцией с LDAP каталогами** расположен список **Название сервера** и панель инструментов.

В списке **Название сервера** отображаются подключения к серверам, синхронизация с LDAP каталогами которых настроена.

Панель инструментов содержит набор инструментов для работы с подключениями.

В правой части рабочей области **Управление интеграцией с LDAP каталогами** 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*
Автоматически синхронизировать	Признак того, что синхронизация выполняется по указанному расписанию (см. *Период синхронизации*)
Период синхронизации	Тип периодичности выполнения синхронизации (см. *Параметры повторения*)
Параметры повторения	Значение периодичности выполнения синхронизации ***Например***, при заданных значениях • *Синхронизировать* – `Каждые N минут`, • *Параметры повторения* – `15 минут`, синхронизация будет выполняться каждые 15 минут.
LDAP сервер	Сетевой идентификатор сервера, с LDAP каталогами которого производится синхронизация
LDAP глобальный порт	Порт для подключения глобального LDAP каталога. **Примечание:** данная настройка доступна только для Active Directory
LDAP порт	Порт для подключения доменного каталога
Использовать глобальный каталог	Признак того, что для синхронизации используется глобальный LDAP каталог **Примечание:** данная настройка доступна только для Active Directory
Атрибуты фильтрации	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: `OU=Users,dc=company,dc=com`
Логин	Логин для доступа к серверу синхронизации
Пароль	Пароль для доступа к серверу синхронизации
Дата последней синхронизации	Дата и время завершения последней синхронизации
Статус последней синхронизации	Выполнена успешно (*success*), не выполнялась (пустое поле) или закончилась ошибкой (*error*)

Внимание!

Чтобы узнать, выполняется ли соединение с сервером по указанным в блоке **Настройки соединения** данным, необходимо нажать кнопку **Проверить соединение**.

Настройка интеграции с LDAP каталогами описана в разделах:

- Создание подключения к серверу (см. п. 3.2.1 на стр. 52);
- Редактирование подключения к серверу (см. п. 3.2.2 на стр. 52);
- Удаление подключения к серверу (см. п. 3.2.3 на стр. 52);
- Запуск синхронизации с сервером (см. п. 3.2.4 на стр. 53).

3.2.1. Создание подключения к серверу

Чтобы создать подключение к серверу:

1. Перейдите в раздел **Управление -> LDAP Синхронизация**.
2. На панели инструментов нажмите  **Добавить**.
3. Укажите параметры для нового подключения (см. п. 3.2 на стр. 50).
4. Нажмите **Проверить соединение**, чтобы выполнить контрольную проверку подключения к серверу.
5. Нажмите **Сохранить**.

3.2.2. Редактирование подключения к серверу

Чтобы отредактировать подключение к серверу:

1. Перейдите в раздел **Управление -> LDAP Синхронизация**.
2. В списке **Название сервера** щелчком левой кнопки мыши выберите требуемый сервер.
3. На панели инструментов нажмите  **Редактировать**.
4. Измените параметры подключения (см. п. 3.2 на стр. 50).
5. Нажмите **Проверить соединение**, чтобы выполнить контрольную проверку подключения к серверу.
6. Нажмите **Сохранить**.

3.2.3. Удаление подключения к серверу

Чтобы удалить существующее подключение к серверу, выполните следующие шаги:

1. Перейдите в раздел **Управление -> LDAP Синхронизация**.
2. В списке **Название сервера** 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**.

3.2.4. Запуск синхронизации с сервером вручную

Чтобы запустить синхронизацию с сервером вручную, выполните следующие шаги:

1. Перейдите в раздел **Управление -> LDAP Синхронизация**.
2. В списке **Название сервера** 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.

3.3. Управление пользователями Системы и их ролями

Для работы пользователя в Системе используются следующие сущности:

- *Пользователь* – учетная запись (см. п. 3.3.1 на стр. 53);
- *Роль* – набор прав, которые могут быть присвоены Пользователю (см. п. 3.3.1.7 на стр. 56);
- *Область видимости* – группа конкретных атрибутов объектов перехвата, к которым могут иметь доступ только указанные пользователи (см. п. 3.3.3 на стр. 59).

3.3.1. Пользователи

Настройка списка пользователей Системы выполняется в разделе **Управление -> Пользователи и роли**, 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
Полное имя	ФИО пользователя
Email	Адрес электронной почты пользователя
Роли	Список ролей пользователя
Области видимости	Список областей видимости пользователя
Описание	Примечание к учетной записи

Параметр	Описание
Статус	Признак того, является ли учетная запись пользователя активной или выключенной

Вы можете выполнять следующие действия при управлении пользователями:

- *Создание учетной записи пользователя (п. 3.3.1.1 на стр. 54);*
- *Редактирование учетной записи пользователя (п. 3.3.1.2 на стр. 55);*
- *Удаление учетной записи пользователя (п. 3.3.1.3 на стр. 55);*
- *Изменение пароля учетной записи пользователя (п. 3.3.1.4 на стр. 55);*
- *Изменение статуса учетной записи пользователя (п. 3.3.1.5 на стр. 55);*
- *Импорт учетной записи пользователя (п. 3.3.1.6 на стр. 56);*
- *Задание пользователю роли (п. 3.3.1.7 на стр.56);*
- *Задание пользователю области видимости (п. 3.3.1.8 на стр. 56).*

3.3.1.1. Создание учетной записи пользователя

Чтобы создать учетную запись:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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:** рекомендации по составлению имен и паролей пользователей приведены в разделе Приложение А на стр. 120.
Подтверждение пароля	Пароль учетной записи
Email	Адрес электронной почты пользователя
Полное имя	ФИО пользователя
Описание	Примечание к учетной записи

5. Нажмите **Сохранить**.

3.3.1.2. Редактирование учетной записи пользователя

Чтобы изменить параметры существующей учетной записи:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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. п. 3.3.1 на стр.53).
6. Нажмите **Сохранить**.

3.3.1.3. Удаление учетной записи пользователя

Чтобы удалить учетную запись:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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**.

3.3.1.4. Изменение пароля учетной записи пользователя

Чтобы изменить учетную запись:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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:**
>
> Рекомендации по составлению имен и паролей пользователей приведены в разделе Приложение А на стр. 120.

6. Нажмите **Сохранить**.

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

3.3.1.5. Изменение статуса учетной записи пользователя

Чтобы изменить статус учетной записи:

1. Перейдите в раздел **Управление -> Пользователи и роли**.

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**.

3.3.1.6. 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 -> Пользователи и роли**.
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**.

3.3.1.7. Задание пользователю роли

Чтобы задать пользователю роль:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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. п. 3.3.2 на стр.57).
6. Нажмите **Сохранить**.

3.3.1.8. Задание пользователю области видимости

Чтобы задать пользователю область видимости:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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. п. 3.3.3 на стр. 59).
6. Нажмите **Сохранить**.

3.3.2. Роли

Настройка списка ролей выполняется в разделе **Управление -> Пользователи и роли**, на вкладке **Роли**.

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

В списке ролей отображаются роли пользователей Системы.

Панель инструментов содержит набор инструментов для работы с ролями.

Раскрывающееся меню определяет количество ролей, отображаемых на странице.

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 (п. 3.3.2.1 на стр. 57);*
- *Редактирование роли (п. 3.3.2.2 на стр. 58);*
- *Удаление роли (п. 3.3.2.3 на стр. 59).*

3.3.2.1. Создание роли

Чтобы создать новую роль, выполните следующие действия:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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.

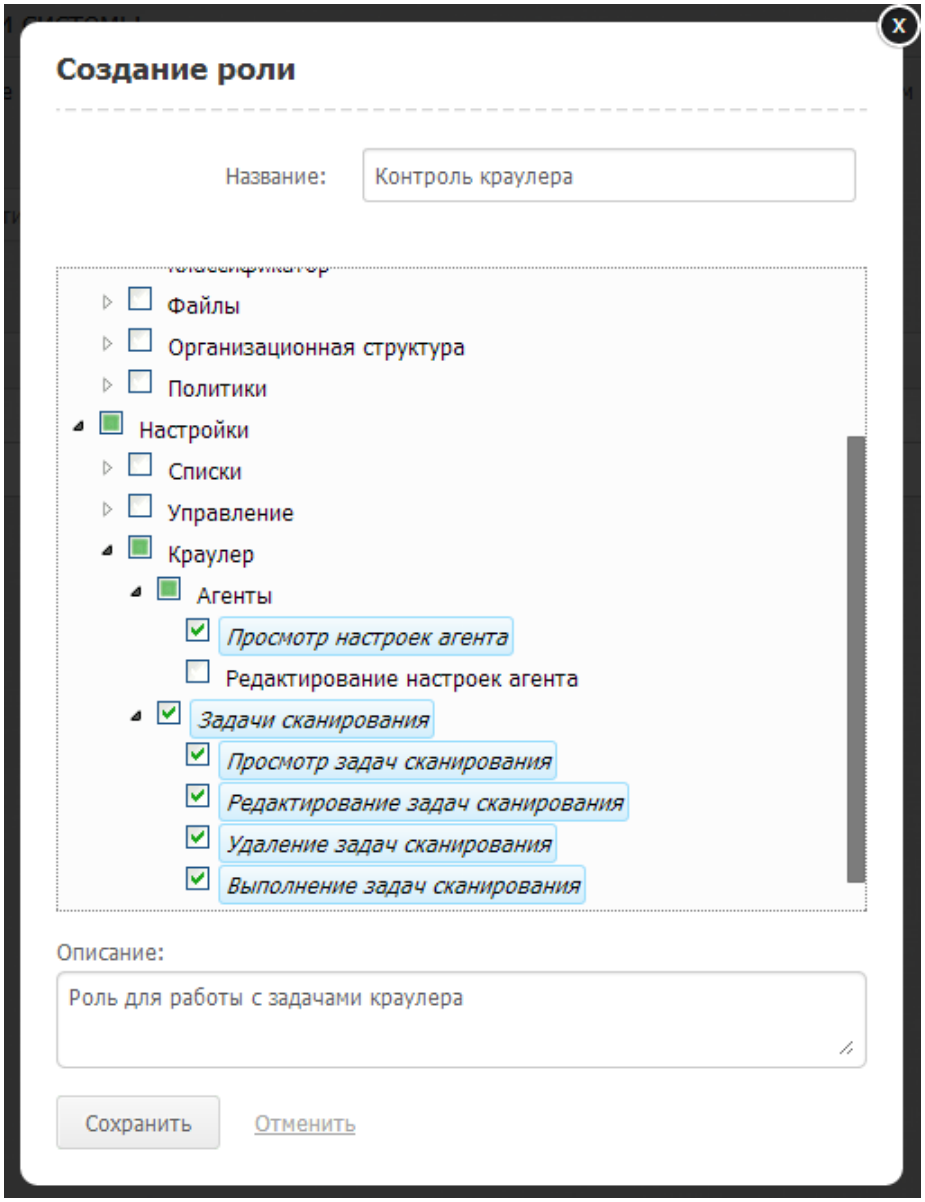


Рисунок 4. Создание роли

5. Нажмите **Сохранить**.

3.3.2.2. Редактирование роли

Чтобы изменить параметры существующей роли, выполните следующие действия:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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**.

3.3.2.3. Удаление роли

Чтобы удалить роль:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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**.

3.3.3. Области видимости

Область видимости – это набор атрибутов объектов перехвата: объекты с такими атрибутами будут доступны только определенным пользователям. Назначение областей видимости пользователям описано в п. 3.3.1.8 на стр. 56.

Настройка списка областей видимости выполняется в разделе **Управление -> Пользователи и роли** 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 (п. 3.3.3.1 на стр. 59);*
- *Редактирование области видимости (п. 3.3.3.2 на стр. 62);*
- *Удаление области видимости (п. 3.3.3.3 на стр. 62).*

3.3.3.1. Создание области видимости

Чтобы создать область видимости:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
2. Перейдите на вкладку **Области видимости**.

