INFOWATCH

InfoWatch Traffic Monitor 4.1

Руководство по установке и конфигурированию

INFOWATCH TRAFFIC MONITOR 4.1

Руководство по установке и конфигурированию

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

СОДЕРЖАНИЕ

ВВЕДЕНИЕ ... 5
Аудитория ... 5
Структура руководства ... 5
Дополнительная документация ... 5
Условные обозначения ... 6
Техническая поддержка пользователей ... 6

ГЛАВА 1. ОБЗОР INFOWATCH TRAFFIC MONITOR ... 7
1.1. Функции InfoWatch Traffic Monitor ... 7
1.2. InfoWatch Traffic Monitor Standard и InfoWatch Traffic Monitor Enterprise ... 8
1.3. Состав InfoWatch Traffic Monitor ... 8

ГЛАВА 2. ПОДГОТОВКА К УСТАНОВКЕ ... 10
2.1. Схемы развертывания Системы ... 10
2.1.1. Прием копии SMTP-трафика с почтового сервера ... 10
2.1.2. Перехват SMTP-трафика ... 12
2.1.3. Прием копии трафика при помощи Sniffer ... 13
2.1.4. Прием HTTP-трафика, передаваемого по протоколу ICAP ... 17
2.1.5. Прием объектов, перехваченных InfoWatch Device Monitor ... 19
2.1.6. Прием объектов от DeviceLock ... 21
2.1.7. Проверка файлов, находящихся в корпоративной сети ... 22
2.2. Аппаратные и программные требования ... 24
2.2.1. Sniffer ... 25
2.2.2. Модуль IW ICAP ... 25
2.2.3. Crawler ... 26
2.2.4. Консоль управления ... 27

ГЛАВА 3. УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ ... 28
3.1. Установка серверных компонентов ... 28
3.2. Настройка сервера Traffic Monitor ... 37
3.2.1. Проверка автозапуска процессов ... 37
3.2.2. Кластер Traffic Monitor с одной Подсистемой Анализа ... 38
3.2.3. Настройка сервера через Traffic Monitor веб-интерфейс для установки «все-в-одном» ... 39
3.2.3.1. Настройка NTP-сервера ... 39
3.2.3.2. Настройка отправки уведомлений о превышении порога для индикаторов ... 40
3.2.3.3. Установка лицензии на перехватчики ... 40
3.2.4. Настройки сервера Traffic Monitor для распределенной архитектуры ... 41
3.2.4.1. Настройка синхронизации времени ... 41
3.2.4.2. Настройка соединения с сервером СУБД Oracle ... 42
3.2.4.3. Установка лицензии на перехватчики ... 42
3.2.5. Установка и настройка модуля взаимодействия с удаленной базой данных ... 44
3.2.5.1. Установка клиентской части модуля взаимодействия с удаленной БД (филиал) ... 44
3.2.5.2. Установка серверной части модуля взаимодействия с удаленной БД (центральный офис) ... 45
3.3. Настройки перехватчиков ... 47
3.3.1. Настройка пересылки скрытых копий ... 48
3.3.2. Интеграция Postfix и сервера Traffic Monitor ... 49
3.3.3. Настройка Sniffer ... 51

3.3.3.1. Настройка работы сервера Traffic Monitor в качестве Sniffer ... 51
3.3.3.2. Настройка сервера Traffic Monitor на прием копии трафика от Sniffer ... 52
3.3.3.3. Создание кластера Traffic Monitor ... 52
3.3.4. Настройка ICAP ... 53
3.3.4.1. Рекомендации по настройке ICAP для Blue Coat SG Series ... 54
3.3.4.2. Рекомендации по настройке SQUID ... 54
3.3.5. Установка и настройка Crawler ... 55
3.3.5.1. Установка сервера и сканера Crawler ... 55
3.3.5.2. Настройка сетевых правил доступа ... 58
3.4. Настройка подсистемы мониторинга для распределенной архитектуры ... 60
3.4.1. Настройка адреса сервера синхронизации времени для подсистемы мониторинга ... 60
3.4.2. Настройка соединения с серверами ... 60
3.4.3. Настройка порогов срабатывания для индикатора нагрузки ... 63
3.4.4. Настройка запуска служб ... 63
3.4.5. Настройка механизма уведомлений ... 63
3.4.5.1. Настройка отправки уведомлений о превышении порога для индикаторов ... 63
3.4.5.2. Настройка отправки писем-уведомлений с помощью Postfix ... 64
3.5. Установка Консоли управления ... 64
3.6. Настройка параметров анализа объектов ... 66

ГЛАВА 4. ОБНОВЛЕНИЕ СИСТЕМЫ ... 67
4.1. Порядок обновления Системы ... 67
4.2. Создание резервной копии базы данных ... 69
4.2.1. Определение размера резервной копии ... 69
4.2.2. Проверка хранилища резервной копии ... 69
4.2.3. Создание папок для резервной копии ... 70
4.2.4. Создание вспомогательных файлов на Linux ... 70
4.2.5. Создание списка файлов, подлежащих резервному копированию ... 71
4.2.6. Остановка системы IWTM ... 72
4.2.7. Остановка БД Oracle ... 72
4.2.8. Копирование файлов БД в хранилище резервных копий ... 73
4.3. Восстановление базы данных из резервной копии ... 73
4.4. Обновление схемы базы данных ... 74
4.5. Внесение изменений в файлы новой версии ... 75
4.5.1. Изменение сценария обработки объектов ... 75
4.5.2. Изменение конфигурационного файла tm.conf ... 76

ГЛАВА 5. УДАЛЕНИЕ СИСТЕМЫ ... 77
5.1. Схема базы данных ... 77
5.2. Модуль взаимодействия с удаленной базой данных ... 77
5.3. Модуль IW ICAP ... 78
5.4. Сервер Traffic Monitor ... 78
5.5. Sniffer ... 79
5.6. Консоль управления ... 79

ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ИМЕН И ПАРОЛЕЙ ... 80

ПРИЛОЖЕНИЕ В. РАЗРЕШЕНИЕ ПРОБЛЕМ ... 82

ПРИЛОЖЕНИЕ С. ЛИЦЕНЗИИ ТРЕТЬИХ СТОРОН ... 83

ГЛОССАРИЙ ... 84

УКАЗАТЕЛЬ ... 89

ВВЕДЕНИЕ

В настоящем руководстве вы можете найти сведения по установке, настройке, обновлению, а также удалению системы InfoWatch Traffic Monitor.

Аудитория

Руководство рассчитано на пользователей, обладающих следующими навыками:

- администрирование СУБД Oracle;
- установка и 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. 7).*

  Содержит общие сведения о Системе.

- *Глава 2. Подготовка к установке (стр. 10).*

  Описывает требования к аппаратному и программному обеспечению, необходимому для работы Системы; порядок установки компонентов Системы.

- *Глава 3. Установка и настройка Системы(стр. 28).*

  Содержит рекомендации по установке компонентов Системы и пошаговое описание установки.

- *Глава 4. Обновление системы (стр. 67).*

  В разделе содержится информация по обновлению компонентов Системы.

- *Глава 5. Удаление системы (стр. 77).*

  Приводятся сведения по удалению компонентов Системы.

- *Приложение А. Рекомендации по составлению имен и паролей (стр. 80).*

  Приводится набор правил для составления имен и паролей пользователей, даются рекомендации по составлению надежных паролей.

- *Приложение В. Разрешение проблем (стр. 82).*

  В приложении описываются проблемы, которые могут возникнуть в процессе установки и настройки Системы, а также способы их разрешения.

- *Приложение С. Лицензии третьих сторон (стр. 83).*

  Содержит информацию о лицензиях на стороннее программные компоненты, использованные в продукте.

Дополнительная документация

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

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

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

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

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

- *«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.)	Нажмите кнопку **Старт**
Курсив	При описании таблиц, в примерах, описаниях – названия и значения атрибутов объектов	После выполнения запроса *Запрещено*

`Шрифт Courier New`	Имена файлов, примеры текста программ; значения параметров конфигурационных файлов, примеры настройки	Проверка запуска Traffic Monitor осуществляется командами:
		`service iw-trafmon status`
		`service iw-caserv 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 `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[AUTO_RESTART]`

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

  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.

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

Перед обращением в службе технической поддержки мы рекомендуем вам посетить раздел База знаний на нашем сайте: http://cp.infowatch.com/kb/. Возможно там уже содержится ответ, на интересующий вас вопрос или описано решение возникшей у вас проблемы.

ГЛАВА 1. ОБЗОР INFOWATCH TRAFFIC MONITOR

В этой главе:

- *Функции InfoWatch Traffic Monitor (п. 1.1 на стр. 7)*
- *InfoWatch Traffic Monitor Standard и InfoWatch Traffic Monitor Enterprise (п. 1.2 на стр. 8)*
- *Состав InfoWatch Traffic Monitor (п. 1.3 на стр. 8).*

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 SMTP-трафика. Возможен перехват трафика (или копии трафика), передаваемого через почтовый relay-сервер; перехват копии трафика, проходящего через оборудование с поддержкой технологии CISCO SPAN.
- Перехват HTTP-трафика. Возможен перехват трафика, передаваемого через прокси-сервер, поддерживающий ICAP-протокол, перехват копии трафика, проходящего через оборудование с поддержкой технологии CISCO SPAN.

  > **Примечание:**
  >
  > При интеграции с прокси-сервером Blue Coat возможен перехват HTTPS-трафика, если прокси-сервер обрабатывает HTTPS-трафик как HTTP-трафик.

- Перехват копии ICQ-трафика (протокол OSCAR), проходящего через оборудование с поддержкой технологии CISCO SPAN. При подключении ICQ через HTTP Система перехватывает ICQ-трафик аналогично HTTP-трафику.

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

- Проверка файлов, находящихся в корпоративной сети (открытых сетевых папок, локальных дисков рабочих станций и файлового хранилища SharePoint 2007), с помощью подсистемы Crawler.
- 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) Перехват перечисленных данных осуществляется системой InfoWatch Device Monitor.
- Анализ теневых копий файлов, перехваченных системой DeviceLock ЗАО «Смарт Лайн Инк» (версии 6.3 и выше).
- Анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности.
- Фильтрация перехваченного трафика путем выдачи разрешения/запрещения на доставку определенных данных.

  > **Примечание:**
  >
  > Функция недоступна при работе с копией трафика.

1.2. InfoWatch Traffic Monitor Standard и InfoWatch Traffic Monitor Enterprise

Начиная с версии InfoWatch Traffic Monitor 3.5, предусмотрено две редакции Системы: Traffic Monitor Standard и Traffic Monitor Enterprise.

InfoWatch Traffic Monitor Standard имеет более низкие, чем Traffic Monitor Enterprise, аппаратно-программные требования (подробнее см. п. 2.2 на стр. 24).

Также Traffic Monitor Standard имеет ряд ограничений по функциям, а именно:

- Обеспечивается перехват объектов только в режиме копии;
- Выполняется периодическое удаление объектов при превышении определенного объема, занимаемого хранящимися в базе данных объектами. Существует возможность установки защиты от этого удаления на отдельные объекты.

Подробное описание этих функций см. в документе «*InfoWatch Traffic Monitor. Руководство пользователя*».

InfoWatch Traffic Monitor Enterprise обеспечивает полный набор предоставляемых Системой функций.

1.3. Состав InfoWatch Traffic Monitor

Подсистема InfoWatch Traffic Monitor	Назначение подсистемы
Подсистема обработки	Извлечение из перехваченных объектов значимой информации и вложений, определение форматов вложений и передача извлеченных текстов в подсистему анализа.
Подсистема анализа	Анализ текстовых данных, извлеченных из перехваченных объектов (тексты писем, сообщений, запросов, а также тексты, извлеченные из вложений). Состоит из следующих модулей: Модуль детектирования текстовых объектов, Модуль лингвистического анализа, Модуль детектирования цифровых отпечатков
Подсистема перехвата трафика	Перехват и передача на обработку трафика: объектов или их копий. Состоит из следующих модулей: Модуль Sniffer, Модуль Device Monitor, Модуль DeviceLock Adapter
Подсистема применения политик	На основе результатов работы подсистемы анализа и подсистемы обработки выполняет вынесение вердикта 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, Модуль принятия решений
Подсистема хранения	Хранение информации о перехваченных объектах, результатах их анализа и применения политик, а также предоставление возможности для просмотра хранящейся информации посредством запросов из консоли управления. Представляет собой базу данных. Состоит из следующих модулей: Модуль взаимодействия с удаленной БД, Модуль загрузки объектов в БД, Модуль хранения настроек системы, Модуль хранения объектов

Подсистема InfoWatch Traffic Monitor	**Назначение подсистемы**
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 отчетности, Модуль управления конфигурацией, Модуль управления правами пользователей, Консоль управления

ГЛАВА 2. ПОДГОТОВКА К УСТАНОВКЕ

В этой главе:

- *Схемы развертывания Системы (п. 2.1 на стр. 10).*
- *Аппаратные и программные требования (п. 2.2 на стр. 24).*

2.1. Схемы развертывания Системы

В этом разделе описаны наиболее общие схемы развертывания Системы:

- *Прием копии SMTP-трафика с почтового сервера (п. 2.1.1 на стр. 10)*
- *Перехват SMTP-трафика (п. 2.1.2 на стр. 12)*
- *Прием копии трафика при помощи Sniffer (п. 2.1.3 на стр. 13)*
- *Прием HTTP-трафика, передаваемого по протоколу ICAP (п. 2.1.4 на стр. 17)*
- *Прием объектов, перехваченных InfoWatch Device Monitor (п. 2.1.5 на стр. 19)*
- *Прием объектов от DeviceLock (п. 2.1.6 на стр. 21)*
- *Проверка файлов, находящихся в корпоративной сети (п. 2.1.7 на стр. 22)*

Для каждой схемы приведен порядок развертывания.

2.1.1. Прием копии SMTP-трафика с почтового сервера

Наиболее простая в применении схема. Обеспечивает контроль информации, исходящей из корпоративной системы доставки почты. На Traffic Monitor отправляются скрытые копии писем (BCC).

Вариант 1. Система устанавливается в одном офисе, филиалов нет (см. рис. 1).

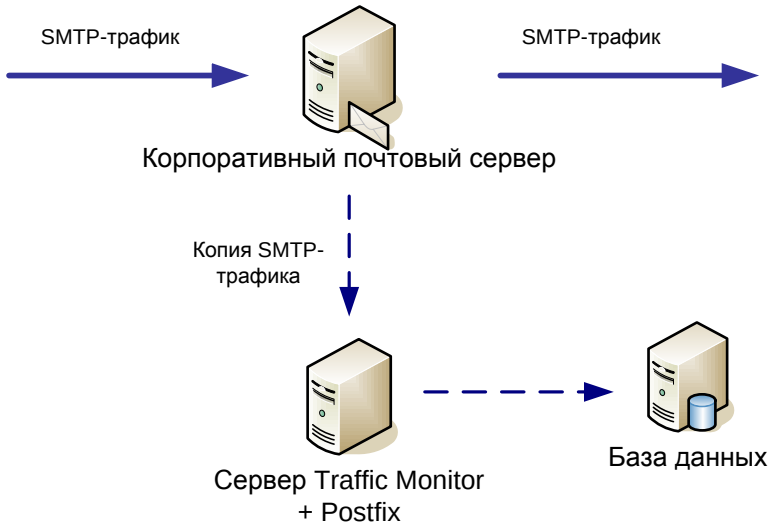


Рисунок 1. Перехват копии SMTP-трафика

Вариант 2. SMTP-трафик, перехваченный в филиалах, передается в центральный офис по медленному каналу связи (см. рис. 2). В центральном офисе SMTP-трафик загружается в базу данных.

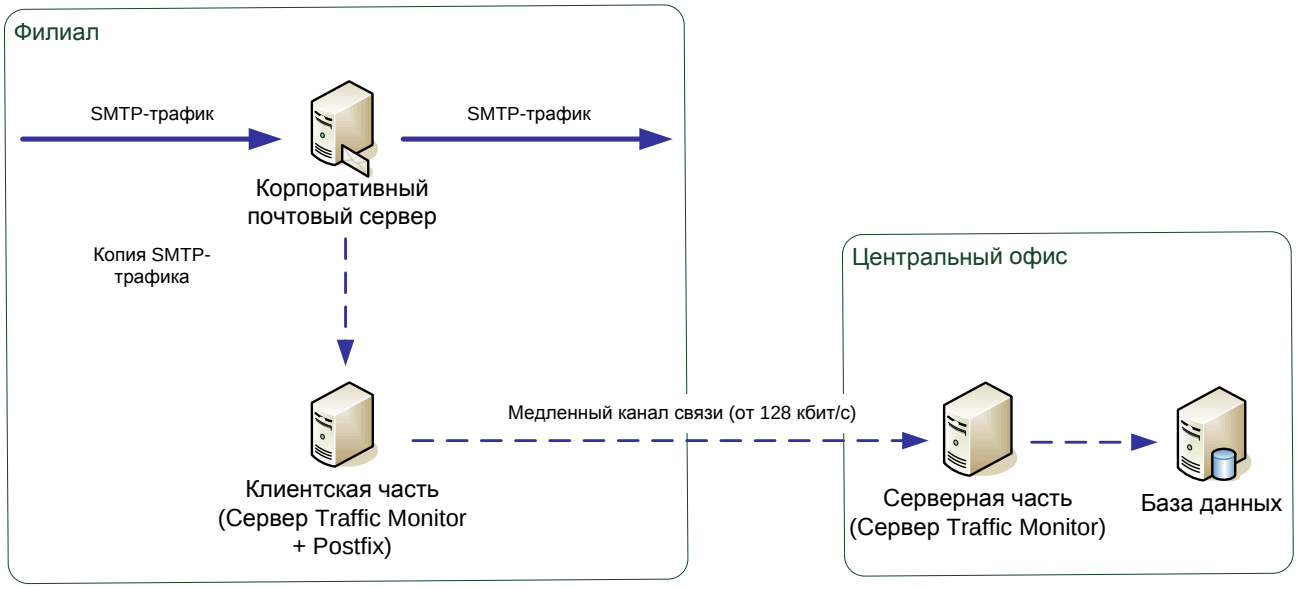


Рисунок 2. Передача копии SMTP-трафика из филиала в центральный офис

Далее приводится общий порядок развертывания для обоих вариантов. Различия имеются только при установке сервера Traffic Monitor.

Шаг 1. Проверка аппаратных и программных требований к Системе

Убедитесь, что среда, в которой будет развернута Система, удовлетворяет аппаратным и программным требованиям:

- Серверная часть - п. 2.2 на стр. 24.
- **Ошибка! Источник ссылки не найден.** - п. **Ошибка! Источник ссылки не найден.** на стр. **Ошибка! Закладка не определена.**.

Шаг 2. Настройка пересылки скрытых копий

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. 3.3.1 на стр. 48.

Шаг 3. Установка и настройка сервера Traffic Monitor

1. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor (п. 3.2.1 на стр. 37)
2. Установите сервер Traffic Monitor (п. 3.1 на стр. 28)
3. Убедитесь, что включен автозапуск процесса `iw_smtpd` (п. 3.2.1 на стр. 37)
4. Установите лицензию на перехватчик SMTP-трафика (п. 3.2.3.3 на стр. 40)
5. Настройте интеграцию с Postfix (п. 3.3.2 на стр. 49)
6. Если **с**истема разворачивается по схеме на рис. 2 (загрузка данных из филиалов в центральный офис происходит по медленным каналам связи, не меньше 128 Кбит/с):
    - В каждом удаленном филиале, где нужно перехватывать SMTP-трафик, на компьютере, где установлен сервер Traffic Monitor, установите и настройте клиентскую часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.1 на стр. 44).
    - В центральном офисе на компьютере, где установлен сервер Traffic Monitor, установите серверную часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.2 на стр. 45).

Шаг 4. Установка консоли управления

1. Установите Консоль управления (п. 3.5 на стр. 64).
2. В консоли управления выполните настройки, необходимые для анализа и обработки объектов на сервер Traffic Monitor (подготовка и загрузка на сервер конфигурации, создание базы эталонных документов, дополнительные настройки).

   В сценарии обработки объектов установите для перехватчика *Smtp* транспортный режим *Copy*.

   Информация по выполнению этих настроек содержится в п. 3.6 на стр. 66 и документе «*InfoWatch Traffic Monitor. Руководство пользователя*».

2.1.2. Перехват SMTP-трафика

Схема обеспечивает контроль информации, проходящей через корпоративную систему доставки почты. Сервер Traffic Monitor используется в качестве relay-сервера (подключение «в разрыв»).

Вариант 1. Система устанавливается в одном офисе, филиалов нет (см. рис. 1).

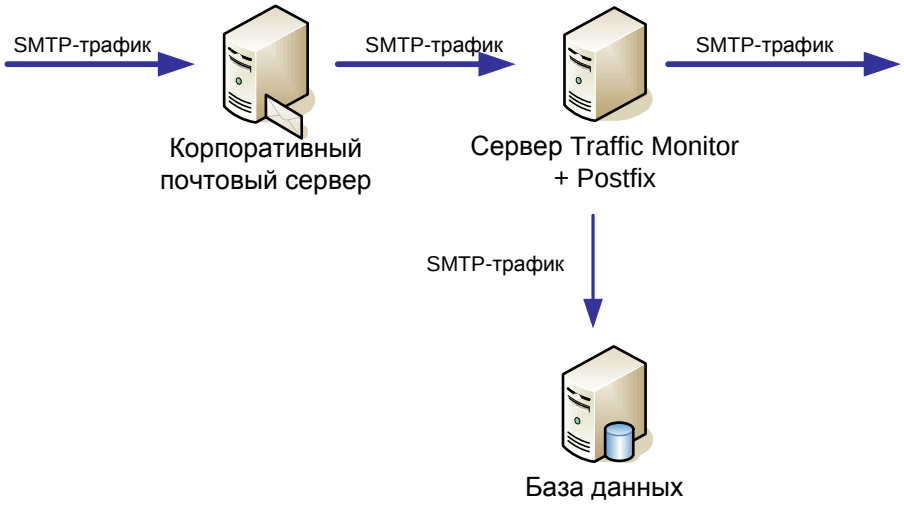


Рисунок 3. Перехват SMTP-трафика

Вариант 2. SMTP-трафик, перехваченный в филиалах, передается в центральный офис по медленному каналу связи (см. рис. 2). В центральном офисе SMTP-трафик загружается в базу данных.

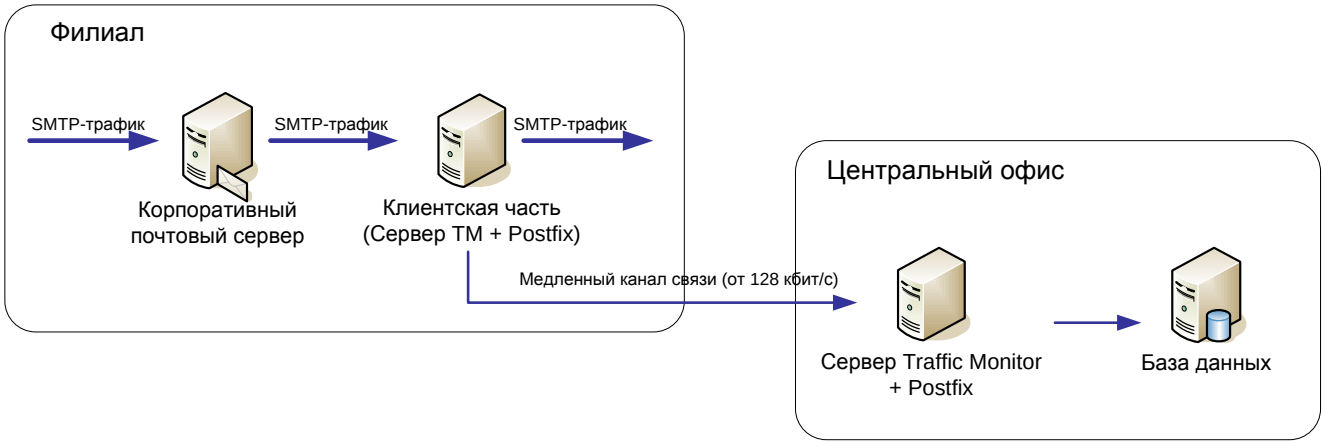


Рисунок 4. Передача SMTP-трафика из филиала в центральный офис

Далее приводится общий порядок развертывания для обоих вариантов. Различия имеются только при установке сервера Traffic Monitor.

Шаг 1. Проверка аппаратных и программных требований к Системе

Убедитесь, что среда, в которой будет развернута Система, удовлетворяет аппаратным и программным требованиям:

- Серверная часть - п. 2.2 на стр. 24.
- **Ошибка! Источник ссылки не найден.** - п. **Ошибка! Источник ссылки не найден.** на стр. **Ошибка! Закладка не определена.**.

Шаг 2. Настройка параметров Postfix

Почтовый сервер Postfix должен быть установлен и настроен до установки сервера Traffic Monitor. О настройке Postfix см. 3.3.2 на стр. 49.

Шаг 3. Установка и настройка сервера Traffic Monitor

1. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor. Используйте ключ запуска kickstart **IWDBX** (п. 3.1 на стр. 28)
2. Установите и настройте сервер часть Traffic Monitor (п. 3.1 на стр. 28)
3. Установите лицензию на перехватчик SMTP-трафика (п. 3.2.3.3 на стр. 40)
4. Убедитесь, что включен автозапуск процессов `iw_smtpd` и `iw_deliverd` (п. 3.2.1 на стр. 37)
5. Настройте пересылку скрытых копий (Настройка пересылки скрытых копий стр. 48)
6. Если **с**истема разворачивается по схеме на рис. 4 (загрузка данных из филиалов в центральный офис происходит по медленным каналам связи, не меньше 128 Кбит/с):
    - В каждом удаленном филиале, где нужно перехватывать SMTP-трафик, на компьютере, где установлен сервер Traffic Monitor, установите и настройте клиентскую часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.1 на стр. 44).
    - В центральном офисе на компьютере, где установлен сервер Traffic Monitor, установите серверную часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.2 на стр. 45).

