INFOWATCH

InfoWatch Traffic Monitor 4.1

Руководство администратора

INFOWATCH TRAFFIC MONITOR 4.1

Руководство администратора

© 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 ... 6
Аудитория ... 6
Структура руководства ... 6
Дополнительная документация ... 7
Условные обозначения ... 7
Техническая поддержка пользователей ... 8

ГЛАВА 1. ОБЗОР INFOWATCH TRAFFIC MONITOR ... 9
1.1. Функции InfoWatch Traffic Monitor ... 9
1.2. Состав InfoWatch Traffic Monitor ... 10

ГЛАВА 2. МОНИТОРИНГ ... 11
2.1. Подсистема мониторинга для распределенной архитектуры ... 11
2.1.1. Настройка адреса сервера синхронизации времени для подсистемы мониторинга ... 12
2.1.2. Настройка соединения с серверами ... 12
2.1.2.1. Настройка соединения с сервером Device Monitor ... 14
2.1.3. Настройка порогов срабатывания для индикатора нагрузки ... 14
2.1.4. Настройка запуска служб ... 15
2.1.5. Настройка механизма уведомлений ... 15
2.1.5.1. Настройка отправки уведомлений о превышении порога для индикаторов ... 15
2.1.5.2. Настройка отправки писем-уведомлений с помощью Postfix ... 16
2.1.6. Просмотр индикаторов мониторинга ... 16
2.2. Подсистема мониторинга для установки «все-в-одном» ... 17
2.2.1. Интерфейс веб-консоли ... 18
2.2.1.1. Раздел General ... 19
2.2.1.2. Раздел Network ... 20
2.2.1.3. Раздел System monitoring ... 21
2.2.2. Настройка адреса сервера синхронизации времени ... 22
2.2.3. Управление лицензиями ... 22
2.2.3.1. Отправка запроса на обновление лицензии ... 23
2.2.3.2. Установка лицензии ... 23
2.2.4. Работа с индикаторами мониторинга ... 23
2.2.4.1. Настройка уведомлений подсистемы мониторинга ... 23
2.2.5. Скачивание дистрибутива Management Console ... 24
2.2.6. Сбор диагностических данных ... 24

ГЛАВА 3. КОНФИГУРИРОВАНИЕ ПЕРЕХВАТЧИКА CRAWLER ... 25
3.1. Настройка сетевых правил доступа ... 25
3.2. Конфигурационные файлы Crawler ... 27
3.2.1. Конфигурационный файл сервера Crawler ... 27
3.2.1.1. Изменение учетной записи, от имени которой запускается служба сервера Crawler ... 28
3.2.2. Конфигурационный файл сканера Crawler ... 28
3.3. Работа с журналами Crawler ... 29

ГЛАВА 4. АДМИНИСТРИРОВАНИЕ БАЗЫ ДАННЫХ ... 30
4.1. Проведение регламентных работ на сервере базы данных ... 30
4.2. Табличные пространства в базе данных InfoWatch Traffic Monitor ... 31
4.2.1. Статусы ежедневных табличных пространств ... 32

4.3. Управление ежедневными табличными пространствами ... 33
4.3.1. Настройка размещения файлов на файловой системе ... 33
4.3.2. Индексирование данных в ежедневных табличных пространствах ... 34
4.3.3. Архивирование ежедневных табличных пространств ... 36
4.3.4. Восстановление ежедневных табличных пространств ... 37
4.3.5. Удаление ежедневных табличных пространств ... 38
4.4. Резервное копирование базы данных ... 39
4.4.1. Создание резервной копии базы данных ... 40
4.4.1.1. Определение размера резервной копии ... 40
4.4.1.2. Проверка хранилища резервной копии ... 40
4.4.1.3. Создание папок для резервной копии ... 40
4.4.1.4. Создание вспомогательных файлов на Linux ... 41
4.4.1.5. Создание списка файлов, подлежащих резервному копированию ... 42
4.4.1.6. Остановка системы IWTM ... 43
4.4.1.7. Остановка БД Oracle ... 43
4.4.1.8. Копирование файлов БД в хранилище резервных копий ... 43
4.4.2. Восстановление базы данных из резервной копии ... 44
4.4.2.1. Восстановление на той же БД ... 44
4.4.2.2. Восстановление на новой БД ... 44

ГЛАВА 5. АДМИНИСТРИРОВАНИЕ СЕРВЕРНОЙ ЧАСТИ INFOWATCH TRAFFIC MONITOR ... 46
5.1. Процессы Traffic Monitor Server ... 46
5.1.1. Список процессов Traffic Monitor Server ... 46
5.1.2. Работа с процессами Traffic Monitor Server ... 48
5.1.3. Проверка результатов обновления конфигурации (процесс iw_updater) ... 50
5.2. Настройка параметров работы Traffic Monitor Server (файл tm.conf) ... 51
5.2.1. Секция [*GENERAL*] ... 52
5.2.2. Секция [*AUTO_RESTART*] ... 53
5.2.3. Секция [*SMTPD*] ... 54
5.2.4. Секция [*MESSED*] ... 55
5.2.5. Секция [*DELIVERD*] ... 56
5.2.6. Секция [*QUEUE*] ... 56
5.2.7. Секция [*SNIFFER*] ... 57
5.2.8. Секция [HTTP] ... 57
5.2.9. Секция [ICQ] ... 58
5.2.10. Секция [SMTP] ... 59
5.2.11. Секция [*PROXY*] ... 59
5.2.12. Секция [*PROXY_ICQ*] ... 60
5.2.13. Секция [*PROXY_HTTP*] ... 61
5.2.14. Секция [*PROXY_SMTP*] ... 63
5.2.15. Секция [*CAS*] ... 63
5.2.16. Секция [*ENCODE_DETECTOR*] ... 66
5.2.17. Секция [*DBLOADER*] ... 66
5.2.18. Секция [*FILTER*] ... 67
5.2.19. Секция [*ORACLE*] ... 67
5.2.20. Секция [*EXPRESSD*] ... 67
5.2.21. Секция [*EXTRACTOR*] ... 69
5.2.22. Секция [*UPDATER*] ... 69
5.2.23. Секция [*WARPD*] ... 70
5.2.24. Секция [*ADLIBITUM*] ... 70
5.3. Настройка использования OCR для различных перехватчиков (файл tm_ocr.conf) ... 70

5.3.1. Секция [*MESSED*] ... 71
5.3.2. Секция [*EXPRESSD*] ... 71
5.3.3. Секция [*EXTRACTOR*] ... 72
5.4. Настройка параметров работы с HTTP-запросами, передаваемыми по протоколу ICAP (файл icap.conf) ... 72
5.5. Настройка параметров обработки архивов вложений (файл detector.conf) ... 73
5.6. Синхронизация базы отпечатков эталонных документов между несколькими серверами ... 75
5.7. Настройка максимального размера добавляемого эталонного документа (файл casdbcfg.conf) ... 77
5.8. Настройка правил фильтрации для Sniffer ... 77
5.9. Управление загрузкой объектов в удаленную базу данных ... 78
5.9.1. Параметры приема объектов на стороне сервера ... 78
5.9.2. Параметры отправки объектов на стороне клиента ... 79
5.9.3. Настройка ширины полосы пропускания для канала передачи данных (клиент) ... 80
5.9.4. Просмотр статистической информации по загрузке объектов в удаленную базу данных ... 80
5.10. Архивирование каталога очереди сообщений ... 81
5.11. Протоколирование работы Системы ... 82
5.12. Перемещение объектов между очередями (утилита iw_qtool) ... 82
5.13. Загрузка очередей объектов ... 84
5.14. Восстановление работоспособности системы в аварийных ситуациях ... 84

ПРИЛОЖЕНИЕ А. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ УТИЛИТЫ АВТОАРХИВИРОВАНИЯ ... 86
A.1. Настройка параметров архивирования ... 86
A.1.1. Параметры конфигурационного файла ... 86
A.2. Запуск автоархивирования ... 87
A.2.1. Запуск вручную ... 87
A.2.2. Автоматический запуск ... 87
A.3. Определение переменных окружения ... 88
A.3.1. Поиск путей к модулям ... 88
A.3.2. Задание переменной окружения ORACLE_HOME ... 88
A.3.3. Быстрый запуск автоархивирования ... 89
A.4. Повторное автоматическое архивирование восстановленного табличного пространства ... 89
A.5. Сообщения об ошибках ... 89

ПРИЛОЖЕНИЕ В. ИНДИКАТОРЫ МОНИТОРИНГА ... 91

ПРИЛОЖЕНИЕ С. РАЗРЕШЕНИЕ ПРОБЛЕМ ... 96

ГЛОССАРИЙ ... 98

УКАЗАТЕЛЬ ... 103

ВВЕДЕНИЕ

В настоящем руководстве изложены сведения по администрированию InfoWatch Traffic Monitor: настройка системы после установки, восстановление после сбоев, проведение регламентных работ.

Аудитория

Информация, содержащаяся в руководстве, предназначена для администраторов InfoWatch Traffic Monitor Server, знакомых с основами работы в среде операционных систем Microsoft Windows и Linux.

Руководство рассчитано на пользователей, обладающих следующими навыками:

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

Структура руководства

В настоящем руководстве вы можете найти следующую информацию:

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

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

- *Глава 2. Мониторинг (стр. 11)*

  Описание установки и использования подсистемы мониторинга, предоставляющей возможность удаленно следить за показателями работы серверов, на которых установлены компоненты InfoWatch Traffic Monitor, и работающих на них служб.

- *Глава 3. Конфигурирование перехватчика Crawler (стр. 25)*

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

- *Глава 4. Администрирование базы данных (стр. 30)*

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

- *Глава 5. Администрирование серверной части InfoWatch Traffic Monitor (стр. 46)*

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

- *Приложение A. Инструкция по использованию утилиты автоархивирования (стр. 86)*

  Описание порядка настройки автоматического архивирования ежедневных табличных пространств с помощью специальной утилиты, входящей в состав дистрибутива Системы.

  Перечисление и описание индикаторов, используемых подсистемой мониторинга для проверки состояния компонентов Системы, а также описание действий, которые может предпринять администратор системы при достижении индикаторами пороговых значений.

- *Приложение C. Разрешение проблем (стр. 96)*

  Описание проблем, которые могут возникнуть в процессе эксплуатации Системы, а также способы их разрешения.