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

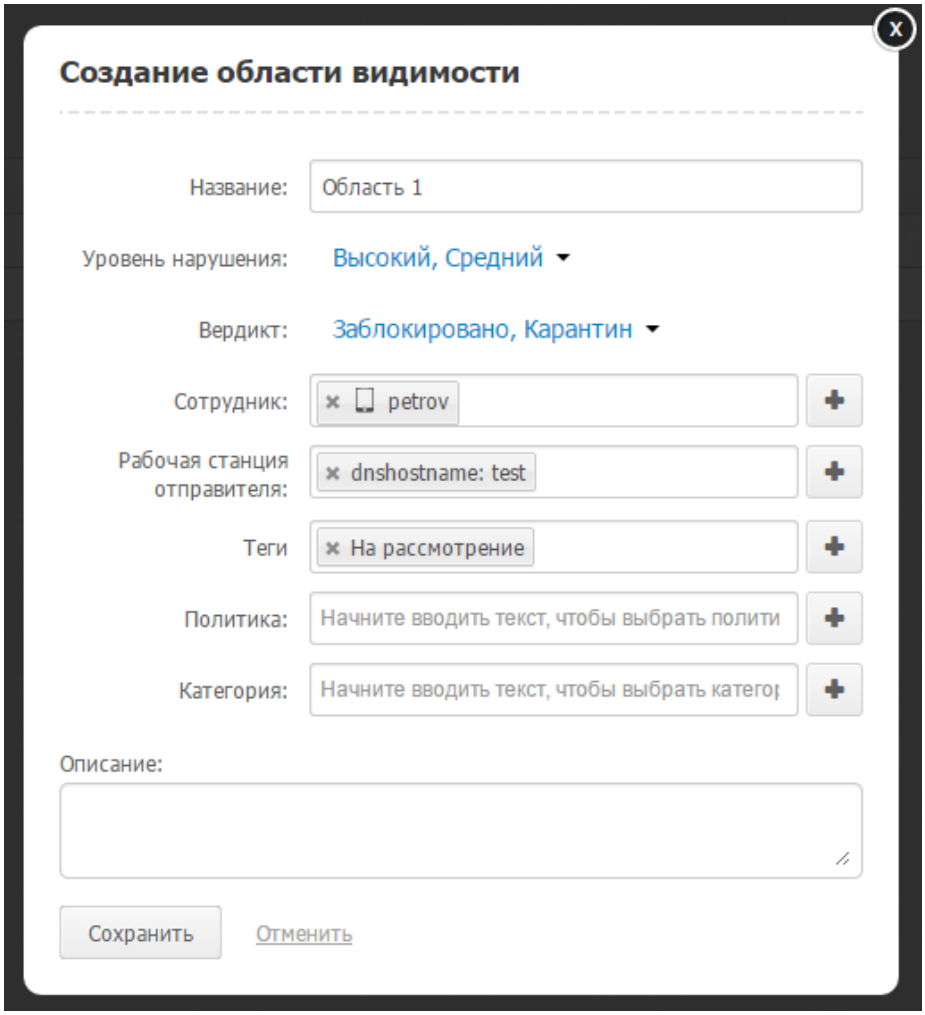


Рисунок 5. Создание области видимости

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) *Пользователь*:
      - введите первые символы наименования пользователя и выберите требуемое значение из выпадающего списка

        или

      - нажмите  **Добавить** и в появившемся окне, в списке пользователей, установите флажки требуемым пользователям.
   e) *Рабочая станция отправителя* – аналогично пункту d.
   f) *Теги* – аналогично пункту d.
   g) *Политика* – аналогично пункту d.
   h) *Категория* – аналогично пункту d.
   i) *Описание* - введите текст описания в поле.

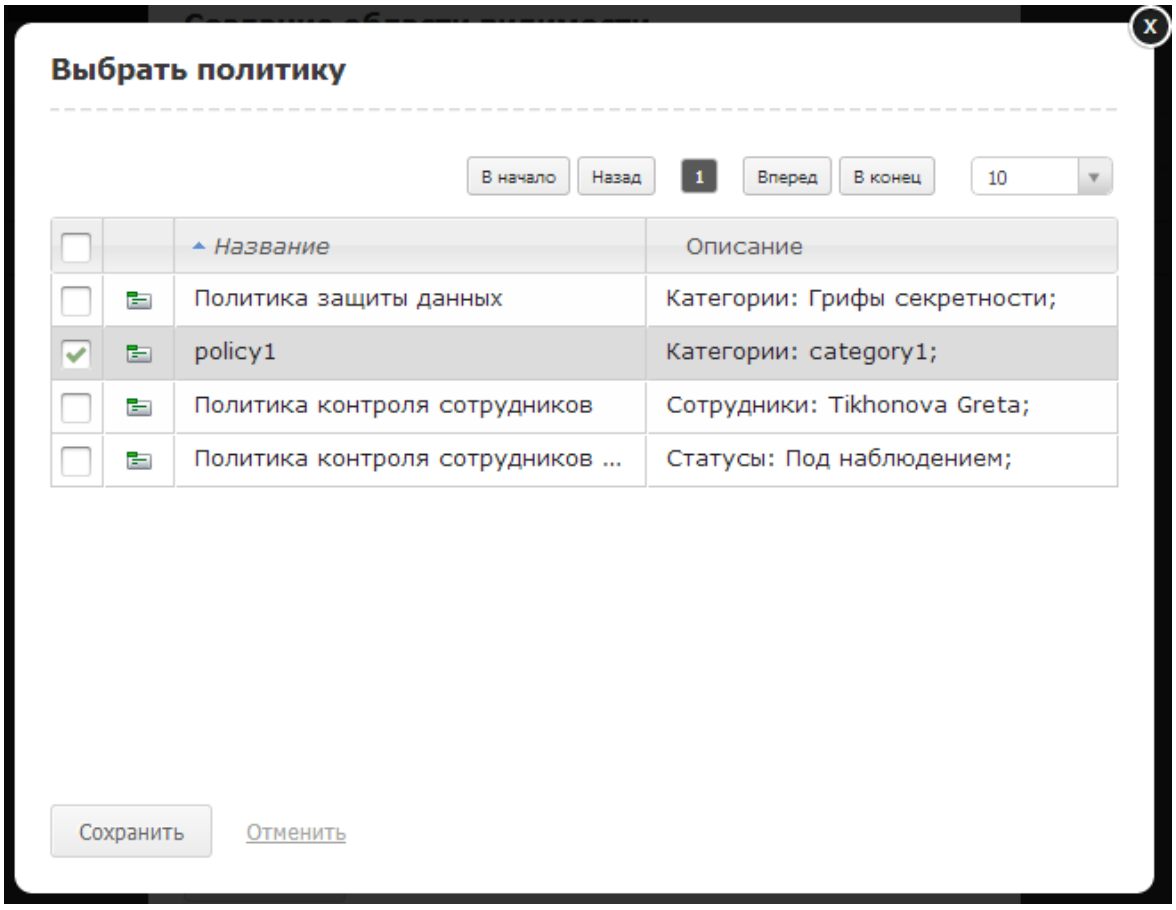


Рисунок 6. Добавление политики в область видимости

> **Примечание:**
>
> Рекомендуется обращать внимание на подсказки Например надпись: «*Начните ввод, чтобы выбрать тег*» указывает на то, что при вводе первых символов названия тега в поле **Теги** будет открыт раскрывающийся список, в котором пользователь может выбрать требуемый тег.

5. Нажмите **Сохранить**.

3.3.3.2. Редактирование области видимости

Чтобы изменить параметры области видимости:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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. п. 3.3.3.1 на стр. 59).
5. Нажмите **Сохранить**.

3.3.3.3. Удаление области видимости

Чтобы удалить область видимости:

1. Перейдите в раздел **Управление -> Пользователи и роли**.
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**.

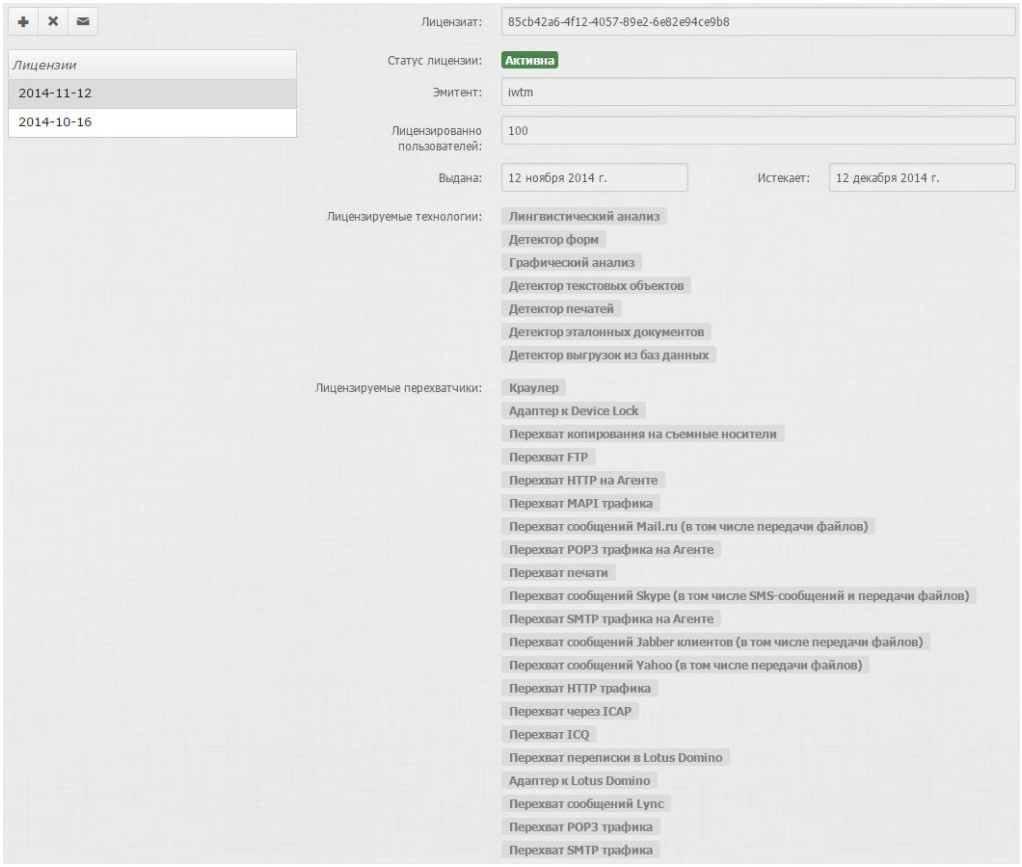
3.4. Управление лицензиями

> **Внимание!**
>
> Описание лицензирования Системы приведено в п. 1.3 на стр. 21.

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 правой 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.

3.4.1. 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`.

3.4.2. 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 лизензируемых 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.

3.4.3. 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**.

3.4.4. Запрос лицензии

Чтобы отправить запрос на получение лицензии:

1. На панели инструментов нажмите  **Запросить лицензию**.
2. Отправьте автоматически сформированное письмо, при необходимости указав дополнительную информацию в теле письма.