Шаг 4. Установка консоли управления

1. Установите Консоль управления (п. 3.5 на стр. 64).
2. В консоли управления выполните настройки, необходимые для анализа и обработки объектов на сервере Traffic Monitor (подготовка и загрузка на сервер конфигурации, создание базы эталонных документов, дополнительные настройки).

   В сценарии обработки объектов установите для перехватчика *Smtp* транспортный режим *Normal* или *Transparent*.

   Информация по выполнению этих настроек содержится в п. 3.6 на стр. 66 и документе «*InfoWatch Traffic Monitor. Руководство пользователя*».

2.1.3. Прием копии трафика при помощи Sniffer

Трафик (SMTP, HTTP, ICQ) проходит через коммутатор CISCO, оборудованный SPAN-портом. Копия трафика направляется на Sniffer. Sniffer передает копию трафика на сервер Traffic Monitor для анализа и загрузки в базу данных.

Для увеличения производительности можно создавать кластеры серверов Traffic Monitor. Один кластер может содержать два экземпляра серверов Traffic Monitor. Не рекомендуется использовать более 3 кластеров.

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

Возможно несколько вариантов развертывания.

Вариант 1. Перехват и анализ копии трафика выполняется на одном компьютере (см. рис. 5). Кластер не создается. Система устанавливается в одном офисе, филиалов нет.

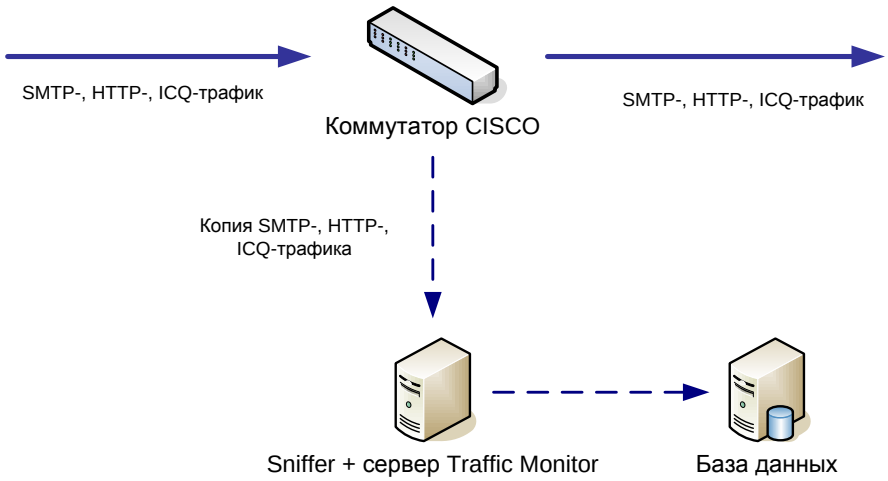


Рисунок 5. Перехват и анализ трафика на одном компьютере

Вариант 2. Перехват и анализ копии трафика выполняется на разных компьютерах, кластеризация не используется (см. рис. 6). Система устанавливается в одном офисе, филиалов нет.

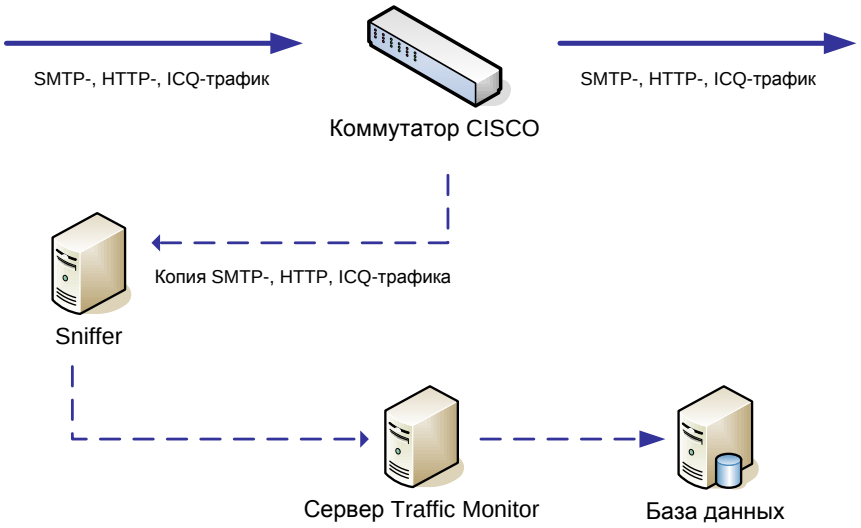


Рисунок 6. Перехват и анализ копии трафика на разных компьютерах

Вариант 3. Перехват и анализ копии трафика выполняется на разных компьютерах. Для увеличения производительности создан кластер из двух экземпляров сервера Traffic Monitor (см. рис. 7). Система устанавливается в одном офисе, филиалов нет.

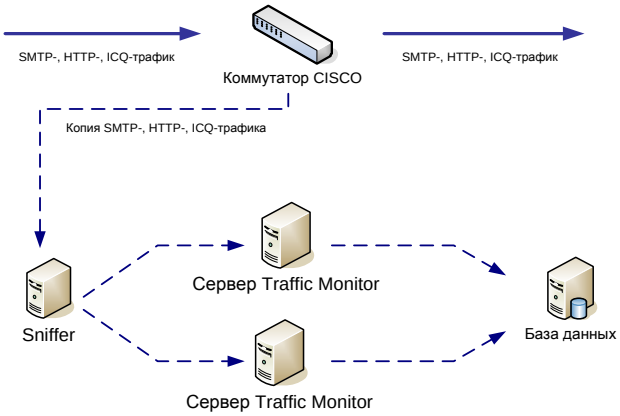


Рисунок 7. Кластер из двух экземпляров сервера Traffic Monitor

Вариант 4. Перехват и анализ копии трафика выполняется на разных компьютерах. Кластер не создается. Копия трафика из филиала передается в центральный офис по медленному каналу связи. В центральном офисе копия трафика загружается в базу данных (см. рис. 8).

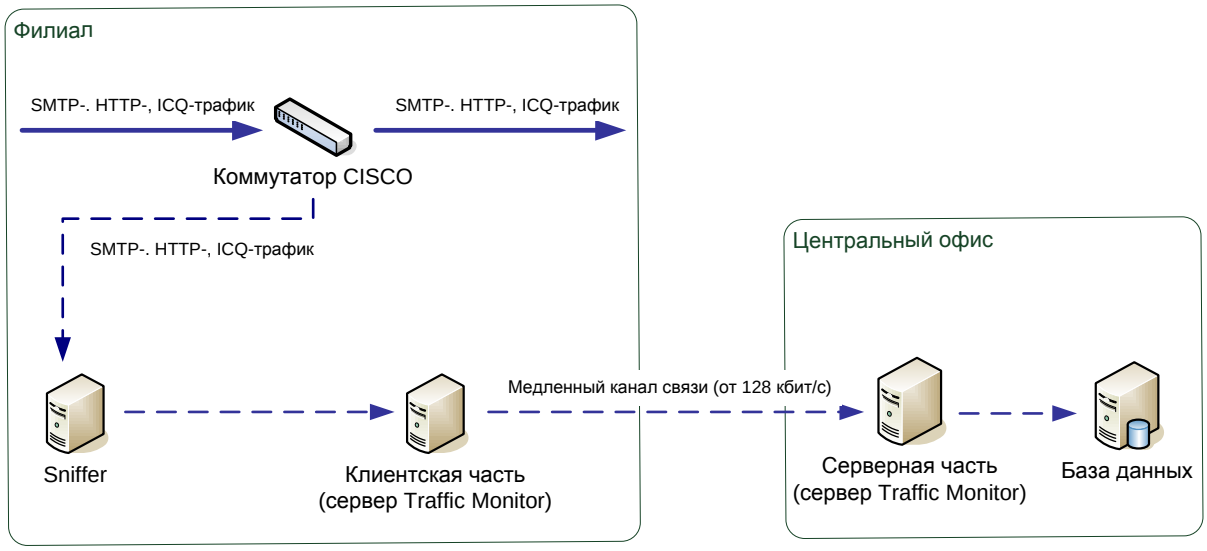


Рисунок 8. Перехват копии трафика через Sniffer и загрузка в удаленную базу данных

Далее приводится общий порядок развертывания для всех рассмотренных вариантов. Различия имеются только при установке сервера Traffic Monitor.

Шаг 1. Проверка аппаратных и программных требований к Системе

Убедитесь, что среда, в которой будет развернута Система, удовлетворяет аппаратным и программным требованиям:

- Серверная часть - п. 2.2 на стр. 24.
- Sniffer - п. 2.2.1 на стр. 25.
- **Ошибка! Источник ссылки не найден.** - п. **Ошибка! Источник ссылки не найден.** на стр. **Ошибка! Закладка не определена.**.

Шаг 2. Установка и настройка Sniffer и сервера Traffic Monitor

Вариант 1 (см. рис. 5). Перехват и анализ трафика выполняется на одном компьютере. Увеличение производительности не требуется (кластеризация не нужна). Система будет установлена в одном офисе, удаленных филиалов нет:

1. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor. Используйте ключ запуска kickstart **IWDBX** (п. 3.1 на стр. 28)
2. Установите сервер Traffic Monitor. Используйте ключ запуска kickstart **IWTMX** (п. 3.1 на стр. 28)
3. Настройте сервер на работу в качестве Sniffer (п. 3.3.3.1 на стр. 51, вариант 2)
4. Настройте параметры приема копии трафика от Sniffer (п. 3.3.3.2 на стр. 52).
5. Установите лицензию на необходимые перехватчики (п. 3.2.3.3 на стр. 40).

Вариант 2 (см. рис. 6). Перехват и анализ трафика выполняется на разных компьютерах. Увеличение производительности не требуется (кластеризация не нужна). Система будет установлена в одном офисе, удаленных филиалов нет:

1. На одном компьютере:
   - Установите сервер Traffic Monitor. Используйте ключ запуска kickstart **IWTMX** (п. 3.1 на стр. 28).
   - Настройте сервер Traffic Monitor на работу в качестве Sniffer (п. 3.3.3.1 на стр. 51, вариант 1).
2. На другом компьютере:

- Установите сервер Traffic Monitor. Используйте ключ запуска kickstart **IWTMX** (п. 3.1 на стр. 28).
- Установите лицензию на необходимые перехватчики (п. 3.2.3.3 на стр. 40).
- Настройте параметры приема копии трафика от Sniffer (п. 3.3.3.2 на стр. 52).

3. На третьем компьютере:

- Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor. Используйте ключ запуска kickstart **IWDBX** (п. 3.1 на стр. 28).

Вариант 3 (см. рис. 7). Перехват и анализ трафика выполняется на разных компьютерах. Необходимо увеличить производительность Системы (требуется кластеризация). Система будет установлена в одном офисе, удаленных филиалов нет:

1. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor. Используйте ключ запуска kickstart **IWDBX** (п. 3.1 на стр. 28).
2. На компьютере, где будет работать Sniffer:
   - Используйте ключ запуска kickstart **IWTMX** (п. 3.1 на стр. 28).
   - Настройте сервер на работу в качестве Sniffer (п. 3.3.3.1 на стр. 51, вариант 1).
3. На компьютере, где будет работать экземпляр кластера Traffic Monitor:
   - Установите сервер Traffic Monitor. Используйте ключ запуска kickstart **IWTMX** (п. 3.1 на стр. 28).
   - Установите лицензию на необходимые перехватчики (п. 3.2.3.3 на стр. 40).
   - Настройте параметры приема копии трафика от Sniffer (п. 3.3.3.2 на стр. 52).
   - Укажите параметры кластеризации (п. 3.3.3.3 на стр. 52).

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

> **Важная информация!**
>
> Если используется Модуль Детектирования Цифровых Отпечатков, то в Системе должен функционировать только одна Подсистема Анализа.
>
> При наличии в Системе нескольких экземпляров сервера Traffic Monitor настройте Подсистему Анализа только на одном экземпляре сервера Traffic Monitor (см. п. 3.2.2 на стр. 38).

Вариант 4 (см. рис. 8). Перехват и анализ трафика выполняется на разных компьютерах. Увеличение производительности не требуется (кластеризация не нужна). Система будет установлена в центральном офисе и в удаленных филиалах.

В каждом удаленном филиале, где требуется перехватывать копию трафика:

1. На компьютере, где будет работать Sniffer:

- Используйте ключ запуска kickstart **IWTMX** (п. 3.1 на стр. 28).
- Настройте сервер на работу в качестве Sniffer (п. 3.3.3.1 на стр. 51, вариант 1).

2. На компьютере, где будет работать филиальный сервер Traffic Monitor:
   - Установите и настройте серверную часть Traffic Monitor. Используйте ключ запуска kickstart **IWTMX** (п. 3.1 на стр. 28).
   - Установите лицензию на необходимые перехватчики (п. 3.2.3.3 на стр. 40).
   - Установите и настройте клиентскую часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.1 на стр. 44).
   - Настройте параметры приема копии трафика от Sniffer (п. 3.3.3.2 на стр. 52).

В центральном офисе:

1. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor. Используйте ключ запуска kickstart **IWDBX**.
2. Установите и настройте серверную часть Traffic Monitor. Используйте ключ запуска kickstart **IWTMX** (п. 3.1 на стр. 28).
3. Установите лицензию на необходимые перехватчики (п. 3.2.3.3 на стр. 40).
4. Установите и настройте серверную часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.2 на стр. 45).

Шаг 3. Установка консоли управления

1. Установите Консоль управления (п. 3.5 на стр. 64).
2. В консоли управления выполните настройки, необходимые для анализа и обработки объектов на сервер Traffic Monitor (подготовка и загрузка на сервер конфигурации, создание базы эталонных документов, дополнительные настройки).

   В сценарии обработки объектов установите для перехватчиков, принимающих копию трафика от Sniffer (*Smtp*, *Http*, *Icq*) транспортный режим *Copy*.

   Информация по выполнению этих настроек содержится в п. 3.6 на стр. 66 и документе «*InfoWatch Traffic Monitor. Руководство пользователя*».

2.1.4. Прием HTTP-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 будет использоваться автоматически устанавливаемый модуль IW ICAP.

Схема поддерживает *Нормальный* или *Прозрачный* транспортные режимы. В *Нормальном* транспортном режиме после обработки трафика сервером Traffic Monitor, на прокси-сервер будут возвращаться результаты анализа: разрешение или запрет на дальнейшую передачу перехваченных данных. В *Прозрачном* транспортном режиме после обработки трафика сервером Traffic Monitor, будет создана теневая копия, и данные будут направлены адресату.

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

Важная информация!

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.

Вариант 1. Система устанавливается в одном офисе, филиалов нет (см. рис. 9).

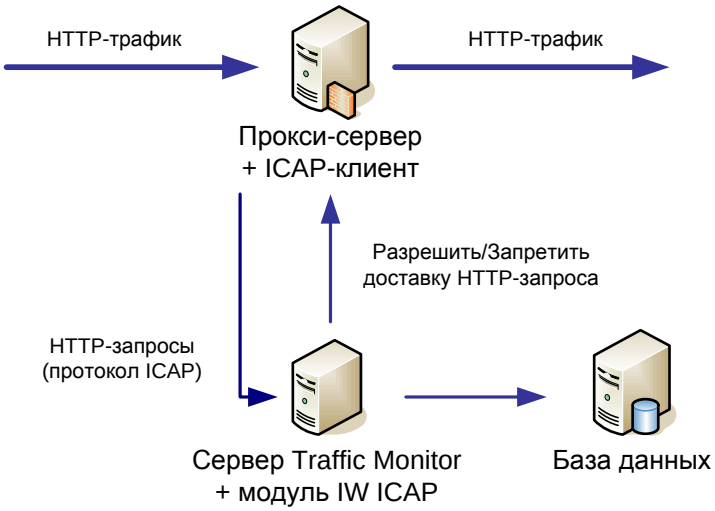


Рисунок 9. Перехват HTTP-трафика, передаваемого по протоколу ICAP

Вариант 2 . Перехват, анализ и фильтрация HTTP-трафика осуществляется в филиале. Перехваченный HTTP-трафик передается в центральный офис по медленному каналу связи. В центральном офисе копия трафика загружается в базу данных (см. рис. 10).

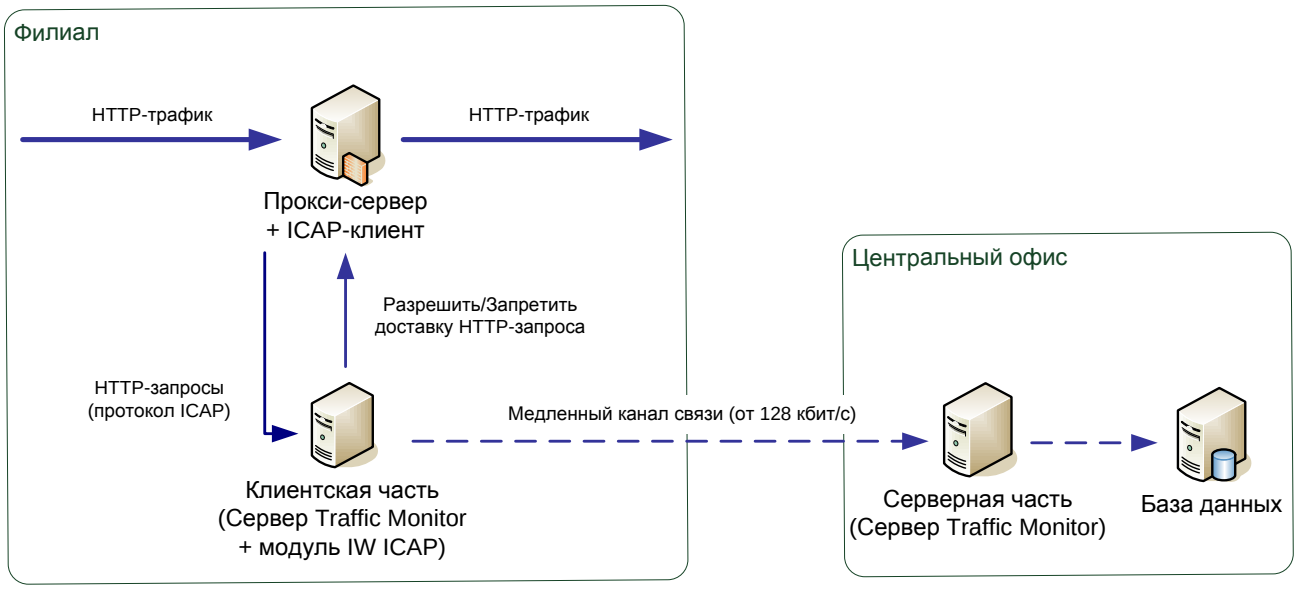


Рисунок 10. Перехват HTTP-трафика, в филиале и загрузка в удаленную базу данных

Далее приводится общий порядок развертывания для всех рассмотренных вариантов. Различия имеются только при установке сервера Traffic Monitor.

Шаг 1. Проверка аппаратных и программных требований к Системе

Убедитесь, что среда, в которой будет развернута Система, удовлетворяет аппаратным и программным требованиям:

- Серверная часть - п. 2.2 на стр. 24.
- Модуль IW ICAP - п. 2.2.2 на стр. 25.
- **Ошибка! Источник ссылки не найден.** - п. **Ошибка! Источник ссылки не найден.** на стр. **Ошибка! Закладка не определена.**.

Шаг 2. Установка и настройка сервера Traffic Monitor

Для развертывания системы **Вариант 1**, совершите следующие действия:

1. Установите сервер Traffic Monitor (см. п. 3.1 на стр. 28.)
2. Установите лицензию на перехватчик HTTP-трафика (п. 3.2.3.3 на стр. 40).
3. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor. (см. п. 3.1 на стр. 28.)
4. Настройте параметры перехвата HTTP-запросов на прокси-сервере (см. п. 3.3.4 на стр. 53).

Для развертывания системы **Вариант 2**, совершите следующие действия:

1. Установите сервер Traffic Monitor в центральном офисе (см. п. 3.1 на стр. 28.)
2. В центральном офисе на компьютере, где установлен сервер Traffic Monitor, установите серверную часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.2 на стр. 45).
3. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor в центральном офисе (см. п. 3.1 на стр. 28.)
4. Установите сервер Traffic Monitor в филиальном офисе (см. п. 3.1 на стр. 28.)
5. В каждом удаленном филиале, где нужно перехватывать SMTP-трафик, на компьютере, где установлен сервер Traffic Monitor, установите и настройте клиентскую часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.1 на стр. 44).
6. Настройте параметры перехвата HTTP-запросов на прокси-сервере (см. п. 3.3.4 на стр. 53).

Шаг 3. Установка консоли управления

1. Установите Консоль управления (п. 3.5 на стр. 64).
2. В консоли управления выполните настройки, необходимые для анализа и обработки объектов на сервере Traffic Monitor (подготовка и загрузка на сервер конфигурации, создание базы эталонных документов, дополнительные настройки).

   В сценарии обработки объектов установите для перехватчика *Http* транспортный режим *Normal* или *Transparent*.

   Информация по выполнению этих настроек содержится в п. 3.6 на стр. 66 и документе «*InfoWatch Traffic Monitor. Руководство пользователя*».

2.1.5. Прием объектов, перехваченных InfoWatch Device Monitor

Объекты (теневые копии файлов, задания на печать), перехваченные системой InfoWatch Device Monitor, передаются на сервер Traffic Monitor для анализа и загрузки в базу данных.

Вариант 1. Система устанавливается в одном офисе, филиалов нет (см. рис. 11).

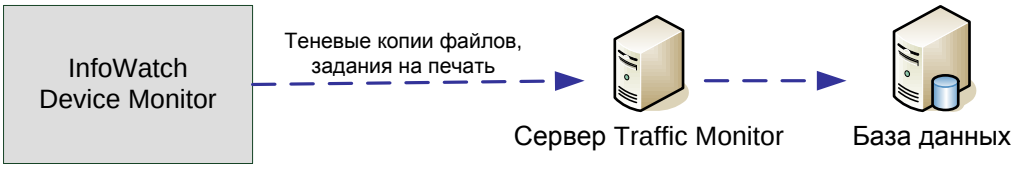


Рисунок 11. Прием объектов от InfoWatch Device Monitor

Вариант 2. В филиале установлена система InfoWatch Device Monitor. Объекты, перехваченные InfoWatch Device Monitor, передаются для анализа на сервер Traffic Monitor. Затем объекты передаются в центральный офис. В центральном офисе объекты загружаются в базу данных (см. рис. 12).

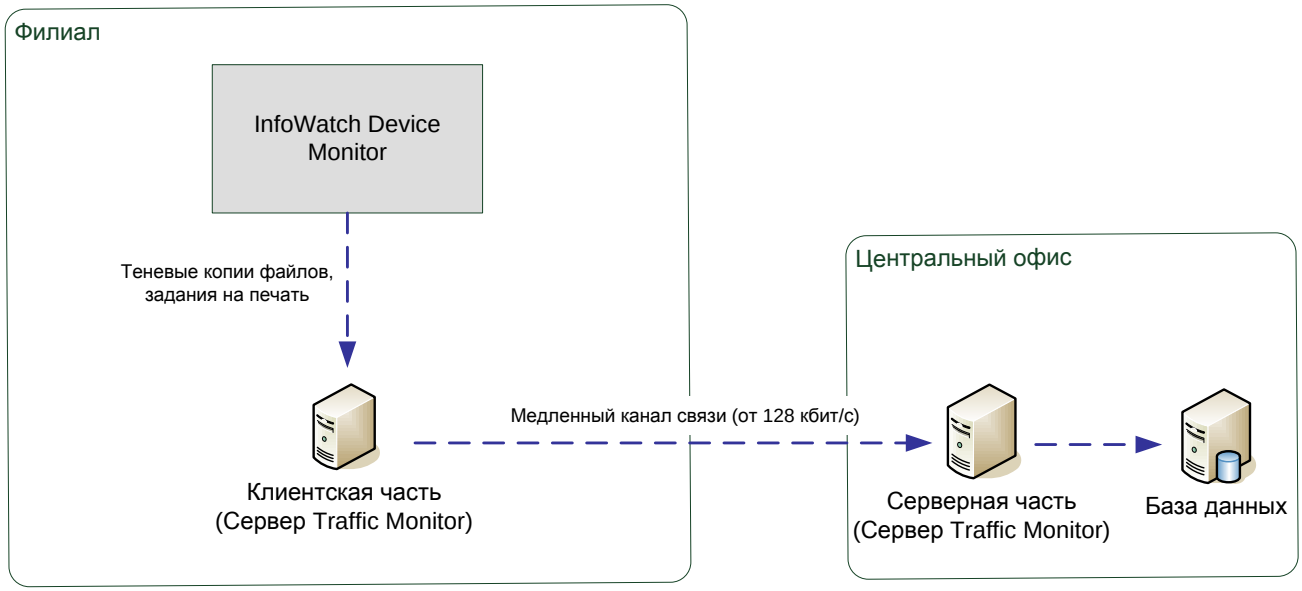


Рисунок 12. Прием объектов от InfoWatch Device Monitor и загрузка в удаленную базу данных

Далее приводится общий порядок развертывания для всех рассмотренных вариантов. Различия имеются только при установке сервера Traffic Monitor.