Дополнительная документация

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

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

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

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

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

- *«InfoWatch Device Monitor. Руководство пользователя»*

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

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

  В документе описывается установка и первоначальная настройка InfoWatch DeviceLock Adapter.

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

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

- *«InfoWatch OCR для IWTM 4.1. Руководство по установке».*

  Документ описывает порядок установки и встраивания модуля IW OCR, предназначенного для извлечения текста из изображений в перехваченных файлах.

Условные обозначения

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

Стиль оформления	Область применения	Пример
Полужирный шрифт	Названия элементов графического пользовательского интерфейса (кнопки, команды меню и пр.), компоненты системы (при первом упоминании)	Для перемещения объектов из одной очереди в другую используется утилита **iw_qtool**
Курсив	При описании таблиц, в примерах, описаниях – названия и значения атрибутов объектов	База контентной фильтрации содержит термин *Договор*

`Шрифт Courier New`	Имена файлов, примеры текста программ; значения параметров конфигурационных файлов, примеры настройки	Проверка запуска Traffic Monitor Server осуществляется 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. 9).*
- *Состав InfoWatch Traffic Monitor (п. 1.2 на стр. 10).*

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 протоколам HTTPS (при анализировании обрабатывается Системой как HTTP-трафик) и 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. 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 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. МОНИТОРИНГ

Подсистема мониторинга выполняет следующие функции:

- мониторинг работы всех серверов, входящих в состав решения InfoWatch Traffic Monitor (как физических, так и виртуальных);
- мониторинг всех программных компонент, входящих в состав решения (ОС, СУБД, БД, процессы и т.д.);
- контроль значений индикаторов для каждого сервера и компонента. Под контролем подразумевается периодическое получение значения индикатора и сравнение значения индикатора с пороговым значением. Подробнее об индикаторах см. п. п. 2.1.6 на стр. 16 и Приложение В;
- возможность включения и отключения мониторинга отдельных индикаторов и отдельных серверов;
- отправка на почту уведомлений о выходе значений индикаторов из нормальных пределов.

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

Если система InfoWatch Traffic Monitor установлена так, что сервер базы данных (kickstart запускалась с опцией **IWDBX**) установлен отдельно от сервера (серверов) Traffic Monitor (kickstart с опцией **IWTMX**), то подсистема мониторинга будет работать на сервере базы данных. Для того чтобы выполнялась диагностика всех серверов, входящих в решение, администратор системы должен выполнить ряд дополнительных настроек. Подробнее см. п. 2.1 на стр. 11.

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. Подробнее см. п. 2.2 на стр.17.

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

2.1. Подсистема мониторинга 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**), то подсистема мониторинга будет работать на сервере базы данных. Для того чтобы выполнялась диагностика всех серверов, входящих в решение, администратор системы должен выполнить ряд дополнительных настроек:

- *Настройка адреса сервера синхронизации времени (п. 2.1.1 на стр. 12)*
- *Настройка соединения с серверами (п. 2.1.2 на стр. 12)*
- *Настройка порогов срабатывания для индикатора нагрузки (п. 2.1.3 на стр. 14)*
- *Настройка запуска служб (п. 2.1.4 на стр. 15)*
- *Настройка механизма уведомлений (п. 2.1.5 на стр. 15)*
- *Просмотр индикаторов мониторинга (п. 2.1.6 на стр. 16)*

2.1.1. 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).

2.1.2. 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; подробнее см. п. 2.1.2.1 на стр. 14).

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.

2.1.2.1. Настройка соединения с сервером Device Monitor

Если в схеме развёртывания системы InfoWatch Traffic Monitor присутствует InfoWatch Device Monitor (на ТМ пересылаются данные, перехваченные Device Monitor), то вы можете настроить индикатор Device Monitor Status, обеспечивающий проверку работоспособности сервера Device Monitor. Для этого:

1. В конфигурационном файле /etc/nagios/iwmon/iwmon-hosts.cfg:
   - Расскомментируйте секцию host, где указан сервер Infowatch Device Monitor Server. В параметре address укажите актуальный IP-адрес сервера Device Monitor
   - Расскомментируйте секцию hostgroup для группы DM-servers.
2. В конфигурационном файле /etc/nagios/iwmon/iwmon-services-dm.cfg раскомментируйте блок define service.
3. В конфигурационном файле /etc/nagios/iwmon/iwmon-commands.cfg раскомментируйте блок с командой iwmon_check_dm.

2.1.3. 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.

2.1.4. 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
```

2.1.5. Настройка механизма уведомлений

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

В разделе:

- *Настройка отправки уведомлений о превышении порога для индикаторов (п. 2.1.5.1 на стр. 15)*
- *Настройка отправки писем-уведомлений с помощью Postfix (п. 2.1.5.2 на стр. 16)*

2.1.5.1. 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.

2.1.5.2. Настройка отправки писем-уведомлений с помощью Postfix

Если Система установлена так, что:

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

2.1.6. Просмотр индикаторов мониторинга

Мониторинг доступен через веб-интерфейс по следующему адресу: http://имя_сервера/nagios/, где `имя_сервера` – имя или IP-адрес сервера, на котором расположена подсистема мониторинга.

Параметры учетной записи для доступа, по умолчанию:

- пользователь **nagiosadmin**
- пароль **nagiosadmin**

Изменить имя пользователя или пароль для доступа можно в файле `/etc/nagios/htpasswd.users` с помощью следующей команды:

```
htpasswd /etc/nagios/htpasswd.users <ИМЯ ПОЛЬЗОВАТЕЛЯ>
```

Просмотр состояния системы и хостов

Общее состояние системы, а также состояние каждого из серверов, на которых развёрнута Система, может принимать одно из следующих значений:

- работает,
- частично неработоспособно,
- полностью неработоспособно.

Просмотр состояния индикаторов

Просмотр состояния индикаторов осуществляется в разделе **Services**.

Для каждого индикатора отображается следующая информация:

- **Service** – название индикатора.
- **Status** – текущее значение индикатора:
  - – CRITICAL, значение проверяемого параметра превышает критический порог;
  - – WARNING, значение проверяемого параметра находится в зоне предупреждения (если такая предусмотрена);
  - – OK, значение параметра находится в норме.
- **Last Check** – дата и время последней проверки.
- **Duration** – время, которое индикатор находится в текущем статусе.
- **Attempt** – номер попытки (из общего числа возможных попыток), с которой был получено значение индикатора.
- **Status Information** – подробная информация о результатах проверки.

Если значение индикатора получить не удалось, то считается, что текущее значение индикатора превышает пороговое значение.

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

- `iwmon-services-ntp.cfg` – настройка проверки синхронизации времени (индикатор **NTP time**);
- `iwmon-services-db.cfg` – настройка индикаторов для базы данных;
- `iwmon-services-loadavg.cfg` – настройка параметров нагрузки на серверы (индикатор **Current Load**);
- `iwmon-services-traffic.cfg` – настройка списка проверяемых подсетей (индикатор **Check Traffic**);
- `iwmon-services-dm.cfg` – включение диагностики сервера Device Monitor (индикатор **Device Monitor Status**);
- `iwmon-services.cfg` – настройка остальных индикаторов.

В Приложении В на стр. 91 перечислены все индикаторы с указанием пороговых значений, периодичности, с которой запускается проверка, а также приведены рекомендации для действий администратора при достижении индикаторами пороговых значений.

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

2.2. Подсистема мониторинга для установки «все-в-одном»

Если система InfoWatch Traffic Monitor установлена так, что все серверные компоненты (сервер базы данных, серевра 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.

Чтобы войти в веб-консоль:

1. В адресной строке любого браузера введите IP-адрес сервера Traffic Monitor.
2. Укажите параметры учётной 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 учётной записи, заданные по умолчанию. Настоятельно рекомендуется после установки Консоли управления изменить пароль учётной записи администратора пользователей. О том, как это сделать, см. *«InfoWatch Traffic Monitor. Руководство пользователя»*.

3. Нажмите **Authentificate**.

Далее в разделе описаны следующие возможности веб-консоли:

- *Интерфейс веб-консоли (см. п. 2.2.1 на стр. 18)*
- *Настройка адреса сервера синхронизации времени (см. п. 2.2.2 на стр. 22)*
- *Управление лицензиями (см. п. 2.2.3 на стр. 22)*
- ***Ошибка! Источник ссылки не найден.*** *(см. п.* ***Ошибка! Источник ссылки не найден.*** *на стр.* ***Ошибка! Закладка не определена.****)*
- *Работа с индикаторами мониторинга (см. п. 2.2.4 на стр. 23)*
- *Скачивание дистрибутива Management Console (см. п. на стр. 2.2.5 на стр. 24)*
- *Сбор диагностических данных (см. п. 2.2.6 на стр. 24)*

2.2.1. Интерфейс веб-консоли

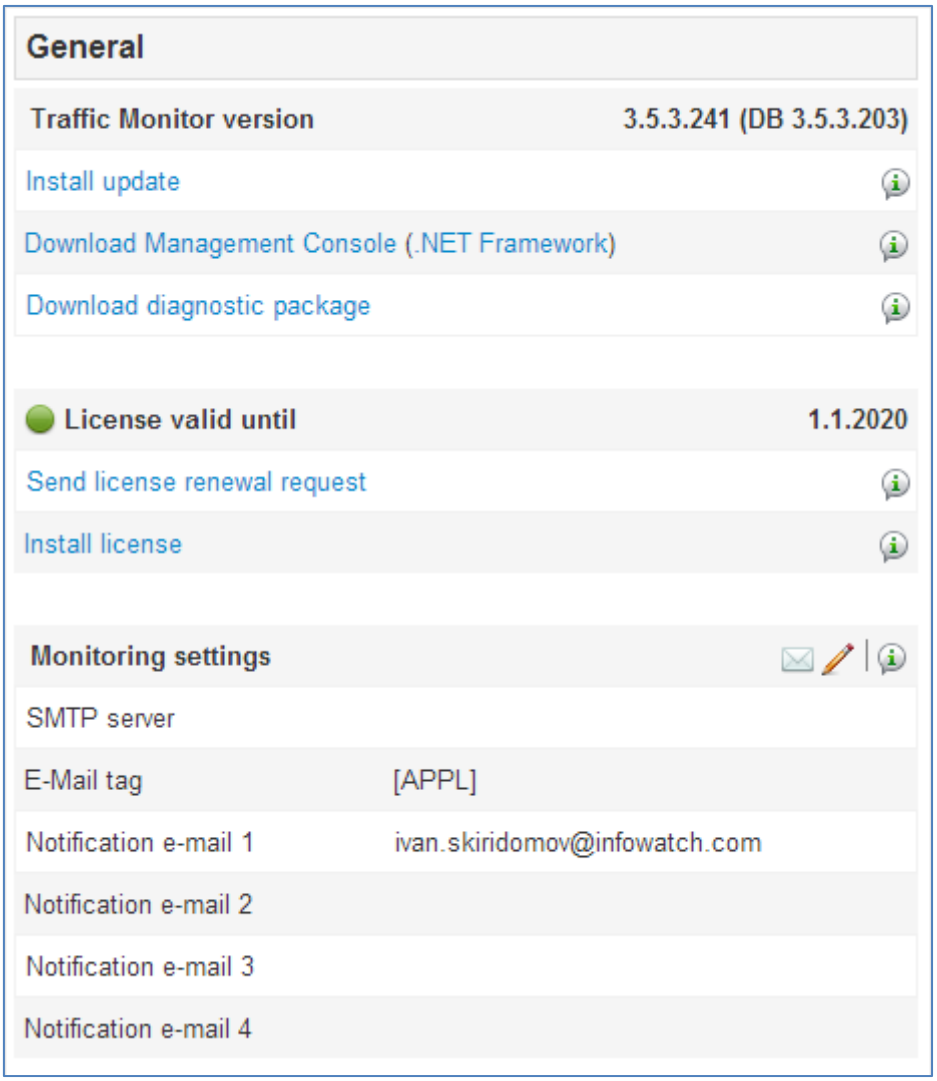
В данном разделе приведено описание элементов веб-консоли, с помощью которой администратор может управлять сервером Traffic Monitor, а также приведены ссылки на другие подразделы данного документа, где вы можете узнать подробности о возможностях диагностики и управления сервером с помощью того или иного элемента.

Веб-консоль IWTM условно разделена на три основных области:

- **General** – установка обновлений, загрузка Консоли управления, управление лицензиями и уведомлениями мониторинга: см. п. 2.2.1.1 на стр. 19.
- **Network** – управление сетевыми параметрами: см. п. 2.2.1.2 на стр. 20.
- **System monitoring** – индикаторы мониторинга: см. п. 2.2.1.3 на стр. 21.

2.2.1.1. Раздел General

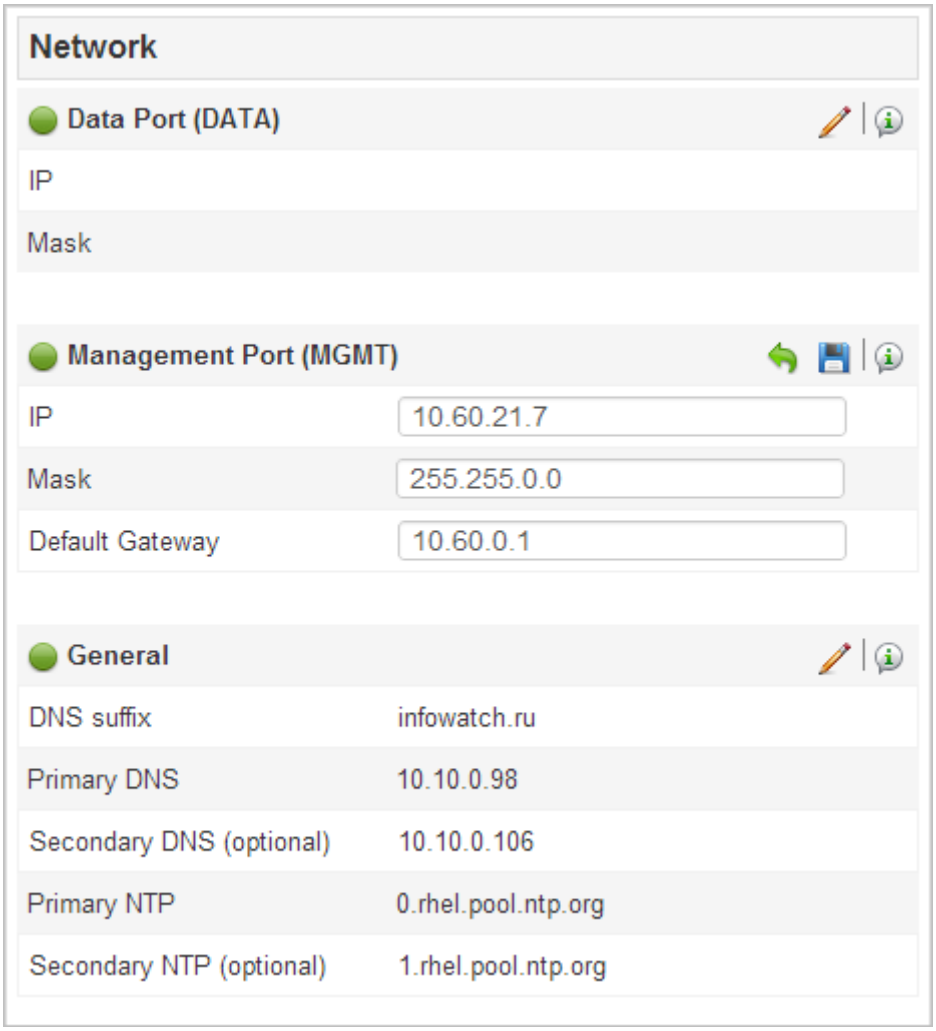
В разделе **General** расположена информация о версии системы, сроке действия лицензии, доступны установка обновлений, загрузка Консоли управления, а также управление лицензиями и уведомлениями мониторинга.



Параметр	Описание, ссылки
Traffic Monitor version	Версия сервера Traffic Monitor. В скобках указана версия базы данных.
Install Update	Установка обновлений сервера. Подробнее см. п. **Ошибка! Источник ссылки не найден.** на стр. **Ошибка! Закладка не определена.**.
Download Management Console (.Net Framework)	Загрузка дистрибутива Консоли Управления Traffic Monitor. Подробнее см. п. 2.2.5 на стр. 24
Download diagnostic package	Сбор диагностических данных. Подробнее см. п. п. 2.2.6 на стр. 24
License valid until	Дата окончания действия установленной лицензии.
Send license renewal request	Отправка запроса на обновление лицензии. Подробнее см. п. 2.2.3.1 на стр. 23.
Install license	Установка лицензии. Подробнее см. п. 2.2.3.2 на стр. 23.
Monitoring settings	Группа настроек уведомлений от подсистемы мониторинга. Подробнее см. п. 2.2.4.1 на стр. 23

2.2.1.2. Раздел Network

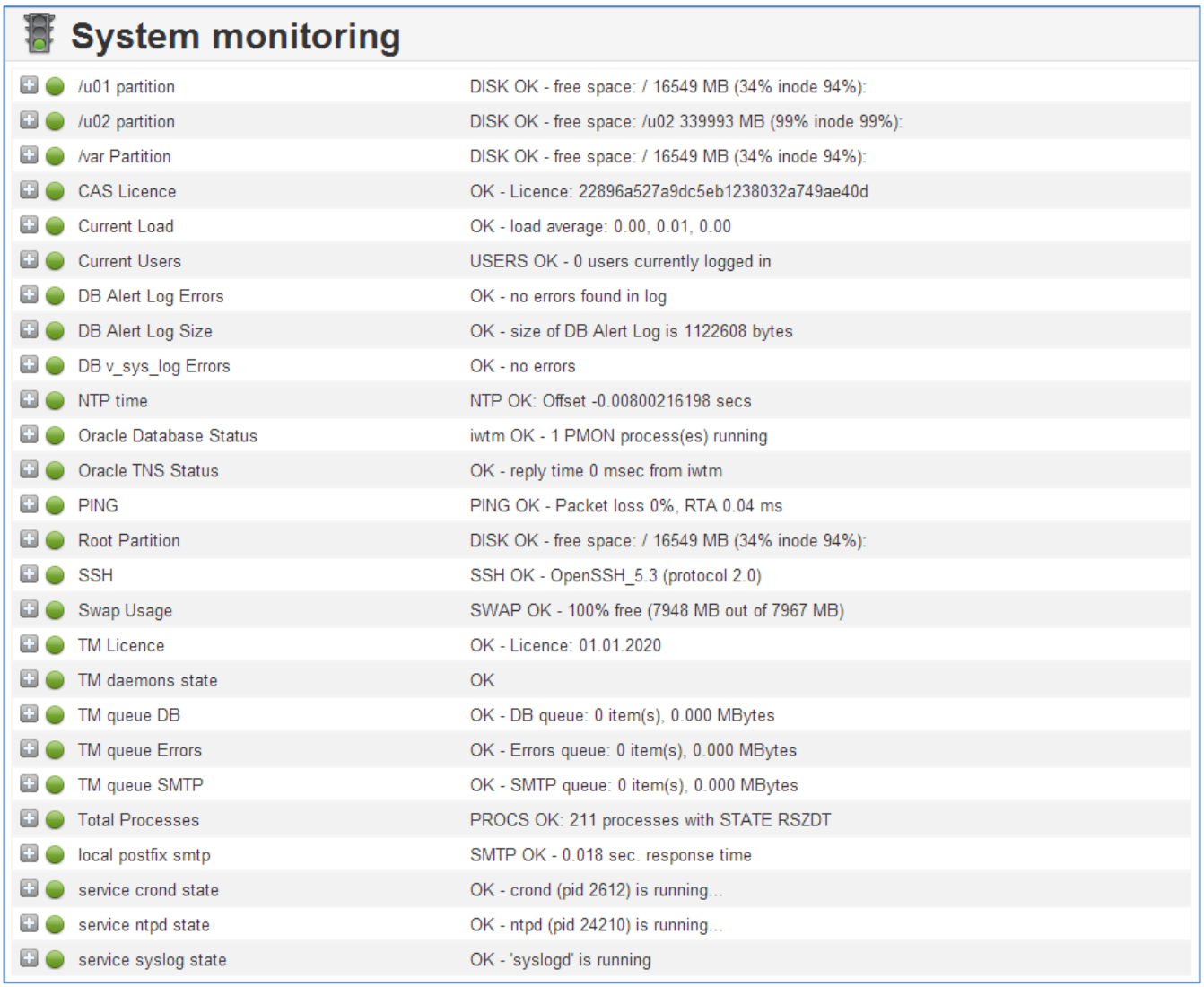
В разделе **Network** отображается и настраивается информация о сетевых подключениях сервера IWTM.



Параметр	Описание
Data Port (DATA)	Сетевые параметры порта, используемого для передачи трафика на анализ с серверов ICAP, SPAN-копии; из системы InfoWatch Device Monitor и т.д.
Management Port (MGMT)	Сетевые параметры порта, используемого для подключения Консоли Управления к серверу IWTM. Также данный порт может использоваться для передачи трафика на анализ.
General	Общие сетевые параметры сервера IWTM: DNS, NTP

2.2.1.3. Раздел System monitoring

В разделе **System monitoring** расположены индикаторы подсистемы мониторинга, позволяющие диагностировать состояние тех или иных компонент системы.



Для каждого индикатора отображается его текущее состояние:

- – значение параметра находится в норме
- – значение проверяемого параметра находится в зоне предупреждения (если такая предусмотрена)
- – значение проверяемого параметра превышает критический порог.

Общая информация о текущем состоянии индикатора указана в строке; чтобы получить более подробные данные, нажмите в начале строки индикатора.

Описание индикаторов, их пороговых значений, периодов опроса, а также действия, которые должен предпринять администратор системы при достижении индикаторами пороговых значений, приведены в Приложении А на стр. 91.

2.2.2. Настройка адреса сервера синхронизации времени

Основные сетевые параметры сервера InfoWatch Traffic Monitor задаются в процессе установки (см. документ «*InfoWatch Traffic Monitor. Руководство по установке и конфигурированию*». 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 **General**, нажмите  **Edit**.
2. Укажите IP-адрес NTP-сервера в поле **Primary NTP**
3. При необходимости вы можете задать параметр **Secondary NTP**.
4. Сохраните изменения, нажав  **Save**.
5. После изменения IP адресов необходимо выполнить команду `service network restart`.

2.2.3. Управление лицензиями

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. 2.2.4.1 на стр. 23.

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.