3.5. 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	Подробнее
⊟	Сервер IWTM	
	Общая нагрузка системы (сервера БД)	OK - load average: 0.95, 0.50, 0.60
	Общая нагрузка системы (сервера перехвата)	OK - load average: 0.01, 0.12, 0.57
	Общая нагрузка системы (серверные компоненты Системы)	OK - load average: 0.01, 0.12, 0.57
	Количество активных пользователей	USERS OK - 1 users currently logged in
	Ошибки в alert логе	OK - no errors found in log
	Размер alert лога базы данных	OK - size of DB Alert Log is 163971 bytes
	Наличие патчей базы данных Oracle	OK -- patches 17402822 applied
	Наличие ошибок в журнале базы данных	OK - no errors
	Состояние локального почтового сервера	SMTP OK - 0.154 sec. response time
	Отклонение системного времени	NTP OK: Offset -0.0003759860992 secs
	Состояние базы данных Oracle	iwtm OK - 1 PMON process(es) running
	Состояние службы доступа к базе данных	OK - reply time 0 msec from iwtm
	Доступность сервера	PING OK - Packet loss = 0%, RTA = 0.10 ms
	Свободное место в корневой партиции	DISK OK - free space: / 130518 MB (72% inode=98%):
	Состояние службы синхронизации времени	OK - ntpd (pid 1783) is running...
	Состояние сервиса syslog	OK - 'rsyslogd' is running
	Доступность сервера по SSH	SSH OK - OpenSSH_5.3 (protocol 2.0)
	Использование файла подкачки	SWAP OK - 96% free (11445 MB out of 11999 MB)
	Наличие дампов памяти	CRITICAL - There are TM coredump files. 2 item(s).
	Состояние компонентов системы	OK

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.

> **Внимание!**
>
> 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 alert логе БД/ DB Alert Log Errors
  - Доступность сервера/Server availability
  - Использование файла подкачки/ Swap usage
  - Размер alert лога БД/ DB Alert log Size
- каждые 10 минут – для параметров:
  - Доступность сервера по SSH/ SSH availability
  - Состояние базы данных Oracle/ Oracle 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**.

Настройка параметров индикаторов выполняется в конфигурационных файлах, расположенных в каталоге `/etc/nagios/iwmon/`:

- `iwmon-services-ntp.cfg` – настройка проверки синхронизации времени (индикатор **Отклонение системного времени**);
- `iwmon-services-db.cfg` – настройка индикаторов для базы данных;
- `iwmon-services-loadavg.cfg` – настройка параметров нагрузки на серверы (индикатор **Общая нагрузка системы (сервер БД/ сервер перехвата/ серверные компоненты Системы)**);
- `iwmon-services.cfg` – настройка остальных индикаторов.

Подробная информация о порядке настройки работы индикаторов содержится в документации Nagios: http://nagios.sourceforge.net/docs/nagioscore/3/en/objectdefinitions.html.

ГЛАВА 4. КОНФИГУРИРОВАНИЕ ПЕРЕХВАТЧИКА CRAWLER

Подсистема Crawler системы InfoWatch Traffic Monitor выполняют 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**.

Более подробная информация о настройке Crawler изложена в следующих разделах:

- *Настройка сетевых правил доступа (п. 4.1 на стр. 66)*
- *Конфигурационные файлы Crawler (п. 4.2 на стр. 68)*
- *Работа с журналами Crawler (п. 4.3 на стр. 70)*

4.1. Настройка сетевых правил доступа

Если сегменты сети, где развернута система InfoWatch Traffic Monitor с Crawler, разделены между собой межсетевыми экранами, для корректной работы Crawler должны быть открыты TCP порты **6556** (подключение сканера Crawler к серверу Crawler) и **1337** (подключение Веб-сервера InfoWatch Traffic Monitor к серверу Crawler).

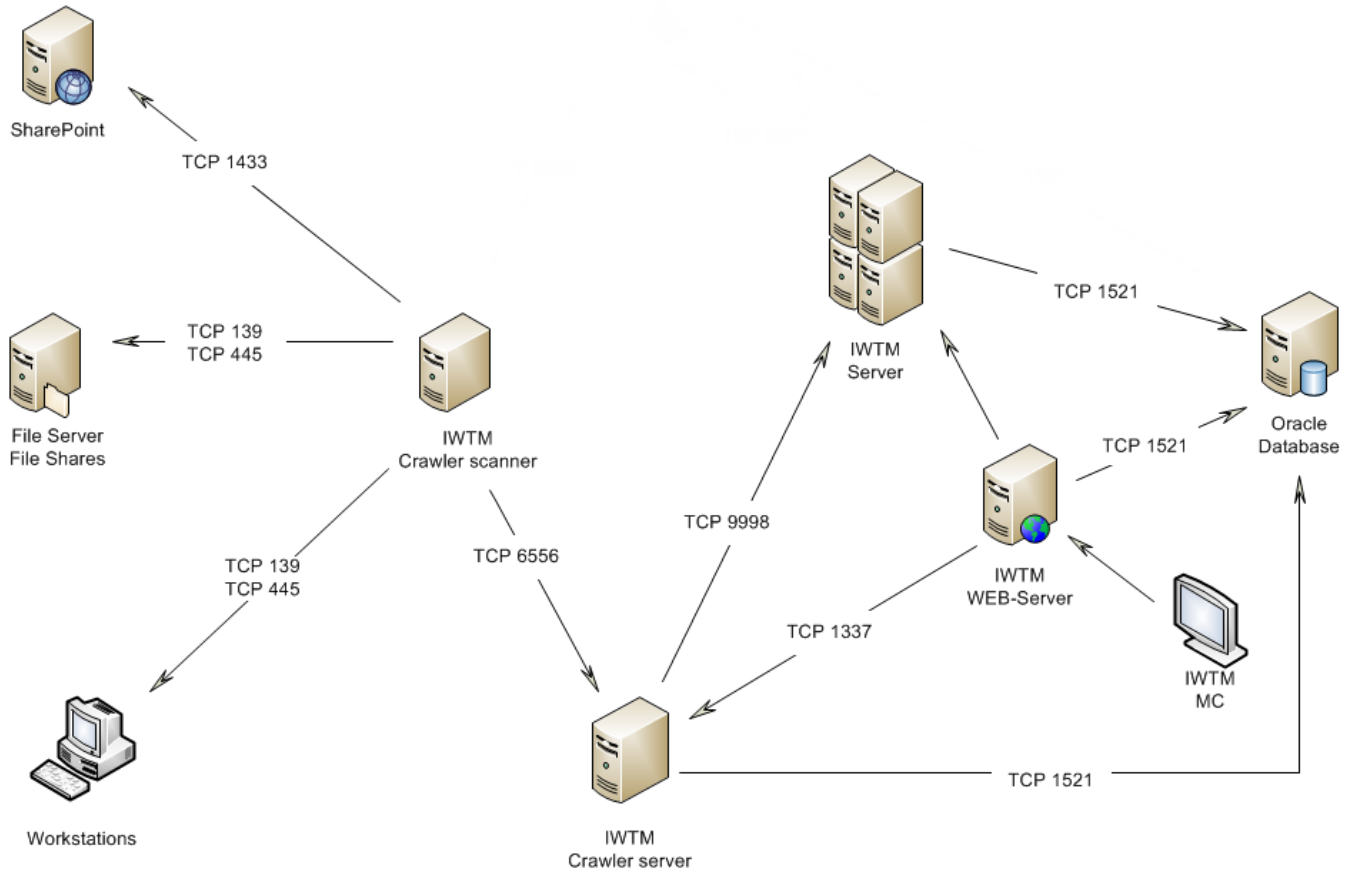
Более подробно информацию о сетевых портах, доступность которых необходима для эффективной работы системы, смотрите на следующей схеме и в таблице с пояснениями.

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.



Подключение	Порт	Комментарии
Сканер Crawler – сервер Crawler	TCP 6556	
Сервер Crawler – БД IWTM	TCP 1521	
Сервер Crawler – IWTM	TCP 9998	
Веб-сервер IWTM – сервер Crawler	TCP 1337	
Сканер Crawler – рабочие станции и файловые сервера	TCP 139 TCP 445	
Сканер Crawler – файловое хранилище SharePoint (сервер MS SQL)	TCP 1443	

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

> **Внимание!**
>
> 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**.

Примечание:

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**.

4.2. Конфигурационные файлы Crawler

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

- **Сервер Crawler** – `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. п. 4.2.1 на стр. 68.
- **Сканер Crawler** – `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. п. 4.2.2 на стр. 69.

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

4.2.1. Конфигурационный файл сервера Crawler

Администратор, обслуживающий систему, может выполнить некоторые низкоуровневые настройки сервера Crawler 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 Crawler (см. п. 4.2 на стр. 68).

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 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 Crawler. 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. 4.2.1.1 на стр. 69.

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

  `<value>номер_порта</value>`

4.2.1.1. Изменение учетной записи, от имени которой запускается служба сервера Crawler

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

1. На компьютере, где работает сервер Crawler, в списке служб Windows найдите службу `iw_crawler_server` и остановите ее.
2. В конфигурационном файле сервера `InfoWatch.Crawler.Server.exe.config` (подробнее см. п. 4.2.1 на стр. 68), 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 Crawler.
4. Запустите службу сервера.

4.2.2. Конфигурационный файл сканера Crawler

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.

Единственный параметр, который может понадобиться изменить администратору системы, **– строка соединения с сервером Crawler**. 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 Crawler Вы можете в параметре `address` вместо указанного в примере значения `localhost` указать необходимый **IP-адрес или имя сервера**.

Для разных доменов или рабочих групп можно отключить **использование шифрованного соединения**, изменив значение параметра `bindingConfiguration` с `EncryptedBinding` на `PlainBinding`.

Изменять остальные параметры настоятельно не рекомендуется.

4.3. Работа с журналами Crawler

Администратор системы может получить информацию о работе сканера и сервера Crawler из файлов журналов, расположенных в домашней директории пользователя, от имени которого запускается сервис, в поддиректории `%appdata%\InfoWatch\TM\Logs`. Так, например, если сканер Crawler установлен с параметрами по умолчанию, то он запускается от имени Local System Account и для Windows 7 журналы сканера Crawler располагаются в директории:

```
C:\Windows\System32\config\systemprofile\AppData\Roaming\InfoWatch\TM\Logs
```

Примечание:

При установке на ОС Windows 7 журналы сервера Crawler 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. п. 4.2 на стр. 68), 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 Crawler

Настройка уровня логирования выполняется в конфигурационных файлах (`InfoWatch.Crawler.Server.exe.config` и `InfoWatch.Crawler.Scanner.exe.config`: см. п. 4.2 на стр. 68).

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**.

ГЛАВА 5. КОНФИГУРИРОВАНИЕ INFOWATCH LYNC ADAPTER

InfoWatch Lync Adapter состоит из двух модулей: Infowatch Transfer Service 2.0 и IW OCS Filter.

Конфигурационный файл IW OCS Filter `InfoWatch.OcsAddon.Service.exe` по умолчанию расположен в директории `C:\Program Files\InfoWatch\InfoWatch OCS Filter`. Кроме прочих, конфигурационный файл имеет следующие параметры, которые могут быть полезны администратору:

Параметр	Описание
`MessageWindow`	Число сообщений в текстовом чате, после которого формируется событие.
`MessageIdleTime`	Таймаут (в секундах), по истечении которого генерируется событие в случае текстового чата и передачи файла.
`AvConfLimitTime`	Максимальное время (в часах), по истечение которого генерируется событие аудио/видео-конференции.

ГЛАВА 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 сервер базы данных (kickstart запускалась с опцией **IWDBX**) установлен отдельно от сервера (серверов) Traffic Monitor (kickstart с опцией **IWTMX**), то подсистема мониторинга будет работать на каждом из серверов. Для того чтобы выполнялась диагностика всех серверов, входящих в решение, администратор Системы должен выполнить ряд дополнительных настроек (см. п. 6.1 на стр. 72).

Если система InfoWatch Traffic Monitor установлена так, что все серверные компоненты (сервер базы данных, сервера TM) расположены на одном компьютере (то есть программа-инсталлятор kickstart запускалась с опцией **IWALLX**), то подсистема мониторинга будет работать на этом же компьютере.

Просмотр индикаторов мониторинга осуществляется также администратором Системы (см. п. 3.5 на стр. 64).

Подробная информация о работе с приложением Nagios, на базе которого реализована подсистема мониторинга, содержится в сопутствующей документации:
http://nagios.sourceforge.net/docs/nagioscore/3/en/toc.html.