Шаг 1. Проверка аппаратных и программных требований к Системе

Убедитесь, что среда, в которой будет развернута Система, удовлетворяет аппаратным и программным требованиям:

- Серверная часть - п. 2.2 на стр. 24.
- **Ошибка! Источник ссылки не найден.** - п. **Ошибка! Источник ссылки не найден.** на стр. **Ошибка! Закладка не определена.**.

Шаг 2. Установка и настройка сервера Traffic Monitor

Для развертывания системы **Вариант 1**, совершите следующие действия:

5. Установите сервер Traffic Monitor (см. п. 3.1 на стр. 28.)
6. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor. (см. п. 3.1 на стр. 28.)

Для развертывания системы **Вариант 2**, совершите следующие действия:

7. Установите сервер Traffic Monitor в центральном офисе (см. п. 3.1 на стр. 28.)
8. В центральном офисе на компьютере, где установлен сервер Traffic Monitor, установите серверную часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.2 на стр. 45).
9. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor в центральном офисе (см. п. 3.1 на стр. 28.)
10. Установите сервер Traffic Monitor в филиальном офисе (см. п. 3.1 на стр. 28.)
11. В каждом удаленном филиале, где нужно перехватывать SMTP-трафик, на компьютере, где установлен сервер Traffic Monitor, установите и настройте клиентскую часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.1 на стр. 44).

Шаг 3. Установка консоли управления

1. Установите Консоль управления (п. 3.5 на стр. 64).
2. В консоли управления выполните настройки, необходимые для анализа и обработки объектов на сервере Traffic Monitor (подготовка и загрузка на сервер конфигурации, создание базы эталонных документов, дополнительные настройки).

   В сценарии обработки объектов установите для перехватчика *Device* транспортный режим *Copy*.

   Информация по выполнению этих настроек содержится в п. 3.6 на стр. 66 и документе «*InfoWatch Traffic Monitor. Руководство пользователя*».

2.1.6. Прием объектов от DeviceLock

Объекты, перехваченные системой DeviceLock, передаются на сервер Traffic Monitor для анализа и загрузки в базу данных.

Вариант 1. Система устанавливается в одном офисе, филиалов нет (см. рис. 13).

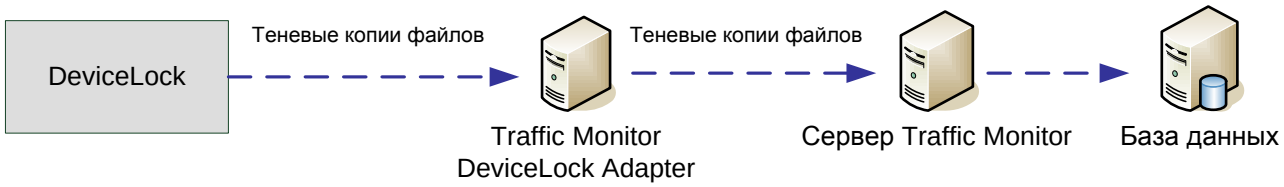


Рисунок 13. Прием объектов от DeviceLock

Вариант 2. В филиале установлена система DeviceLock. Объекты, перехваченные DeviceLock, передаются для анализа на сервер Traffic Monitor. Затем объекты передаются в центральный офис. В центральном офисе объекты загружаются в базу данных (см. рис. 14).

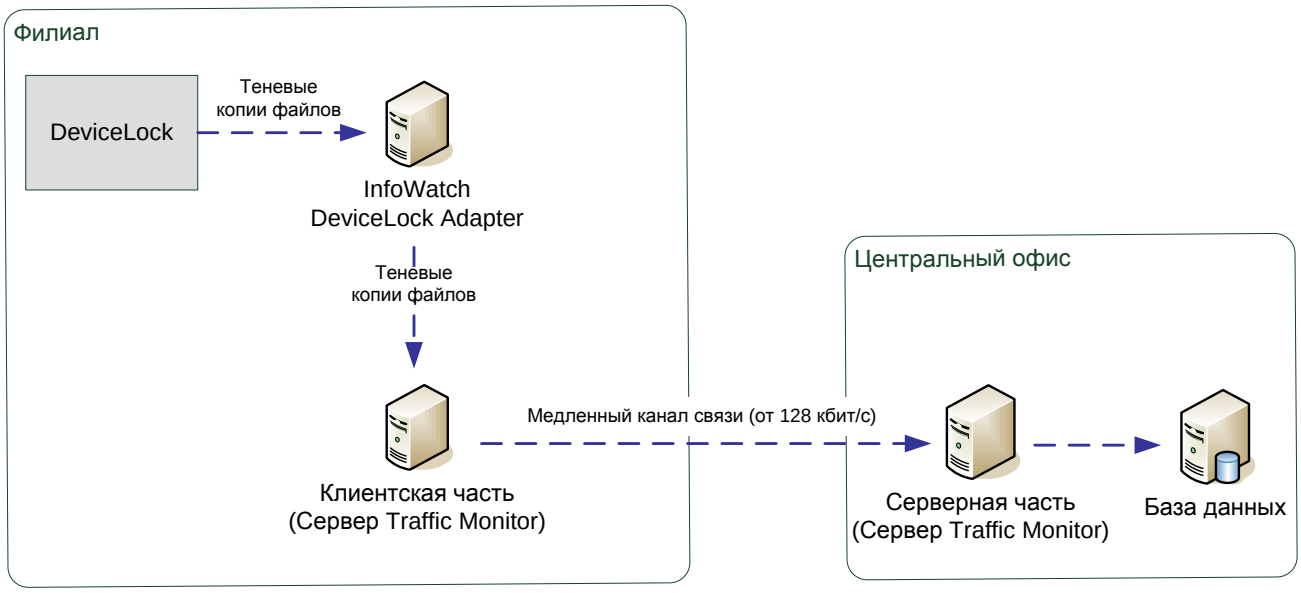


Рисунок 14. Прием объектов DeviceLock в филиале и загрузка в удаленную базу данных

Далее приводится общий порядок развертывания для всех рассмотренных вариантов. Различия имеются только при установке сервера Traffic Monitor.

Шаг 1. Проверка аппаратных и программных требований к Системе

Убедитесь, что среда, в которой будет развернута Система, удовлетворяет аппаратным и программным требованиям:

- Серверная часть - п. 2.2 на стр. 24.

- **Ошибка! Источник ссылки не найден.** - п. **Ошибка! Источник ссылки не найден.** на стр. **Ошибка! Закладка не определена.**.
- InfoWatch DeviceLock Adapter - см. документ «InfoWatch DeviceLock Adapter. Руководство по установке и конфигурированию».

Шаг 2. Установка и настройка сервера Traffic Monitor

Для развертывания системы **Вариант 1**, совершите следующие действия:

1. На сервер, который должен выполнять прием объектов, установите и настройте InfoWatch DeviceLock Adapter. Рекомендации приводятся в документах:
- «*InfoWatch DeviceLock Adapter. Руководство по установке и конфигурированию*».
- «*InfoWatch DeviceLock Adapter. Руководство администратора*».
2. Установите сервер Traffic Monitor (см. п. 3.1 на стр. 28.)
3. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor. (см. п. 3.1 на стр. 28.)

Для развертывания системы **Вариант 2**, совершите следующие действия:

1. Установите сервер Traffic Monitor в центральном офисе (см. п. 3.1 на стр. 28.)
2. В центральном офисе на компьютере, где установлен сервер Traffic Monitor, установите серверную часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.2 на стр. 45).
3. Установите и настройте сервер СУБД Oracle со схемой БД Traffic Monitor в центральном офисе (см. п. 3.1 на стр. 28.)
4. Установите сервер Traffic Monitor в филиальном офисе (см. п. 3.1 на стр. 28.)
5. В филиале, на компьютере, где установлен сервер Traffic Monitor, установите и настройте клиентскую часть модуля взаимодействия с удаленной БД (см. п. 3.2.5.1 на стр. 44).
6. На сервер, который должен выполнять прием объектов, установите и настройте InfoWatch DeviceLock Adapter. Рекомендации приводятся в документах:
- «*InfoWatch DeviceLock Adapter. Руководство по установке и конфигурированию*».
- «*InfoWatch DeviceLock Adapter. Руководство администратора*».

Шаг 3. Установка консоли управления

1. Установите Консоль управления (п. 3.5 на стр. 64).
2. В консоли управления выполните настройки, необходимые для анализа и обработки объектов на сервер Traffic Monitor (подготовка и загрузка на сервер конфигурации, создание базы эталонных документов, дополнительные настройки).

   В сценарии обработки объектов установите для перехватчика *Dla* транспортный режим *Copy*.

   Информация по выполнению этих настроек содержится в п. 3.6 на стр. 66 и документе «*InfoWatch Traffic Monitor. Руководство пользователя*».

2.1.7. Проверка файлов, находящихся в корпоративной сети

Перехватчик Crawler позволяет выполнять проверку файлов, находящихся в корпоративной сети:

- Сканирование сетевых папок, открытых для удаленного доступа по протоколу SMB.
- Сканирование локальных дисков рабочих станций, работающих под управлением ОС Windows.
- Сканирование документов, хранящихся в БД Microsoft SharePoint 2007.

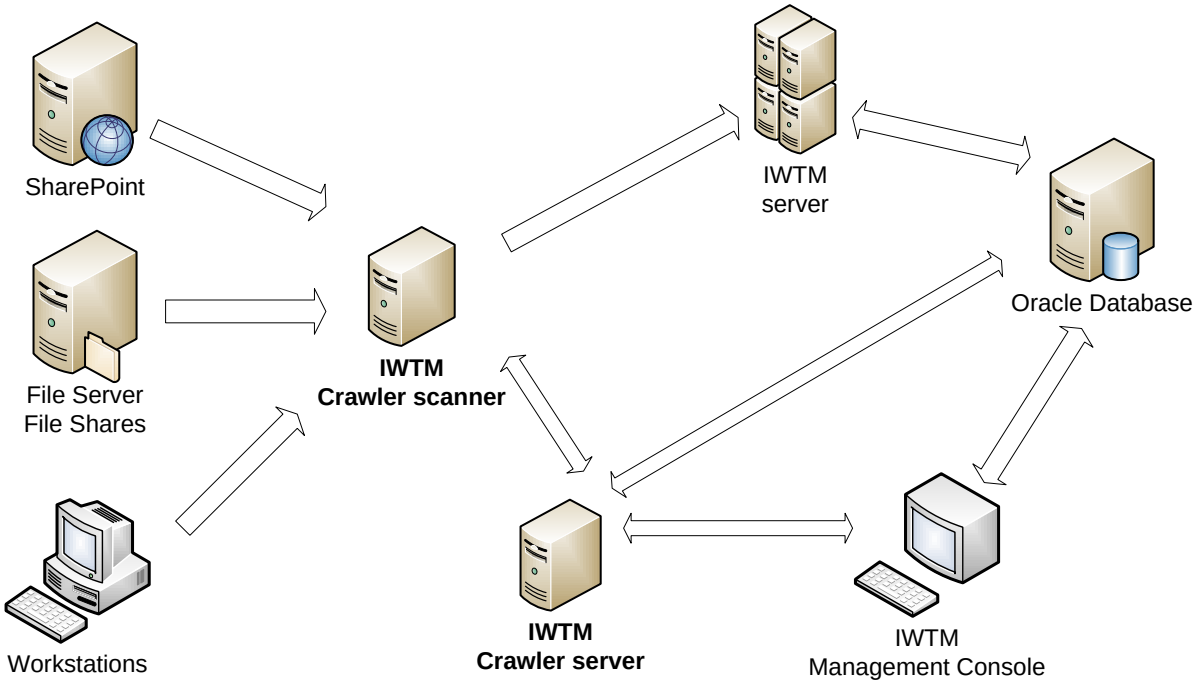


Рисунок 15. Сканирование корпоративной сети с помощью IW Crawler

InfoWatch Crawler выполняет сканирование в следующем порядке:

1. Рабочие станции, группы рабочих станций, файловые сервера или файловые хранилища, перечисленные в задании сканирования, проверяются на наличие доступных данных.
2. Каждый найденный файл, удовлетворяющий условиям поиска, временно копируется в рабочую директорию сканера.
3. Файл отправляется для анализа на сервер InfoWatch Traffic Monitor, где обрабатывается в соответствии с действующим сценарием обработки объектов.

Далее приводится общий порядок развертывания системы с перехватчиком Crawler.

Шаг 1. Проверка аппаратных и программных требований к Системе

Убедитесь, что среда, в которой будет развернута Система, удовлетворяет аппаратным и программным требованиям:

- Серверная часть - п. 2.2 на стр. 24.
- Компьютер для сервера Crawler и компьютер для сканера Crawler - п. 2.2.3 на стр. 26
- **Ошибка! Источник ссылки не найден.** - п. **Ошибка! Источник ссылки не найден.** на стр. **Ошибка! Закладка не определена.**.

Шаг 2. Установка и настройка сервера Traffic Monitor

Установите и настройте сервер Traffic Monitor (п. 3.1 на стр. 28).

Шаг 3. Установка и настройка Crawler

Установите и настройте Crawler (п. 3.3.5 на стр. 55).

Шаг 4. Установка и настройка Консоли управления

1. Установите Консоль управления (п. 3.5 на стр. 64).
2. В Консоли управления выполните настройки, необходимые для анализа и обработки объектов на сервере Traffic Monitor (подготовка и загрузка на сервер конфигурации, создание базы эталонных документов, дополнительные настройки).

3. Настройте соединение Консоли управления с сервером.
4. Настройте общие параметры работы сканера Crawler.
5. В сценарии обработки объектов установите для перехватчика *Crawler* транспортный режим *Copy*. Убедитесь, что в сценарии обработки объектов присутствует функция `CheckCrawlerPolicy(root)`.

Информация по выполнению настроек, осуществляющихся из Консоли управления, содержится в п. 3.6 на стр. 66 и документе «*InfoWatch Traffic Monitor. Руководство пользователя*».

2.2. Аппаратные и программные требования

Требования к аппаратной конфигурации СУБД для **Traffic Monitor Enterprise** определяются на основании выбранной схемы развертывания и параметров сети, куда устанавливается Система. Поэтому спецификация оборудования для каждого случая рассчитывается отдельно.

> **Важная информация!**
>
> Для Traffic Monitor Enterprise сервер Traffic Monitor и сервер СУБД Oracle должны быть установлены на разных компьютерах. При этом на компьютере, исполняющем роль сервера СУБД Oracle, не рекомендуется устанавливать и запускать приложения (особенно серверные) или использовать этот компьютер в качестве файл-сервера.

Для увеличения производительности Системы рекомендуется организовать как можно больше отдельных физических устройств ввода-вывода (volumes). При этом будут потери в объеме данных, но будут реализована возможность параллельного выполнения операций ввода-вывода и значительно увеличена пропускная способность базы данных.

Пример:

Исходный 12-дисковый массив хранения можно организовать следующим образом:

- Три RAID 5, состоящих из 3-х физических дисков – для ежедневных табличных пространств; при этом каждая файловая система должна располагаться на отдельном массиве;
- Один RAID 1, состоящий из 2-х физических дисков – для системных файлов, основного табличного пространства и временных файлов данных;
- Один диск, предназначенный для «горячей замены» (hot swap).

При настройке кэширования рекомендуются следующие параметры: кэш на запись – 80%; кэш на чтение – 20%.

Traffic Monitor Standard может быть установлен на сервере только в режиме "Все - в - одном" (см. Установка серверных компонентов на стр. 28).

Для Traffic Monitor Standard типовая конфигурация сервера приводится в расчете на суммарную скорость входящего и исходящего трафика 100 Мбит/с (с ограничением на объем полезного трафика не более 50 Мбит/с на один тип трафика):

- Сервер: поддерживаются конфигурации, допустимые для Red Hat Enterprise Linux Server версии 6: см. https://hardware.redhat.com/.

  Рекомендуется HP ProLiant DL 320 G6 Server.
- Процессор: Intel® Xeon® E5540 2.53 ГГц.
- Оперативная память: DDR3 из расчета 4 Гб + по 2 Гб на каждый перехватчик.
- Жесткий диск: SAS, 2 x 300 Гб (10000 rpm) с RAID 1.

Требования к остальным компонентам системы приведены в разделах:

- *Sniffer (п. 2.2.1 на стр. 25)*
- *Модуль IW ICAP (п. 2.2.2 на стр. 25)*
- *Crawler (п. 2.2.3 на стр. 26)*

- ***Ошибка! Источник ссылки не найден.*** *(п.* ***Ошибка! Источник ссылки не найден.*** *на стр.* ***Ошибка! Закладка не определена.****)*

2.2.1. Sniffer

Требования к сетевому оборудованию

Sniffer может получать копию трафика от коммутатора с поддержкой функции SPAN (рекомендованная модель - Cisco Catalyst 2960 Series).

После установки коммутатора настройте SPAN-порт в режиме RX/TX согласно сопроводительной документации используемого коммутатора.

Требования к аппаратному обеспечению

Минимальные требования при скорости трафика 50 Мбит/с:

- Процессор: Intel Core2 Duo E6750 (частота 2,66 ГГц)
- Оперативная память: 8 Гб.

Типовая конфигурация Sniffer при суммарной скорости входящего и исходящего трафика 50 Мбит/с:

- Сервер: поддерживаются конфигурации, допустимые для Red Hat Enterprise Linux Server версии 6: см. https://hardware.redhat.com/.

  Рекомендуемая конфигурация – HP ProLiant DL 360 G7 Server.
- Процессор: двухъядерный Intel® Xeon® E5502 1.87ГГц.
- Оперативная память: 8 Гб DDR3.
- Жесткий диск: SAS 300 Гб (10000 rpm).

Требования к сетевым картам:

Общие требования	Рекомендуемые модели сетевых карт
Поддержка NAPI и режима *Promiscuous mode*.	Intel Corporation 82540EM Gigabit Ethernet Controller Broadcom Corporation NetXtreme II BCM5708 1GB
Поддержка Gigabit Ethernet	Допускается использование сетевых карт серии Intel PRO/1000 GT

На Sniffer должны быть установлены как минимум две сетевые карты:

- сетевая карта для приема копии трафика от одного SPAN-порта коммутатора CISCO. Если прием трафика будет осуществляться с нескольких SPAN-портов (могут быть настроены как на одном, так и на разных коммутаторах), то для каждого SPAN-порта потребуется отдельная сетевая карта.
- сетевая карта для взаимодействия с прочими объектами сети. В частности, для передачи трафика на сервер Traffic Monitor или для взаимодействия с базой данных (если Sniffer и сервер Traffic Monitor установлены на одном компьютере).

2.2.2. Модуль IW ICAP

При интеграции с модулем IW ICAP передача HTTP-запросов осуществляется через прокси-сервер. Для передачи HTTP-запросов на сервер Traffic Monitor по протоколу ICAP необходим ICAP-клиент. Система поддерживает работу с ICAP-клиентами встроенными в прокси-сервер.

> **Важная информация**
>
> Сервер Traffic Monitor и прокси-сервер с ICAP-клиентом должны находиться в одной подсети.

Поддерживаются следующие прокси-серверы:

- SQUID версии не ниже 3.1.7, с включенной поддержкой ICAP.
- Cisco IronPort S10.

- Blue Coat SG Series с лицензией на ICAP. Поддерживается совместимость с рядом моделей, выпускаемых компанией Blue Coat Systems в настоящее время. Производитель постоянно обновляет модельный ряд, поэтому перед тем, как использовать конкретную модель устройства Blue Coat Proxy SG необходимо уточнить совместимость с модулем IW ICAP в службе технической поддержки компании InfoWatch.

> **Примечание:**
>
> Если требуется перехват HTTPS-трафика, настройте прокси-сервер так, чтобы HTTPS трафик обрабатывался и передавался на сервер InfoWatch Traffic Monitor как HTTP-трафик.

Описание установки и настройки вы можете найти в сопроводительной документации к выбранному прокси-серверу. Рекомендации по настройке прокси-серверов см. в п. 3.3.4 на стр. 53.

ICAP-сервер входит в состав модуля интеграции с ICAP. Модуль устанавливается на одном компьютере с сервером Traffic Monitor (см. требования в п. 2.2 на стр. 24). Дополнительных требований к аппаратному и программному обеспечению модуля не предъявляется.

2.2.3. Crawler

Требования к используемому экземпляру сервера InfoWatch Traffic Monitor:

- минимум 6 Гб оперативной памяти
- в файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[AUTO_RESTART]`, должен быть включен автозапуск процесса `iw_expressd`:

```
autorestart = On
```

Компьютер, на который планируется установка **сервера Crawler**, должен отвечать следующим минимальным требованиям:

- Процессор: от 2-х ядер
- Оперативная память: 200 Мб незанятой памяти
- Жесткий диск; 1 Гб свободного пространства
- Операционная система:
  - Microsoft Windows XP / Vista / 7 / 8
  - Microsoft Windows Server 2003 / 2008 / 2012
- Платформа Microsoft .Net Framework 4.0

Компьютер, на который планируется установка **сканера Crawler**, должен отвечать следующим минимальным требованиям:

- Процессор: от 2-х ядер
- Оперативная память: 200 Мб незанятой памяти
- Жесткий диск; не менее 10 Гб свободного пространства для временного хранения файлов, скопированных с проверяемых ресурсов
- Операционная система:
  - Microsoft Windows XP / Vista / 7 / 8
  - Microsoft Windows Server 2003 / 2008 / 2012
- Платформа Microsoft .Net Framework 4.0
- Пропускная способность сетевого канала между сканером Crawler и сервером Traffic Monitor должна быть не меньше, чем пропускная способность канала связи между сканером Crawler и сканируемыми сетевыми узлами (рабочие станции и файловые сервера).

Важная информация!

Рекомендуется выбирать расположение компьютера, на котором будет работать сканер Crawler, так, чтобы он находился в сегменте сети, максимально близком к тем сегментам, которые будут подлежать сканированию. Удаленность может существенно увеличить нагрузку на сеть.

Важная информация!

Если сегменты сети, где развернута система InfoWatch Traffic Monitor с Crawler, разделены между собой межсетевыми экранами, для корректной работы Crawler должны быть открыты порты **6557** (подключение Консоли управления InfoWatch Traffic Monitor к серверу Crawler) и **6556** (подключение сканера Crawler к серверу Crawler).

2.2.4. Консоль управления

Требования к аппаратному обеспечению

Оборудование	Минимальные требования	Рекомендуемые требования
Процессор	Celeron с частотой 1.7 ГГц и выше	Pentium IV с частотой 3 ГГц и выше
Оперативная память	512 Мб	1 Гб
Жесткий диск	1 Гб свободного пространства	1 Гб свободного пространства

Требования к программному обеспечению

Программное обеспечение	Требования
Операционная система	Microsoft Windows XP Service Pack 3
Платформа .Net Framework	Microsoft .Net Framework 3.5 SP1

ГЛАВА 3. УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ

Порядок установки системы InfoWatch Traffic Monitor определяется схемой развертывания, выбранной с учетом вида трафика, планируемого для перехвата, типа перехвата (фильтрация трафика либо работа с его копией), а также инфраструктурой сети, где разворачивается система. Более подробно см. п. 2.1 на стр. 10.

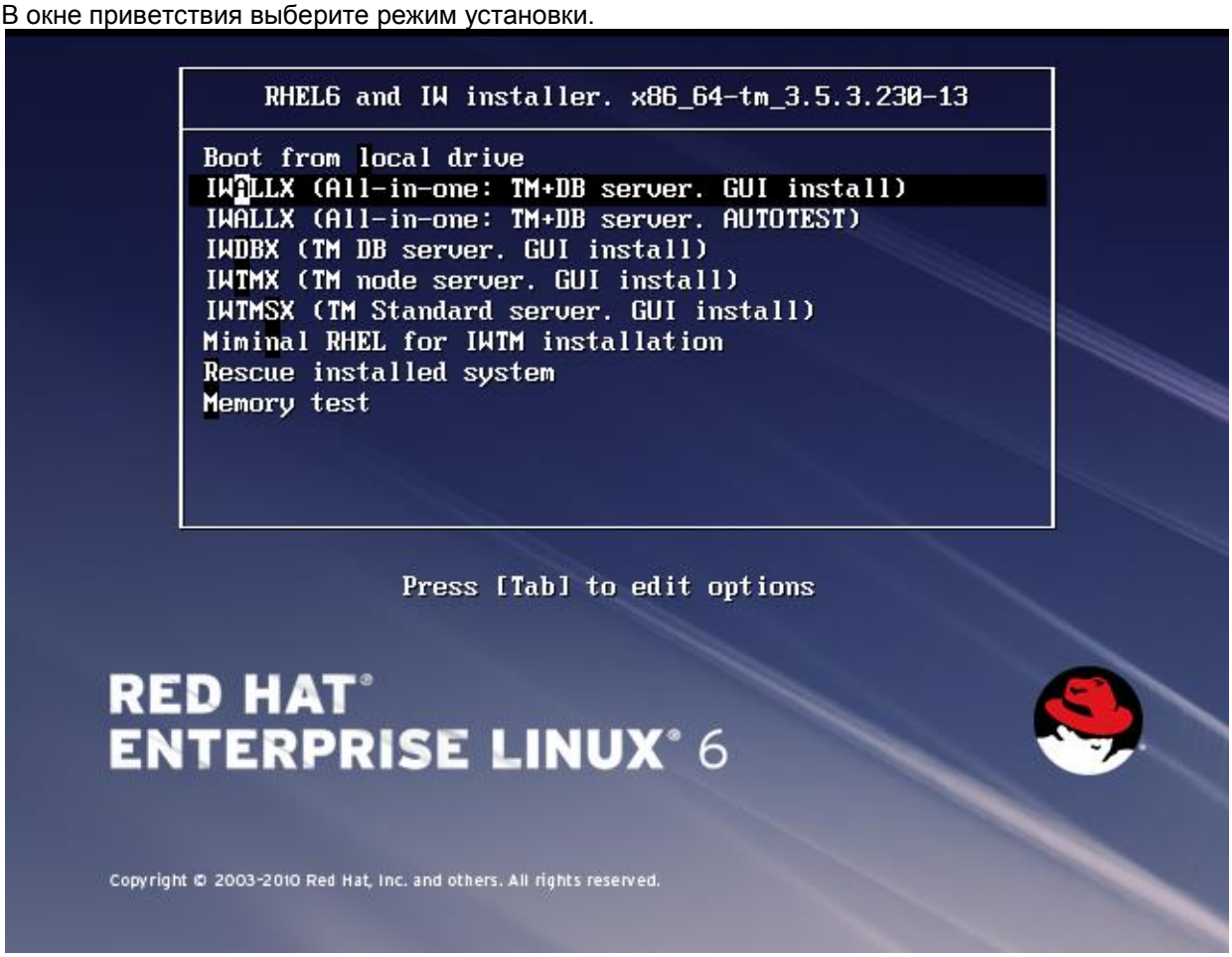
Далее описан порядок установки и настройки отдельных компонентов системы:

- *Установка серверных компонентов (п. 3.1 на стр. 28)*
- *Настройка сервера Traffic Monitor (п. 3.2 на стр. 37)*
- *Настройки перехватчиков (п. 3.3 на стр. 47)*
- *Настройка подсистемы мониторинга для распределенной архитектуры (п. 3.4 на стр. 60)*
- *Установка Консоли управления (п. 3.5 на стр. 64)*
- *Настройка параметров анализа объектов (п. 3.6 на стр. 66)*

3.1. Установка серверных компонентов

Установка серверных компонентов системы InfoWatch Traffic Monitor выполняется с помощью программы-инсталлятора (**kickstart**), автоматически запускающегося с дистрибутивного диска:

1. В окне приветствия выберите режим установки.