- Если требуется изменить настройки передачи трафика согласно новой схеме развертывания, замените лицензионный ключ с учётом 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 лицензии на другой компьютер функциональность InfoWatch Traffic Monitor будет недоступна.
- При полной переустановке системы InfoWatch Traffic Monitor вам потребуется заново установить лицензию. Поэтому рекомендуется сохранить файл `iw_license.dat` на внешнем носителе информации.

Чтобы установить новый лицензионный ключ или заменить текущий:

1. Запросите лицензионный ключ как описано в п. 2.2.3.1 на стр. 23.
2. Установите полученный лицензионный ключ как описано в п. 2.2.3.2 на стр. 23.

2.2.3.1. Отправка запроса на обновление лицензии

Чтобы запросить обновлённую 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. Не изменяйте этот код.

2. Отправьте письмо.

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

2.2.3.2. Установка лицензии

Чтобы установить лицензию Traffic Monitor:

1. Разместите лицензионный ключ (файл **iw_license.dat**), полученный от InfoWatch в результате запроса (см. п. 2.2.3.1 на стр. 23), 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 **ОК**.
4. Дождитесь установки лицензии (статус **Installing license…**).

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

2.2.4. Работа с индикаторами мониторинга

Подсистема мониторинга системы InfoWatch Traffic Monitor обеспечивает удаленный мониторинг параметров сервера, сетевых служб и других индикаторов состояния системы.

Подсистема периодически получает значения индикаторов и сравнивает полученные результаты с пороговыми значениями. Вы можете просмотреть информацию о текущем состоянии индикаторов в веб-консоли, в разделе **System monitoring**. Чтобы получить более подробные данные, нажмите  в начале строки индикатора.

Описание индикаторов, их пороговых значений, периодов опроса, а также действия, которые должен предпринять администратор системы при достижении индикаторами пороговых значений, приведены в Приложении В на стр. 91.

Подсистема мониторинга также обеспечивает отправку уведомлений администратору системы в случае, если хотя бы один из индикаторов достигает порогового значения. О том, как настроить отправку уведомлений, см. п. 2.2.4.1 на стр. 23.

2.2.4.1. Настройка уведомлений подсистемы мониторинга

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 придёт тестовое письмо.

2.2.5. Скачивание дистрибутива Management Console

Приложение InfoWatch Traffic Monitor Management Console (Консоль Управления) – это основной инструмент для управления настройками Системы и мониторинга результатов её работы. Подробнее о работе с Консолью управления см. документ *«InfoWatch Traffic Monitor. Руководство пользователя»*.

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**.

О порядке установки Консоли Управления см. документ «*InfoWatch Traffic Monitor. Руководство по установке и конфигурированию*».

2.2.6. Сбор диагностических данных

В случае возникновения каких-либо проблем с системой, которые невозможно решить с помощью стандартных процедур, описанных в пользовательской документации и в разделе База знаний на сайте InfoWatch (http://cp.infowatch.com/kb/), вы можете обратиться в службу технической поддержки InfoWatch. Для решения некоторых проблем может потребоваться сбор диагностических данных о системе.

Веб-консоль IWTM позволяет собирать диагностическую информацию с сервера Traffic Monitor с помощью утилиты **sosreport** - стандартной утилиты Linux, предназначенной для сбора подробной информации о системе: характеристики оборудования, список установленных пакетов, произведенные настройки и т.п.

Чтобы получить диагностические данные о системе:

1. В веб-консоли, в разделе **Monitoring settings**, нажмите **Download diagnostic package**.
2. Дождитесь окончания процесса сбора информации (отображается статус «**collecting…**»), не производите никаких настроек.
3. Когда появится ссылка **download link**, нажмите на неё для загрузки пакета с диагностическими данными.

Полученный файл вида `sosreport-iwdb-xxx-yyy.tar.xz`, где `xxx` – имя сервера, а `yyy` – дата и время формирования файла, можно отправлять в службу технической поддержки.

ГЛАВА 3. КОНФИГУРИРОВАНИЕ ПЕРЕХВАТЧИКА CRAWLER

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

Подсистема Crawler работает как один из перехватчиков Traffic Monitor.

В работе Crawler участвуют следующие компоненты системы InfoWatch Traffic Monitor:

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

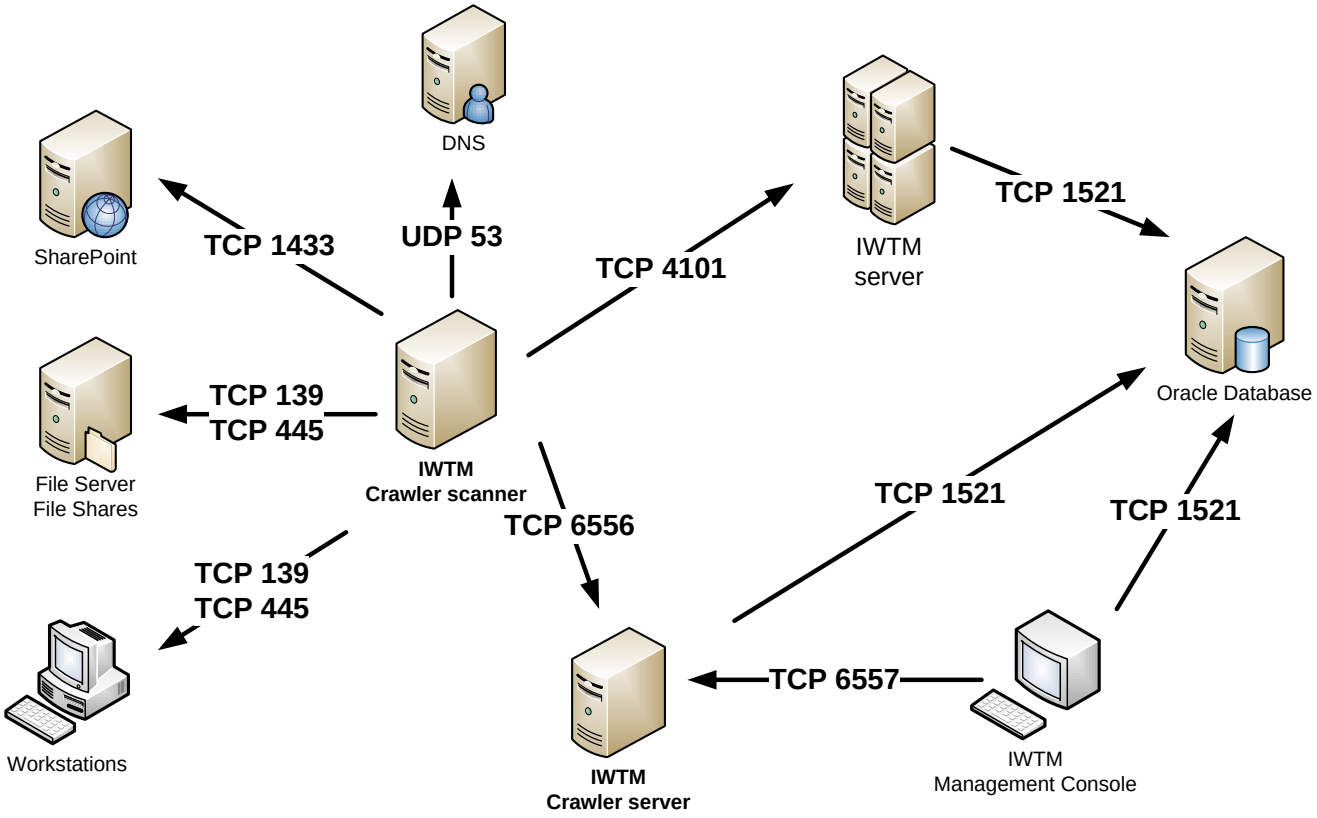
Более подробная информация о настройке Crawler изложена в следующих разделах:

- *Настройка сетевых правил доступа (п. 3.1 на стр. 25)*
- *Конфигурационные файлы Crawler (п. 3.2 на стр. 27)*
- *Работа с журналами Crawler (п. 3.3 на стр. 29)*

3.1. Настройка сетевых правил доступа

Если сегменты сети, где развернута система InfoWatch Traffic Monitor с Crawler, разделены между собой межсетевыми экранами, для корректной работы Crawler должны быть открыты TCP порты **6556** (подключение сканера Crawler к серверу Crawler) и **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 в 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` (подробнее см. п. 5.2.20 на стр. 67)
Сканер Crawler – файловое хранилище SharePoint (сервер MS SQL)	TCP 1443	

Если какие-либо компоненты системы принадлежат разным контроллерам доменов, то для работы Crawler в такой системе должно быть настроено доверительное отношение (Domain Trust) этих контроллеров. Однако необходимо учитывать, что удалённость 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.

3.2. Конфигурационные файлы Crawler

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

- **Сервер Crawler** – `InfoWatch.Crawler.Server.exe.config`. Расположен в том же каталоге, что и исполняемый файл `InfoWatch.Crawler.Server.exe` (по умолчанию – `C:\Program Files\InfoWatch\Crawler\Server` для 32-битных систем и `C:\Program Files (x86)\InfoWatch\Crawler\Server` для 64-битных). Подробнее см. п. 3.2.1 на стр. 27.
- **Сканер Crawler** – `InfoWatch.Crawler.Scanner.exe.config`. Расположен в том же каталоге, что и исполняемый файл `InfoWatch.Crawler.Scanner.exe` (по умолчанию – `C:\Program Files\InfoWatch\Crawler\Scanner` для 32-битных систем и `C:\Program Files (x86)\InfoWatch\Crawler\Scanner` для 64-битных). Подробнее см. п. 3.2.2 на стр. 28.

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

3.2.1. Конфигурационный файл сервера Crawler

Администратор, обслуживающий систему, может выполнить некоторые низкоуровневые настройки сервера Crawler с помощью конфигурационного файла `InfoWatch.Crawler.Server.exe.config`. Конфигурационный файл размещается в том же каталоге, что и исполняемый файл `InfoWatch.Crawler.Server.exe` (по умолчанию - `C:\Program Files\InfoWatch\Crawler\Server` для 32-битных систем и `C:\Program Files (x86)\InfoWatch\Crawler\Server` для 64-битных).

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

Первоначальная настройка параметров выполняется во время установки Crawler (см. п. 3.2 на стр. 27).

Далее описаны параметры, которые может потребоваться изменять. Изменять остальные параметры настоятельно не рекомендуется.

- **Строка соединения с базой данных**. Если изменились параметры подключения к БД Oracle с используемой схемой IWTM, в разделе `<connectionStrings>`, параметр `CrawlerEntities`, внесите соответствующие изменение в значение `connectionString`.
- **Пароль учетной записи владельца схемы IWTM**, от имени которой выполняется подключение к БД. Если пароль изменился, укажите новый пароль в разделе `<appSettings>`:

  ```
  <add key="NewDbPassword" value="новый_пароль" />
  ```

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

  > **Примечание:**
  >
  > Если требуется сменить учётную запись, от имени которой запускается сервер, то перед первым запуском службы сервера необходимо ввести пароль от БД в поле `NewDbPassword`, так как зашифрованный пароль может быть расшифрован только пользователем, зашифровавшим его. Подробнее см. п. 3.2.1.1 на стр. 28.

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

  ```
  <value>номер_порта</value>
  ```

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

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

1. На компьютере, где работает сервер Crawler, в списке служб Windows найдите службу `iw_crawler_server` и остановите её.
2. В конфигурационном файле сервера `InfoWatch.Crawler.Server.exe.config` (подробнее см. п. 3.2.1 на стр. 27), в параметре `NewDbPassword` введите пароль учетной записи владельца схемы IWTM, от имени которой выполняется подключение к БД. Сохраните изменения в конфигурационном файле.
3. Вернитесь к службе `iw_crawler_server` и вызовите её **Свойства** (**Действия -> Свойства** или выберите в контекстном меню, открывающемся по нажатию правой кнопки мыши на строке сервиса). На вкладке Вход в систему укажите параметры учётной записи, от имени которой должна запускаться служба сервера Crawler.
4. Запустите службу сервера.

3.2.2. Конфигурационный файл сканера Crawler

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

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

Параметры, которые могут понадобиться для изменения администратором Системы:

Параметр	Описание
Address	Строка соединения с сервером Crawler. При изменении расположения сервера Crawler вы можете указать необходимый IP-адрес или имя сервера. Для разных доменов или рабочих групп можно отключить использование шифрованного соединения, изменив значение параметра `bindingConfiguration` с `EncryptedBinding` на `PlainBinding`
FilesSentToTmLogPath	Директория, в которой будет сохранен файл, содержащий список файлов, подготовленных для отправки на сервер Traffic Monitor для анализа. Значение по умолчанию - %appdata%\InfoWatch\TM\ScanLogs
LogFilesSentToTm	Показатель того, будет ли сохраняться на компьютере список файлов, подготовленных для отправки на сервер Traffic Monitor (значение `true`), или не будет (значение `false`)
SendFilesToTM	Показатель того, будут ли файлы, перехваченные подсистемой Crawler, отправляться для анализа на сервер Traffic Monitor (значение `true`) или не будут (значение `false`). Важная информация! Данный параметр имеет силу, если параметру `LogFilesSentToTm` указано значение `true`

> **Важная информация!**
>
> Изменять параметры, не описанные в данном пункте, настоятельно не рекомендуется.

3.3. Работа с журналами Crawler

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

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

Изменение расположения файлов журнала

Расположение файлов журнала определяется в конфигурационных файлах (`InfoWatch.Crawler.Server.exe.config` и `InfoWatch.Crawler.Scanner.exe.config`: см. п. 3.2 на стр. 27), в секции *<configuration>*, значение для `<listeners>`, например:

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

Настройка уровня логирования Crawler

Настройка уровня логирования выполняется в конфигурационных файлах (`InfoWatch.Crawler.Server.exe.config` и `InfoWatch.Crawler.Scanner.exe.config`: см. п. 3.2 на стр. 27).

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

ГЛАВА 4. АДМИНИСТРИРОВАНИЕ БАЗЫ ДАННЫХ

В этой главе:

- *Проведение регламентных работ на сервере базы данных (п. 4.1 на стр. 30).*
- *Табличные пространства в базе данных InfoWatch Traffic Monitor (п. 4.2 на стр. 31).*
- *Управление ежедневными табличными пространствами (п. 4.3 на стр. 33).*
- *Резервное копирование базы данных (п. 4.4 на стр. 39).*

4.1. Проведение регламентных работ на сервере базы данных

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

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

1. Закройте все экземпляры Management Console. Убедитесь, что отсутствуют соединения со схемой БД Traffic Monitor из других программ; если такие соединения есть – отключите их.
2. На сервере Traffic Monitor остановите процессы ТМ:

   ```
   service iw-trafmon stop
   ```

3. Убедитесь, что не настроен автозапуск процессов ТМ:

   ```
   ll /etc/cron*
   crontab -l
   ```

   Если в файле `crontab` присутствует такая настройка, отключите её на период выполнения регламентных работ.

4. На сервере базы данных получите список заданий, запускающихся по расписанию. Для этого в sqlplus, из-под учетной записи владельца схемы выполните запрос:

   ```
   select JOB_NAME, STATE
   from user_scheduler_jobs u
   where u.enabled = 'TRUE'
   ```

5. Выключите задания, выполнив сценарий:

   ```
   BEGIN
     dbms_scheduler.disable('JOB_1',true);
     …
     dbms_scheduler.disable('JOB_N',true);
   COMMIT;
   END;
   /
   ```

   где `JOB_1… JOB_N` – имена выключаемых заданий.

6. Убедитесь, что ни одно задание не выполняется, выполнив запрос:

   ```
   SELECT job_name
   FROM user_scheduler_running_jobs
   ```

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

```
BEGIN
  dbms_scheduler.stop_job('имя_задания');
COMMIT;
END;
/
```

7. Выполните необходимые работы с базой данных.
8. По окончании необходимых работ, с сервера Traffic Monitor проверьте соединение с сервером базы данных:

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

   Здесь `db_login` и `db_password` – имя и пароль владельца схемы базы данных, а `tns_name` – имя службы TNS.

   Если проверка пройдена успешно, то в ответ на выполнение команды будет выведено приглашение SQL *Plus:

   ```
   SQL>
   ```

9. Если на Шаге 3 вы отключали автозапуск процессов в `crontab`, то включите его.
10. Запустите процессы Traffic Monitor Server:

    ```
    service iw-trafmon start
    ```

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

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

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

12. Включите выполнение ранее отключенных заданий:

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

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

4.2. Табличные пространства в базе данных InfoWatch Traffic Monitor

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

Тип табличного пространства	Назначение
Основное	Хранение настроек, которые нужны для анализа и обработки объектов (конфигурация, теги, цвета и пр.). Управление системой через Management Console (роли, учетные записи пользователей и др.)
Ежедневное	Хранение объектов, перехваченных в течение одних суток. Хранение информации о результатах анализа и обработки объектов (разобранный объект, категории, термины и др.)

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

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

Параметры, предназначенные для управления сегментами данных, задаются при настройке схемы базы данных, но могут быть переопределены после создания схемы (см. п. 4.3 на стр. 33).

Информация по статусам ежедневных табличных пространств приводится в п. 4.2.1 на стр. 32.

4.2.1. Статусы ежедневных табличных пространств

> **Примечание:**
>
> Список ежедневных ТП и их текущий статус можно посмотреть в Management Console (раздел **Использование БД**).

Список статусов с кодами приводится в таблице 1.

Таблица 1. Статусы ежедневных ТП

Код статуса	Название	Значение	Описание
1	ReadWrite	Чтение и запись	Присваивается каждому новому ежедневному ТП. Можно добавлять, изменять, удалять данные, хранящиеся в ежедневном ТП (например, выборка объектов по запросу, присвоение объекту тегов и т. п.)
2	Offline	Отключено от базы данных	Присваивается в результате выполнения процедуры отключения ежедневного ТП от базы данных. Пользователи не смогут получить доступ к данным, пока ТП не будет восстановлено
3	Restored	Восстановлено	Присваивается табличному пространству, которое было восстановлено из архива Пользователи могут просматривать и изменять данные, хранящиеся в ТП (выборка объектов по запросу, присвоение объекту тегов и т. п.)
4	InProgress	В обработке	Промежуточные состояния. Используются в процедурах отключения и восстановления ежедневных ТП. Время, в течение которого ежедневное ТП находится в каждом из этих состояний, зависит от размера отключаемого ТП, а также от производительности и загрузки сервера базы данных. Максимальное время составляет 1 час. Превышение этого значения свидетельствует о возникновении ошибочной ситуации. Для разрешения ошибки обратитесь в службу технической поддержки
5	ReadOnly	Только чтение	
6	PreparedForOffline	Подготовлено к отключению	

В таблице 2 приводятся возможные переходы между статусами. Знак «+» означает, что переход возможен. Знаком «-» отмечены невозможные переходы.

Таблица 2. Переходы между статусами ежедневных ТП

Исходный статус	Конечный статус					
	ReadWrite	ReadOnly	Offline	Restored	InProgress	PreparedForOffline
ReadWrite	-	+	-	-	+	-
ReadOnly	-	-	-	-	+	-
Offline	-	-	-	-	-	+
Restored	-	-	-	-	+	-
InProgress	-	-	-	-	-	+
PreparedForOffline	-	-	+	+	-	-

4.3. Управление ежедневными табличными пространствами

В этом разделе:

- *Настройка размещения файлов на файловой системе (п. 4.3.1 на стр. 33).*
- *Индексирование данных в ежедневных табличных пространствах (п. 4.3.2 на стр. 34).*
- *Архивирование ежедневных табличных пространств (п. 4.3.3 на стр. 36).*
- *Восстановление ежедневных табличных пространств (п. 4.3.4 на стр. 37).*
- *Удаление ежедневных табличных пространств (п. 4.3.5 на стр. 38).*

4.3.1. Настройка размещения файлов на файловой системе

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

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

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

Первый день – ежедневное табличное пространство создается в файловой системе 1.

Второй день – ежедневное табличное пространство создается в файловой системе 2.

Третий день – ежедневное табличное пространство создается в файловой системе 3.

Четвертый день – ежедневное табличное пространство создается в файловой системе 1.

…

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

Пример сценария, изменяющего количество отдельных мест хранения ежедневных ТП:

```
BEGIN
   part.set_df_path_cnt('4');
COMMIT;
```

```
END;
/
```

Важная информация!

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

Пример сценария изменяющего пути для расположения ежедневных ТП:

```
BEGIN
   part.set_df_path('/test1/', 1);
   part.set_df_path('/test2/', 2);
   part.set_df_path('/test3/', 3);
   part.set_df_path('/test4/', 4);
COMMIT;
END;
/
```

Примечание:

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

4.3.2. Индексирование данных в ежедневных табличных пространствах

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

Примечание:

При необходимости вы можете останавливать и запускать задание вручную (см. п. 4.1 на стр. 30).

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

```
select t.REQ_START_DATE, t.actual_start_date, t.RUN_DURATION
from sys.user_scheduler_job_run_details t
where t.job_name='IWTM_SYNC_INDEXES' and t.LOG_DATE > sysdate - 3/24
```

По результатам запроса выводится информация о работе задания на индексацию данных за последние 3 часа. Если интервал индексации не менялся, то задание должно запускаться каждые 10 минут и выполняться менее чем за 20 минут. При сильной загрузке базы данных следует выполнять эту проверку периодически, с интервалами в несколько часов.

Изменение интервала индексации

Примечание:

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

Чтобы изменить интервал индексации, запустите сценарий:

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

```
COMMIT;
END;
/
```

где:

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

Далее показано несколько примеров использования сценария.

Пример 1. Запуск индексации 1 раз в минуту

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

Пример 2. Запуск индексации 1 раз в 2 часа

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

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

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

4.3.3. Архивирование ежедневных табличных пространств

Важная информация!

1. Помимо описанного штатного способа, вы можете настроить автоматическое архивирование ежедневных табличных пространств с помощью специальной утилиты, входящей в состав дистрибутива Системы. Работа с утилитой описывается в приложении А на стр. 86.
2. Если в качестве интервала времени используются месяцы или годы, то рекомендуется в расчете использовать максимальное значение интервала. Для месяца – 31 день. Для года – 366 дней. Например, чтобы удалять ежедневные ТП старше 4-х лет, в задании IWDROP укажите интервал 366*4=1464 дня.

С целью освобождения пространства на жестком диске вы можете периодически архивировать устаревшие данные. Архив с данными рекомендуется размещать на внешних носителях информации. При необходимости эти данные могут быть восстановлены.

Шаг 1. Выборка ежедневных табличных пространств и файлов данных

Список отключаемых табличных пространств можно получить, выполнив запросы к базе данных от имени владельца схемы базы данных. Запросы составляются в соответствии со стратегией архивирования, принятой в вашей организации. Например, для выборки ежедневных ТП, в которых хранятся объекты, перехваченные более 100 дней назад, можно применить следующий запрос:

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

Важная информация!

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

Для выборки файлов данных в этом случае создается следующий запрос:

```
SELECT f.file_name
FROM dba_data_files f
WHERE f.tablespace_name in
   (
      SELECT t.tbs_name
      FROM tbs_list t
      WHERE t.part_date < trunc(SYSDATE) - 100 + 23 / 24 AND t.status IN (1, 2)
   )
```

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

Примечание:

Полный список кодов и значений статусов приведен в таблице 1.

Шаг 2. Отключение ежедневных табличных пространств от базы данных

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

1. От имени владельца схемы базы данных вызовите процедуру:

```
BEGIN
  -- Вызов процедуры
  part.part_disconnect(.дата_табличного_пространства., true);
COMMIT;
END;
/
```

   где `.дата_табличного_пространства.` – дата перехвата объектов, хранящихся в табличном пространстве. Эту дату можно узнать, выполнив запрос на выбор списка ежедневных ТП, подлежащих архивированию. Например, для ежедневного ТП, где хранятся объекты, перехваченные 3 февраля 2008 года, вызов процедуры будет выглядеть следующим образом:

```
BEGIN
  -- Вызов процедуры
  part.part_disconnect(TO_DATE('03.02.2008','dd.mm.yyyy'),
   true);
COMMIT;
END;
/
```

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

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

Шаг 3. Перенос файлов данных

Перенесите файлы данных, принадлежащие отключенным ежедневным ТП, на другой носитель информации.

Список файлов данных для всех отключенных табличных пространств нужно взять из запроса, описанного на шаге 2.

4.3.4. Восстановление ежедневных табличных пространств

> **Важная информация!**
>
> Табличное пространство можно восстанавливать только в той схеме базы данных, в которой оно было отключено (даже если эта схема была обновлена). Не допускается полная переустановка схемы базы данных, от которой было отключено табличное пространство, так как в этом случае вы не сможете восстановить табличное пространство.

Шаг 1. Проверка прав на восстановление данных

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

Шаг 2. Перемещение файлов данных

Для восстановления ежедневного ТП необходимо переместить файлы данных этого табличного пространства с внешнего носителя в нужный каталог.

Шаг 3. Подключение ежедневного табличного пространства

> **Важная информация!**
>
> Не подключайте ежедневное ТП во время работы заданий IWADDPARTS, IWDROP. Это может привести к повреждению данных.

1. От имени владельца схемы базы данных вызовите процедуру:

```
BEGIN
  part.part_restore(.дата_табличного_пространства., .путь_к_файлам_данных.);
COMMIT;
END;
/
```

> **Важная информация!**
>
> Путь к файлам данных должен начинаться и заканчиваться символом «/».

Если, например, ежедневное ТП, где хранятся объекты, перехваченные 3 февраля 2008 года, необходимо подключить в каталог /u01/oracle/data/, то вызов процедуры будет таким:

```
BEGIN
  part.part_restore(to_date('03.02.2008','dd.mm.yyyy'), '/u01/oracle/data/');
COMMIT;
END;
/
```

После выполнения процедуры статус ежедневного ТП изменится на *Восстановлено*.

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

4.3.5. Удаление ежедневных табличных пространств

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

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

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

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

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

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

Определение интервала времени для удаления ежедневных ТП

По умолчанию, процедура IWDROP выполняет удаление всех ежедневных табличных пространств, которые были созданы более 100 дней назад. Чтобы изменить этот интервал, от имени владельца схемы базы данных выполните следующий сценарий:

```
BEGIN
  part.set_drop_part_date_lag('drop_interval');
COMMIT;
END;
/
```

где `drop_interval` – период времени (в днях), который должен пройти от момента создания табличного пространства до удаления табличного пространства.

Включение запуска процедуры по расписанию

По умолчанию, автоматическое удаление ежедневных ТП отключено. Чтобы включить удаление всех ежедневных ТП согласно расписанию (ежедневно, в 00 ч. 30 мин. 00 с.), от имени владельца схемы базы данных выполните следующий сценарий:

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

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

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

Ручной запуск процедуры

Если вам требуется немедленный запуск процедуры удаления ежедневных ТП (например, из-за нехватки места в файловой системе - см. Приложение В на стр. 91 - был изменен интервал удаления, но следующий запуск задания произойдёт нескоро), от имени владельца схемы базы данных выполните следующий сценарий:

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

4.4. Резервное копирование базы данных

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

Опытные администраторы промышленных баз данных Oracle могут выполнять резервное копирование на работающей БД (процедура «горячего бэкапа») с помощью программы RMAN, рекомендуемой компанией Oracle (см. документацию Oracle), предварительно переведя БД Oracle в режим ARCHIVELOG.

Для специалистов, не являющихся администраторами Oracle, то есть не располагающих стандартными методами создания резервной копии БД, рекомендуется описанная ниже процедура «холодного бэкапа», выполняемая на остановленной БД. Данная процедура также может применяться для переноса базы данных с одного сервера на другой.

Далее в разделе:

- *Создание резервной копии базы данных (п. 4.4.1 на стр. 40);*
- *Восстановление базы данных из резервной копии (п. 4.4.2 на стр. 44).*

4.4.1. Создание резервной копии базы данных

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

- *Определение размера резервной копии (п. 4.4.1.1 на стр. 40);*
- *Проверка хранилища резервной копии (п. 4.4.1.2 на стр. 40);*
- *Создание папок для резервной копии (п. 4.4.1.3 на стр. 40);*
- *Создание вспомогательных файлов на Linux (п. 4.4.1.4 на стр. 41);*
- *Создание списка файлов, подлежащих резервному копированию (п. 4.4.1.5 на стр. 42);*
- *Остановка системы IWTM (п. 4.4.1.6 на стр. 43);*
- *Остановка БД Oracle (п. 4.4.1.7 на стр. 43);*
- *Копирование файлов БД в хранилище резервных копий (п. 4.4.1.8 на стр. 43).*

4.4.1.1. Определение размера резервной копии

Чтобы определить размер базы данных:

1. На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
2. Откройте Oracle SQL*Plus и подключитесь как пользователь sysdba:

   ```
   OS> sqlplus / as sysdba
   ```

   Если система была установлена с помощью 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
   ```

4.4.1.2. Проверка хранилища резервной копии

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

- Размещаться на компьютере, отличном от того, где работает база данных.
- Доступно с компьютеров, где работают сервера и базы данных, подлежащие 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.