6.1. Настройки подсистемы мониторинга

> **Внимание!**
>
> Если система InfoWatch Traffic Monitor установлена так, что все серверные компоненты (сервер базы данных, сервера TM) расположены на одном компьютере, то настройка подсистемы мониторинга выполняется при установке в автоматическом режиме, и изменять конфигурацию не требуется.

Настройка подсистемы мониторинга включает следующие задачи:

- Настройка в случае раздельной установки Traffic Monitor Enterprise и базы данных (см. п. 6.1.1 на стр. 73);
- Настройка адреса сервера синхронизации времени для подсистемы мониторинга (см. п. 6.1.2 на стр. 74);
- Настройка соединения с серверами (см. п. 6.1.3 на стр. 75);
- Настройка порогов срабатывания для индикатора нагрузки (см. п. 6.1.4 на стр. 77);
- Настройка запуска служб (см. п. 6.1.5 на стр. 77);
- Настройка механизма уведомлений (см. п. 6.1.6 на стр. 77).

6.1.1. Настройка в случае раздельной установки Traffic Monitor Enterprise и базы данных

По умолчанию при любой установке kickstart Nagios настроен на проверку состояния локальной базы данных. Однако Traffic Monitor Enterprise и база данных могут быть установлены на разные серверы.

> **Примечание.**
>
> Если подсистемы Traffic Monitor Enterprise установлены на двух и более серверах, все серверы Traffic Monitor должны быть подключены к одной базе данных.

В случае раздельной установки подсистема мониторинга будет совершать попытки подключения к базе данных, что вызовет ошибки следующиего вида:

```
IWTM;DB_ALERT_LOG_ERRORS;CRITICAL;SOFT;1;CRITICAL - Log file '/u01/app/oracle/diag/rdbms/iwtm/iwtm/trace/alert_iwtm.log' missing

IWTM;DB_ALERT_LOG_SIZE;CRITICAL;SOFT;1;CRITICAL - Missing 'DB Alert Log' file

IWTM;DB_ORACLE_PATCHES_CHECK;CRITICAL;SOFT;1;Remote command execution failed: /usr/lib64/nagios/plugins/iwmon_check_oracle_patches: line 25: /u01/app/oracle/product/db_1/OPatch/opatch: No such file or directory

IWTM;DB_SYSLOG_ERRORS;CRITICAL;SOFT;1;CRITICAL - SQLPlus returned 1

IWTM;ORACLE_DATABASE_STATUS;CRITICAL;SOFT;1;iwtm Database is DOWN
```

Следующие шаги описывают конфигурацию Nagios, при которой подключение выполняется по SSH с использованием RSA ключей (без запроса паролей):

1. В конфигурационном файле `iwmon-hosts.cfg`, расположенном в каталоге `/etc/nagios/iwmon/`, укажите IP-адреса и вхождения в группы для сервера Traffic Monitor и сервера базы данных:

   ```
   define host
   { use linux-server host_name IWTM alias "Infowatch Traffic Monitor Server"
   address  <ip(TME_1)> retry_interval 1 max_check_attempts 5 },

   define host
   { use linux-server host_name DB alias "Infowatch Traffic Monitor DB Server"
   address <ip(DB)> },

   define hostgroup
   { hostgroup_name DB-servers alias Oracle Database for IW Traffic Monitor
   Servers members DB }

   define hostgroup
   { hostgroup_name TMcap-servers alias IW Traffic Monitor Capture Stack Servers
   members IWTM }

   define hostgroup
   { hostgroup_name TMcas-servers alias IW Traffic Monitor Content Analysis
   Servers members IWTM }

   define hostgroup
   { hostgroup_name IW-Linux-servers alias All IW Servers members IWTM,DB }
   ```

   где `<ip(TME_1)>` - IP-адрес сервера Traffic Monitor;

   `<ip(DB)>` - IP-адрес сервера базы данных;

   `<IWTM>` - имя хоста сервера Traffic Monitor;

   `<DB>` - имя хоста Базы Данных

Если подсистемы Traffic Monitor Enterprise установлены более чем на один сервер, укажите IP-адреса и вхождения в группы для остальных серверов Traffic Monitor. Конфигурационный файл `iwmon-hosts.cfg` будет выглядеть следующим образом:

```
define host
{ use linux-server host_name IWTM alias "Infowatch Traffic Monitor Server"
address  <ip(TME_1)> retry_interval 1 max_check_attempts 5 },

define host
{ use linux-server host_name IWTM2 alias "Infowatch Traffic Monitor Server"
address <ip(TME_2)> retry_interval 1 max_check_attempts 5 },

define host
{ use linux-server host_name DB alias "Infowatch Traffic Monitor DB Server"
address <ip(DB)> },

define hostgroup

{ hostgroup_name TMcap-servers alias IW Traffic Monitor Capture Stack Servers
members IWTM,IWTM2 }

define hostgroup
{ hostgroup_name TMcas-servers alias IW Traffic Monitor Content Analysis
Servers members IWTM,IWTM2 }

define hostgroup
{ hostgroup_name  DB-servers
        alias     Oracle Database for IW Traffic Monitor Servers ;
        members         DB }

define hostgroup
{ hostgroup_name IW-Linux-servers alias All IW Servers members IWTM,IWTM2,DB
}
```

где `<ip(TME_1)>` - IP-адрес основного сервера Traffic Monitor;

`<ip(TME_2)>` - IP-адрес дополнительного сервера Traffic Monitor;

`<ip(DB)>` - IP-адрес сервера базы данных;

`<IWTM>` - имя хоста основного сервера Traffic Monitor;

`<IWTM2>` - имя хоста второстепенного сервера Traffic Monitor;

`<DB>` - имя хоста Базы Данных.

2. Запустите скрипт `iwmon-setup.sh`:

   ```
   /etc/nagios/iwmon-scripts/iwmon-setup.sh
   ```

3. Перезапустите Nagios, выполнив следующую команду:

   ```
   service nagios restart
   ```

6.1.2. 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).

6.1.3. Настройка соединения с серверами

В конфигурационном файле `iwmon-hosts.cfg`, расположенном в каталоге `/etc/nagios/iwmon/`, укажите все IP-адреса и вхождения серверов в группы.

> **Внимание!**
>
> Не создавайте файлов с расширением `.cfg` в каталоге /`etc/nagios/iwmon/`, так как это может приводить к ошибкам. При необходимости создать резервные копии или другие конфигурационные файлы, сохраняйте их в другой каталог.

Каждый из используемых серверов (хостов) описывается секцией `host`. Для обеспечения соединения с реальными серверами, используемыми Системой:

1. Измените перечень серверов, удаляя или добавляя секции для реально существующих серверов. Лишние секции можно закомментировать символами #. Если все компоненты системы установлены на одном сервере, то достаточно оставить только одну секцию `host`.
2. Для каждого сервера в строке `address` замените IP адрес, указанный по умолчанию (127.0.0.1), на адрес этого сервера.

> **Внимание!**
>
> Не рекомендуется изменять названия групп, названия серверов и алиасы серверов, достаточно указать нужные IP-адреса и, при необходимости, указать вхождения серверов в группы.

В секциях `hostgroup` должны присутствовать описания для следующих групп серверов:

- TMcap-servers – сервера перехвата;
- TMcas-servers – сервера с Подсистемой Анализа;
- DB-servers – сервера с БД Oracle, используемой InfoWatch Traffic Monitor;
- IW-Linux-servers – все сервера, содержащие серверные компоненты InfoWatch Traffic Monitor;

В каждой секции `hostgroup`, в строке `members` через запятую необходимо перечислить имена серверов, входящих в эту группу.

Ниже приведены примеры настройки конфигурационного файла в общем случае и для случая, когда все серверные компоненты Системы установлены на одном хосте.

Пример 1. Настройки по умолчанию.

Используются следующие сервера:

- `TMcap1` - сервер перехвата 1 и `TMcap2` - сервер перехвата 2;
- `TMcas` - сервер с Подсистемой Анализа;
- `DB` - сервер базы данных.

```
define host{
        use                     linux-server
        host_name               TMcap1
        alias                   "TM capture stack server1"
        address                 127.0.0.1
        }

define host{
        use                     linux-server
        host_name               TMcap2
        alias                   "TM capture stack server2"
```

```
        address                 127.0.0.1
        }

define host{
        use                     linux-server
        host_name               TMcas
        alias                   "TM Cas Server"
        address                 127.0.0.1
        }

define host{
        use                     linux-server
        host_name               DB
        alias                   "Oracle DB for IW TM"
        address                 127.0.0.1
        }

# Host groups
define hostgroup{
        hostgroup_name  TMcap-servers ; The name of the hostgroup
        alias           IW Traffic Monitor Capture Stack Servers ; Long name of the group
        members          TMcap1,TMcap2     ; Comma separated list of hosts that belong to
this group
        }

define hostgroup{
        hostgroup_name  TMcas-servers ; The name of the hostgroup
        alias             IW Traffic Monitor Content Analysis Servers ; Long name of the
group
        members           TMcas      ; Comma separated list of hosts that belong to this
group
        }

define hostgroup{
        hostgroup_name  DB-servers ; The name of the hostgroup
        alias           Oracle Database for IW Traffic Monitor Servers ; Long name of the
group
        members         DB     ; Comma separated list of hosts that belong to this group
        }

define hostgroup{
        hostgroup_name  IW-Linux-servers ; The name of the hostgroup
        alias           All IW Servers ; Long name of the group
        members          TMcap1,TMcap2,TMcas,DB     ; Comma separated list of hosts that
belong to this group
        }
```

Пример 2. Все серверные компоненты Системы установлены на одном хосте.

Достаточно оставить одну секцию `host`. Однако должны присутствовать все предустановленные секции `hostgroup`, где в строке `members` указано имя описанного хоста.

```
define host{
       use                     linux-server
       host_name              IWTM
       alias                    "Traffic Monitor server"
       address                127.0.0.1
       }
define hostgroup{
       hostgroup_name  TMcap-servers
       alias                    IW Traffic Monitor Capture Stack Servers
       members              IWTM
       }
define hostgroup{
       hostgroup_name  TMcas-servers
       alias                    IW Traffic Monitor Content Analysis Servers
       members              IWTM
```

```
        }
define hostgroup{
        hostgroup_name   DB-servers
        alias                   Oracle Database for IW Traffic Monitor Servers
        members             IWTM
        }
define hostgroup{
        hostgroup_name   IW-Linux-servers
        alias                   All IW Servers
        members             IWTM
        }
```

Запуск программы настройки

В каталоге /etc/nagios/iwmon-scripts выполните сценарий iwmon-setup.sh. По запросу введите пароли root для подключения к каждому из серверов.

> **Примечание:**
>
> Следует учитывать, что при задержке ввода пароля более двух минут работа сценария будет остановлена. В этом случае вам потребуется повторно запустить сценарий.

В результате на каждом сервере, указанном на шаге 2, будет создан агент nagios с требуемыми пользователями, и будут размещены ssh-ключи.

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 запуска служб

Запустите службы nagios и apache для веб-интерфейса:

```
service nagios start
service nginx start
```

Настройте автозапуск служб apache и nagios:

```
chkconfig nginx on
chkconfig nagios on
```

6.1.6. 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 (п. 6.1.6.1 на стр. 78)*
- *Настройка отправки писем-уведомлений с помощью Postfix (п. 6.1.6.2 на стр. 79)*

6.1.6.1. 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 SMPT-сервер, на котором установлена подсистема мониторинга, 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 выбрать нужный индикатор, используйте описание в 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 секции индикатора отсутствует параметр `notifications_enabled`, добавьте его вручную.

6.1.6.2. 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 и конфигурированию*», раздел «Схемы развертывания Системы»),

  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.