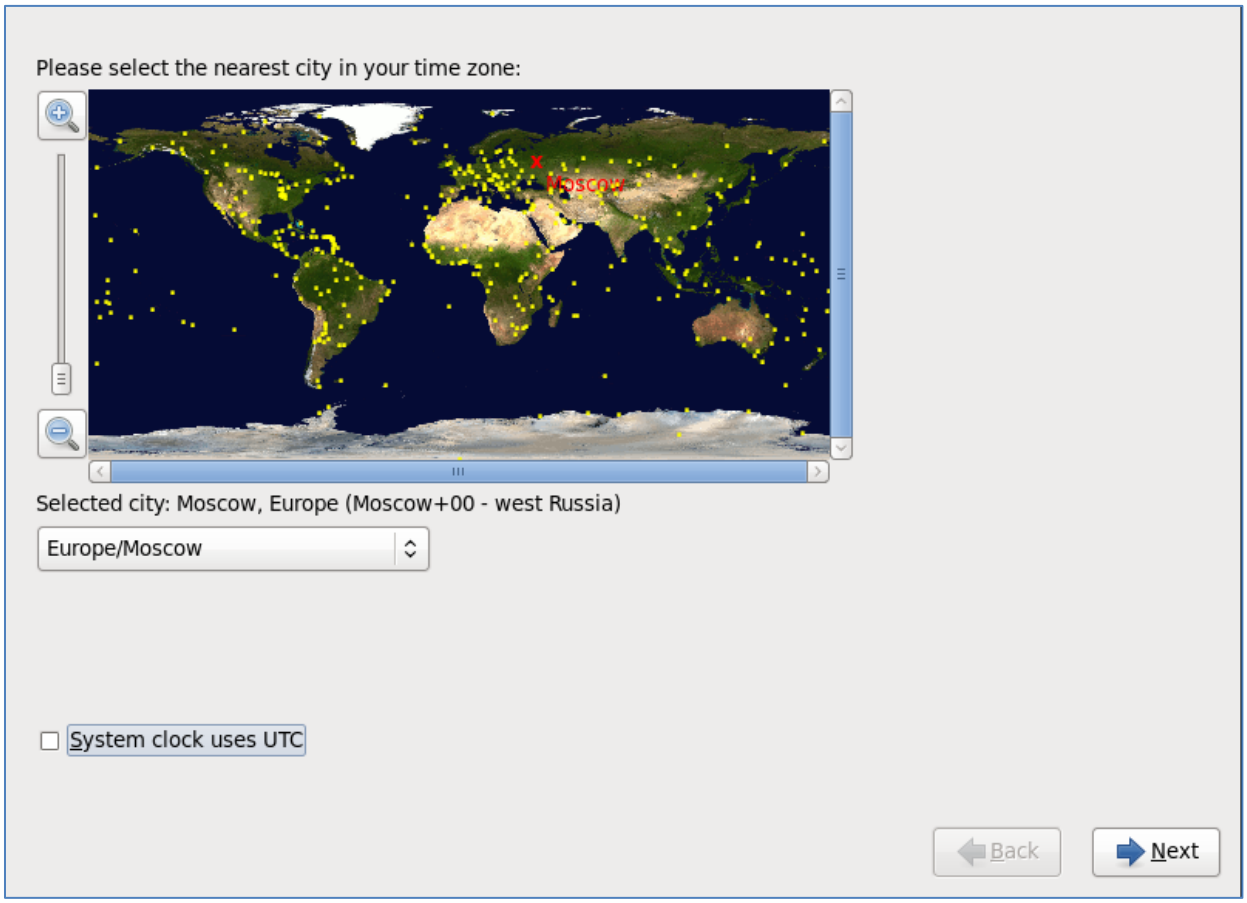


В зависимости от целевого назначения сервера (сервер Traffic Monitor; сервер базы данных, или установка обоих компонент на один компьютер) и редакцию Системы (полный вариант - Traffic

Monitor Enterprise, либо облегченный вариант Traffic Monitor Standard), будет различаться набор устанавливаемых компонент:

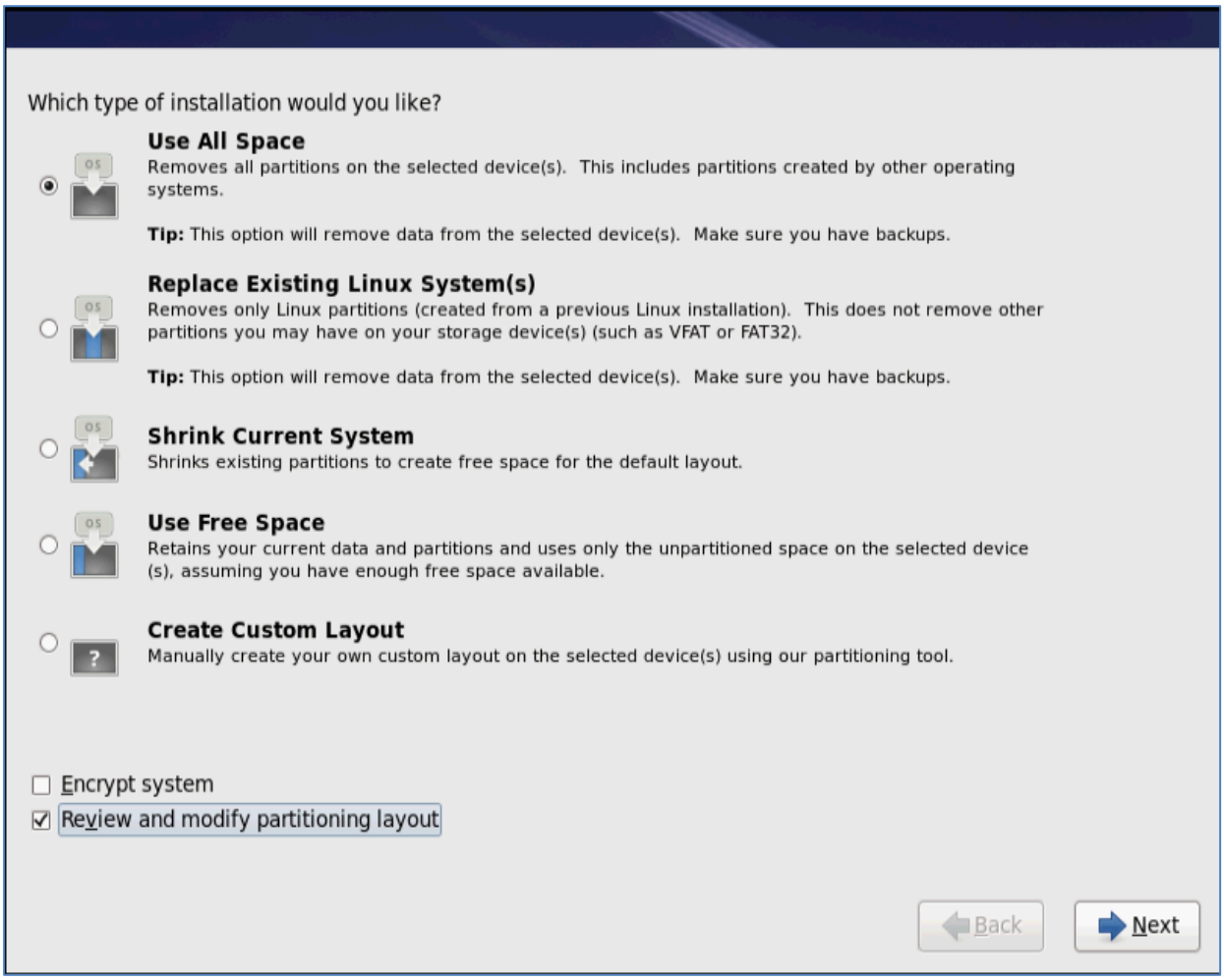
Режим установки	**Ключ запуска kickstart**	**Порядок установки и настройки компонент инсталлятором**
Установка сервера Traffic Monitor на отдельный компьютер	**IWTMX**	• Установка ОС Linux • Установка RPM пакетов сервера IWTM • Установка подсистемы мониторинга
Установка сервера СУБД Oracle со схемой БД Traffic Monitor на отдельный компьютер	**IWDBX**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка и настройка СУБД Oracle • Установка схемы базы данных IW Traffic Monitor • Установка подсистемы мониторинга
Режим "Все - в - одном": все компоненты устанавливаются на один сервер **Внимание!** Не рекомендуется для промышленного использования на трафике компании. Используется для пилотных установок.	**IWALLX**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка и настройка СУБД Oracle • Установка схемы базы данных IW Traffic Monitor • Установка RPM пакетов сервера IWTM • Установка подсистемы мониторинга
Установка InfoWatch Traffic Monitor Standard	**IWTMSX**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка и настройка СУБД Oracle Standard • Установка схемы базы данных IW Traffic Monitor • Установка RPM пакетов сервера IWTM • Установка подсистемы мониторинга

2. Укажите настройки часового пояса для сервера.



3. Выберите способ разбиения дискового пространства:

- Все имеющиеся разделы на выбранном диске будут удалены, и будет выполнена разбивка диска по умолчанию.
- На выбранном диске будут удалены разделы Linux, а затем выполнена разбивка диска по умолчанию.
- Сжатие существующих разделов для освобождения места.
- Разбивка диска по умолчанию производится только на свободном месте выбранного диска.
- Создание разделов на выбранном диске выполняется вручную.



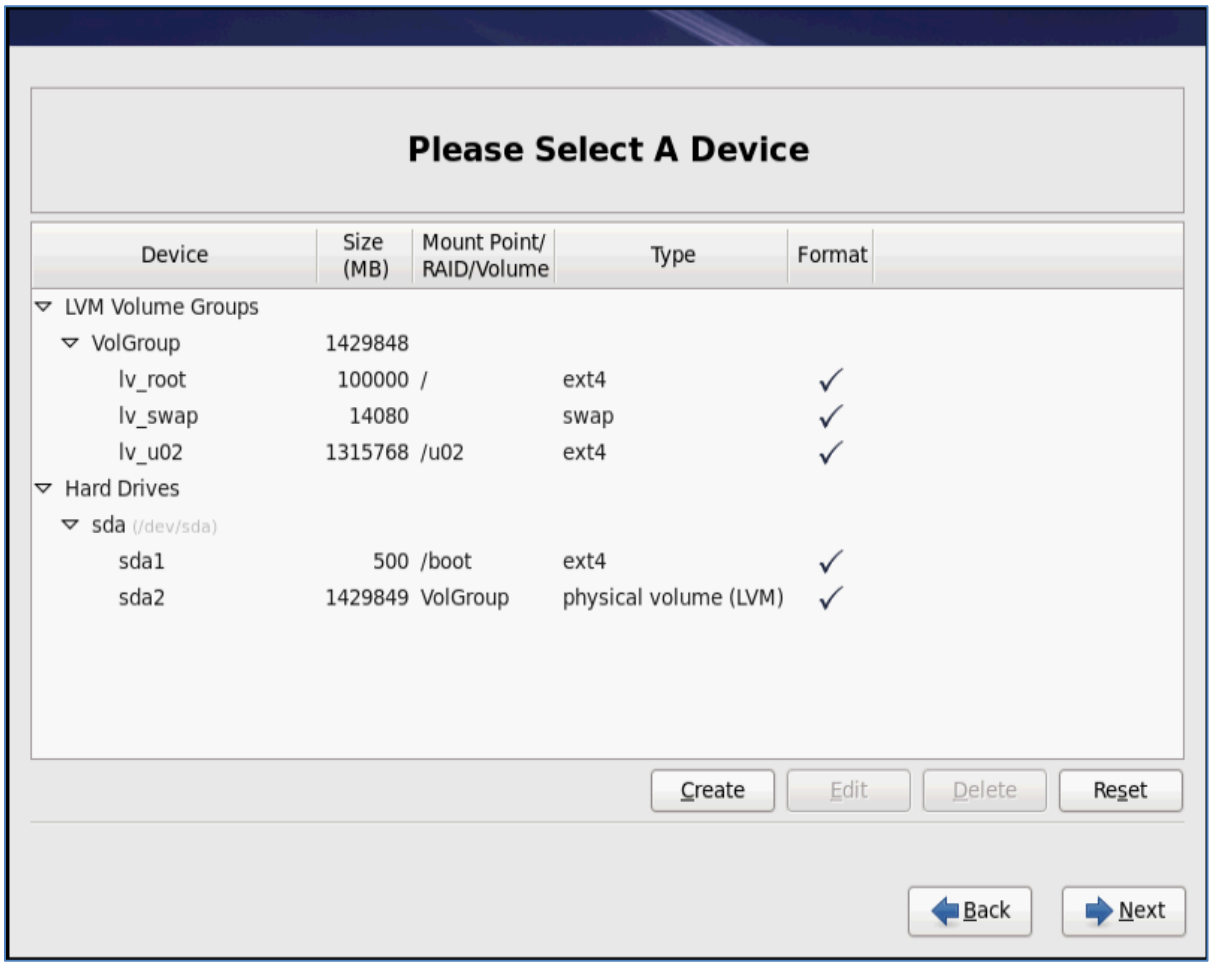
Выберите первый вариант (**Use all space**), отметьте **Review and modify partitioning layout** и нажмите **Next**.

4. Измените разбиение разделов в соответствии со следующими рекомендациями:

Режим установки	Корневой раздел root	Раздел /u02	SWAP
IWTMX (только сервер ТМ)	не менее 200 Гб	не нужен	оставить установленный по умолчанию
IWDBX (только сервер БД)	не менее 100 Гб	все остальное свободное место	
IWALLX (все-в-одном)	не менее 100 Гб	все остальное свободное место	
IWTMSX (ТМ Standard)	не менее 60 Гб	достаточно 400 Гб	

Важная информация!

Для систем, которые должны работать со значительными объемами данных, при установке сервера СУБД Oracle следует учитывать рекомендации по организации массива хранения, приведенные в требованиях к серверным компонентам (п. 2.2 на стр. 24).



Чтобы изменить параметры корневого раздела с установленных по умолчанию на рекомендуемые:

a) Выберите раздел **lv_root** и нажмите **Edit**.

b) В поле **Size** укажите рекомендуемое значение (например, для IWALLX - 100000 Mb).

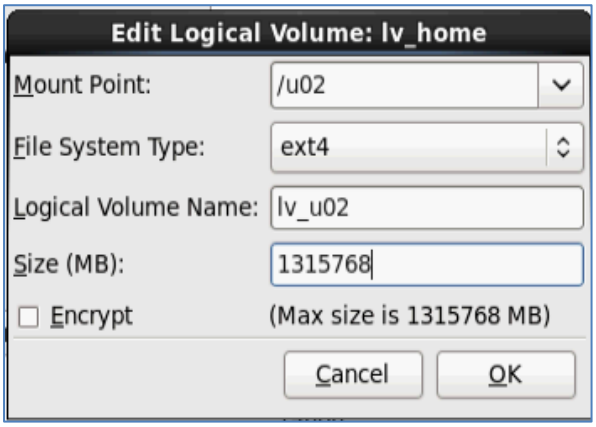
c) Нажмите **OK**.

Чтобы задать параметры раздела **/u02**:

a) Выберите раздел **lv_ home** и нажмите **Edit**.

b) Укажите следующие параметры:

- **Mount Point** - **/u02**
- **Logical Volume Name** – **lv_u02**
- При установке сервера БД рекомендуется выбрать тип файловой системы **ext3**
- **Size** – весь доступный объем указан в поле **Max size**



c) Нажмите **OK**.

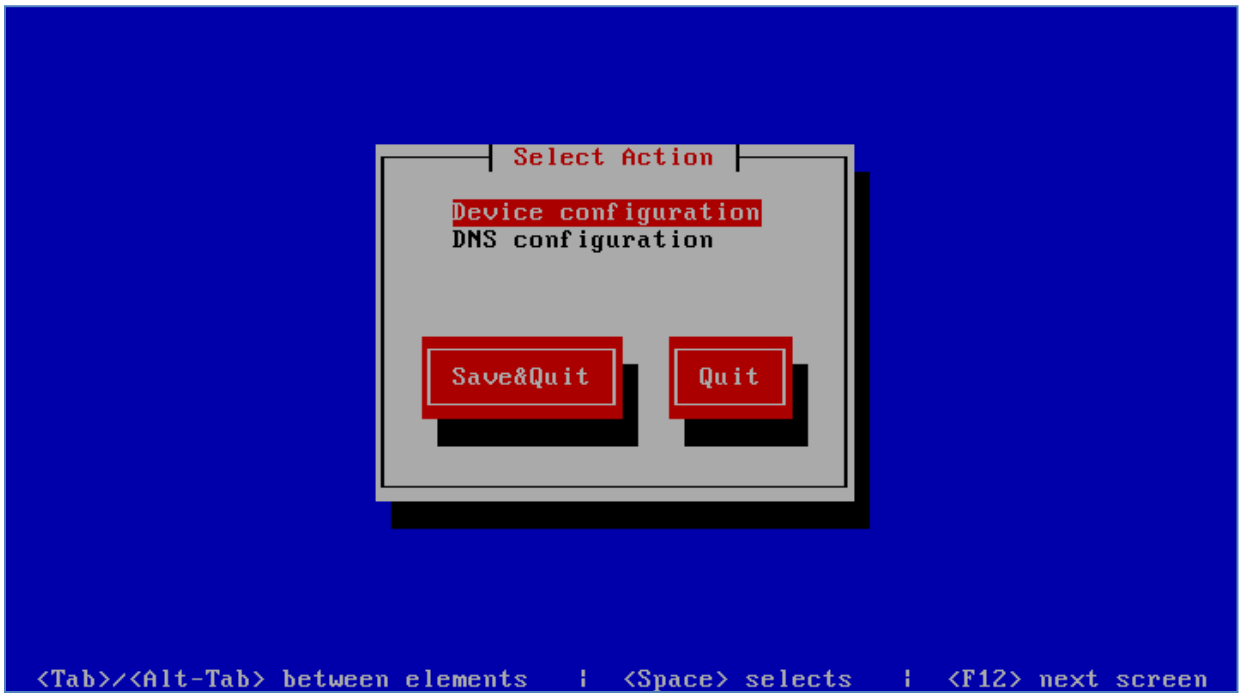
Чтобы удалить раздел **/u02**, выберите раздел **lv_ home** и нажмите **Delete**.

После того, как вы укажете параметры разбиения диска, нажмите **Next**.

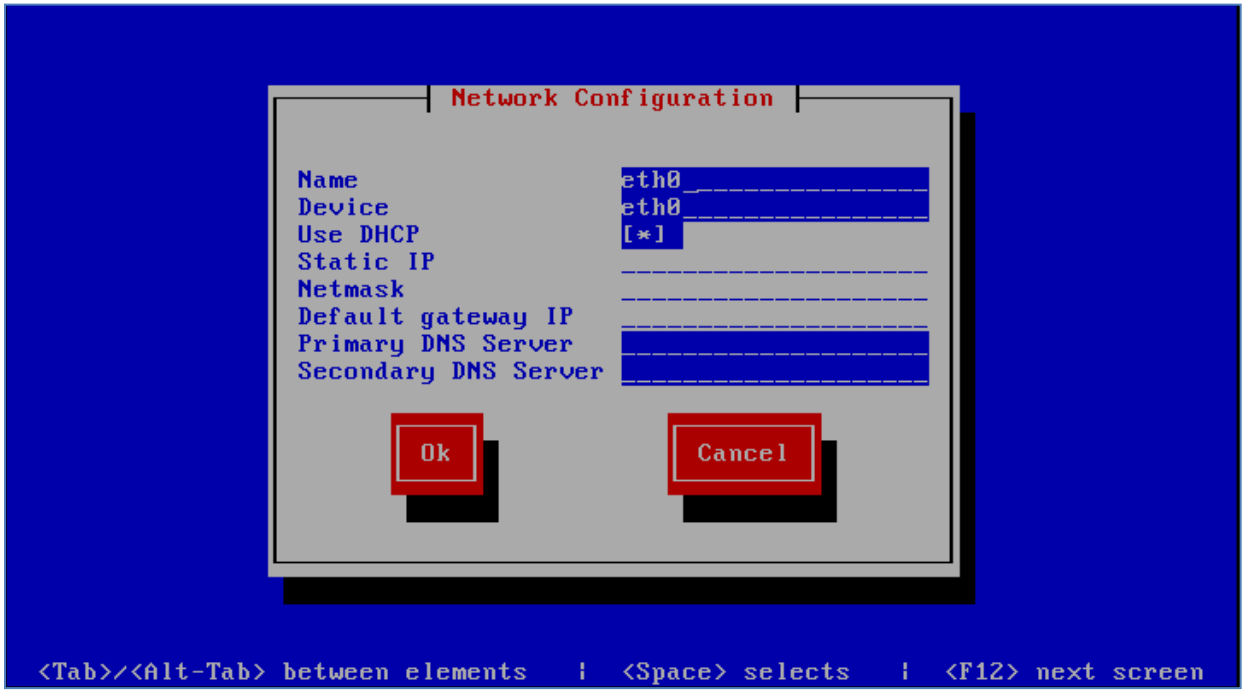
5. Начнется процесс разбиения диска, а затем – установки операционной системы. Прогресс выполнения обоих процессов будет отображаться на экране.



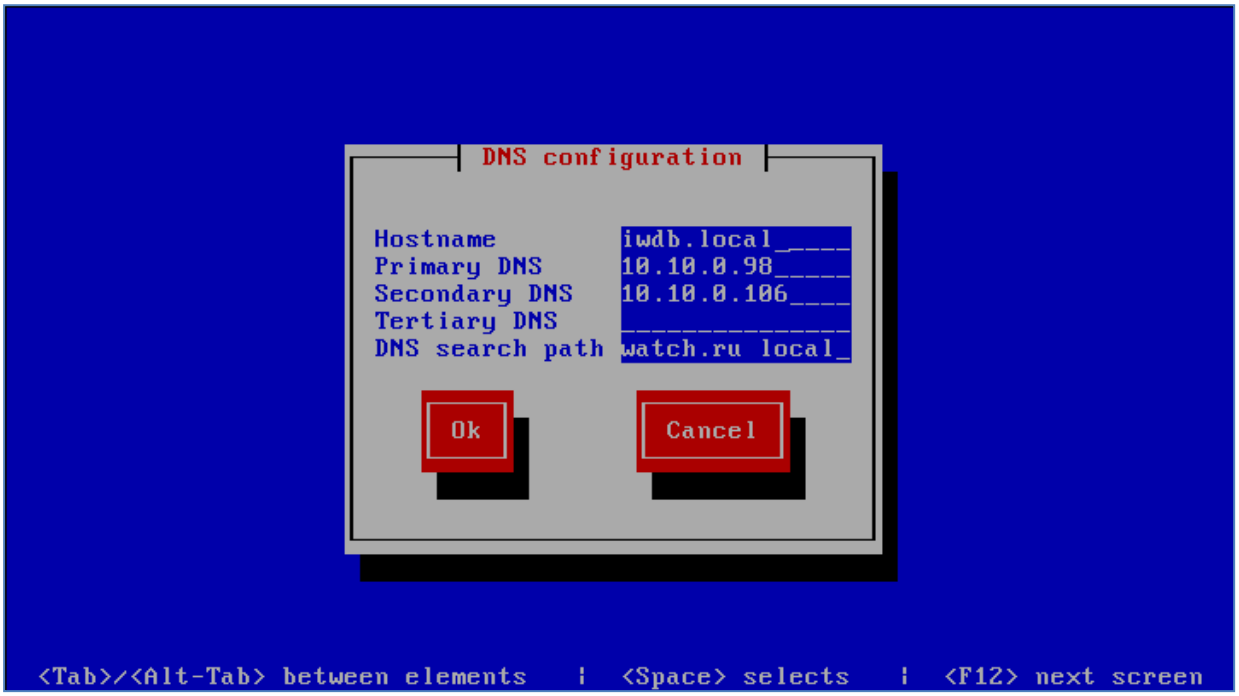
По окончании установки операционной системы будет выполнена перезагрузка и будет предложено выполнить настройку сетевых параметров.