   > **Внимание!**
   >
   > 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
   ```

ГЛАВА 7. АДМИНИСТРИРОВАНИЕ БАЗЫ ДАННЫХ

В этой главе:

- *Проведение регламентных работ на сервере базы данных (п. 7.1 на стр. 80).*
- *Табличные пространства в базе данных InfoWatch Traffic Monitor (п. 7.2 на стр. 81).*
- *Управление ежедневными табличными пространствами (п. 7.3 на стр. 82).*
- *Резервное копирование базы данных (п. 7.4 на стр. 90).*

7.1. Проведение регламентных работ на сервере базы данных

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

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

1. Закройте все окна браузера, отображающие Консоль управления. Убедитесь, что отсутствуют соединения со схемой БД Traffic Monitor из других программ. Если такие соединения есть, отключите их.
2. На сервере Traffic Monitor остановите процессы TM:

   ```
   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
   ```

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

   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.

7.2. 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 присваивается имя *<Schema Owner>_YYYY_MM_DD.* Здесь

- *Schema Owner*– владелец схемы базы данных.
- *YYYY_MM_DD* – дата ТП (соответствует дате перехвата объектов, которые будут храниться в этом ТП).

Параметры, предназначенные для управления сегментами данных, задаются при настройке схемы базы данных, но могут быть переопределены после создания схемы (см. п. 0 на стр. 82).

При использовании типа установки **IWTMSX**, 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. Руководство пользователя*).

7.3. Управление ежедневными табличными пространствами

В этом разделе:

- *Настройка размещения файлов на файловой системе (п. 7.3.1 на стр. 82).*
- *Индексирование данных в ежедневных табличных пространствах (п. 7.3.2 на стр. 84).*
- *Архивирование ежедневных табличных пространств (п. 7.3.3 на стр. 85).*
- *Восстановление ежедневных табличных пространств (п. 7.3.4 на стр. 88).*
- *Удаление ежедневных табличных пространств (п. 7.3.5 на стр. 88).*

7.3.1. Настройка размещения файлов на файловой системе

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

При установке системы с помощью поставляемого инсталлятора (kickstart: см. документ «*InfoWatch Traffic Monitor. Руководство по установке и конфигурированию*») задается использование одного ежедневного табличного пространства, расположенного в `/u02/oradata/`.

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

Внимание!

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

Пример сценария, изменяющего пути для расположения ежедневных ТП:

```
BEGIN
   part.set_df_path('/test1/', 1);
   part.set_df_path('/test2/', 2);
   part.set_df_path('/test3/', 3);
   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.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 trunc(e.date_of_capture) d, m.code, e.object_id,
nvl(lengthb(os.source),0)+nvl(length(os.xml.getclobval()),0) binary_size,
nvl(sum(length(o.text)), 0) text_size
from envelope e
inner join monitor m on e.monitor_id = m.monitor_id
inner join object_source os on os.object_id = e.object_id
inner join object o on o.part_date = e.date_of_capture and o.root_object_id =
e.object_id
where e.date_of_capture between to_date('05.05.2014', 'dd.mm.yyyy') and
to_date('14.05.2014', 'dd.mm.yyyy')
group by trunc(e.date_of_capture), m.code, e.object_id,
nvl(lengthb(os.source),0)+nvl(length(os.xml.getclobval()),0)
) 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 SQLDeveloper.

7.3.2. 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. п. 7.1 на стр. 80).

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.

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.

Далее показано несколько примеров использования сценария.

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;
/
```

7.3.3. 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.

> **Внимание!**
>
> 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. п. 7.3.3.1 на стр. 86);
- Вручную – для архивирования выбранного ЕТП (см. п. 7.3.3.2 на стр. 86).

7.3.3.1. Автоматическое архивирование ежедневных табличных пространств

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.

7.3.3.2. Архивирование ежедневных табличных пространств вручную

Архивирование ЕТП вручную производится в порядке, представленном ниже.

Шаг 1. 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_name, t.part_date
FROM tbs_list t
WHERE t.part_date < trunc(SYSDATE) - 100 + 23 / 24 AND
      t.status IN (1, 2)
```

Внимание!

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 (1, 2)
   )
```

где `t.status IN (1, 2)` указывает на то, что для архивации выбраны табличные пространства со статусами *Чтение и запись* (код статуса `1`) и *Только чтение* (код статуса `2`).

Шаг 2. Отключение ежедневных табличных пространств от базы данных

> **Внимание!**
>
> Не отключайте ежедневные ТП во время работы заданий IWADDPARTS, IWTM_DELETE_TABLESPACES, так как это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:

   ```
   begin
     -- Call the procedure
     pkg_part.archive_tablespace(N);
   end;
   ```

   где `:N` – это значение атрибута `tbs_id` целевого ТП из таблицы `tbs_list`.

   После выполнения этого сценария статус ежедневного ТП изменится на *Отключено от базы данных*.

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

Шаг 3. 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'
```

7.3.4. Восстановление ежедневных табличных пространств

Внимание!

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.

Шаг 1. 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'
```

Внимание!

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

Шаг 2. Подключение ежедневного табличного пространства

Внимание!

Не подключайте ежедневное ТП во время работы заданий IWADDPARTS 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.

7.3.5. 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.

Внимание!

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.

Внимание!

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;
/
```

7.4. 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 (п. 7.4.1 на стр. 90);*
- *Восстановление базы данных из резервной копии (п. 7.4.2 на стр. 95).*

7.4.1. Создание резервной копии базы данных

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

- *Определение размера резервной копии (п. 7.4.1.1 на стр. 91);*
- *Проверка хранилища резервной копии (п. 7.4.1.2 на стр. 91);*
- *Создание папок для резервной копии (п. 7.4.1.3 на стр. 91);*
- *Создание вспомогательных файлов на Linux (п. 7.4.1.4 на стр. 92);*
- *Создание списка файлов, подлежащих резервному копированию (п. 7.4.1.5 на стр. 93);*

- *Остановка системы IWTM (п. 7.4.1.6 на стр. 94);*
- *Остановка БД Oracle (п. 7.4.1.7 на стр. 94);*
- *Копирование файлов БД в хранилище резервных копий (п. 7.4.1.8 на стр. 94).*

7.4.1.1. 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
   ```

   Если система была установлена с помощью программы-инсталлятора (kickstart), для удобства можете воспользоваться командой **wsqlplus**.

   Дождитесь подключения – об этом будет свидетельствовать сообщение **Connected**.
3. 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);
   ```
4. Запишите получившийся размер базы данных.
5. Выйдите из Oracle SQL*Plus:

   ```
   SQL> exit
   ```

7.4.1.2. 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.

7.4.1.3. Создание папок для резервной копии

> **Внимание!**
>
> 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
```

7.4.1.4. 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**.

   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`.

   Вам нужно скопировать самые актуальные файлы. Чтобы найти файлы с самой поздней датой и временем изменения, выполните:

   ```
   OS> ll
   ```

9. Переименуйте файл так, чтобы впоследствии его можно было легко найти, например:

   ```
   controlfilebackupMMDDYY.trc
   ```

7.4.1.5. 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/flash_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
```

7.4.1.6. 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
```

7.4.1.7. Остановка БД Oracle

> **Внимание!**
>
> 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
```

7.4.1.8. 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.

   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.

7.4.2. 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. п. 7.4.2.1 на стр. 95.
- Если старая БД не может больше использоваться, создайте новую и восстановите данные на ней: см. 7.4.2.2 на стр. 95.

7.4.2.1. 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. Установите БД Oracle согласно инструкции, приведенной в документе «*InfoWatch Traffic Monitor. Руководство по установке и конфигурированию*».
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/flash_recovery_area/iwtm/`.
   e. Проверьте права.

      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/flash_recovery_area/iwtm/ -R
```

4. Запустите базу данных.

```
OS> dbstart $ORACLE_HOME
```

7.4.2.2. 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.

ГЛАВА 8. АДМИНИСТРИРОВАНИЕ СЕРВЕРНОЙ ЧАСТИ INFOWATCH TRAFFIC MONITOR

В этой главе:

- *Модули и процессы Traffic Monitor Server (п. 8.1 на стр. 97);*
- *Настройка параметров работы Traffic Monitor Server (п. 8.2 на стр. 102);*
- *Настройка использования OCR для различных перехватчиков (п. 8.3 на стр. 112);*
- *Настройка параметров работы с HTTP-запросами, передаваемыми по протоколу ICAP (файл icap.conf) (п. 8.4 на стр. 112);*
- *Настройка параметров обработки архивов вложений (файл extractors.conf) (п. 8.5 на стр. 113);*
- *Архивирование каталога очереди сообщений (п. 8.6 на стр. 115);*
- *Протоколирование работы Системы (п. 8.7 на стр. 116);*
- *Перемещение объектов между очередями (утилита iw_qtool) (п. 8.8 на стр. 116);*
- *Загрузка очередей объектов (п. 8.9 на стр. 118);*
- *Восстановление работоспособности системы в аварийных ситуациях (п. 0 на стр. 119).*

8.1. Модули и процессы Traffic Monitor Server

В этом разделе:

- *Список модулей Traffic Monitor Server (п. 8.1.1 на стр. 97);*
- *Работа с процессами Traffic Monitor Server (п. 8.1.2 на стр. 101).*

8.1.1. Список модулей Traffic Monitor Server

Работа с процессами осуществляется посредством работы с модулями: модуль может включать процесс или группу процессов.

Имя модуля	Описание модуля и путь к конфигурационному файлу
`iw_adlibitum`	Управляет процессами получения актуальных данных с сервера Active Directory. Путь к файлу: /opt/iw/tm5/etc/adlibitum.conf
`iw_agent`	Требуется для управления конфигурацией Системы. Путь к файлу: /opt/iw/tm5/etc/agent.conf
`iw_agent_kicker`	Вспомогательный процесс для модуля `iw_agent`. Путь к файлу: /opt/iw/tm5/etc/agent_kicker.conf

Имя модуля	Описание модуля и путь к конфигурационному файлу
iw_blackboard	Осуществляет взаимодействие применяемых политик и базы данных. Путь к файлу: /opt/iw/tm5/etc/blackboard.conf
iw_blackboard_kicker	Вспомогательный процесс для iw_blackboard Путь к файлу: /opt/iw/tm5/etc/blackboard_kicker.conf
iw_bookworm	Выполняет роль справочника в Системе. Путь к файлу: /opt/iw/tm5/etc/bookworm.conf
iw_capstack	Выполняет обработку трафика, передаваемого по протоколам POP3 и IMAP. Путь к файлу: /opt/iw/tm5/etc/capstack.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. Путь к файлу: /opt/iw/tm5/etc/cas.conf
iw_config_compiler	Переводит конфигурационный файл сервера контентного анализа в бинарный вид для возможности использования конфигурации в контентном анализе. Путь к файлу: /opt/iw/tm5/etc/config_compiler.conf
iw_crawler_kicker	Вспомогательный процесс для подсистемы Crawler (сама подсистема работает на сервере, отличном от Traffic Monitor Server). Путь к файлу: /opt/iw/tm5/etc/crawler_kicker.conf
iw_deliver	Выполняет доставку писем. Отправляет SMTP-письма получателям в случае, если доставка письма разрешена из Management Console (только в нормальном и прозрачном транспортных режимах). Также этот процесс доставляет SMTP-письма, которые по той или иной причине (например, ввиду отсутствия связи с почтовым relay-сервером или почтовым клиентом) не смог доставить процесс **iw_messed**. Путь к файлу: /opt/iw/tm5/etc/deliver.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 обработаные данные направляются процессу **iw_loader** для сохранения в базу данных. Путь к файлу: /opt/iw/tm5/etc/expressd.conf
iw_icap	Обрабатывает HTTP-трафик. Принимает HTTP-запросы от ICAP-клиента. Извлекает данные из HTTP-запросов. Затем извлеченные данные добавляются в XML-контекст. Готовый XML-контекст передается подсистеме анализа и принятия решения для проверки. По окончании анализа передает ICAP-клиенту ответ с разрешением/запрещением на доставку HTTP-запроса. Также передает HTTP-запрос процессу **iw_loader** для сохранения в базу данных. Путь к файлу: /opt/iw/tm5/etc/icap.conf

Имя модуля	Описание модуля и путь к конфигурационному файлу
iw_licensed	Подсистема лицензирования. Производит мониторинг и обработку установленных в Системе лицензий. Путь к файлу: /opt/iw/tm5/etc/licensed.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. Путь к файлу: /opt/iw/tm5/etc/loader.conf
iw_luaengined	Процесс, обеспечивающий выполнение LUA-скрипта согласно действующей политике Путь к файлу: /opt/iw/tm5/etc/luaengined.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. Путь к файлу: /opt/iw/tm5/etc/messed.conf
iw_notifier_kicker	Вспомогательный процесс для отправки уведомлений из Системы. Путь к файлу: /opt/iw/tm5/etc/notifier_kicker.conf
iw_proxy	Принимает копию трафика и передает ее модулю iw_messed, разбив на http-, icq- и smtp-трафик. Включает следующие процессы: • iw_proxy_http - процесс, принимающий копию HTTP-трафика. Принимает HTTP-запрос, формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа и принятия решения. 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. Путь к файлу: /opt/iw/tm5/etc/proxy.conf
iw_qmover_client	Работает на Traffic Monitor Server, установленном в филиале. Отправляет перехваченные объекты в базу данных центрального офиса. Путь к файлу: /opt/iw/tm5/etc/qmover_client.conf

Имя модуля	Описание модуля и путь к конфигурационному файлу
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. Путь к файлу: /opt/iw/tm5/etc/qmover_server.conf
iw_report_kicker	Вспомогательный процесс для создания отчетов. Путь к файлу: /opt/iw/tm5/etc/report_kicker.conf
iw_sample_compiler	Процесс, создающий цифровые отпечатки из загруженных эталонных файлов Путь к файлу: /opt/iw/tm5/etc/sample_compiler.conf
iw_selection_kicker	Вспомогательный процесс для работы с фильтрами (запросами). Путь к файлу: /opt/iw/tm5/etc/selection_kicker.conf
iw_serman	Регистрирует и хранит регистрационную информацию сервисов, взаимодействующих с интерфейсом пользователя. Путь к файлу: /opt/iw/tm5/etc/serman.conf
iw_smtpd	Процесс, принимающий SMTP-письма. В случае интеграции с почтовым сервером Postfix принимает входящие сообщения от Postfix. Если интеграция с Postfix отсутствует, сообщения принимаются то 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**. Путь к файлу: /opt/iw/tm5/etc/smtpd.conf
iw_sniffer	Процесс, перехватывающий трафик, который передается по протоколам SMTP, HTTP, ICQ, POP3 и IMAP. Путь к файлу: /opt/iw/tm5/etc/sniffer.conf
iw_system_check	Процесс, занимающийся сбором данных от службы Nagios и предоставляющий полученные данные для выведения в Консоли управления. Путь к файлу: /opt/iw/tm5/etc/selection_kicker.conf
iw_updater	Процесс, загружающий конфигурацию из базы данных на Traffic Monitor Server. Путь к файлу: /opt/iw/tm5/etc/updater.conf
iw_warpd	Управляет процессами извлечения данных из контейнеров, вложенных в перехваченные объекты. Путь к файлу: /opt/iw/tm5/etc/warpd.conf
iw_whiteboard	Позволяет серверным процессам публиковать сообщения в интерфейсе пользователя. Путь к файлу: /opt/iw/tm5/etc/whiteboard.conf

Имя модуля	Описание модуля и путь к конфигурационному файлу
iw_xml2liro	Процесс, преобразовывающий xml-контекст, полученный из трафика, в бинарный формат liro. Путь к файлу: /opt/iw/tm5/etc/xml2liro.conf

8.1.2. Работа с процессами Traffic Monitor Server

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

> **Примечание:**
>
> Имя владельца задается при установке Traffic Monitor Server и прописывается в конфигурационных файлах процессов, в секции Permissions, в параметре user. Для стабильной работы Системы рекомендуется оставить значение этого параметра без изменений.

Во время работы состояние процессов Traffic Monitor Server проверяется сценарием pguard, который 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 pguadr 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.

> **Примечания:**
>
> 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

Внимание!

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

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 параметров работы Traffic Monitor Server

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.

Названия конфигурационных файлов соответствуют названиям тех компонентов, для настройки которых они используются. Например, для конфигурирования компонента `iw_loader` используется конфигурационный файл **loader.conf**.

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

Различают общие настраиваемые параметры (см. п. 8.2.1 на стр. 102) и параметры, специфичные для каждого из конфигурационных файлов (см. п. 8.2.2 на стр. 104).

8.2.1. Общие настраиваемые параметры конфигурационных файлов

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

Внимание!

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

К общим настраиваемым параметрам конфигурационных файлов относятся:

- Секция Logging (см. п. 8.2.1.1 на стр. 103);
- Секция Startup (см. п. 8.2.1.2 на стр. 103);
- Секция Nookdir (см. п. 8.2.1.3 на стр. 103);
- Секция Serman (см. п. 8.2.1.4 на стр. 104).

8.2.1.1. Секция Logging

Имя процесса	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.

> **Внимание!**
>
> 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.

8.2.1.4. Секция Serman

> **Примечание:**
>
> Секция `Serman` присутствует в следующих конфигурационных файлах:
>
> adlibitum, agent, blackboard, bookworm, licensed, sample_compiler, system_check, whiteboard.

Имя процесса	Описание процесса и путь к файлу
`Host`	IP-адрес сервера, на котором работает служба `iw_serman`
`Password`	Пароль пользователя. Используется для подключения к Serman
`Port`	Порт для подключения к Serman
`ServiceHost`	IP-адрес сервера где установлен компонент. Используется для регистрации в Serman. **Примечание:** если все компоненты Системы установлены на одном компьютере, возможно указать значение 127.0.0.1.
`ServiceName`	Имя сервиса при регистрации в службе serman
`ServicePort`	Порт для подключения к сервису
`Username`	Имя пользователя. Используется для подключения к Serman

8.2.2. Специфичные настраиваемые параметры конфигурационных файлов

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.

Имя процесса	Описание процесса и путь к файлу
`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

8.2.2.3.1. Секция Icq

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

Параметр	Описание
`MessageWindow`	Количество сообщений диалога, по достижении которого ICQ-диалог сохраняется в файловую очередь. Значение по умолчанию `10`.
`DialogTimeout`	Интервал времени (в минутах), по истечению которого с момента перехвата последнего ICQ-сообщения необходимо сохранить диалог в файловую очередь. Значение по умолчанию `5`.
`DialogBytesCount`	Размер диалога (в байтах), по достижении которого ICQ-диалог сохраняется в файловую очередь. Значение по умолчанию `500`.
`FakeFileTransferPort`	Порт, с помощью перенаправления на который блокируются попытки передачи файлов. Значение по умолчанию `62225`.

8.2.2.3.2. 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
`MinHeader`	Минимальный объем текста (в байтах) для одного блока переменной в кодировке URL, который будет передан на сервер контентного анализа. Значение по умолчанию `10`.
`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.

Параметр	Описание
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.
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.
LogBlock	Запись в системный журнал сообщений о блокировке перехваченных HTTP-запросов. Запись ведется, если установлено значение true. По умолчанию запись отключена – значение false.
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.
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.
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.
SkipStat4XX	Отключает сохранение в очередь HTTP-запросов с ответом прокси-сервера вида "*4XX*", где *XX* – любые цифры. Значение по умолчанию false.
IcqFilter	Возможность перехвата ICQ-сообщений (если установлено значение true), передаваемых через прокси-сервер (поверх HTTP). По умолчанию возможность включена.
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".
MessageWindow	Количество сообщений диалога, по достижении которого ICQ-диалог (при перехвате ICQ поверх HTTP) сохраняется в файловую очередь. Значение по умолчанию 10.
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.

Параметр	Описание
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.
DialogBytesCount	Размер диалога (в байтах), по достижении которого ICQ-диалог (при перехвате ICQ поверх HTTP) сохраняется в файловую очередь. Значение по умолчанию 500.
FakeFileTransferPort	Порт, с помощью перенаправления на который блокируются попытки передачи файлов. Значение по умолчанию 62225.
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.
DataPoolSize	Максимальный объем выделенной памяти для обработки соединений, в Мб. Значение по умолчанию 1024.

8.2.2.3.3. Секция Smtp

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

Параметр	Описание
MaxMsgSize	Размер SMTP-сообщения (в байтах), при превышении которого сообщение не обрабатывается Системой. Значение по умолчанию – 52428800.

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

8.2.2.5.1. Секция Analysis

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

Параметр	Описание
Classifier	Контентный анализ
CreditCardDetector	Детектор кредитных карт
FormAnalysis	Детектор форм
Researcher	Детектор текстовых объектов
RfPassportDetector	Детектор паспортов граждан РФ
StampDetector	Детектор печатей и штампов
Stamper	Детектор эталонных документов
TableAnalysis	Детектор выгрузок из БД

8.2.2.5.2. Секция Classifier

Параметр	Описание
`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.

8.2.2.5.3. Секция Tableanalysis

Параметр	Описание