6. Для настройки параметров сетевой карты:
   - Выберите **Device configuration**.
   - Выберите сетевой интерфейс **eth0**.
   - Убедитесь, что отмечен параметр **Use DHCP**. При необходимости, измените другие параметры, затем нажмите **OK**.
   - Нажмите **Save**, чтобы сохранить сделанные настройки.



7. Для настройки DNS конфигурации, выберите **DNS configuration** и укажите необходимые параметры сетевых настроек сервера. Затем нажмите **OK**.



8. Проверьте выполненные сетевые настройки. Если настройки некорректны, введите **N** и укажите правильные параметры (см. шаги 6 и 7). Если настройки корректны, введите **Y** для подтверждения.

```
eth0: NIC Link is Up 10000 Mbps
 done.
                                                          [  OK  ]
/etc/hosts:
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
10.60.21.30      iwdb.local iwdb

DNS configuration (/etc/resolv.conf):
; generated by /sbin/dhclient-script
search infowatch.ru local
nameserver 10.10.0.98
nameserver 10.10.0.106

IP configuration (ip addr show):
1: lo:
    inet 127.0.0.1/8 scope host lo
2: eth0:
    inet 10.60.21.30/16 brd 10.60.255.255 scope global eth0

IP ROUTE configuration (ip route show):
169.254.0.0/16 dev eth0  scope link  metric 1002
10.60.0.0/16 dev eth0  proto kernel  scope link  src 10.60.21.30
default via 10.60.0.1 dev eth0
HOSTNAME: iwdb.local
Are the network settings correct (Y/n)? _
```

9. При отдельной установке сервера Traffic Monitor (опция **IWTMX**), укажите IP-адрес сервера СУБД (**Enter IWDB ip adress**). В результате файл `$ORACLE_HOME/network/admin/tnsnames.ora` будет настроен на работу с указанным адресом.

10. Перед установкой схемы базы данных (если выбрана опция **IWDBX**, **IWALLX** или **IWTMSX**) вам будет предложено указать необходимый язык схемы (**Language for IWDB Scheme**). На этом языке будут созданы такие предустановленные сущности, как классификатор, отчеты, запросы, сценарий «по умолчанию». Для русского языка выберите **ru**.

В результате установки в системе будут созданы следующие учетные записи:

Учетная запись	**Имя**	**Пароль**
Суперпользователь OS Linux (root)	root	xxXX1234

Учетная запись	Имя	Пароль
Oracle администратор	sys	xxXX1234
	system	xxXX1234
Oracle: владелец схемы базы данных	iwtm	xxXX1234
Oracle: пользователь Linux части СУБД, от имени которого перехваченные объекты будут загружаться в базу данных	iwtm_linux	xxXX1234
Консоль управления: администратор пользователей	administrator	xxXX1234
Консоль управления: офицер безопасности	officer	xxXX1234
Пользователь Linux, от имени которого будут запускаться серверные процессы Oracle	oracle	xxXX1234
Пользователь Linux, от имени которого будут запускаться серверные процессы Traffic Monitor	iwtm	Без пароля
Группа владельца инсталляции клиента СУБД Oracle , в состав которой включены пользователи iwtm, oracle	oinstall	–

> **Важная информация!**
>
> Настоятельно рекомендуется сразу же по окончании установки сменить пароль учетных записей `root` и `oracle`.

Имя сервера (hostname) будет иметь следующий формат:

```
iwdb-xxxxxxxxxxxxxxxx.local
```

где вместо `iwdb` (тип установки – база данных) может быть `iwtm` (сервер Traffic Monitor), `iwall` (все-в-одном) или `iwts` (Traffic Monitor Standard),

а xxxxxxxxxxxxxxxx –серийный номер (Serial Number) сервера.

Для дальнейшей настройки сервера необходимо:

- Указать сервер синхронизации времени (см. п. 3.2.3.1 на стр. 39)
- Настроить отправку уведомлений от подсистемы мониторинга (см. п. 3.2.3.2 на стр. 40)
- При необходимости, установить коммерческую лицензию InfoWatch Traffic Monitor. Непосредственно после установки на сервере присутствует ознакомительная лицензия, действующая в течение 30 дней с момента установки. Подробнее о лицензиях см. п. 3.2.3.3 на стр. 40.
- Убедиться, что индикаторы мониторинга находятся в норме: все индикаторы должны находиться в состоянии **Normal**. Подробнее о подсистеме мониторинга см. документ «*InfoWatch Traffic Monitor. Руководство администратора*».
- Настроить перехватчики (см. п. 3.3 на стр. 47), необходимые для работы системы в соответствии с выбранной схемой развертывания (см. п. 2.1 на стр. 10).

3.2. Настройка сервера Traffic Monitor

В этом разделе:

- *Проверка автозапуска процессов (п. 3.2.1 на стр. 37)*
- *Кластер Traffic Monitor с одной Подсистемой Анализа (п. 3.2.2 на стр. 38)*
- *Настройка сервера через Traffic Monitor веб-интерфейс для установки «все-в-одном» (п. 3.2.3 на стр. 39)*
- *Настройки сервера Traffic Monitor для распределенной архитектуры (п. 3.2.4 на стр. 41)*
- *Установка и настройка модуля взаимодействия с удаленной базой данных (п. 3.2.5 на стр. 44)*

3.2.1. Проверка автозапуска процессов

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

Процесс	В каких случаях необходим автозапуск процесса	По умолчанию автозапуск включен
iw_smtpd	Перехват SMTP-трафика в режиме почтового релея	Да
iw_messed	Обработка SMTP-трафика в любом режиме (релей или Sniffer)	Да
iw_deliverd	Только если Система выполняет досылку заблокированного SMTP-трафика (нормальный транспортный режим)	Нет
iw_sniffer	На компьютере с установленным Sniffer	Да
iw_proxy SMTP iw_proxy HTTP iw_proxy ICQ	Обработка копии SMTP-, HTTP- и ICQ-трафика через Sniffer. Включите автозапуск только для необходимых перехватчиков	Включен для перехватчиков HTTP и ICQ
iw_icap	Перехват и обработка HTTP-трафика, передаваемого на сервер Traffic Monitor по протоколу ICAP. Процесс появляется, если установлен модуль IW ICAP	Да
iw_expressd	Прием объектов перехваченных системой InfoWatch Device Monitor Прием объектов перехваченных системой DeviceLock	Да
iw_qmover_server	В центральном офисе. Если нужно принимать объекты из филиала. Процесс появляется, если установлена серверная часть модуля взаимодействия с удаленной базой данных	Да
iw_qmover_client	В филиале. Если нужно передавать объекты на сервер Traffic Monitor центрального офиса для загрузки в базу данных. Процесс появляется, если установлена клиентская часть модуля взаимодействия с удаленной базой данных	Да
iw_dbloader iw_updater iw_warpd	Автозапуск должен быть включен при любой схеме внедрения	Да

Процесс	В каких случаях необходим автозапуск процесса	По умолчанию автозапуск включен
iw_adlibitum	Только на одном экземпляре сервера Traffic Monitor	Да

Важная информация!

Отключите автозапуск нелицензированных процессов, отвечающих за перехват трафика (**iw_smtpd**, **iw_proxy**, **iw_expressd**, **iw_icap**). Это позволит уменьшить количество сообщений в журнале протоколирования.

Чтобы включить/отключить автозапуск процесса:

1. Для корректной смены параметров остановите серверные процессы Traffic Monitor:

   ```
   service iw-trafmon stop
   ```

2. В файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[AUTO_RESTART]` выполните настройки:

   - Чтобы включить автозапуск для процесса, установите в блоке процесса:

     ```
     autorestart = On
     ```

     Пример (включение `iw_sniffer`):

     ```
     iw_sniffer:
     autorestart = On
     ```

   - Чтобы отключить автозапуск для процесса, установите в блоке процесса:

     ```
     autorestart = Off
     ```

3. Запустите процессы Traffic Monitor:

   ```
   service iw-trafmon start
   ```

3.2.2. Кластер Traffic Monitor с одной Подсистемой Анализа

Важная информация!

Сведения в данном разделе относятся только к случаю, когда используется Модуль Детектирования Цифровых Отпечатков.

Подсистема Анализа выполняет анализ текста перехваченных объектов с помощью следующих методов:

- **Лингвистический анализ**. Определение тематики текста на основании найденных терминов.
- **Детектирование текстовых объектов**. Поиск в тексте таких объектов, как номера телефонов, паспортов, кредитных карт и пр.
- **Детектирование цифровых отпечатков**. Поиск в тексте фрагментов, относящихся к конфиденциальной документации компании.

При использовании Модуля Детектирования Цифровых Отпечатков в Системе должен функционировать только один экземпляр Подсистемы Анализа.

Если в Системе имеется несколько экземпляров сервера Traffic Monitor, то необходимо настроить передачу текста на анализ со всех экземпляров сервера на общую Подсистему Анализа.

Чтобы настроить работу одной Подсистемы анализа для нескольких экземпляров Traffic Monitor:

1. На всех экземплярах сервера Traffic Monitor остановите работу Подсистемы Анализа:

   ```
   service iw-caserv stop
   ```

2. На компьютере, где будет работать Подсистема Анализа, в файле `/usr/local/infowatch/tm3/etc/tm.conf`, в секции `[CAS]`, измените адрес сервера на `0.0.0.0`:

```
ListenAddr=0.0.0.0
```

3. На других экземплярах сервера Traffic Monitor в файле `/usr/local/infowatch/tm3/etc/tm.conf`, в секции `[FILTER]`, укажите адрес и порт компьютера, где работает Подсистема Анализа.
4. На компьютере, где будет работать Подсистема Анализа, запустите эту подсистему:

```
service iw-caserv start
```

3.2.3. Настройка сервера через Traffic Monitor веб-интерфейс для установки «все-в-одном»

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** или **IWTMSX**), то администратор получает возможность упрощенного управления с помощью веб-интерфейса, доступного из браузера любой рабочей станции локальной сети.

С помощью веб-консоли после установки и настройки сервера IWTM в инфраструктуру, администратор может выполнить следующие настройки:

- Указать сервер синхронизации времени (см. п. 3.2.3.1 на стр. 39)
- Настроить отправку уведомлений от подсистемы мониторинга (см. п. 3.2.3.2 на стр. 40)
- При необходимости, установить коммерческую лицензию InfoWatch Traffic Monitor. Непосредственно после установки на сервере присутствует ознакомительная лицензия, действующая в течение 30 дней с момента установки. Подробнее о лицензиях см. п. 3.2.3.3 на стр. 40.
- Убедиться, что индикаторы мониторинга находятся в норме: все индикаторы должны находиться в состоянии  **Normal**. Подробнее о подсистеме мониторинга см. документ «*InfoWatch Traffic Monitor. Руководство администратора*».

Чтобы войти в веб-консоль:

1. В адресной строке любого браузера введите IP-адрес сервера Traffic Monitor.
2. Укажите параметры учетной записи администратора пользователей Консоли Управления Traffic Monitor (TM Management Console):
   a. В поле **Login** введите **administrator**
   b. В поле **Password** укажите **xxXX1234**

   > **Важная информация!**
   >
   > Выше указаны параметры этой учетной записи, заданные по умолчанию. Настоятельно рекомендуется после установки Консоли управления изменить пароль этой учетной записи: о том, как это сделать, см. *«InfoWatch Traffic Monitor. Руководство пользователя»*.
3. Нажмите **Authentificate**.

3.2.3.1. Настройка NTP-сервера

Основные сетевые параметры сервера InfoWatch Traffic Monitor задаются в процессе установки (см. п. 3.1 на стр. 28, шаги 6 и 7). Однако для корректной синхронизации времени на сервере 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. В веб-консоли, в области **Network**, в разделе **DNS/NTP**, нажмите  **Edit**.
2. Укажите IP-адрес NTP-сервера в поле **Primary NTP**
3. Сохраните изменения, нажав  **Save**.

> **Важная информация!**
>
> При необходимости вы можете задать параметр **Secondary NTP** в файле файле `/etc/ntp.conf`.

3.2.3.2. Настройка отправки уведомлений о превышении порога для индикаторов

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

Чтобы настроить отправку уведомлений от подсистемы мониторинга на указанные адреса администраторов системы:

1. В веб-консоли, в разделе **Monitoring settings**, нажмите **Edit**.
2. Укажите параметры отправки уведомлений:
   - **SMTP server** – адрес почтового сервера, используемого для отправки.
   - **E-Mail tag** – префикс, который будет включаться в заголовки всех писем, отправляемых подсистемой мониторинга.

     > **Примечание:**
     >
     > Для проектов на технической поддержке InfoWatch укажите **[SUP]**. Для проектов внедрения или пилотных проектов InfoWatch введите **[PRJ]**, где **PRJ** – код проекта внедрения/пилота.

   - **Notification e-mail** – адреса, на которые должны высылаться уведомления.

     > **Примечание:**
     >
     > Для проектов, находящихся на поддержке InfoWatch, желательно включить в список адрес **monitoring@infowatch.com**.

3. Сохраните изменения, нажав **Save**.
4. Проверьте корректность выполненных настроек: нажмите **Send test email**. Если параметры указаны верно, то на указанные адреса придет тестовое письмо.

3.2.3.3. Установка лицензии на перехватчики

Для работы InfoWatch Traffic Monitor требуется действующая лицензия. Ознакомительная лицензия действует в течение 30 дней с момента установки сервера Traffic Monitor. Чтобы продолжить эксплуатацию Системы, необходимо установить коммерческую лицензию на перехватчики, которые вы планируете использовать.

Текущее состояние лицензии отображается в веб-консоли администратора. В строке **License valid until**… указана дата окончания лицензии. Также в разделе **System monitoring** присутствует индикатор **TM Licence**. Если состояние индикаторов будет сигнализировать о приближении даты окончания (**Warning** – меньше 2-х недель; **Critical** – меньше 2-х дней), то администратору будут высланы уведомления на адрес, заданный как описано в п. 3.2.3.2 на стр. 40.

При установке и использовании лицензионного ключа нужно учитывать следующее:

- Если период действия ознакомительной лицензии истек, то работа перехватчиков будет остановлена. Установите коммерческую лицензию или удалите Систему (см. главу 5 на стр. 77).
- Если требуется изменить настройки передачи трафика согласно новой схеме развертывания (см. п. 2.1 на стр. 10), замените лицензионный ключ с учетом новых перехватчиков.

- Лицензионный ключ (файл `iw_license.dat`) жестко привязан к аппаратной конфигурации того компьютера, на котором был сгенерирован запрос на лицензию. Таким образом, при переносе файла `iw_license.dat` на другой компьютер функциональность InfoWatch Traffic Monitor будет недоступна. Также требуется замена лицензионного ключа после замены системной платы на компьютере с сервером Traffic Monitor.
- При полной переустановке операционной системы и/или системы InfoWatch Traffic Monitor вам потребуется заново установить лицензию. Поэтому рекомендуется сохранить файл `iw_license.dat` на каком-либо носителе информации.

Чтобы запросить лицензию:

1. В веб-консоли, в разделе **General**, нажмите **Send license renewal request**.

   В результате будет сформировано письмо в службу технической поддержки. В теле письма будет содержаться уникальный код, сгенерированный специально для данного экземпляра сервера Traffic Monitor. Не изменяйте этот код.

2. Отправьте письмо.

В сроки, установленные Service Level Agreement, вам будет выслан файл лицензионного ключа **iw_license.dat**.

Чтобы установить полученный лицензионный ключ Traffic Monitor:

1. Разместите лицензионный ключ (файл **iw_license.dat**), полученный от InfoWatch в результате запроса, на компьютере, с которого запущена веб-консоль, или на ресурсе, к которому он имеет доступ.
2. В веб-консоли, в разделе **General**, нажмите **Install license**
3. В окне открытия файла выберите файл **iw_license.dat** и нажмите **OK**.
4. Дождитесь установки лицензии (статус **Installing license…**).

В результате успешной установки дата окончания лицензии (отображается в строке **License valid until**) должна быть обновлена.

3.2.4. Настройки сервера Traffic Monitor для распределенной архитектуры

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**), администратор системы должен следующие настройки на сервере Traffic Monitor:

- *Настройка синхронизации времени (п. 3.2.4.1 на стр. 41)*
- *Настройка соединения с сервером СУБД Oracle (п. 3.2.4.2 на стр. 42)*
- *Установка лицензии на перехватчики (п. 3.2.4.3 на стр. 42)*

Подсистема мониторинга настраивается на сервере базы данных, как описано в п. 3.2.3 на стр. 39.

3.2.4.1. 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 сервис 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 NPT, воспользуйтесь командой **ntpdate -q <IP>** (IP замените на 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 (IP замените на актуальный адрес вашего NTP-сервера):

   ```
   server 10.10.0.98
   ```

7. Запустите сервис 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
   ```

10. Если вы используете Подсистему Мониторинга Traffic Monitor, не забудьте также отредактировать файл **/etc/nagios/iwmon/iwmon-services-ntp.conf**, указав IP-адрес NTP сервера (см. п. 3.4.1 на стр. 60).

3.2.4.2. Настройка соединения с сервером СУБД Oracle

Если сервер СУБД Oracle установлен отдельно от сервера Traffic Monitor (вначале устанавливался сервер с опцией **IWDBX**, затем – с опцией **IWTMX**), то для обеспечения соединения с базой данных, на сервере Traffic Monitor, в файле `$ORACLE_HOME/network/admin/tnsnames.ora` раскомментируйте и настройте параметры соединения, например:

```
IWTM =
  (DESCRIPTION =
    (ADDRESS_LIST =
     (ADDRESS = (PROTOCOL = TCP)(HOST = iwtm)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = iwtm)
    )
  )
```

где `HOST` – сетевое имя сервера СУБД Oracle, а SERVICE_NAME = iwtm – параметр, определяющий имя сервиса экземпляра базы данных.

3.2.4.3. Установка лицензии на перехватчики

Ознакомительная лицензия на перехватчики действует в течение 30 дней с момента установки сервера Traffic Monitor. Чтобы продолжить эксплуатацию Системы, установите коммерческую лицензию на перехватчики, которые вы планируете использовать.

Коммерческий лицензионный ключ представляет собой файл `iw_license.dat`, который поставляется по запросу. Для получения коммерческого лицензионного ключа вам потребуется специальный файл `iw_customer.dat`. Этот файл генерируется при помощи утилиты **iw_lickey**, входящей в состав Traffic Monitor.

При установке и использовании лицензионного ключа нужно учитывать следующее:

- Если период действия ознакомительной лицензии истек, то работа перехватчиков будет остановлена. Установите коммерческую лицензию или удалите Систему (см. главу 5 на стр. 77).
- Если требуется изменить настройки передачи трафика согласно новой схеме развертывания (см. п. 2.1 на стр. 10), замените лицензионный ключ с учетом новых перехватчиков.
- Лицензионный ключ (файл `iw_license.dat`) жестко привязан к аппаратной конфигурации того компьютера, на котором был сгенерирован запрос на лицензию (файл `iw_customer.dat`). Таким образом, при переносе файла `iw_license.dat` на другой компьютер функциональность InfoWatch Traffic Monitor будет недоступна. Также требуется замена лицензионного ключа после замены системной платы на компьютере с сервером Traffic Monitor.
- Если в Системе имеется кластер серверов Traffic Monitor, то для каждого экземпляра Traffic Monitor требуется отдельный лицензионный ключ. Например, если в Системе три экземпляра сервера Traffic Monitor, то всего должно быть сгенерировано три файла `iw_customer.dat` (по одному файлу от каждого экземпляра). Для каждого такого файла будет выслан отдельный файл `iw_license.dat`.

> **Важная информация!**
>
> Если данный экземпляр Traffic Monitor будет функционировать только как Sniffer (см. п. 2.1.3 на стр. 13, варианты 2 – 4), то установка лицензии на нем не требуется.

- При полной переустановке операционной системы и/или системы InfoWatch Traffic Monitor вам потребуется заново установить лицензию. Поэтому рекомендуется сохранить файл `iw_license.dat` на каком-либо носителе информации.

Чтобы установить новый лицензионный ключ или заменить текущий:

1. Запустите утилиту **iw_lickey**, расположенную в каталоге `/usr/local/infowatch/tm3/bin`. В результате работы данной утилиты в каталоге `/usr/local/infowatch/tm3/bin` будет создан файл `iw_customer.dat`.
2. Отправьте файл `iw_customer.dat` по электронной почте на адрес менеджера отдела продаж компании InfoWatch. После получения файла `iw_customer.dat` менеджер направит вам по электронной почте файл `iw_license.dat`.
3. Сохраните файл `iw_license.dat`, полученный от сотрудника InfoWatch, в каталог `/usr/local/infowatch/tm3/etc`. Если в каталоге уже имеется файл `iw_license.dat`, то сохраните новый файл взамен старого.

   > **Важная информация!**
   >
   > Файл с лицензионным ключом должен устанавливаться на тот же компьютер, где был сгенерирован файл `iw_customer.dat`.

   Если вы используете лицензию на перехват HTTP-трафика по протоколу ICAP, то укажите в качестве владельца файла `iw_license.dat` пользователя – владельца сервера Traffic Monitor (по умолчанию `iwtm`):

   ```
   chown iwtm:oinstall iw_license.dat
   ```

   > **Примечание:**
   >
   > Владелец сервера Traffic Monitor указан в файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[GENERAL]`, параметр `user`.

4. Чтобы новая лицензия вступила в действие, перезапустите процессы Traffic Monitor:

   ```
   service iw-trafmon restart
   ```

> **Важная информация!**
>
> Отключите автозапуск нелицензированных процессов, отвечающих за перехват трафика (**iw_smtpd**, **iw_proxy**, **iw_expressd**). Это позволит уменьшить количество сообщений в журнале протоколирования.

3.2.5. Установка и настройка модуля взаимодействия с удаленной базой данных

Если схема развертывания системы (см. п. 2.1 на стр. 10) выбрана таким образом, что объекты, перехваченные в филиале, должны передаваться в удаленную базу данных, находящуюся в центральном офисе, по медленному каналу связи, то необходимо установить модуль взаимодействия с удаленной базой данных в следующей конфигурации:

- в филиале установите клиентскую часть модуля на компьютере с сервером Traffic Monitor: см. п. 3.2.5.1 на стр. 44;
- в центральном офисе установите серверную часть модуля на компьютере с сервером Traffic Monitor: см. п. 3.2.5.2 на стр. 45).

3.2.5.1. Установка клиентской части модуля взаимодействия с удаленной БД (филиал)

Шаг 1. Установка и настройка общих параметров

1. На компьютер с сервером Traffic Monitor установите пакет `iwtm_qmover-x.x.x-x.x86_64.rpm` (где x.x.x-x номер версии InfoWatch Traffic Monitor), расположенный в папке `/opt/distr/infowatch/traffic-monitor-x.x.x-x/Linux`. Для этого от имени пользователя `root` выполните команду вида:

   ```
   rpm -i /opt/distr/infowatch/traffic-monitor-4.1.0-112/Linux/iwtm_qmover-4.1.0-112.x86_64.rpm
   ```

   Пакет будет установлен в каталог:

   ```
   /usr/local/infowatch/tm3
   ```

2. Создайте резервную копию конфигурационного файла `qmover.conf` с помощью команды:

   ```
   cp /usr/local/infowatch/tm3/etc/qmover.conf /usr/local/infowatch/tm3/etc/qmover.conf.bak
   ```

3. Запустите сценарий `qmover-setup.sh`:

   ```
   /usr/local/infowatch/tm3/qmover-setup.sh
   ```

4. Настройте параметры клиента:

   - `Select remote queue setup type?`

     Выберите `client`.

   - `Enter TM EE qmover server's IP address.`

     IP-адрес, сервера (в центральном офисе), на который клиент будет передавать перехваченные объекты. Значение по умолчанию `127.0.0.1`.

   - `Enter TM EE qmover server's port number.`

     Порт сервера, на который будут передаваться перехваченные объекты. Значение по умолчанию 16888.

5. Перезапустите Traffic Monitor:

   ```
   service iw-trafmon restart
   ```

Шаг 2. Настройка автозапуска процессов

Включите автозапуск для процесса `iw_qmover_client`. Отключите автозапуск для процессов `iw_dbloader`, `iw_deliverd` и `iw_adlibitum`.

Чтобы включить/отключить автозапуск процесса:

1. Для корректной смены параметров остановите процессы Traffic Monitor:

   ```
   service iw-trafmon stop
   ```

2. В файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[AUTO_RESTART]` выполните настройки:

   - Чтобы включить автозапуск для процесса, установите в блоке процесса:

     ```
     autorestart = On
     ```

     Пример (включение `iw_qmover_client`):

     ```
     iw_qmover_client:
     autorestart = On
     ```

   - Чтобы отключить автозапуск для процесса, установите в блоке процесса:

     ```
     autorestart = Off
     ```

3. Запустите процессы Traffic Monitor:

   ```
   service iw-trafmon start
   ```

Шаг 3. Изменение ширины полосы пропускания для канала передачи данных

По умолчанию полоса пропускания имеет ширину 128 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 в пределах от 128 Кбит/с до 2 Мбит/с включительно.

Чтобы настроить ограничения на ширину полосы пропускания,

на стороне клиента (филиал) настройте crond на запуск утилиты `iw_qmover_channel_width_setter` с нужными интервалами.

Утилита запускается с обязательными параметрами:

```
iw_qmover_channel_width_setter <полоса_пропускания>
```

где `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 /usr/local/infowatch/tm3/bin/iw_qmover_channel_width_setter 128
00 18 * * * iwtm /usr/local/infowatch/tm3/bin/iw_qmover_channel_width_setter 256
```

3.2.5.2. Установка серверной части модуля взаимодействия с удаленной БД (центральный офис)

Шаг 1. Установка

На компьютер с сервером Traffic Monitor установите пакет `iwtm_qmover-x.x.x-x.x86_64.rpm` (где `x.x.x-x` номер версии InfoWatch Traffic Monitor), расположенный в папке. `/opt/distr/infowatch/traffic-monitor-x.x.x-x/Linux`. Для этого от имени пользователя `root` выполните команду вида:

```
rpm -i /opt/distr/infowatch/traffic-monitor-4.1.0-112/Linux/ iwtm_qmover-4.1.0-112.x86_64.rpm
```

Пакет будет установлен в каталог:

```
/usr/local/infowatch/tm3
```

Шаг 2. Настройка конфигурации

1. Создайте резервную копию конфигурационного файла `qmover.conf` с помощью команды:

   ```
   cp /usr/local/infowatch/tm3/etc/qmover.conf /usr/local/infowatch/tm3/etc/qmover.conf.bak
   ```

2. Запустите сценарий `qmover-setup.sh`:

   ```
   /usr/local/infowatch/tm3/qmover-setup.sh
   ```

3. Настройте параметры сервера:

   - `Select remote queue setup type?`

     Выберите `server`.