`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. **Например:** `WinWords = 10.` Будет работать – пустая таблица с 11 столбцами, в названии которых есть хотя бы одно слово; не будет работать – таблица, в которой 2 столбца с названиями из 2 слов для каждого и 1 строка, в каждой из ячеек которой по 1 слову. Значение по умолчанию – `10.`

8.2.2.5.4. Секция Thrift

Параметр	Описание
ServerPort	Порт, на котором сервер контентного анализа принимает входящие соединения. Значение по умолчанию – 9992.

8.2.2.6. Конфигурационный файл expressd.conf

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. п. 8.2.2.6.2Секция Expressd, параметр Http на стр. 110)
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 писем. Когда нагрузка на систему будет снижена, прием писем возобновляется. Значение по умолчанию 10.
OCR	Настройка использования технологии OCR (см. п. 8.2.2.6.3 на стр. 110).
TempDir	Директория для хранения временных файлов. Значение по умолчанию – /tmp.

Параметр	Описание
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 систем InfoWatch Device Monitor и DeviceLock, укажите то же число обрабатывающих потоков, которое задано на сервере InfoWatch Device Monitor (или в настройках DeviceLock Adapter). За настройку числа обрабатывающих потоков InfoWatch Device Monitor и DeviceLock Adapter отвечает параметр `NumberOfConnections` в конфигурационном файле `InfoWatch.DeviceMonitor.Server.exe.config` и `InfoWatch.DeviceLockAdapter.exe.config` соответственно (подробнее см. «*InfoWatch Device Monitor. Руководство по установке и конфигурированию*» и «*InfoWatch DeviceLock Adapter. Руководство администратора*»).

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 Crawler
DLA	Использование OCR для файлов, полученных от DeviceLock Adapter
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
MMP	Использование OCR для файлов, полученных от MMP Monitor
NRPC	Использование OCR для файлов, полученных от Lotus Adapter
Print	Использование OCR для файлов, полученных от Print Monitor
SMTP	Использование OCR для файлов, полученных от SMTP Monitor
Skype	Использование OCR для файлов, полученных от Skype Monitor
XMPP	Использование OCR для файлов, полученных от XMPP Monitor
Yahoo	Использование OCR для файлов, полученных от Yahoo 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
`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**.

Параметр	Описание
ListenAddr	Адрес сетевого интерфейса сервера, на котором запущен процесс прослушивания. Задается при установке.
ListenPort	Порт сервера, на котором запущен процесс прослушивания. Задается при установке.

8.3. Настройка использования OCR для различных перехватчиков

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. п. Секция Expressd, параметр Ocr на стр. 110);
- **messed.conf** – требуется указать значение *true* параметру OCR, если нужно включить использование OCR для писем, проходящих через почтовый relay-сервер (см. п. Конфигурационный файл messed.conf на стр.111).
- **warpd.conf** (расположен в директории `/opt/iw/tm5/etc/`) **–** в секции `Warp` требуется указать параметру `EnableOCR` значение *true*.

8.4. 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
ResourceLimits	Ограничение размера ресурсов. В подразделе Limits указываются секции: • `Core` – размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение `-1` (отсутствие ограничений на размер дампа памяти). Значение `0` указывают, если запись не ведется. Значение по умолчанию `-1;` • `Nofile` – максимальное число открытых файлов. Рекомендуется указывать значение `-1 (отсутствие ограничений на число открытых файлов)` для повышения производительности при большом объеме трафика. Для нагруженных систем рекомендуемое значение – не менее `8000`.
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`.
PathTemporary	Путь к хранилищу временных файлов ICAP-сервера (по умолчанию `/opt/iw/tm5/tmp/icap`).

Параметр	Описание и примеры настройки
error_html	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).
min_text_length	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.
min_data_length	Минимальный объем (в байтах) URL-переменной, который будет включен в текстовый блок для передачи на контентный анализ. Значение по умолчанию 10 байт.
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.
disable_ipv6	Отключение (disable_ipv6 = *true*) и включение (disable_ipv6 = *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 disable_ipv6 = *true*.

8.5. Настройка параметров обработки архивов вложений (файл extractors.conf)

В файле /opt/iw/tm5/etc/extractors.conf хранится база данных сигнатур, с помощью которых определяется тип файлов при распаковке архивов и вложений.

Сведения об общих параметрах приведены в таблице:

Параметр	Описание и примеры настройки
AllowCoreDump	Если время работы процесса экстрактора превышает значение, указанное для TimeoutInSec, процесс завершается принудительно (значение *true*) или продолжается (значение *false*).
DefaultTextCharset	Если кодировка содержимого 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 подходящую. Значение по умолчанию "UTF-8".
Dreamcatcher	Директория, в которой хранятся файлы, которые не удалось распаковать.
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 – cp1251,cp866.

Параметр	Описание и примеры настройки
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.
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.

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.

В остальных секциях указываются сигнатуры, при помощи которых детектируются типы файлов, находящиеся во вложениях и архивах. Каждая секция содержит одинаковый набор параметров:

Параметр	Описание и примеры настройки
Extension	Расширение файла архива. Необязательный параметр, необходим для корректной работы некоторых архиваторов, которые требуют наличия правильного расширения входных файлов. **Пример** `Ext = arj`

Name	Имя формата. Используется для точного определения имени формата при распаковке файла.
	Для определения/уточнения формата может включать также список имен:
	`"defaultname, name1(code1), name2(code2)"`
	В этом случае формат определяется на основании кода (*codeN*), присвоенного файлу при распаковке. Например, если распаковка завершается с кодом *code1*, то считается, что файл имеет формат *name1*. Список имен может также включать имя по умолчанию (*defaultname*), которое будет присваиваться в случаях, когда код не присвоен:
	Пример 1 (одно имя формата)
	`text/xml`
	Пример 2 (список имен формата)
	`"application/arj, UNKNOWN(9), text/encrypted(4)"`
	По умолчанию формат файла определяется как application/arj. Если формат архива не удается определить, ему присваивается имя UNKNOWN. Для зашифрованного архива используется имя формата text/encrypted.

Параметр	Описание и примеры настройки

Signature	Сигнатура формата, которая представляет собой «образцовую» последовательность значений (байтов) с начальным смещением и масками. Эта последовательность необходима для однозначного определения формата файлов по их содержимому
	Сигнатура может включать до 16 триад вида:
	`[OFFSET]:BYTE_VALUE/[MASK]`
	Допускается также и строковая сигнатура, например, `"BZh"` для BZIP2. Эта сигнатура означает указанную последовательность байтов от смещения `0`. Поиск строковых сигнатур выполняется без учета регистра символов.
	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	Признак того, что при обработке файла не будет учитываться регистр символов. Значение по умолчанию – `false`.
CreateTags	Признак того, что при обработке с помощью экстракторов Traffic Monitor происходит извлечение метаинформации из файла.

8.6. 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`.

8.7. Протоколирование 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

> **Внимание!**
>
> 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.

8.8. Перемещение объектов между очередями (утилита iw_qtool)

Необходимость перемещения объектов из одной очереди в другую может возникнуть, когда объекты не загружаются в базу данных.

Для перемещения объектов из одной очереди в другую используется утилита **iw_qtool**. Порядок перемещения следующий. Наиболее старые объекты из очереди-источника перемещаются в начало очереди-приемника, таким образом, новые объекты будут перемещены в конец очереди-приемника. По окончании операции выводится количество перемещенных объектов.

> **Примечание:**
>
> Утилиту iw_qtool нужно запускать от имени владельца InfoWatch Traffic Monitor. Для этого смените пользователя при помощи команды su - iwtm или выполните команду от имени пользователя напрямую при помощи команды sudo -u iwtm <команда>.

Команды для работы с утилитой iw_qtool:

Название команды	Описание, синтаксис, примеры

`stat`	Показывает количество объектов в очереди.
	Синтаксис:
	`iw_qtool stat имя_очереди`
	Пример (просмотр статистики по очереди объектов, загружаемых в базу данных):
	`/opt/iw/tm5/bin/iw_qtool stat /opt/iw/tm5/queue/db`

`move`	Перемещает объекты из одной очереди в другую.
	Внимание! В процессе перемещения объектов утилита создает временные файлы в текущем каталоге. Поэтому в данном случае рекомендуется запускать утилиту iw_qtool из каталога `/opt/iw/tm5`.
	Синтаксис:
	`iw_qtool move очередь_источник очередь_приемник [количество_объектов]`
	Параметры:
	• `очередь_источник` – полное имя очереди, из которой нужно переместить объекты. Если указанной очереди не существует, то работа утилиты завершится ошибкой;
	• `очередь_приемник` – полное имя очереди, в которую нужно переместить объекты. Если указанная очередь не существует, то она будет создана в процессе работы утилиты.
	• `количество_объектов` – ограничение на количество перемещаемых объектов (необязательный параметр). Если этот параметр не задан, то будут перемещены все объекты, находящиеся в очереди-источнике.
	Пример (перенос объектов из очереди errors в очередь db):
	`iw_qtool move opt/iw/tm5/queue/errors opt/iw/tm5/queue/db`

`put`	Помещает одиночный объект в очередь.
	Внимание! Для выполнения команды необходимо иметь права на запись в текущий каталог.
	Синтаксис:
	`iw_qtool put очередь_получатель xml_файл_объекта файл_объекта`
	Параметры:
	• `очередь_получатель` – полное имя очереди, в которую нужно поместить объект. Если указанной очереди не существует, то работа утилиты завершится ошибкой;
	• `xml_файл_объекта` – полное имя XML файла объекта. Если указанного файла не существует, то работа утилиты завершится ошибкой.
	• `файл_объекта` – полное имя файла с данными объекта. Если указанного файла не существует, то работа утилиты завершится ошибкой.
	Пример (помещение объекта в очередь db):
	`iw_qtool put opt/iw/tm5/queue/db /home/iwtm/000000000.dat.xml /home/iwtm/000000000.dat`

8.9. Загрузка очередей объектов

Чтобы обеспечить загрузку имеющихся очередей объектов:

1. Остановите процессы Traffic Monitor:

   ```
   OS:root> service iwtm stop
   ```

2. Отключите автозапуск процессов **iw_proxy**, **iw_smtpd**, **iw_expressd** и **iw_icap** в конфигурационном файле каждого процесса:

   ```
   "Startup" : {"Enabled" : false}
   ```

3. Запустите процессы Traffic Monitor

   ```
   service iwtm start
   ```

4. Дождитесь, пока будут обработаны все объекты в файловой очереди.

> **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/blackboard	.dat
queue/blackboard_errors	.dat
queue/xml2liro_loader	.dat
queue/whiteboard	.dat
queue/errors	.xml & .dat
queue/xml2liro-errors	.xml & .dat
queue/rails_connector_errors	.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.
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/smtp	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/xml2liro_loader	xml2liro	loader
queue/blackboard	luaengined	blackboard
queue/blackboard_errors	ошибка при обработке blackboard	нет
queue/whiteboard	luaengined	whiteboard
queue/rails_connector_errors	ошибки на вставке данных loader	нет
queue/xml2liro-errors	ошибки обработки xml2liro	нет

8.10. Восстановление работоспособности системы в аварийных ситуациях

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

1. Остановите процессы Traffic Monitor Server, выполнив команду:

   ```
   service iwtm stop
   ```

2. Переместите объекты из ошибочных очередей в обычные. Процедура выполняется при помощи утилиты `iw_qtool` (см. п. 8.8 на стр. 116).

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.

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	

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/System load	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 минуту – хотя бы одна цифра превышает соответствующее значение 10.0,8.0,6.0 за 15, 5, 1 минуту – ни одна цифра не превышает соответствующее значение 10.0,8.0,6.0 за 15, 5, 1 минуту	30 мин.
Количество активных пользователей /Current users	Количество пользователей, зарегистрированных на хосте	– >50 пользователей – от 20 до 50 – < 20 пользователей	30 мин.
Ошибки в alert логе БД/DB Alert Log Errors	Наличие ошибок в Alert Log	– есть ошибки – нет ошибок	5 мин.
Доступность сервера/Server availability	Доступность Linux серверов	– > 500 мл с – от 100 до 500 мл с – < 100 мл с	5 мин.
Доступность сервера postfix / Postfix server availability	Доступность Postfix сервера	– не доступен – доступен	30 мин.
Доступность сервера по SSH/ SSH availability	Проверяет наличие ssh сервиса на заданной группе серверов	– >= 10 секунд – < 10 секунд	10 мин.
Доступность сервера Device Monitor	Проверяет доступность DM сервера **Важно!** Настройте индикатор следующим образом:	– нет соединения – есть соединение	30 мин.