   - `Enter TM EE qmover server's port number.`

     Укажите порт, на котором сервер прослушивает объекты, поступающие от клиентов (из филиалов). Значение по умолчанию `16888`.

   - `Enter number of clients.`

     Укажите число клиентов, от которых сервер будет принимать объекты.

   - `Please enter IP address of client N.`

     Укажите IP-адрес клиента N. Значение по умолчанию `127.0.0.1`. Для каждого клиента выводится отдельный запрос.

     В результате будет создан конфигурационный файл `/usr/local/infowatch/tm3/etc/qmover.conf` с указанными параметрами.

Важная информация!

При изменении параметров филиалов (изменение количества филиалов или их IP-адресов) следует:

- либо восстановить резервную копию файла `qmover.conf`, а затем запустить сценарий `qmover-setup.sh` с новыми параметрами; восстановление резервной копии производится с помощью команды:

  ```
  cp /usr/local/infowatch/tm3/etc/qmover.conf.bak /usr/local/infowatch/tm3/etc/qmover.conf
  ```

- либо вручную внести изменения в файл `qmover.conf`.

Шаг 3. Настройка автозапуска

Настройте автозапуск для процесса `iw_qmover_server`:

1. Для корректной смены параметров остановите серверные процессы Traffic Monitor:

   ```
   service iw-trafmon stop
   ```

2. В файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[AUTO_RESTART]` в блоке процесса `iw_qmover_server` установите: `autorestart = On`:

3. Запустите процессы Traffic Monitor:

   ```
   service iw-trafmon start
   ```

Шаг 4. Создание разных очередей для клиентов

По умолчанию объекты от всех клиентов (филиалы) загружаются в общую очередь `/usr/local/infowatch/tm3/queue/db`. В эту же очередь загружаются объекты, перехваченные в локальной сети центрального офиса (т.е. из сети на стороне базы данных).

С целью повышения надежности приема объектов необходимо создать отдельную очередь для каждого клиента. Настройка очередей выполняется на сервере в центральном офисе.

Чтобы создать отдельную очередь для приема объектов от клиента,

1. Откройте файл `/usr/local/infowatch/tm3/etc/qmover.conf`.
2. В секции `[client_N]` (N – порядковый номер клиента) измените значение параметра `QueuePath`, указав полный путь к директории, в которой нужно разместить очередь. Очередь будет создана в указанном месте при первом соединении сервера с клиентом.

   Повторяйте п. 2, пока не будут заданы очереди для каждого клиента.

   > **Важная информация!**
   >
   > Очереди от всех клиентов должны размещаться на одном разделе жесткого диска.

3. Для очереди каждого клиента задайте параметры перемещения объектов в основную очередь. Запустите утилиту `iw_qtool` с параметрами:

   ```
   iw_qtool move <очередь-источник> <очередь-приемник>
   ```

   Здесь:

   - `очередь-источник` – полный путь к директории с очередью клиента N (должен совпадать со значением `QueuePath` в секции `[client_N]`).
   - `очередь-приемник` – полный путь к основной очереди сервера (по умолчанию используется `queue/db`).

   Например:

   ```
   iw_qtool move /u01/client_1 /usr/local/infowatch/tm3/queue/db
   ```

4. Настройте в crond автоматический запуск утилиты `iw_qtool` с требуемой периодичностью.

3.3. Настройки перехватчиков

В данном разделе описан порядок и примеры настройки перехватчиков для различных схем развертывания Системы:

Схема развертывания	Настройка перехватчиков	Ссылка на раздел
Прием копии SMTP-трафика с почтового сервера (п. 2.1.1 на стр. 10)	Настройка пересылки скрытых копий	п. 3.3.1 на стр. 48
Перехват SMTP-трафика посредством интеграции с Postfix (см. п. 2.1.2 на стр. 12) Также рекомендуется при получении Системой копии SMTP-трафика (см. п. 2.1.1 на стр. 10)	Настройка параметров интеграции с Postfix	п. 3.3.2 на стр. 49
Прием копии трафика при помощи Sniffer (п. 2.1.3 на стр. 13)	Настройка Sniffer	п. 3.3.3 на стр. 51
	Настройка параметров кластеризации для серверов Traffic Monitor, входящих в кластер	

Прием HTTP-трафика, передаваемого по протоколу ICAP (п. 2.1.4 на стр. 17)	Настройка ICAP	п. 3.3.4 на стр. 53
Проверка файлов, находящихся в корпоративной сети (п. 2.1.7 на стр. 22)	Установка и настройка Crawler	п. 3.3.5 на стр. 55

3.3.1. Настройка пересылки скрытых копий

> **Важная информация!**
>
> В данном разделе приведена инструкция по настройке пересылки скрытых копий SMTP-сообщений (BCC – Blind Carbon Copy) на сервер Traffic Monitor (см. п. 2.1.1 на стр. 10) 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. Для этого выполните перечисленные ниже действия.

Шаг 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**. Затем нажмите **Next**.
3. На шаге **Address space** создайте новое адресное пространство для перенаправления трафика. Для этого нажмите **Add**. В открывшемся диалоговом окне укажите параметры адресного пространства и нажмите **OK**. Затем нажмите **Next**.
4. На шаге **Network Settings** выберите **Route mail through the following smart hosts** и нажмите **Add**. В открывшемся диалоговом окне укажите IP-адрес сервера TM, на который необходимо перенаправлять почту, и нажмите **OK**. Затем нажмите **Next**.
5. На шаге **Configure smart host authentication settings** выберите **None** – по умолчанию Postfix на сервере TM не требует авторизации. Нажмите **Next**.
6. На шаге **Source Server** выберите сервер, на котором будет работать этот коннектор. Нажмите **Next**.
7. На шаге **New Connector** убедитесь, что параметры коннектора заданы верно, и нажмите **New**. Затем дождитесь окончания процесса создания и нажмите **Finish**.

   Окно мастера создания коннектора будет закрыто.

Шаг 2. Создание контакта, на который будет производиться перенаправление копий 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 будет производиться перенаправление копий почтовых сообщений.

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

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

   Окно мастера создания контакта будет закрыто.

Шаг 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**. Затем 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 раскрывшемся окне **Select Recepient** выберите ранее созданный контакт, затем нажмите **OK**. В окне мастера создания транспортного правила нажмите **Next**.
5. При необходимости, на шаге **Exceptions** вы можете настроить исключения из правила. Например, чтобы не копировалась почта от отдельных пользователей, вы можете установить флажок для исключения **except when the message is from people** и в параметрах исключения выбрать необходимых пользователей. Нажмите **Next**.
6. На шаге **Create Rule** убедитесь, что параметры правила заданы верно, и нажмите **New**. Затем дождитесь окончания процесса создания и нажмите **Finish**.

3.3.2. Интеграция Postfix и сервера Traffic Monitor

Необходимость интеграции с Postfix определяется в зависимости от схемы развертывания Системы и от того, установлен ли сервер ТМ один компьютер с БД или нет:

<table>
<tr><th colspan="2">Вариант развертывания Системы</th><th>Интеграция с Postfix</th></tr>
<tr><td rowspan="2">Доставка SMTP-трафика осуществляется корпоративной почтовой системой. Система получает только копию SMTP-трафика. Для корректного приема копии трафика рекомендуется интеграция с Postfix (см. п. 2.1.1 на стр. 10)</td><td>Сервер ТМ установлен отдельно от базы данных (ключ кикстарта IWTM)</td><td>Обязательна</td></tr>
<tr><td>Все компоненты установлены на один сервер (ключ кикстарта IWALL или IWTMS)</td><td>Выполнена по умолчанию</td></tr>
<tr><td rowspan="2">Система осуществляет перехват и доставку SMTP-трафика посредством интеграции с Postfix (см. п. 2.1.2 на стр. 12)</td><td>Сервер ТМ установлен отдельно от базы данных (ключ кикстарта IWTM)</td><td>Обязательна</td></tr>
<tr><td>Все компоненты установлены на один сервер (ключ кикстарта IWALL или IWTMS)</td><td>Выполнена по умолчанию</td></tr>
<tr><td colspan="2">Система получает копию SMTP-трафика через Sniffer (см. п. 2.1.3 на стр. 13)</td><td>Не требуется</td></tr>
<tr><td colspan="2">Перехват SMTP-трафика не требуется (например, Traffic Monitor будет использоваться только как Sniffer)</td><td>Не требуется</td></tr>
</table>

Интеграция сервера Traffic Monitor с почтовым сервером Postfix реализуется следующим образом. Postfix принимает входящие SMTP-письма на **25** порт. Далее входящие SMTP-письма передаются процессу **iw_smtpd** на порт **2025**. Traffic Monitor анализирует полученные SMTP-письма. После анализа процесс **iw_messed** передает письма, доставка которых разрешена, на порт **2020** почтового сервера Postfix (см. рис. 16). Почтовый сервер Postfix либо напрямую доставляет письма адресатам, либо передает их следующему почтовому relay-серверу.



Рисунок 16. Интеграция с Postfix

Важная информация!

В схеме развертывания, использующей сервер Traffic Monitor в качестве relay-сервера, другие почтовые сервера (Microsoft Exchange и пр.), функционирующие в корпоративной почтовой системе, должны быть настроены на отправку исходящих сообщений на сервер Postfix.

Для корректного взаимодействия системы InfoWatch Traffic Monitor с 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/start.html.

3. Если InfoWatch Traffic Monitor будет участвовать в доставке SMTP-трафика (п. 2.1.2 на стр. 12 - подключение «в разрыв»):

   - в файле `main.cf` задайте параметр `relayhost`. В качестве значения введите IP-адрес корпоративного почтового сервера, которому SMTP-письма будет передаваться после анализа в Traffic Monitor.
   - в файле `master.cf` в конец файла допишите 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>
   ```

4. В файле `main.cf` проверьте, что в параметре `mynetworks` корректно указана подсеть, где расположены сервера exchange.

5. 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.

6. Проверьте корректность синтаксиса файлов конфигурации:

   ```
   service postfix check
   ```

7. Перезапустите Postfix:

   ```
   service postfix restart
   ```

3.3.3. Настройка Sniffer

Sniffer устанавливается вместе с сервером Traffic Monitor, но при некоторых схемах развертывания (см. п. 2.1.3 на стр. 13, варианты 2 – 4) требуется отдельная установка сервера Traffic Monitor, функционирующего только как Sniffer. Аппаратно-программные требования к компьютерам, куда выполняется установка Sniffer, приведены в п. 2.2.1 на стр. 25.

В этом разделе:

- *Настройка работы сервера Traffic Monitor в качестве Sniffer (п. 3.3.3.1 на стр. 51).*
- *Настройка сервера Traffic Monitor на прием копии трафика от Sniffer (п. 3.3.3.2 на стр. 52).*
- *Создание кластера Traffic Monitor (п. 3.3.3.3 на стр. 52).*

3.3.3.1. 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 iw-trafmon stop
   ```

2. В файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[AUTO_RESTART]`, 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:

     ```
     iw_sniffer:
         autorestart = On
     ```

     b. Отключите автозапуск других процессов: `autorestart = Off`.

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

     a. Включите автозапуск процессов `iw_sniffer`. `iw_dbloader`, `iw_updater`, `iw_warpd` и `iw_adlibitum`. Также включите автозапуск для нужных перехватчиков трафика: `iw_proxy ICQ`, `iw_proxy HTTP`, `iw_proxy SMTP`:

     ```
     autorestart = On
     ```

     b. Отключите автозапуск других процессов: `autorestart = Off`.

3. В файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[SNIFFER]`, задайте параметры перехвата трафика:

   - `Host`. IP-адрес, на который нужно принимать входящие соединения.

- `Port`. Порт, через который нужно принимать входящие соединения

4. Запустите процессы Traffic Monitor:

```
service iw-trafmon start
```

3.3.3.2. Настройка сервера Traffic Monitor на прием копии трафика от Sniffer

Настройка выполняется на компьютере с сервером Traffic Monitor. Настройка необходима и в том случае, когда Sniffer и сервер Traffic Monitor установлены на одном компьютере.

В конфигурационном файле `/usr/local/infowatch/tm3/etc/tm.conf`, выполните настройки:

- В секциях `[PROXY_SMTP]`, `[PROXY_HTTP]`, `[PROXY_ICQ]` задайте параметры для используемых перехватчиков: `SnifferHost` (IP-адрес Sniffer) и `SnifferPort` (порт, через который Sniffer принимает входящие соединения)
- В секциях `[SMTP]`, `[HTTP]`, `[ICQ]` задайте параметры:

Параметр	Пояснения
`Interface`	Сетевой интерфейс, через который будут поступать данные от коммутатора. Допускаются следующие варианты: • каждому перехватчику назначается отдельный сетевой интерфейс; • всем перехватчикам назначается один сетевой интерфейс
`OpenTimeout`	Время сохранения соединения (в сек) при отсутствии пакетов. Рекомендуемое значение – `600`.
`LiveTimeout`	Время ожидания (сек), в течение которого соединение должно перейти в состояние *ESTABLISHED*. Если состояние не изменилось, то соединение автоматически прекращается. Рекомендуемое значение – `86400`
`CloseTimeout`	Время сохранения соединения (в сек) при переходе в состояние *TIME_WAIT*. Рекомендуемое значение – `300`
`QueueMemorySize`	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`.

- В секции `[PROXY_HTTP]` установите значение `Off` для параметра `SkipNegotiate`.
- Если необходимо перехватывать ICQ-трафик, передаваемый через прокси-сервер (поверх HTTP), то в секции `[PROXY_HTTP]` установите `On` для параметра `IcqFilter`.

3.3.3.3. Создание кластера Traffic Monitor

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

> **Важная информация!**
>
> Один кластер может содержать до двух экземпляров сервера Traffic Monitor. Не рекомендуется использовать более 3-х кластеров.
>
> При использовании кластера сетевое соединение между Sniffer и сервером Traffic Monitor должно обеспечивать скорость передачи в два раза превышающую 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 `/usr/local/infowatch/tm3/etc/tm.conf` задайте параметры кластеризации:

1. В секциях `[PROXY_SMTP]`, `[PROXY_HTTP]`, `[PROXY_ICQ]` для каждого используемого перехватчика укажите значение параметра `ClusterID`.
2. В секциях `[SMTP]`, `[HTTP]`, `[ICQ]` для каждого используемого перехватчика укажите значение типа балансировки - параметр `Balancer`. Возможные значения:
   - `Connection`. Для каждого нового TCP-соединения выбирается экземпляр Traffic Monitor Server с `iw_proxy`. Таким образом, поочередно задействуются все экземпляры сервера Traffic Monitor.
   - `SrcIp`. 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.

   Вариант `SrcIp` необходимо указать для перехватчика `PROXY_HTTP`, если нужен перехват ICQ-сообщений, передаваемых через прокси-сервер (поверх HTTP). В остальных случаях рекомендуется вариант `Connection`

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. 17).

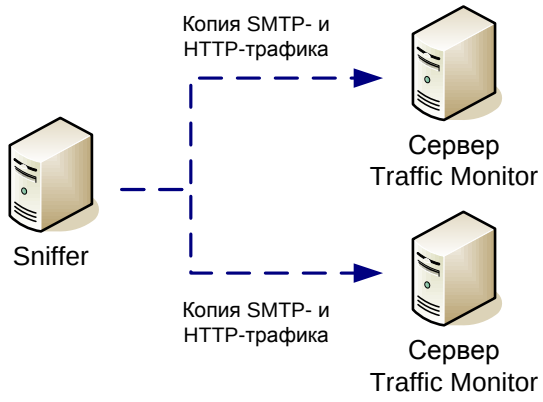


Рисунок 17. Создание кластера из двух серверов Traffic Monitor

Для создания кластера на каждом экземпляре сервера Traffic Monitor нужно выполнить следующие настройки в файле `/usr/local/infowatch/tm3/etc/tm.conf`:

- Секция `[SMTP]`:

  ```
  Balancer = Connection
  ```

- Секция `[HTTP]`:

  ```
  Balancer = Connection
  ```

- Секция `[PROXY_SMTP]`:

  ```
  SnifferClusterID = smtp
  ```

- Секция `[PROXY_HTTP]`:

  ```
  SnifferClusterID = http
  ```

3.3.4. Настройка ICAP

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

Для обеспечения перехвата HTTP-трафика, передаваемого по протоколу ICAP (см. п. 2.1.4 на стр. 17) необходимо настроить параметры перехвата HTTP-запросов на прокси-сервере.

Важная информация!

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.

Также в разделе:

- *Рекомендации по настройке ICAP для Blue Coat SG Series (п. 3.3.4.1 на стр. 54)*
- *Рекомендации по настройке SQUID (п. 3.3.4.2 на стр. 54)*

3.3.4.1. 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, под учетной записью администратора.

Примечания:

Процедура настройки, которая приводится далее, 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**.

     Важная информация!

     Значение поля **Plain ICAP port** должно совпадать со значением параметра `ListenPort` в файле `/usr/local/infowatch/tm3/etc/icap.conf`, секция `[ICAP]`. Если параметр `ListenPort` имеет другое значение, то откорректируйте его.
   - На панели **ICAP v1.0 Options** настройте параметры:
     - **Method supported**: выберите **request modification**
     - **Send**: установите флажки **Authenticated User**, **Client address** и **Server address**.
3. Перейдите в раздел **Health Checks ► General**. Убедитесь, что включена проверка состояния для серверов – на вкладке **Health Checks** отображаются адреса:

   `icap.tm`
4. Проверьте доступность всех перечисленных серверов, нажав кнопку **Perform health check**.

3.3.4.2. Рекомендации по настройке SQUID

В настройках прокси-сервера задайте следующие параметры:

- разрешите использование ICAP;

- обязательно установите режим работы ICAP-сервера: 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 этот модуль.

Пример настройки ICAP для SQUID 3.1.7

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 (по умолчанию – 1344).

3.3.5. Установка и настройка Crawler

Перехватчик Crawler 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.

Для установки обоих компонентов подсистемы Crawler (сервер и сканер) используется единый дистрибутив.

> **Важная информация!**
>
> С одной схемой БД Traffic Monitor может успешно работать **только один** экземпляр сервера Crawler. Один сервер Crawler в текущей реализации Системы может поддерживать **только один** экземпляр сканера Crawler.

Требования к аппаратному и программному обеспечению компьютеров, на которые будет выполняться установка компонент, перечислены в п. 2.2.3 на стр. 26.

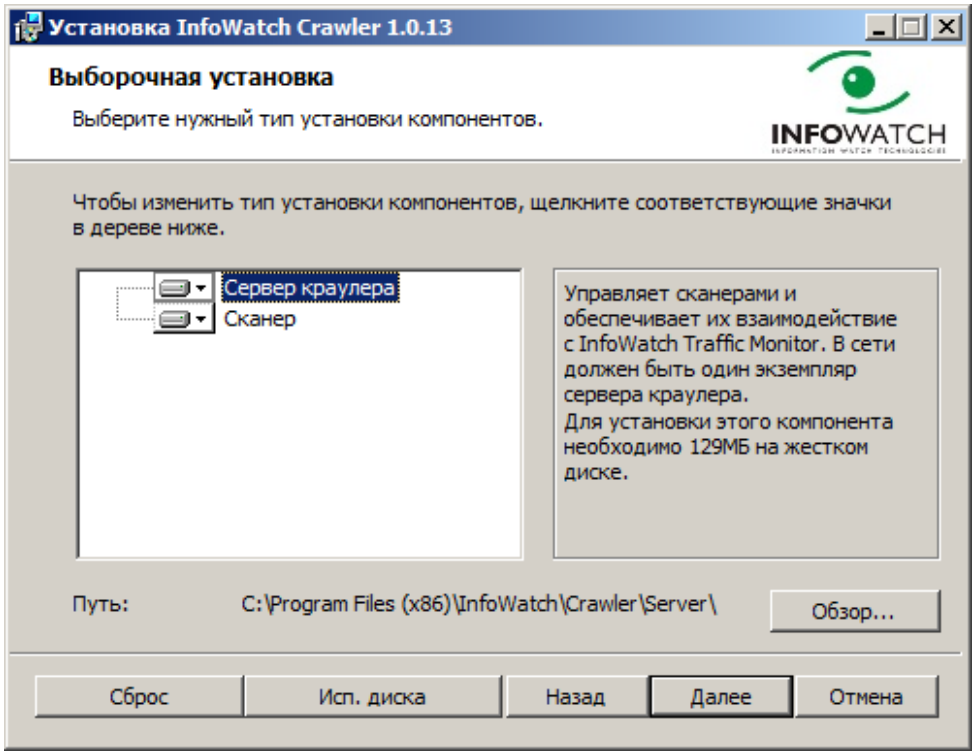
Более подробная информация об установке и настройке Crawler изложена в следующих разделах:

- *Установка сервера и сканера Crawler (п. 3.3.5.1 на стр. 55)*
- *Настройка сетевых правил доступа (п. 3.3.5.2 на стр. 58)*

3.3.5.1. Установка сервера и сканера Crawler

Чтобы установить Crawler:

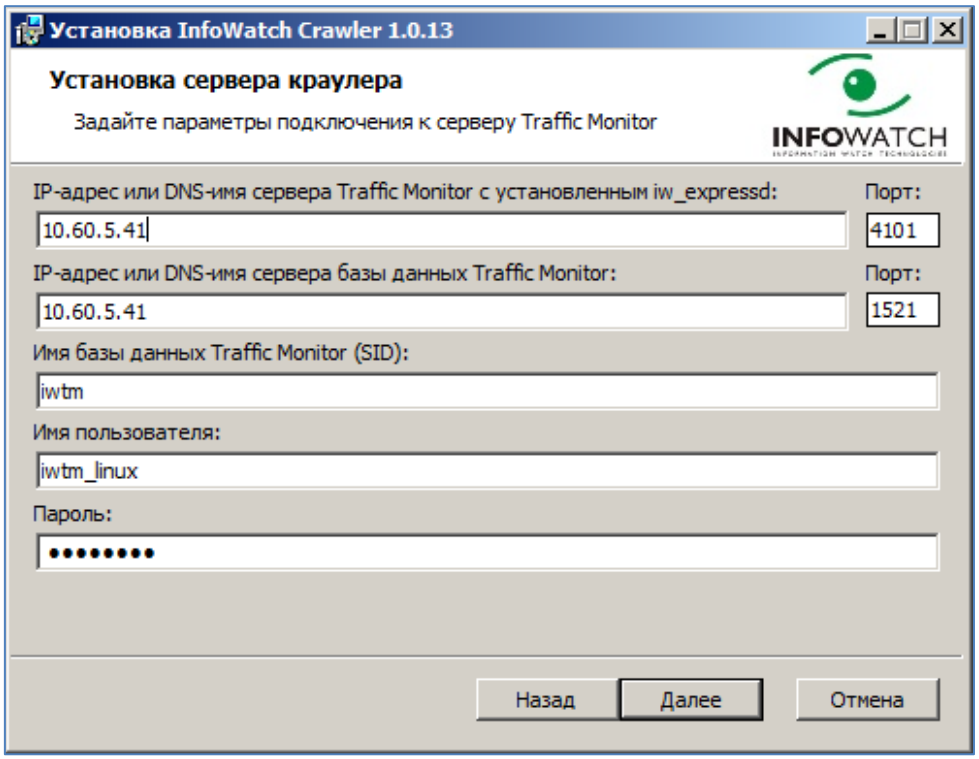
1. Запустите установочный пакет `Crawler_vx.x.x.xxx.msi`, где `x.x.x.xxx` – номер версии.
2. В окне приветствия мастера установки InfoWatch Crawler нажмите **Далее**.
3. На шаге **Выборочная установка** определите, какие компоненты Crawler нужно установить и в какую директорию:
   - **Сервер краулера** – установка службы `InfoWatch.Crawler.Server`, управляющей заданиями сканирования и обеспечивающей взаимодействие с сервером, базой данных и Консолью управления Traffic Monitor.
   - **Сканер** – установка службы `InfoWatch.Crawler.Scaner`, осуществляющей сканирование сетевых папок и файловых хранилищ согласно заданным пользователем параметрам.