	1. Раскомментируйте секцию DM в конфигурационном файле `/etc/nagios/iwmon/iwmon-hosts.cfg`, укажите IP. 2. Раскомментируйте секцию DM в конфигурационном файле `/etc/nagios/iwmon/iwmon-commands.cfg` 3. Раскомментируйте строки в конфигурационном файле `/etc/nagios/iwmon/iwmon-services-dm.cfg` 4. Убедитесь, что в конфигурационных файлах нет ошибок: `nagios -v /etc/nagios/nagios.cfg` 5. Перезапустите сервис nagios: `service nagios restart`		
Использование файла подкачки/Swap usage	Наличие свободного места в swap (виртуальная память)	– свободно < 10% – свободно от 10 % до 20% – свободно > 20%	5 мин.
Свободное место в корневой партиции/Root Partition free space	Наличие свободного места в корневой файловой системе	– < 10 000 Mb – от 10 000 Mb до 20 000 Mb – > 20 000 Mb	30 мин.
Свободное место в партиции /var/Var Partition free space	Наличие свободного места в файловой системе `/var`	– < 10 000 Mb – от 10 000 Mb до 20 000 Mb – > 20 000 Mb	30 мин.
Состояние службы синхронизации времени/NTP status	Характеризует доступность службы синхронизации времени	– NTP сервер доступен – NTP сервер не доступен	30 мин.
Отклонение системного времени/NTP time deviation	Характеризует лаг времени на серверах Системы и сервере NTP	– > 40 секунд – от 20 до 40 секунд – < 20 секунд can't create socket connection **Примечание:** Данная ошибка возникает, если Системе не удалось установить соединение с NTP-серверами или в конфигурации Системы не указано ни одного NTP-сервера. Убедитесь, что в конфигурационных файлах ntp.conf и iwmon-services-ntp.cfg указан один и тот же корректный NTP-сервер.	360 мин.

Наличие дампов памяти/Core dump	Проверяет работоспособность сервисов отсутствием падений	– нет дампов – есть дамп	30 мин.
Состояние базы данных Oracle/Oracle Database Status	Проверяет состояние базы данных для указанного SID. Используется стандартный плагин Nagios.	– ok – <ok>	10 мин.
Статус службы доступа к базе данных/Oracle TNS Status	Статус сервиса ntpd	– TNS listener не запущен – TNS listener запущен	10 мин.
Свободное место в основном каталоге БД/Main partition DB free space	Свободное место на партиции хранения основной информации	– < 10 000 Mb – от 10000Mb до 20 000Mb – > 20 000Mb	30 мин.
Свободное место в каталоге событий БД/ Data partition free space	Проверяет количество свободного места в партициях хранения событий.	– < 7% – от 7 до 15% – > 15%	30 мин.
Наличие патчей БД Oracle/Oracle patch status	Проверяет наличие установленных патчей Oracle (17402822, 12919564), необходимых для корректной работы Системы	– не установлен – установлен	30 мин.
Размер alert лога БД/DB Alert log Size	Размер файла Alert Log.	– > 100Mb – от 50 до 100 – < 50Mb	5 мин.
Наличие ошибок в журнале базы данных/DB sys log errors	Проверяет syslog базы данных на наличие ошибок для схемы iwtm	– нет ошибок – есть ошибки	30 мин.
Количество запущенных процессов/Total Processes	Проверяет количество запущенных процессов	– > 600 процессов – от 450 до 600 – < 450 процессов	30 мин.
Состояние сервиса syslog/Service syslog state	Проверяет, запущена ли служба `syslog`	– не запущен – запущен	30 мин.
Состояние компонентов Системы/Services state	Проверяет статусы сервисов системы	– хотя бы один сервис не запущен – все сервисы запущены	30 мин.
Очередь обработки почтового трафика/SMTP queue	Характеризует скорость обработки службой `IW_MESSED` объектов, которые помещают в очередь службы `IW_SMTPD` и `IW_PROXY` (smtp). Количество объектов в очереди.	– > 10000 объектов – от 1000 до 10000 – < 1000 объектов	30 мин.
Очередь загрузки в хранилище/ DB queue	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 – < 1000 объектов	30 мин.
Очередь ошибок обработки	Количество объектов, обработанных с ошибкой службами	– > 1000 объектов – от 200 до 1000	30 мин.

собы- тий/Processing errors queue	IW_EXPRESSD, IW_MESSED, IW_PROXY (http, icq), IW_ICAP. Количество объектов в очереди ошибок.	■ – < 200 объектов	

ГЛОССАРИЙ

Active Directory

LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows

BCC

Blind Carbon Copy. Технология, позволяющая отправить копию письма другому получателю (в дополнение к основному адресату) без указания в оригинальном письме того, что копия была послана кому-то еще

Crawler

Также: Краулер. Подсистема Crawler системы InfoWatch Traffic Monitor позволяет выполнять проверку файлов, находящихся в корпоративной сети, на предмет нарушения корпоративных политик безопасности. Таким образом, InfoWatch Crawler позволяет контролировать файловые ресурсы компании для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных

DeviceLock

Программный комплекс, разработанный ЗАО «Смарт Лайн Инк», контролирующий доступ пользователей к периферийным устройствам и локальным портам компьютеров

DeviceLock Adapter

Модуль подсистемы перехвата трафика. Перехватчик, передающий из системы DeviceLock (Смарт Лайн Инк.) в Traffic Monitor теневые копии файлов, переносимых на съемные носители и отправляемых на печать. См. также: Device Monitor, Теневая копия, Перехватчик, DeviceLock

Device Monitor

Модуль подсистемы перехвата трафика. ПО, предназначенное для контроля доступа пользователей к периферийным устройствам и мониторинга операций по копированию данных на съемные носители и отправкой данных на печать. Передает в TM копии HTTPS, MAPI и FTP трафика, а также копии сообщений из мессенджеров Skype, Yahoo, GTalk и Mail.Ru Agent.

ICAP

Internet Content Adaptation Protocol – протокол, позволяющий контролировать входящий/исходящий HTTP-трафик. Предоставляет возможность модификации содержимого HTTP-запросов (в рамках InfoWatch Traffic Monitor контролируется только исходящий трафик). См. также: Клиент ICAP, Сервер ICAP

InfoWatch Traffic Monitor

Программный комплекс InfoWatch Traffic Monitor (IW TM). Предназначен для осуществления контроля различных информационных каналов передачи данных (SMTP, HTTP, ICQ. В редакции Traffic Monitor Enterprise – также данные, копируемые на съемные носители и отправляемые на печать). Также см.: Traffic Monitor Enterprise, Traffic Monitor Standard

kickstart

Метод быстрой установки, основанный на Red Hat Linux.

LDAP

Lightweight Directory Access Protocol – сетевой протокол для доступа к службе каталогов X.500, использующий TCP/IP

LUN

Logical Unit Number – логический диск, представленный в операционной системе в качестве "физического" диска

Lync Adapter

Модуль, который состоит из IW OCS Filter и InfoWatch Transfer Service.

OCR

Optical Character Recognition – процесс перевода изображений, содержащих печатный или рукописный текст, в электронный текст, пригодный для работы в текстовом редакторе. Предоставляет возможность анализировать извлеченные текстовые данные.

OSCAR

Открытый, но не свободный сетевой протокол, обеспечивающий обмен мгновенными и оффлайновыми текстовыми сообщениями, используется службами обмена мгновенными сообщениями ICQ и AIM

Postfix

Почтовый агент (MTA), интеграция с которым является одним из способов перехвата и доставки SMTP-трафика в Системе. См. также: Почтовый агент

Relay-сервер

Ретранслирующий сервер. С почтового relay-сервера Система может получать SMTP-трафик

Sniffer

Также: Сниффер, Анализатор сетевого трафика. Перехватчик, компонент InfoWatch Traffic Monitor, получающий данные (SMTP, HTTP, ICQ трафик) копии трафика, проходящего через SPAN-порт коммутатора и передающий их в подсистему обработки. См. также: Канал передачи данных, Перехватчик

SPAN

Switched Port Analyzer – технология зеркального копирования трафика с одного порта на другой

SPAN-копия

Реализация режима перехвата копии трафика с коммутатора CISCO. Обеспечивает работу транспортного режима «Копия». См. также: Режим перехвата, SPAN, Режим копии

Traffic Monitor Enterprise

Редакция InfoWatch Traffic Monitor, предоставляющая полный набор возможных функций Системы.

Traffic Monitor Standard

Редакция InfoWatch Traffic Monitor, предоставляющая ограниченный набор функций Системы. В частности, обеспечивает перехват данных только в режиме копии. См. также: Режим копии

Web-Console

См. Веб-консоль управления

Администратор

Предустановленная роль и учетная запись консоли управления, имеющая права на управление другими учетными записями и их правами. Также: Пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. также: Офицер безопасности

БД

База данных.

Веб-консоль управления

Графический интерфейс пользователя. Предназначен для управления системой InfoWatch Traffic Monitor (администрирование Системы, настройка конфигурации, анализ объектов и т. п.)

Ежедневное табличное пространство

Один из типов табличного пространства в базе данных InfoWatch Traffic Monitor. Используется для хранения данных, перехваченных в течение одних суток (перехваченные объекты, информация о результатах анализа и обработки объекта). Ежедневные ТП создаются каждые сутки с таким расчетом, чтобы в базе данных всегда были ТП для работы в ближайшие шесть суток, не включая текущие

Задание на печать

Информация об отправке данных на печать вместе с печатаемым документом

Интеграция с Postfix

Настройка использования почтового сервера Postfix в качестве relay-сервера в схеме перехвата копии SMTP-трафика. См. также: Postfix

Канал передачи данных

Среда, состоящая из технических средств передачи данных, средств программного обеспечения и протоколов передачи данных. Traffic Monitor поддерживает перехват данных в следующих каналах передачи данных: электронная почта (SMTP), веб (HTTP), сервисы мгновенных сообщений (ICQ), теневые копии файлов и события подключения/отключения рабочих станций, задания на печать

Кластер

Группа компьютеров с одинаковым набором установленных компонентов, которая организуется и используется как единый ресурс. См. также: Компонент

Клиент ICAP

Компонент, устанавливаемый на прокси-сервере, поддерживающем функции ICAP. Передает HTTP-запрос или ответ, инкапсулированный в ICAP-сообщение на сервер ICAP. Принимает отклик от сервера ICAP (пропустить/блокировать HTTP-запрос). См. также: ICAP

Компонент

Программная единица Системы, которая может быть установлена независимо от остальных частей Системы

Механизм авторизации

Способ передачи и состав информации о пользователе, которую передает HTTP-клиент для прокси-сервера

Нормальный транспортный режим

Значение атрибута «Транспортный режим». Режим, в котором через Систему проходит реальный трафик и возможна блокировка запрещенных Системой объектов. См. также: Транспортный режим, Режим перехвата

Обработка объекта

Процедура разбора перехваченного объекта, в результате которой объект преобразуется в контекст и ему присваиваются некоторые атрибуты

Объект

Данные, полученные Системой из перехваченного трафика (SMTP-письма, HTTP-запросы, ICQ-сообщения) или от сторонних систем (теневые копии файлов и задания на печать) и преобразованные подсистемой обработки во внутреннее представление

Офицер безопасности

Предустановленная роль и учетная запись консоли управления, имеющая все привилегии, кроме управления пользователями и ролями. См. также: Администратор

Перехват данных

Процесс получения, разбора, рубрикации и преобразования данных (или их копии) в контекст. Осуществляется перехват данных, передаваемых по протоколам SMTP, HTTP, ICQ/OSCAR, IXP. См. также: Перехватчик, Канал передачи данных

Перехватчик

ПО, получающее данные от внешних клиентов, подготавливающее эти данные к дальнейшему анализу и передающее их в подсистему обработки. См. также: Канал передачи данных

Почтовый агент

Также MTA – Mail Transfer Agent. Агент пересылки сообщений, почтовый сервер – программа, передающая почтовые сообщения от одного компьютера к другому

Прокси-сервер

Служба передачи данных между компьютерами-клиентами и сетевыми серверами. Используется Системой при перехвате HTTP-трафика

Режим копии

Значение атрибута «Транспортный режим». Режим, в котором через Систему проходит не сам трафик, а его копия; следовательно, блокировка трафика средствами Системы невозможна. См. также: Транспортный режим, Режим перехвата

Режим перехвата

Способ работы Traffic Monitor с трафиком: обработка реального трафика либо работа с копией. В первом случае в Traffic Monitor направляется реальный трафик, и на дальнейшую отправку перехваченные объекты отправляются только после их обработки и принятия по ним решения. Во втором – в Traffic Monitor направляется копия трафика, и Traffic Monitor никак не влияет на отправку перехваченных объектов. См. также: Трафик, Объект, Канал передачи данных

Сервер ICAP

Серверная компонента, принимающая HTTP-запросы, инкапсулированные в ICAP-сообщение. Извлекает HTTP-запросы из ICAP-сообщения и выполняет их предварительную обработку. Передает отклик с результатами обработки клиенту ICAP. См. также: ICAP

Сервер Traffic Monitor

Компьютер или совокупность компьютеров, на которых расположены компоненты InfoWatch Traffic Monitor, за исключением консоли управления и базы данных.

Система

См. InfoWatch Traffic Monitor

СУБД

Система управления базами данных

Теневая копия

Копия файла, создаваемого на съемном устройстве. Создается только при успешном завершении операции сохранения файла на съемный носитель

ТП

Табличное пространство. Логическая единица структуры хранения данных в БД Oracle, состоящая из одного или нескольких файлов данных

Транспортный режим

Атрибут объекта, задаваемый в сценарии. Должен учитывать реализованный режим перехвата, определяет способ дальнейшей доставки объекта. См. также: Режим перехвата, Режим копии, Нормальный транспортный режим

Трафик

Поток информации в коммуникационной системе. В рамках InfoWatch Traffic Monitor контролируется только исходящий трафик, передаваемый по протоколам SMTP, HTTP и ICQ