Если какой-либо из компонент вам не нужно устанавливать, выберите его и в раскрывшемся списке выберите пункт ✕ **Этот компонент будет полностью недоступен**.

Укажите путь к каталогам, куда будут установлены компоненты, и нажмите **Далее**.

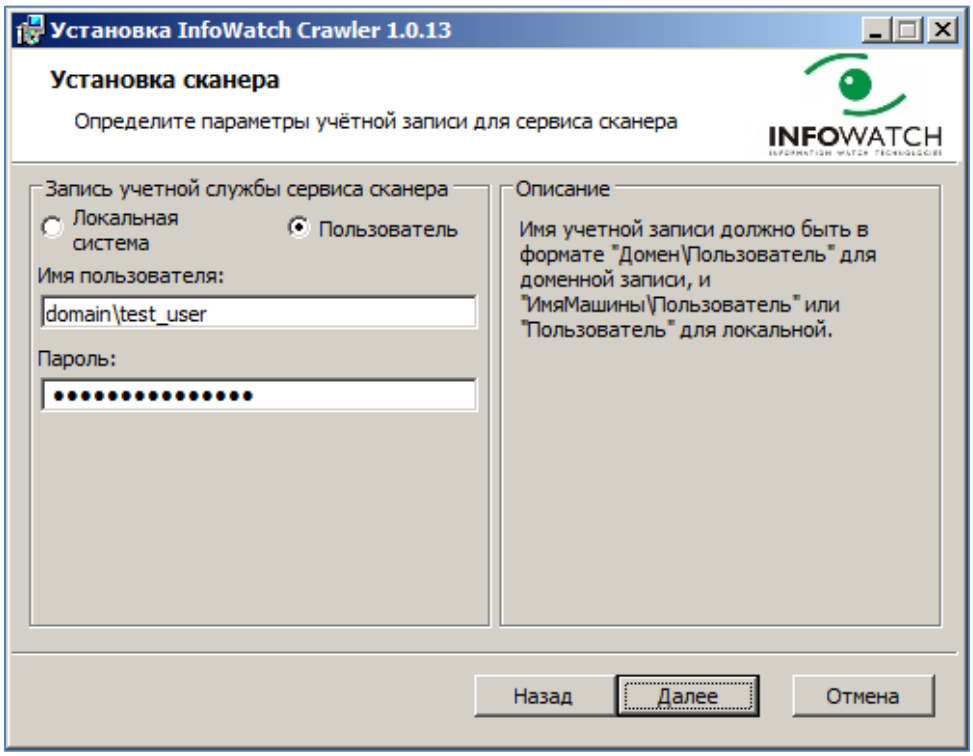
4. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сервер краулера**, укажите параметры соединения службы `InfoWatch.Crawler.Server` с сервером Traffic Monitor.



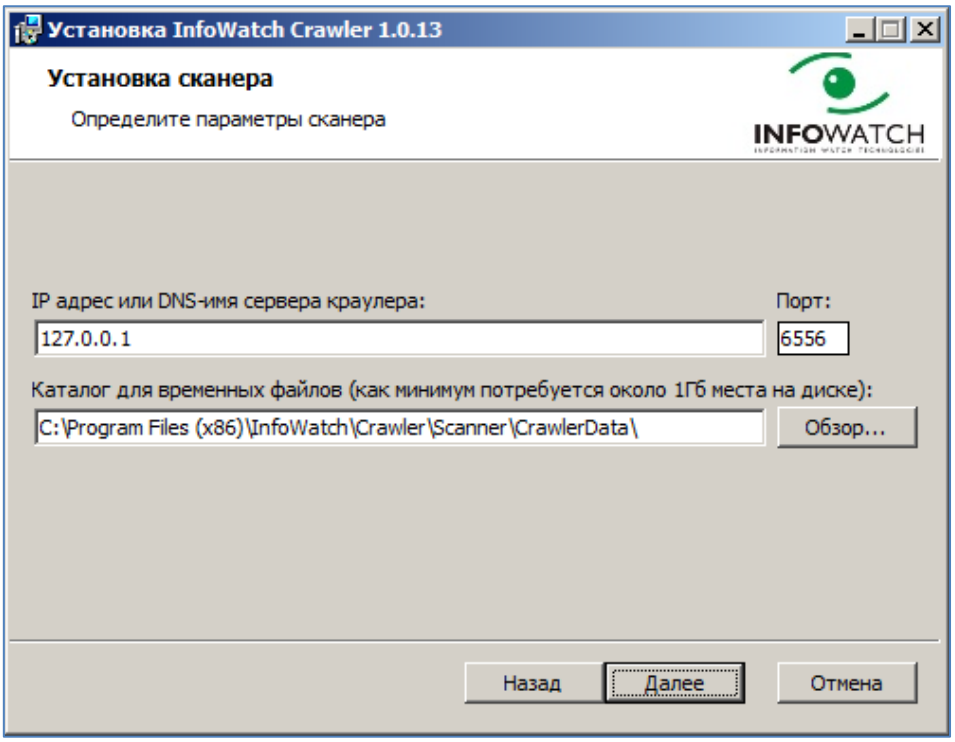
Важная информация!

Имя пользователя должно совпадать с именем учетной записи Oracle, используемой для работы Linux-части IWTM (`iw_adlibitum`, `iw_dbloader`, `iw_updater`). При установке из kickstart с параметрами по умолчанию, это **iwtm_linux**.

5. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сканер**, укажите, от имени какой учетной записи будет запускаться служба `InfoWatch.Crawler.Scaner`. Вы можете выбрать стандартную учетную запись Local System (рекомендуется) или ввести параметры учетной записи, имеющей право на выполнение служб в фоновом режиме (настройка данной возможности выполняется в меню **Панель управления –> Администрирование –> Локальная политика безопасности –> Локальные политики –> Назначение прав пользователя –> Вход в качестве службы**).



6. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сканер**, укажите:
   - IP адрес или DNS имя компьютера, куда установлен компонент **Сервер**;
   - номер порта сервера Crawler;
   - путь к директории, куда сканер будет временно сохранять файлы, скопированные с проверяемых ресурсов.



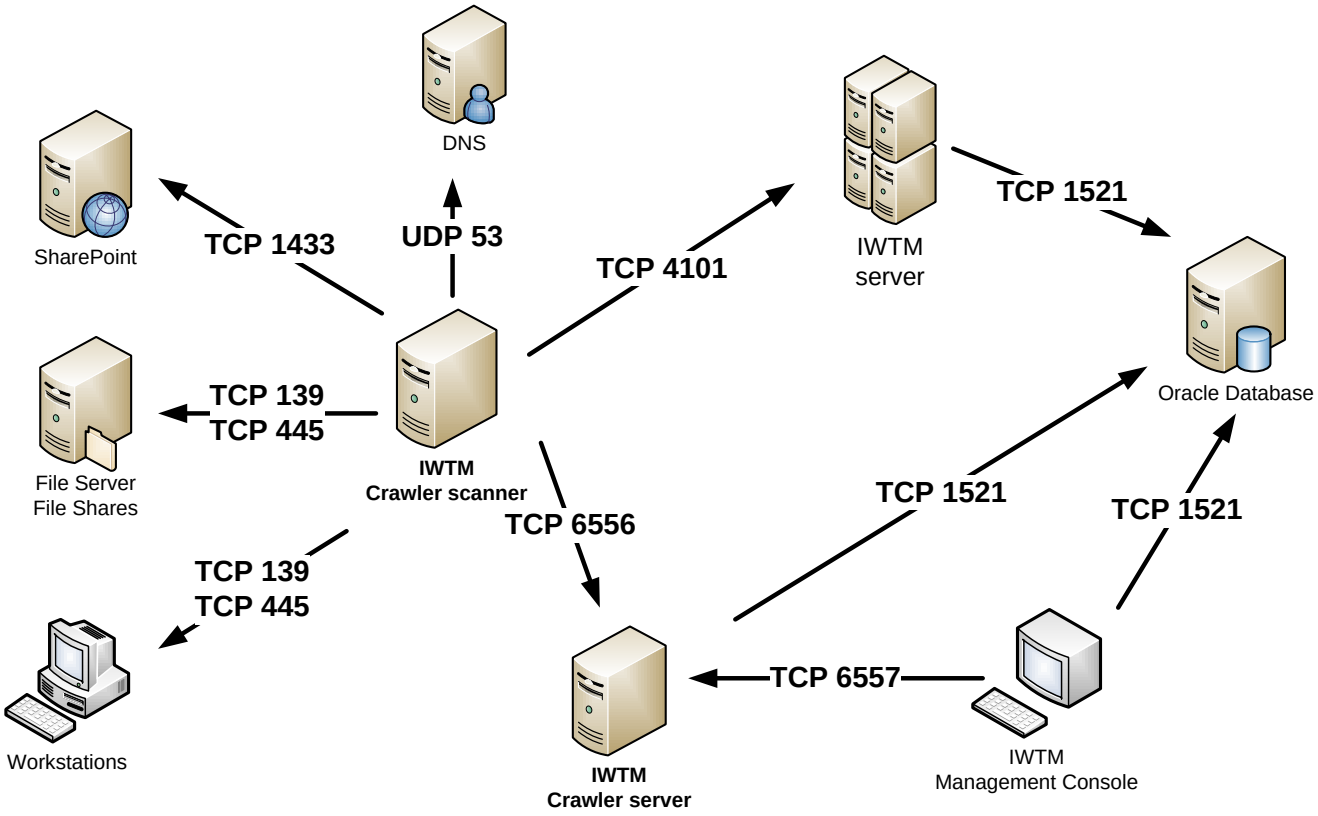
Нажмите **Далее**.

Нажмите **Установить**, чтобы начать установку Crawler. По окончании установки нажмите **Готово**.

3.3.5.2. 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 **6557** (подключение Консоли управления InfoWatch Traffic Monitor к серверу Crawler).

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



Подключение	Порт	Комментарии
Сканер Crawler – сервер Crawler	TCP 6556	
Сервер Crawler – БД IWTM	TCP 1521	
Консоль управления – сервер Crawler	TCP 6557	
Сканер Crawler – DNS сервер	UDP 53	
Сканер Crawler – рабочие станции и файловые сервера	TCP 139 TCP 445	
Сканер Crawler – сервер IWTM	TCP 4101	Настраивается в конфигурационном файле сервера IWTM `tm.conf`, секция `[EXPRESSD]`, параметр `ListenPort`
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 должна 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 будут подлежать сканированию.

3.4. Настройка подсистемы мониторинга для распределенной архитектуры

Подсистема мониторинга InfoWatch Traffic Monitor реализована на базе приложения Nagios, обеспечивающего удаленный мониторинг состояния хостов и сетевых служб.

Если вы выполнили установку системы InfoWatch Traffic Monitor так, что все серверные компоненты (сервер базы данных, сервера TM) расположены на одном компьютере (то есть программа-инсталлятор kickstart запускалась с опцией **IWALLX** или **IWTMSX**), то все основные настройки подсистемы мониторинга уже выполнены, а отправку уведомлений от подсистемы можно настроить с помощью веб-интерфейса: подробнее см. п. 3.2.3.2 на стр. 40.

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 сервере базы данных. Чтобы выполнялась диагностика всех серверов, входящих в решение, необходимо выполнить ряд дополнительных настроек:

- *Настройка адреса сервера синхронизации времени (п. 3.4.1 на стр. 60)*
- *Настройка соединения с серверами (п. 3.4.2 на стр. 60)*
- *Настройка порогов срабатывания для индикатора нагрузки (п. 3.4.3 на стр. 63)*
- *Настройка запуска служб (п. 3.4.4 на стр. 63)*
- *Настройка механизма уведомлений (п. 3.4.5 на стр. 63)*

3.4.1. 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).

3.4.2. 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.

> **Важная информация!**
>
> 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.

Важная информация!

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;
- DM-servers – сервера InfoWatch Device Monitor (не обязательный параметр; по умолчанию отключен).

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.

3.4.3. Настройка порогов срабатывания для индикатора нагрузки

В файле `/etc/nagios/iwmon/iwmon-services-loadavg.cfg` для индикатора (сервиса) `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.

3.4.4. Настройка запуска служб

Запустите службы nagios и apache для веб-интерфейса:

```
service nagios start
service httpd start
```

Настройте автозапуск служб apache и nagios:

```
chkconfig httpd on
chkconfig nagios on
```

3.4.5. Настройка механизма уведомлений

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

В разделе:

- *Настройка отправки уведомлений о превышении порога для индикаторов (п. 3.4.5.1 на стр. 63)*
- *Настройка отправки писем-уведомлений с помощью Postfix (п. 3.2.3.2 на стр. 40)*

3.4.5.1. Настройка отправки уведомлений о превышении порога для индикаторов

Чтобы настроить отправку почтовых уведомлений:

1. В `$HOME` пользователя `nagios` (`/var/log/nagios`) создайте файл `.forward`.
2. В созданном файле `.forward` перечислите e-mail адреса, на которые требуется отправлять уведомления. Адреса указываются по одному на строке.

   Важная информация!

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

3. Определите имя, которое будет указываться в поле «*From:*» в письмах с уведомлениями. Для этого в файле `/etc/passwd` для пользователя `nagios` укажите в поле `gecos` название системы.

   Важная информация!

   Для проектов, находящихся на поддержке InfoWatch, адрес отправителя должен иметь следующий формат:

   ```
   [PRJ]<nagios@example.com>
   ```

   где `PRJ` – код проекта, а `example.com` – используемый вами почтовый домен.

4. С учетом конфигурации вашей локальной сети настройте отправку писем с сервера, где установлена подсистема мониторинга, на адреса, перечисленные в файле `.forward`.

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.

3.4.5.2. Настройка отправки писем-уведомлений с помощью Postfix

Если Система установлена так, что:

- отправка SMTP-писем выполняется с использованием Postfix (см. «*InfoWatch Traffic Monitor. Руководство по установке 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.

   > **Важная информация!**
   >
   > 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
   ```

3.5. Установка Консоли управления

Установочный файл Консоли Управления Traffic Monitor (`setup.exe`) расположен на диске с дистрибутивом Системы, в каталоге `Setup.Gui.Ru`.

Вы также может скачать установочный файл с сервера Traffic Monitor через веб-консоль мониторинга. Чтобы войти в веб-консоль, в адресной строке любого браузера введите IP-адрес сервера Traffic Monitor. Чтобы загрузить дистрибутив Консоли Управления, в веб-консоли, в разделе **General**, нажмите **Download Management Console**.

Чтобы загрузить платформу .Net Framework, требуемую для работы Консоли Управления, в веб-консоли, в разделе **General**, нажмите **.NET Framework**.

Шаг 1. Запуск мастера установки

На рабочей станции, куда вы хотите установить Консоль управления, запустите файл `setup.exe`.

В результате на экран будет выведено окно приветствия мастера установки **"InfoWatch Traffic Monitor Management Console"**. Нажмите кнопку **Далее**.

Шаг 2. Принятие лицензионного соглашения

Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, выберите вариант **Принимаю** и нажмите кнопку **Далее**.

Шаг 3. Выбор каталога для установки

Путь к каталогу, в который будет установлена Консоль управления, задан в поле ввода **Папка**.

Выберите один из вариантов создания ярлыка:

- **для всех**. Ярлык создается для каждого пользователя, зарегистрированного на данном компьютере.
- **только для меня**. Ярлык будет создан только для того пользователя, который выполнял установку.

Нажмите кнопку **Далее**.

Шаг 4. Завершение работы мастера установки

После перехода к окну **Подтверждение установки**, нажмите кнопку **Далее**, чтобы начать установку.

Следуйте дальнейшим указаниям мастера, чтобы завершить установку консоли управления.

Шаг 5. Дополнительные настройки для отправки рапортов

Пользователи, выполняющие анализ объектов в консоли управления, могут направлять рапорты с комментариями по объектам. Для поддержки этой функции на всех компьютерах с установленной консолью управления, которые будут использоваться для отправки рапортов, необходимо внести изменения в настройки операционной системы. Для этого откройте **Панель управления** (**Пуск ► Настройки ► Панель управления**). Затем выберите компонент **Язык и региональные стандарты**. В открывшемся диалоговом окне перейдите на вкладку **Дополнительно** и выберите русский язык для программ, не поддерживающих Юникод.

Шаг 6. Настройка поддержки национальных кодировок и установок времени

Для поддержки национальных кодировок и установок времени укажите в системном реестре значение переменной окружения `NLS_LANG` равным `RUSSIAN_CIS.AL32UTF8`.

Путь к ключу реестра:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\KEY_OraClient11g_home#\NLS_LANG
```

где символ «`#`» означает некоторую цифру. Для `KEY_OraClient11g_home#` значение символа «`#`» будет совпадать со значением этого же символа для каталога `OraHome_#`.

> **Важная информация!**
>
> Если ключ реестра отсутствует по указанному пути, то при работе с национальными кодировками и установками времени (например, при определении настроек дней недели) будут использоваться параметры сервера СУБД Oracle.

3.6. Настройка параметров анализа объектов

Важная информация!

Первоначальная настройка конфигурации может выполняться от имени предустановленной учетной записи офицера безопасности (эта учетная запись создается вместе со схемой базы данных: см. п. 3.1 на стр. 28) или от имени другого пользователя, обладающего необходимыми привилегиями (подробнее см. документ «*InfoWatch Traffic Monitor. Руководство пользователя*»).

Запустите Консоль управления, подключитесь базе данных Traffic Monitor и настройте параметры анализа и обработки объектов:

1. Для поддержки анализа текста перехваченных объектов выполните следующие настройки:
   - Для лингвистического анализа загрузите или составьте классификатор. Система InfoWatch Автолингвист позволяет на основе коллекции текстов автоматически создавать совокупность категорий и терминов. Подробную информацию см. в документе «*InfoWatch Автолингвист. Руководство пользователя*».
   - Для детектирования текстовых объектов настройте список текстовых объектов.
   - Для детектирования цифровых отпечатков составьте и скомпилируйте базу эталонных документов.
2. При необходимости, выполните синхронизацию с Active Directory.
3. Выполните дополнительные настройки (наборы цветов, групп, списков и зон ответственности), необходимые для корректной работы сценария обработки объектов.
4. Настройте и активируйте сценарий обработки объектов.

   Важная информация!

   Если система должна иметь возможность блокировать перехваченные объекты, а именно:

   - в схеме перехвата SMTP-трафика, когда сервер Traffic Monitor подключен «в разрыв» (подробнее см. п. 2.1.2 на стр. 12),
   - в схеме перехвата HTTP-трафика с помощью прокси-сервера с поддержкой ICAP (подробнее см. п. 2.1.4 на стр. 17)

   для перехватчика *Smtp* или *Http* соответственно, в сценарии обработки объектов вместо указанного по умолчанию транспортного режима *Copy* должен быть указан:

   - *Normal* – если система должна иметь возможность блокировки объекта, в зависимости от вердикта, вынесенного объекту. В этом случае для `Monitor.Smtp` или `Monitor.Http` должно быть указано `root.processing.transport_mode = TransportMode.Normal`
   - *Transparent* – если доставка объекта получателям должна осуществляется всегда, вне зависимости от вынесенного вердикта. В этом случае для `Monitor.Smtp` или `Monitor.Http` должно быть указано `root.processing.transport_mode = TransportMode.Transparent`
5. Отправьте настроенную конфигурацию на хосты.

Подробная информация по выполнению перечисленных настроек содержится в документе «*InfoWatch Traffic Monitor. Руководство пользователя*».

Убедиться в корректности выполненных настроек вы можете, выполнив один из предустановленных запросов и просмотрев перехваченные объекты.

ГЛАВА 4. ОБНОВЛЕНИЕ СИСТЕМЫ

Стандартная процедура обновления системы InfoWatch Traffic Monitor с помощью программы-инсталлятора (kickstart) подразумевает полную переустановку не только системных компонент, но и операционной системы сервера. Поэтому при выполнении обновления особое внимание следует уделить сохранению всех изменений, которые были выполнены для системы за время ее эксплуатации и отличают ее от базовой поставки. Это может быть не только содержимое базы данных, но и конфигурационные файлы и сценарии обработки объектов.

В этой главе:

- *Порядок обновления Системы (п. 4.1 на стр. 67).*
- *Создание резервной копии базы данных (п. 4.2 на стр. 69).*
- *Восстановление базы данных из резервной копии (п. 4.3 на стр. 73)*
- *Обновление схемы базы данных (п. 4.4 на стр. 74).*
- *Внесение изменений в файлы новой версии (п. 4.5 на стр. 75).*

4.1. Порядок обновления Системы

На время выполнения обновления сервера Traffic Monitor потребуется отключить перехват всего трафика. Поэтому рекомендуется выполнять обновление в то время, когда трафик и размер файловой очереди минимальны.

Для обновления Системы выполните следующие шаги:

1. Остановите процессы `iw-trafmon` и `iw-caserv`. На компьютерах, где установлен Краулер, остановите службы `InfoWatch.Crawler.Server` и `InfoWatch.Crawler.Scanner`.
2. Сделайте резервную копию файла **database.conf** из директории `/opt/distr/infowatch/csw-auto-install/csw-4.1.NNN`, где `NNN` – номер установленной версии.
3. Сохраните конфигурационные файлы.

   Если в вашей Системе проводилась индивидуальная настройка сценариев обработки объектов, базы эталонных документов и конфигурационного файла, рекомендуется перед началом обновления сохранить необходимые файлы на внешний носитель:

   - сценарии обработки объектов: по умолчанию, они расположены в папке `/usr/local/infowatch/tm3/etc/scripts`
   - базу анализа цифровых отпечатков: `/usr/local/infowatch/tm3/cas/ca_db`
   - конфигурационный файл `/usr/local/infowatch/tm3/etc/tm.conf`
   - списки веб-ресурсов: `etc/scripts/user_resources.list`

   Сохранение должно производиться в хранилище, расположенное вне обновляемых серверов.
4. Установите новую версию серверной части.

   > **Важная информация!**
   >
   > Перед установкой компонентов серверной части убедитесь, что аппаратное и программное обеспечение соответствует требованиям, приведенным в п. 2.2 на стр. 24.

   Для обновления серверной части, необходимо подключить локальный репозиторий с новыми пакетами и выполнить следующие шаги:

   a) Если диск вставлен в дисковод, смонтируйте его командой:

   ```
   # mount /dev/cdrom /mnt/dvd/ -o loop
   ```

   Если образ диска находится в локальной папке (например, `/opt/distr/infowatch/iwks-4.1.XXX-TME.iso`), используйте команду:

`# mount /opt/distr/infowatch/iwks-4.1.XXX-TME.iso /mnt/dvd -o loop`, где `XXX` – номер новой версии.

b) Отредактируйте файл **/etc/yum.repos.d/rhel-dvd.repo** следующим образом:

```
[rhel-dvd]
name=Kickstart_whole_system_rhel6
baseurl=file:///mnt/dvd/
enabled=1
gpgcheck=0

[rhel-dvd-iwtm]
name=IWTM_4.1.XXX_RPMs
baseurl=file:///mnt/dvd/infowatch/traffic-monitor-4.1.XXX/Linux
enabled=1
gpgcheck=0, где XXX – номер новой версии
```

c) Обновите пакеты командами:

```
# yum remove iwtm-*
# yum install iwtm-*
```

d) Если в процессе обновления возникли ошибки, выполните следующие команды:

```
# yum remove iwtm-*
# yum install iwtm-*
```

5. Обновите схему схемы БД

a) Скопируйте на сервер БД файл со схемой из директории `/mnt/dvd/infowatch/traffic-monitor-4.1.XXX/Linux/csw-4.1.XXX.tar.gz` (где `XXX` – номер новой версии) и распакуйте его, выполнив команду:
`tar xvfz csw-4.1.XXX.tar.gz`, где `XXX` – номер новой версии

b) Убедитесь, что файл **database.conf** содержит правильную информацию (вы можете скопировать параметры подключения из файла **database.conf**, оставшегося от предыдущей установки)

c) Выполните команду:

```
alter system set filesystemio_options=setall scope=spfile;
```

d) Перезагрузите базу данных:

```
dbshut $ORACLE HOME
service oracle restart
dbstart $ORACLE HOME
```

e) Выполните скрипт обновления БД командой `./update.sh`.

6. Внесите изменения в файлы новой версии в соответствии с файлами, сохраненными на шаге 3 (п. 4.5 на стр. 75).

7. На сервере БД в файле **/etc/cron.hourly/addm.cron** замените строку

```
find /home/oracle/addm/logs/ -maxdepth 1 -type f -name "*.txt" -name "*.html"
-mtime 60 –delete
```

на строку

```
find /home/oracle/addm/logs/ -maxdepth 1 -type f \( -name '*.txt' -or -name
'*.html' \) -mtime +60 -delete
```

Вы также можете заменить весь файл **/etc/cron.hourly/addm.cron**. Для замены используйте файл **/mnt/dvd/infowatch/extras**.

8. Запустите процессы `iw-trafmon` и `iw-caserv`. На компьютерах, где установлен Краулер, запустите службы `InfoWatch.Crawler.Server` и `InfoWatch.Crawler.Scanner`.

9. Удалите установленную Консоль управления и установите новую версию. Установочные *.msi файлы требуемой локализации можно найти в папке `/mnt/dvd/infowatch/traffic-monitor-4.1.XXX/tm-management-console-windows/`.

> **Важная информация!**
>
> Не используйте старую версию консоли управления для работы с обновленной базой данных.

10. В случае распределенной установки обновление серверной части выполняется на всех компьютерах, а обновление БД – только на компьютере, где установлена БД. По завершении обновления серверной части на компьютере, где установлена БД, необходимо выполнить перезагрузку, после чего произвести обновление БД.

В процессе обновления прием объектов не ведется. По завершении обновления Система работает в штатном режиме.

4.2. Создание резервной копии базы данных

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

- *Определение размера резервной копии (п. 4.2.1 на стр. 69);*
- *Проверка хранилища резервной копии (п. 4.2.2 на стр. 69);*
- *Создание папок для резервной копии (п. 4.2.3 на стр. 70);*
- *Создание вспомогательных файлов на Linux (п. 4.2.4 на стр. 70);*
- *Создание списка файлов, подлежащих резервному копированию (п. 4.2.5 на стр. 71);*
- *Остановка системы IWTM (п. 4.2.6 на стр. 72);*
- *Остановка БД Oracle (п. 4.2.7 на стр. 72);*
- *Копирование файлов БД в хранилище резервных копий (п. 4.2.8 на стр. 73).*

4.2.1. 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 кикстарта, 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
   ```

4.2.2. 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 бэкапированию.
- 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.

4.2.3. Создание папок для резервной копии

> **Важная информация!**
>
> Папки 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 подпапки:

   ```
   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
   ```

4.2.4. 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 копию 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 кикстарта IWTM, для удобства вы можете использовать команду **wsqlplus**.
3. Дождитесь подключения – об этом будет свидетельствовать сообщение **Connected**.
4. Скопируйте (или введите) в командную строку и выполните следующий SQL запрос:

   ```
   SQL> alter database backup controlfile to trace;
   ```

5. Найдите путь к папке, куда был создан trace файл, выполнив команду:

   ```
   SQL> show parameter user_dump;
   ```

   В данной папке 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
   ```

6. Если система была установлена с помощью кикстарта 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

7. Создайте копию файла параметров **spfile** (**pfile**):

   ```
   OS> sqlplus / as sysdba
   SQL> CREATE PFILE from SPFILE;
   ```

8. Найдите путь к папке, куда был создан **pfile** файл, выполнив команду:

   ```
   SQL> show parameter PFILE
   ```

   Будет возвращен путь к папке, где был создан **pfile** (по умолчанию - /u01/app/oracle/product/db_1/dbs/).

   В этой же папке находится файл **initiwtm.ora**, для которого нужно также создать резервную копию.

   Выйдите из Oracle SQL*Plus:

   ```
   SQL> exit
   ```

9. Скопируйте файлы trace и spfile на компьютер с резервной копией, в ранее созданную подпапку **/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
   ```

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

    ```
    controlfilebackupMMDDYY.trc
    ```

4.2.5. Создание списка файлов, подлежащих резервному копированию

Вы можете создать список файлов, подлежащих бэкапированию. 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 бэкапированию. 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
```

4.2.6. 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 iw-trafmon stop
OS> service iw-caserv stop
```

По окончании процедуры резервного копирования сервисы можно запустить с помощью следующих команд:

```
OS> service iw-trafmon start
OS> service iw-caserv start
```

4.2.7. Остановка БД Oracle

> **Важная информация!**
>
> 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
```

4.2.8. 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 папки (со всем содержимым) с помощью ранее созданного списка директорий.

   Если система была установлена с помощью кикстарта и были оставлены параметры по умолчанию, то пути будут такими:

   скопируйте содержимое папки **/u01/app/oracle/oradata/iwtm/** - в папку **/opt/IWTM_Backup_Files/IWTM**,

   а папку **/u02/oradata/** - в папку **/opt/IWTM_Backup_Files/Oradata**
3. С компьютера, где установлена БД, скопируйте файл **/u01/app/oracle/product/db_1/dbs/orapwiwtm** в папку **/opt/IWTM_Backup_Files/Recovery_Aid** компьютера, где расположены файлы резервной копии.

4.3. Восстановление базы данных из резервной копии

Данная процедура описывает восстановление базы данных из резервной копии на сервер, установленный с помощью программы-инсталлятора (kickstart).

1. Остановите процессы Traffic Monitor:

   ```
   OS:root> service iw-trafmon stop
   OS:root> service iw-caserv stop
   ```
2. Остановите базу данных:

   ```
   OS:root> su - oracle
   OS:oracle> dbshut $ORACLE_HOME
   OS:oracle> su -
   ```
3. Запустите Midnight Commander:

   ```
   OS:root> mc
   ```
4. Удалите содержимое **/u02/oradata/**
5. Удалите содержимое **/u01/app/oracle/oradata/iwtm/**
6. При помощи WinScp скопируйте содержимое резервной копии базы данных из **/opt/IWTM_Backup_Files/IWTM/** в **/u02/oradata/**
7. При помощи WinScp скопируйте содержимое резервной копии базы данных из **/opt/IWTM_Backup_Files/Oradata/** в **/u01/app/oracle/oradata/iwtm/**
8. Переименуйте **control01.ctl**, находящийся в **/opt/IWTM_Backup_Files/Oradata/**, в **control02.ctl** и скопируйте его в **/u01/app/oracle/flash_recovery_area/iwtm/**

   ```
   OS:root > chown -R oracle:oinstall /u02/oradata
   OS:root > chown -R  oracle:oinstall /u01/app/oracle/oradata/iwtm/
   OS:root > chown -R oracle:oinstall /u01/app/oracle/flash_recovery_area/iwtm/
   OS:root >su – oracle
   ```
9. Запустите базу данных:

   ```
   OS:oracle> dbstart $ORACLE_HOME
   ```
10. Проверьте, что база данных успешно запущена:

    ```
    OS:oracle >cat  /u01/app/oracle/product/db_1/startup.log
    ```

    Лог должен выглядеть примерно так:

    ```
    ORACLE instance started.
    ```

```
Total System Global Area 1970864128 bytes
Fixed Size                  2214656 bytes
Variable Size            1124074752 bytes
Database Buffers          788529152 bytes
Redo Buffers               56045568 bytes
Database mounted.
Database opened.
```

11. Проверьте журнал ошибок:

```
OS:oracle >tailf /var/log/alert_iwtm.log
```

4.4. Обновление схемы базы данных

1. Подключитесь к базе данных от имени владельца схемы:

```
OS:oracle > sqlplus iwtm@iwtm
```

(для удобства можно использовать вместо sqlplus команду wsqlplus)

Проверьте отсутствие выполняемых задач:

```
SQL:IWTM>SELECT job_name FROM user_scheduler_running_jobs;
```

Если они есть, дождитесь их завершения или устраните причину долгого выполнения.

Проверьте наличие запланированных задач:

```
SQL:IWTM>select * from user_scheduler_jobs u where u.enabled = 'TRUE';
```

Далее пример управления задачами описан, исходя из того, что запрос вывел следующий перечень задач:

- IWADDPARTS
- IWTM_CHECK_MAIN_TS_OVERFLOW
- IWTM_DELETE_OLD_LOGS
- IWTM_POST_IDENTIFICATION
- IWTM_SHRINK_TABLESPACES
- IWTM_SYNC_INDEXES

Если ваш перечень задач отличается от приведенного, внесите изменения в соответствующие запросы.

2. Выключите задачи, чтобы они не запустились во время обновления:

```
SQL:IWTM>
BEGIN
dbms_scheduler.disable('IWADDPARTS', true);
dbms_scheduler.disable('IWTM_CHECK_MAIN_TS_OVERFLOW',true);
dbms_scheduler.disable('IWTM_DELETE_OLD_LOGS',true);
dbms_scheduler.disable('IWTM_POST_IDENTIFICATION',true);
dbms_scheduler.disable('IWTM_SHRINK_TABLESPACES',true);
dbms_scheduler.disable('IWTM_SYNC_INDEXES',true);
COMMIT;
END;
/
```

3. Выйдите из SQLPLUS:

```
SQL:IWTM>exit
```

Если вы подключены к базе данных Oracle через SQLDeveloper или аналог, отключитесь.

4. Перейдите в каталог со сценарием обновления БД:

```
OS:root >cd /opt/distr/infowatch/csw-auto-install/csw-4.1.x.xxx/
```

где 4.1.x.xxx – номер версии Traffic Monitor

5. Запустите сценарий обновления схемы:

```
OS:root >./update.sh
```

6. Проверьте версию схемы БД:

```
SQL:IWTM> SELECT vers.get_schema_version FROM dual;
```

7. Проверьте статус запланированных задач.

```
SQL:IWTM> select * from user_scheduler_jobs u where u.enabled = 'TRUE';
```

Если какие-либо задачи отсутствуют, включите их:

```
SQL:IWTM>
BEGIN
dbms_scheduler.enable('IWADDPARTS');
dbms_scheduler.enable('IWTM_CHECK_MAIN_TS_OVERFLOW');
dbms_scheduler.enable('IWTM_DELETE_OLD_LOGS');
dbms_scheduler.enable('IWTM_POST_IDENTIFICATION');
dbms_scheduler.enable('IWTM_SHRINK_TABLESPACES');
dbms_scheduler.enable('IWTM_SYNC_INDEXES');
COMMIT;
END;
/
```

8. Запустите службы TM:

```
OS:root >service iw-caserv start
OS:root >service iw-trafmon start
```

4.5. Внесение изменений в файлы новой версии

> **Важная информация!**
>
> Изменения в новой версии системы могут быть существенными (например, изменены структура или синтаксис конфигурационных файлов), и использование файлов, сохраненных с предыдущей версии, может привести к неработоспособности системы.
>
> Поэтому если вы хотите изменить настройки с установленных по умолчанию на те, которые вы использовали ранее, выполняйте редактирование аккуратно и учитывайте изменения, описанные в документах Release Notes.

Внесение изменений в файлы новой версии включает:

- Изменение сценария обработки объектов (подробнее см. п. 4.5.1 на стр. 7576);
- Изменение конфигурационного файла tm.conf (подробнее см. п. 4.5.2 на стр. 76).

4.5.1. Изменение сценария обработки объектов

Помимо сценариев обработки объектов (скриптов), использовавшихся до обновления Системы, после обновления в Консоли управления Traffic Monitor в разделе **Скрипты** (**Панель навигации > Конфигурация**) появится новый сценарий обработки объектов – **Default script of version [номер_версии]**, где **[номер_версии]** – версия системы InfoWatch Traffic Monitor, до которой было произведено обновление.

Функции, используемые в сценарии обработки объектов, различаются в системах InfoWatch Traffic Monitor версии 4.1 и предыдущих версий (подробнее о функциях сценариев обработки объектов см. документ «*InfoWatch Traffic Monitor. Руководство пользователя*»). В связи с этим, рекомендуется настроить сценарий обработки объектов **Default script of version [номер_версии]** подобно старому сценарию, учитывая различия в функциях.

Чтобы перенести настройки старого сценария обработки объектов в новый, выполните следующие действия:

1. Скопируйте требуемые секции текста старого сценария обработки объектов.

2. Вставьте скопированные секции в текст нового сценария обработки объектов, учитывая изменения в функциях.
3. Сохраните сценарий обработки объектов **Default script of version [номер_версии]**.
4. Активируйте сценарий обработки объектов **Default script of version [номер_версии]**.

4.5.2. Изменение конфигурационного файла tm.conf

Если в вашей системе проводилась индивидуальная настройка конфигурационного файла `tm.conf`, требуется внести изменения в файл новой версии в соответствии с настроенным файлом (см. п. на стр.).

> **Примечание:**
>
> В новой схеме конфигурационному файлу `tm.conf` соответствует конфигурационный файл `tm.conf.rpmnew`.

Чтобы внести изменения в файл новой версии, выполните следующие действия:

1. Сравните файл старой схемы и файл новой схемы с помощью команды `vimdiff`.
2. Внесите изменения в файл новой схемы в соответствии с файлом старой схемы.
3. Сохраните изменения, сделанные в файле новой схемы.

Переименуйте файл новой схемы так, чтобы его название стало `tm.conf`.

ГЛАВА 5. УДАЛЕНИЕ СИСТЕМЫ

В этой главе:

- *Схема базы данных (п. 5.1 на стр. 77).*
- *Модуль взаимодействия с удаленной базой данных (п. 5.2 на стр. 77).*
- *Модуль IW ICAP (п. 5.3 на стр. 78).*
- *Сервер Traffic Monitor (п. 5.4 на стр. 78).*
- *Sniffer (п. 5.5 на стр. 79).*
- ***Ошибка! Источник ссылки не найден.*** *(п.* ***Ошибка! Источник ссылки не найден.*** *на стр.* ***Ошибка! Закладка не определена.****).*

5.1. Схема базы данных

> **Важная информация!**
>
> Не удаляйте схему базы данных, от которой для архивирования были отключены ежедневные ТП. Иначе вы не сможете восстановить данные из этих табличных пространств.

Шаг 1. Проверка сервера СУБД Oracle

Убедитесь, что:

- версия установленной схемы базы данных соответствует версии программного пакета, используемого для его удаления;
- запущен сервер СУБД Oracle;
- в конфигурационном файле `database.conf` корректно указаны имя и пароль учетной записи, обладающей правами SYSDBA (значения параметров `sysdba` и `sysdba_password`).

Шаг 2. Остановка Traffic Monitor

Перед началом удаления необходимо:

- Остановить все процессы Traffic Monitor:

```
service iw-trafmon stop
```

- Закрыть все экземпляры консоли управления;
- Прекратить все соединения с удаляемой схемой базы данных, осуществляемые из других программ.

Шаг 3. Запуск удаления схемы

Выполните следующую команду:

```
sh uninstall.sh
```

5.2. Модуль взаимодействия с удаленной базой данных

Чтобы удалить модуль взаимодействия с удаленной базой данных:

1. На компьютерах, где установлены клиентские и серверные части модуля, выполните команду:

   ```
   rpm -e iwtm_qmover
   ```

   Если конфигурационный файл (`qmover.conf`) в процессе работы был изменен, то после удаления он будет сохранен на компьютере как `qmover.conf.rpmsave`.

2. На стороне клиента (перехватчика объектов) удалите из cron настройки, изменяющие ширину пропускания для канала передачи данных (пример настроек см. в п. 3.2.5.1 на стр. 44, шаг 2).

5.3. Модуль IW ICAP

Если перехват HTTP-запросов по протоколу ICAP больше не требуется, вы можете отключить модуль IW_ICAP.

Чтобы отключить модуль IW_ICAP:

1. Остановите процессы Traffic Monitor:

   ```
   service iw-trafmon stop
   ```

2. Отключите автозапуск процесса iw_icap в файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[AUTO_RESTART]`:

   ```
   iw_icap:
   autorestart = Off
   ```

3. Запустите процессы Traffic Monitor:

   ```
   service iw-trafmon start
   ```

4. Проверьте состояние процессов Traffic Monitor:

   ```
   service iw-trafmon status
   ```

5. Верните исходные настройки прокси-сервера (пример смены настроек см. в п. 3.3.4 на стр. 53, шаг 2).

При необходимости вы можете удалить rpm-пакет `iwtm_icap`.

Чтобы удалить rpm-пакет модуля IW ICAP:

выполните команду:

```
rpm -e iwtm_icap
```

Если конфигурационный файл (`icap.conf`) в процессе работы был изменен, то после удаления он будет сохранен на компьютере как `icap.conf.rpmsave`.

5.4. Сервер Traffic Monitor

Перед тем как удалять серверную часть Traffic Monitor, удалите:

- Модуль взаимодействия с удаленной базой данных (п. 5.2 на стр. 77 - как клиентскую часть модуля, так и серверную) – если сервер Traffic Monitor использовался при загрузке объектов в удаленную базу данных.
- Модуль IW ICAP (п. 5.3 на стр. 78) – если перехват HTTP-трафика выполнялся путем интеграции с ICAP-сервером.
- Модуль InfoWatch DeviceLock Adapter – если он был установлен в составе Traffic Monitor для приема объектов от DeviceLock. Рекомендации по удалению см. в документе «*InfoWatch DeviceLock Adapter. Руководство по установке и конфигурированию*».

Чтобы удалить Traffic Monitor:

1. Выполните команды:

```
rpm -e iwtm_gpl_components
rpm -e `rpm -qa | grep iwtm`
```

2. Перенастройте компоненты перехвата трафика, настроенные на Traffic Monitor.

Схема перехвата трафика в InfoWatch Traffic Monitor	Необходимые действия после удаления InfoWatch Traffic Monitor
Перехват копии SMTP-трафика (работа с почтовым relay-сервером)	Убедитесь, что параметры Postfix возвращены в исходное состояние. Об изменениях в параметрах Postfix см п. 3.3.2 на стр. 49
Перехват и фильтрация SMTP-трафика выполнялся Системой (интеграция с Postfix)	Убедитесь, что параметры Postfix возвращены в исходное состояние. Об изменениях в параметрах Postfix см. п. 3.3.2 на стр. 49. Настройте доставку SMTP-писем через корпоративный почтовый сервер, минуя InfoWatch Traffic Monitor

После удаления на компьютере остаются только:

- Конфигурационные файлы, в которые были внесены изменения (`tm.conf`, `detector.conf`, `qmover.conf`, `icap.conf`).

  Измененным файлам присваивается суффикс `.rpmsave` (например, `tm.conf.rpmsave`). Файлы, которые не изменялись, будут удалены.
- Очередь объектов.
- Классификатор.
- Файл лицензии.
- Учетная запись пользователя – владельца InfoWatch Traffic Monitor и группа, в состав которой входил этот пользователь.

Если выполнялась интеграция с Postfix, то в процессе удаления происходит возврат к исходным настройкам. Об изменениях, выполняемых при интеграции Traffic Monitor с Postfix, рассказывается в п. 3.3.2 на стр. 49.

5.5. Sniffer

Если Sniffer и остальные компоненты сервера Traffic Monitor установлены на одном компьютере, то Sniffer будет удален вместе с Traffic Monitor (см. п. 5.4 на стр. 78). Дополнительная процедура удаления в этом случае не требуется.

Чтобы удалить Sniffer, установленный отдельно от остальных компонентов Traffic Monitor:

выполните команду:

```
rpm -e `rpm -qa | grep iwtm`
```

После удаления на компьютере остаются только:

- Конфигурационный файл, `tm.conf`, если он был изменен в процессе работы. Файл будет сохранен как `tm.conf.rpmsave` (например, `tm.conf.rpmsave`). Файлы, которые не изменялись, будут удалены.
- Учетная запись пользователя – владельца InfoWatch Traffic Monitor и группа, в состав которой входил этот пользователь.

5.6. Консоль управления

Чтобы удалить Консоль управления:

1. Откройте компонент **Установка и удаление программ**. Для этого в меню **Пуск** выберите пункт **Настройка ► Панель управления**. В окне Панели управления выберите компонент **Установка или удаление программ**.
2. В окне **Установка и удаление программ** выделите пункт **InfoWatch Traffic Monitor Management Console** и нажмите кнопку **Удалить**.

ПРИЛОЖЕНИЕ А. РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ИМЕН И ПАРОЛЕЙ

Общие рекомендации

Длина имени пользователя может составлять от 1 до 10 символов. Имя пользователя может состоять из букв латинского алфавита, цифр и символа подчеркивания «_». Должно начинаться с буквы.

Пароли составляются по следующим правилам:

- Пароль пользователя может состоять из латинских букв, цифр и символов:

  ( ) , ; \ . : ! ~ ` # $ % ^ * - _ + ' [ ] { } | ? < >
- Может начинаться с буквы, цифры или символа. Максимальная длина пароля составляет 30 символов.

Не рекомендуется начинать имена и пароли пользователей с последовательностей: SYS_ и ORA_.

В составе имени и пароля не рекомендуется использовать зарезервированные слова СУБД Oracle:

ACCESS	IDENTIFIED	PUBLIC
ADD	IMMEDIATE	RAW
ALL	IN	RENAME
ALTER	INCREMENT	RESOURCE
AND	INDEX	REVOKE
ANY	INITIAL	ROW
AS	INSERT	ROWID
ASC	INTEGER	ROWNUM
AUDITBETWEEN	INTERSECT	ROWS
BY	INTO	SELECT
CHAR	IS	SESSION
CHECK	LEVEL	SET
CLUSTER	LIKE	SHARE
COLUMN	LOCK	SIZE
COMMENT	LONG	SMALLINT
COMPRESS	MAXEXTENTS	START
CONNECT	MINUS	SUCCESSFUL
CREATE	MLSLABEL	SYNONYM
CURRENT	MODE	SYSDATE
DATE	MODIFY	TABLE

DECIMAL	NOAUDIT	THEN
DEFAULT	NOCOMPRESS	TO
DELETE	NOT	TRIGGER
DESC	NOWAIT	UID
DISTINCT	NULL	UNION
DROP	NUMBER	UNIQUE
ELSE	OF	UPDATE
EXCLUSIVE	OFFLINE	USER
EXISTS	ON	VALIDATE
FILE	ONLINE	VALUES
FLOAT	OPTION	VARCHAR
FOR	OR	VARCHAR2
FROM	ORDER	VIEW
GRANT	PCTFREE	WHENEVER
GROUP	PRIOR	WHERE
HAVING	PRIVILEGES	WITH

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 имя пользователя (в т.ч. записанное наоборот);
- 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.

ПРИЛОЖЕНИЕ В. РАЗРЕШЕНИЕ ПРОБЛЕМ

При запуске процессов iw_messed, iw_deliverd выдается сообщение о том, что не найдены динамические библиотеки СУБД Oracle

В скрипте автозапуска `iw-trafmon` неверно задана переменная окружения `ORACLE_HOME`.

Решение

Откройте скрипт автозапуска серверной части:

`/usr/local/infowatch/tm3/bin/scripts/iw-autorestart.sh`

Проверьте значение переменной окружения `ORACLE_HOME`. Это значение должно совпадать со значением `ORACLE_HOME`, заданным при установке сервера СУБД Oracle.

При запуске процессов iw_messed, iw_deliverd выдается сообщение о том, что нет прав на загрузку динамических библиотек СУБД Oracle

Некорректно выполнена установка сервера Traffic Monitor.

Решение

Необходимо включить пользователя – владельца сервера Traffic Monitor (от имени которого запускаются процессы Traffic Monitor) – в группу `oinstall` (группа владельца инсталляции клиента СУБД Oracle).

Учетная запись пользователя Linux части заблокирована

При установке сервера Traffic Monitor был указан неверный пароль пользователя Linux части.

Решение

Для того чтобы разблокировать учетную запись пользователя Linux части, необходимо выполнить следующие действия:

1. Остановить все процессы Traffic Monitor, выполнив команду:

   ```
   service iw-trafmon stop
   ```

2. В файле `/usr/local/infowatch/tm3/etc/tm.conf` указать корректные имя и пароль пользователя Linux части (секция `[ORACLE]`, параметры Username и Password, соответственно).

3. Разблокировать учетную запись пользователя Linux части, выполнив в SQL *Plus команду:

   ```
   ALTER USER имя_пользователя_Linux_части ACCOUNT UNLOCK
   ```

4. Запустить все процессы Traffic Monitor, выполнив команду:

   ```
   service iw-trafmon start
   ```

ПРИЛОЖЕНИЕ С. ЛИЦЕНЗИИ ТРЕТЬИХ СТОРОН

При создании Системы были использованы разработки третьих сторон, распространяемые на условиях лицензии MIT (http://www.opensource.org/licenses/mit-license.html):

- Lua – http://www.lua.org/license.html
- LuaBind – http://www.rasterbar.com/products/luabind.html
- libxml2 – http://www.xmlsoft.org/

Также использовалось программное обеспечение:

- распространяемое на условиях лицензий BSD (http://www.opensource.org/licenses/bsd-license.php):
  - Stringencoders – http://code.google.com/p/stringencoders/
- распространяемое на условиях GNU GENERAL PUBLIC LICENSE (http://www.gnu.org/licenses/gpl-2.0.html):
  - Pdftotext http://www.foolabs.com/xpdf/
  - Tnef http://sourceforge.net/projects/tnef/
  - Unzip http://www.info-zip.org/UnZip.html
  - libcole.so arturo@directmail.org; andy.scriven@research.natpower.co.uk
  - libhtmltree.so pauljlucas@mac.com

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

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.

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

LDAP

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

Management Console

См. Консоль управления

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

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.

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 двое суток.

Задание на печать

Информация об отправке данных на печать вместе с печатаемым документом

Зона ответственности

Способ разделения перехваченных объектов для ограничения доступа к ним пользователей консоли управления. Объекты, принадлежащие какой-либо зоне ответственности, будут видны только тем пользователям, которые входят в эту зону ответственности (при условии, что пользователь имеет привилегии на просмотр и/или работу с объектами).

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.

Классификатор

Набор данных, необходимых для проведения лингвистического анализа. Содержит перечень категорий, классифицирующих возможные нарушения политики безопасности. Наличие в тексте термина, принадлежащего к определенной категории, позволяет соотнести текст с этой категорией.

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

Консоль управления

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

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.

Прозрачный транспортный режим

Значение атрибута «Транспортный режим». Режим, в котором через Систему проходит реальный трафик, но блокировка запрещенного Системой трафика невозможна. См. также: Транспортный режим, Режим перехвата

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. См. также: Консоль управления

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, Прозрачный транспортный режим

Трафик

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

УКАЗАТЕЛЬ

I

InfoWatch Traffic Monitor.....7

init.ora 69

P

Postfix 50

T

trace –файл.....69

Л

Лицензионный ключ

iw_customer.dat 40, 43

iw_license.dat 40, 43

Лицензирование

iw_lickey 42

P

Рапорт

дополнительная настройка.....65

Резервное копирование БД

копирование 72

размер бэкапа 68

создание 68