4.4.1.3. 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
   ```

4.4.1.4. Создание вспомогательных файлов на Linux

Для обеспечения возможности восстановления из резервной копии, помимо самих файлов данных, вам потребуются вспомогательные файлы: **trace –файл** контрольного файла и 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 возвращён 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
    ```

4.4.1.5. 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
```

4.4.1.6. Остановка системы IWTM

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

Чтобы остановить систему IWTM:

1. На компьютере, где работают процессы IWTM, зайдите в систему от имени пользователя root.
2. Остановите все запущенные процессы IWTM:

```
OS> service 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
```

4.4.1.7. 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
```

4.4.1.8. Копирование файлов БД в хранилище резервных копий

1. Убедитесь, что все сервисы Oracle остановлены. Если сервисы Oracle не остановлены, файлы резервной копии могут быть повреждены и оказаться непригодными для восстановления.
2. На компьютере, где установлена БД, скопируйте 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.

4.4.2. Восстановление базы данных из резервной копии

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

- Если БД была повреждена вследствие сбоя системы или ошибки пользователя, восстановите старую БД. Например, если случайно был удалён важный файл, вы можете восстановить БД до состояния, когда этот файл ещё существовал: см. п. 4.4.2.1 на стр. 44.
- Если старая БД не может больше использоваться, создайте новую и восстановите данные на ней: см. 4.4.2.2 на стр. 44.

4.4.2.1. Восстановление на той же БД

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

Чтобы восстановить БД с помощью создания новой БД:

1. Убедитесь в работоспособности БД. Проверьте существующую схему БД, сервер БД, где размещена эта схема, и компьютер, на котором работает сервер БД.
2. Установите БД Oracle согласно инструкции, приведенной в документе «*InfoWatch Traffic Monitor. Руководство по установке и конфигурированию*».
3. Выполните следующие шаги:
   a. Удалите всё содержимое папок /u02/oradata/ и /u01/app/oracle/oradata/iwtm/
   b. Скопируйте содержимое папки **/opt/IWTM_Backup_Files/Oradata/** в папку **/u01/app/oracle/oradata/iwtm/**
   c. Скопируйте содержимое папки **/opt/IWTM_Backup_Files/IWTM/** в папку **/u02/oradata/**
   d. Переименуйте файл **control01.ctl**, расположенный в папке **/opt/IWTM_Backup_Files/Oradata/**, в **control02.ctl** и скопируйте его в папку **/u01/app/oracle/flash_recovery_area/iwtm/**
   e. Проверьте права.

      При необходимости, измените их:

```
OS> chown oracle:oinstall /u02/oradata –R
OS> chown oracle:oinstall /u01/app/oracle/oradata/iwtm/ -R
OS> chown oracle:oinstall /u01/app/oracle/flash_recovery_area/iwtm/ -R
```

4. Запустите БД

```
OS> dbstart $ORACLE_HOME
```

4.4.2.2. Восстановление на новой БД

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

1. В папке **/opt/IWTM_Backup_Files/Recovery_Aid** отредактируйте файл **initiwtm.ora** так, чтобы он соответствовал структуре каталогов новой БД.

2. Скопируйте отредактированный файл initiwtm.ora в папку **$ORACLE_HOME/dbs** на компьютер, где расположена новая БД.
3. На компьютере, где установлена БД Oracle, войдите в систему от имени пользователя **oracle**.
4. Откройте Oracle SQL*Plus и подключитесь как пользователь **sysdba**:

   ```
   OS> sqlplus / as sysdba
   ```

5. Сгенерируйте файл параметров

   ```
   SQL> create spfile from pfile;
   ```

6. Если нужно переименовать какие-либо файлы, воспользуйтесь следующим сценарием:

   ```
   OS> sqlplus / as sysdba
   SQL> startup mount
   SQL> alter database rename file '/<path_to_proddb_files>/<filename1>' to
   '/<path_to_clonedb_files>/<filename1>';
   …
   SQL> alter database rename file '/<path_to_proddb_files>/<filenameN>' to
   '/<path_to_clonedb_files>/<filenameN>';
   SQL> shutdown immediate
   ```

Здесь `path_to_proddb_files` – это путь к директории, где размещены файлы новой БД, на которую восстанавливается резервная копия, а `path_to_clonedb_files` - путь к директории, где размещены файлы резервной копии.

ГЛАВА 5. АДМИНИСТРИРОВАНИЕ СЕРВЕРНОЙ ЧАСТИ INFOWATCH TRAFFIC MONITOR

В этой главе:

- *Процессы Traffic Monitor Server (п. 5.1 на стр. 46)*
- *Настройка параметров работы Traffic Monitor Server (файл tm.conf) (п. 5.2 на стр. 51)*
- *Настройка использования OCR для различных перехватчиков (файл tm_ocr.conf) (п. 5.3 на стр. 70)*
- *Настройка параметров работы с HTTP-запросами, передаваемыми по протоколу ICAP (файл icap.conf) (п. 5.4 на стр. 72)*
- *Синхронизация базы отпечатков эталонных документов (п. 5.6 на стр. 75)*
- *Синхронизация базы отпечатков эталонных документов (п. 5.6 на стр. 75)*
- *Настройка правил фильтрации для Sniffer (п. 5.8 на стр. 77)*
- *Управление загрузкой объектов в удаленную базу данных (п. 5.9 на стр. 78)*
- *Архивирование каталога очереди сообщений (п. 5.10 на стр. 81)*
- *Протоколирование работы Системы (п. 5.11 на стр. 82)*
- *Перемещение объектов между очередями (утилита iw_qtool) (п. 5.12 на стр. 82)*
- *Загрузка очередей объектов (п. 5.13 на стр. 84)*
- *Восстановление работоспособности системы в аварийных ситуациях (п. 5.14 на стр. 84)*

5.1. Процессы Traffic Monitor Server

В этом разделе:

- *Список процессов Traffic Monitor Server (п. 5.1.1 на стр. 46).*
- *Работа с процессами Traffic Monitor Server (п. 5.1.2 на стр. 48).*
- *Проверка результатов обновления конфигурации (процесс iw_updater) (п. 5.1.3 на стр. 50).*

5.1.1. Список процессов Traffic Monitor Server

Имя процесса	Описание процесса и путь к файлу
iw_smtpd	Процесс, принимающий SMTP-письма. В случае интеграции с почтовым сервером Postfix, принимает входящие сообщения от Postfix. Если интеграция с Postfix отсутствует, то от корпоративного почтового сервера или от почтового клиента (в зависимости от настроек вашей почтовой системы). Принимает входящие сообщения в формате SMTP, преобразует в XML-контекст данные SMTP-конверта. Затем передает SMTP-письмо и XML-контекст процессу **iw_messed**. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_smtpd`

Имя процесса	Описание процесса и путь к файлу
iw_messed	Процесс обработки SMTP-писем. Извлекает данные из SMTP-письма. Затем извлеченные данные добавляются в XML-контекст, полученный от **iw_smtpd**. Готовый XML-контекст (содержащий данные конверта и письма) передается подсистеме анализа и принятия решения для проверки. По окончании анализа **iw_messed** передает SMTP-письма, доставка которых разрешена, компоненту почтовой системы, ответственному за доставку почты (только в нормальном и прозрачном транспортном режиме). В случае интеграции с почтовым сервером Postfix, таким компонентом является Postfix. Если интеграция с Postfix отсутствует, то, в зависимости от настроек вашей почтовой системы, таким компонентом может быть корпоративный почтовый сервер или почтовый клиент. Кроме того, копия проверенного SMTP-письма передается процессу **iw_dbloader** для сохранения в базу данных. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_messed`
iw_deliverd	Процесс доставки писем. Отправляет SMTP-письма получателям в случае, если доставка письма разрешена из Management Console (только в нормальном и прозрачном транспортных режимах). Также этот процесс доставляет SMTP-письма, которые по той или иной причине (например, ввиду отсутствия связи с почтовым relay-сервером или почтовым клиентом) не смог доставить процесс **iw_messed**. `/usr/local/infowatch/tm3/bin/iw_deliverd`
iw_expressd	Процесс обработки объектов, полученных от систем InfoWatch Device Monitor и DeviceLock. При получении данных (теневой копии файла, задания на печать) от InfoWatch Device Monitor или теневой копии файла от DeviceLock Adapter формирует XML-контекст из полученного объекта. Затем передает XML-контекст подсистеме анализа и принятия решения. По окончании анализа передает теневую копию файла процессу **iw_dbloader** для сохранения в базу данных. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_expressd`
iw_proxy	Процесс, принимающий копию трафика (HTTP, ICQ, SMTP). Для приема каждого вида трафика запускается отдельный экземпляр **iw_proxy**. Принимает объект (ICQ-сообщение, HTTP-запрос, SMTP-письмо). Формирует XML-контекст из полученного объекта. Затем XML-контекст передается подсистеме анализа и принятия решения. По окончании анализа копия объекта передается процессу **iw_dbloader** для укладки в базу данных. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_proxy`
iw_cas2d	Процесс сервера контентного анализа. Процесс **iw_cas2d** принимает от подсистемы анализа и принятия решения текстовые запросы в формате plain-text для проведения контентного анализа. По окончании контентного анализа возвращает результат запроса подсистеме анализа и принятия решения. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_cas2d`
iw_updater	Процесс, загружающий конфигурацию из базы данных на Traffic Monitor Server. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_updater`

Имя процесса	Описание процесса и путь к файлу
iw_dbloader	Процесс, загружающий объекты в базу данных. Принимает объекты (проверенные подсистемой анализа и принятия решения) от процессов **iw_messed**, **iw_expressd**, **iw_proxy**. Загружает полученные объекты в базу данных. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_dbloader`
iw_sniffer	Процесс, принимающий копию SMTP-, HTTP-, ICQ-трафика. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_sniffer`
iw_icap	Процесс обработки HTTP-трафика. Принимает HTTP-запросы от ICAP-клиента. Извлекает данные из HTTP-запросов. Затем извлеченные данные добавляются в XML-контекст. Готовый XML-контекст передается подсистеме анализа и принятия решения для проверки. По окончании анализа передает ICAP-клиенту ответ с разрешением/запрещением на доставку HTTP-запроса. Также передает HTTP-запрос процессу **iw_dbloader** для сохранения в базу данных. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_icap`
iw_qmover_client	Работает на Traffic Monitor Server, установленном в филиале. Отправляет перехваченные объекты в базу данных центрального офиса. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_qmover_client`
iw_qmover_server	Работает на Traffic Monitor Server, установленном в центральном офисе. Принимает объекты, полученные от клиента, установленного в филиале. Передает объекты процессу **iw_dbloader** для сохранения в базу данных. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_qmover_server`
iw_warpd	Управляет процессами извлечения данных из архивов, вложенных в перехваченные объекты. Путь к файлу: `/usr/local/infowatch/tm3/bin/iw_warpd`
iw_adlibitum	Управляет процессами получения актуальных данных с сервера Active Directory. Путь к файлу: /usr/local/infowatch/tm3/bin/iw_adlibitum

5.1.2. Работа с процессами Traffic Monitor Server

Все процессы Traffic Monitor Server (за исключением **iw_sniffer, iw_updater** и **iw_warpd**) запускаются от имени владельца Traffic Monitor Server. Процессы **iw_sniffer, iw_updater** и **iw_warpd** запускаются от имени пользователя *root*.

> **Примечание:**
>
> Имя владельца задается при установке Traffic Monitor Server и прописывается в файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[GENERAL]`, параметр `user`.

Во время работы состояние процессов Traffic Monitor Server проверяется сценарием `iw-autorestart.sh`, который в ходе установки прописывается в файле `/etc/crontab`. Один раз в минуту демон **crond** запускает сценарий `iw-autorestart.sh`. Если по какой-либо причине один или несколько процессов Traffic Monitor Server были остановлены, то сценарий `iw-autorestart.sh` перезапускает эти процессы.

Управление работой процессов Traffic Monitor Server выполняется при помощи `iw-trafmon` и `iw-caserv`, находящихся в каталоге `/etc/rc.d/init.d`. Файлы `iw-trafmon` и `iw-caserv` являются сценариями автозапуска для уровней запуска (runlevel) 2, 3, 4, 5.

Сценарий `iw-trafmon` отвечает за запуск процессов: **iw_smtpd**, **iw_messed**, **iw_expressd**, **iw_deliverd**, **iw_proxy**, **iw_dbloader**, **iw_updater**, **iw_sniffer, iw_icap, iw_qmover_server, iw_qmover_client, iw_warpd, iw_adlibitum**.

Примечания:

1. Для перехвата копии трафика через Sniffer (ICQ- HTTP-, SMTP-трафик) запускаются отдельные процессы **iw_proxy**.
2. Процесс **iw_icap** доступен, только если установлен модуль интеграции с ICAP.
3. Процессы **iw_qmover_server, iw_qmover_client** доступны, только если установлен модуль взаимодействия с удаленной базой данных. Каждый процесс запускается на соответствующей стороне (в филиалах **iw_qmover_client,** в центральном офисе **iw_qmover_server**).

Сценарий `iw-caserv` отвечает за запуск процесса **iw_cas2d**, связанного с работой сервера контентного анализа.

Ключи запуска для сценариев `iw-trafmon` и `iw-caserv`:

Ключ запуска	Назначение
`start`	запуск процессов
`stop`	остановка процессов
`restart`	перезапуск процессов
`status`	вывод на экран информации о состоянии процессов

Примеры команд

Действие	Команда
Перезапустить сервер контентного анализа	`service iw-caserv restart`
Проверить состояние процессов Traffic Monitor Server	`service iw-trafmon status`
Проверить состояние сервера контентного анализа	`service iw-caserv status`

Важная информация!

В каталоге `/usr/local/infowatch/tm3/run` хранятся PID-файлы. При аварийном завершении работы необходимо перед запуском процессов стереть все PID-файлы.

Изменение параметров автозапуска процессов

Для каждого процесса, управляемого сценарием `iw-trafmon` можно задать параметры автозапуска в файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[AUTO_RESTART]`.

Перед изменением параметров автозапуска процессов остановите процессы:

```
service iw-trafmon stop
```

Для процессов, которые должны запускаться автоматически укажите значение:

```
autorestart = On
```

Для остальных процессов укажите значение:

```
autorestart = Off
```

После изменения параметров автозапуска запустите процессы:

```
service iw-trafmon start
```

Запуск процессов вручную

Для корректного запуска процессов Traffic Monitor Server необходимо предварительно задать все переменные окружения СУБД Oracle (см. документ «*InfoWatch Traffic Monitor. Руководство по установке и конфигурированию*»).

Вручную все процессы (за исключением **iw_proxy**) запускаются с параметрами файла `tm.conf`:

```
/usr/local/infowatch/tm3/bin/название_процесса -c полный_путь_к_файлу_tm.conf
```

Например:

```
/usr/local/infowatch/tm3/bin/iw_dbloader -c /usr/local/infowatch/tm3/etc/tm.conf
```

Для процесса iw_proxy необходимо также указывать тип перехватчика (icq, http или smtp):

```
/usr/local/infowatch/tm3/bin/iw_proxy -c полный_путь_к_файлу_tm.conf –m тип_перехватчика
```

Например:

```
/usr/local/infowatch/tm3/bin/iw_proxy -c /usr/local/infowatch/tm3/etc/tm.conf –m icq
```

5.1.3. Проверка результатов обновления конфигурации (процесс iw_updater)

Для корректной работы Системы на все экземпляры Traffic Monitor Server должна быть загружена одинаковая конфигурация. Однако возможна ситуация, когда обновление конфигурации на одном или нескольких серверах не было выполнено. В этом случае в консоли управления, в разделе *Версии конфигурации*, будет долгое время (более 15 минут после начала обновления) продолжать отображаться две версии со статусом *Активная*.

Для разрешения проблемы выполните следующие действия:

1. Установите, на каких серверах произошла ошибка обновления. Для этого на каждом экземпляре Traffic Monitor Server проверьте файл:
   `/usr/local/infowatch/tm3/etc/tmserver_version.dat`

   Версия конфигурации, указанная в этом файле, должна совпадать с версией загружаемой конфигурации. Если версия отличается, значит, на этом сервере конфигурация не обновлена.

   > **Примечание:**
   >
   > Если файл `tmserver_version.dat` отсутствует, значит, на сервер еще не загружалась ни одна конфигурация.

2. Проверьте состояние процесса `iw_updater`, выполнив команду:

   ```
   service iw-trafmon status
   ```

3. Выполните одно из следующих действий:

Если `iw_updater` запущен, то перезапустите процессы Traffic Monitor Server:

```
service iw-trafmon restart
```

Если `iw_updater` остановлен, то запустите процессы Traffic Monitor Server:

```
service iw-trafmon start
```

4. Повторите загрузку конфигурации на серверы (см. документ «*InfoWatch Traffic Monitor. Руководство пользователя*»).

Если по-прежнему возникает ошибка загрузки конфигурации, проверьте системный журнал:

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

В системный журнал записываются сообщения об ошибках, возникающих в процессе работы Traffic Monitor Server. Если исправить ошибку не удается, обратитесь в службу технической поддержки.

5.2. Настройка параметров работы Traffic Monitor Server (файл tm.conf)

Все компоненты Traffic Monitor Server используют общий файл настроек `/usr/local/infowatch/tm3/etc/tm.conf`. О порядке установки и первичной настройки файла `tm.conf` см. *документ «InfoWatch OCR для InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*.

> **Важная информация!**
>
> В конфигурационном файле `tm.conf` имеется ряд настроек, которые не рекомендуется изменять. Данные настройки в настоящей документации не описываются.
>
> Часть параметров, указанных в конфигурационном файле, задается при установке Traffic Monitor Server (см. *документ «InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*).

Секции конфигурационного файла описываются в следующих подразделах:

Название секции, ссылка на раздел	Область настройки, которую конфигурирует секция
Секция [*GENERAL]* (п.5.2.1 на стр. 52)	Общие параметры сервера
Секция [*AUTO_RESTART]* (п. 5.2.2 на стр. 53)	Автозапуск процессов сервера
Секция [*SMTPD]* (п. 5.2.3 на стр. 54)	Процесс `iw_smtpd`, выполняющий перехват SMTP-трафика с почтового relay-сервера
Секция [*MESSED]* (п. 5.2.4 на стр. 55)	Процесс `iw_messed`, выполняющий доставку SMTP-писем при интеграции с почтовым relay-сервером
Секция [*DELIVERD]* (п. 5.2.5 на стр. 56)	Процесс `iw_deliverd`, выполняющий доставку SMTP-писем адресатам при интеграции с почтовым relay-сервером
Секция [*QUEUE]* (п. 5.2.6 на стр. 56)	Очередь объектов
Секция [*SNIFFER]* (п. 5.2.7 на стр. 57)	Процесс `iw_sniffer`, принимающий копию SMTP-, HTTP-, ICQ-трафика
Секция [HTTP] (п. 5.2.8 на стр. 57)	Перехват HTTP-трафика с помощью Sniffer
Секция [ICQ] (п. 5.2.9 на стр. 58)	Перехват ICQ-трафика с помощью Sniffer
Секция [SMTP] (п. 5.2.10 на стр. 59)	Перехват SMTP-трафика с помощью Sniffer
Секция [*PROXY*] (п. 5.2.11 на стр. 59)	Общие настройки процессов `iw_proxy`, принимающих копию трафика (HTTP, ICQ, SMTP) и передающих XML-контекст, сформированный из полученного объекта, подсистеме анализа и принятия решения
Секция [*PROXY_ICQ]* (п. 5.2.12 на стр. 60)	Обработка копий ICQ-сообщений, полученных от Sniffer
Секция [*PROXY_HTTP]* (п. 5.2.13 на стр. 61)	Обработка HTTP-запросов, а также ICQ-сообщений (при перехвате ICQ поверх HTTP), полученных от Sniffer
Секция [*PROXY_SMTP]* (п. 5.2.14на стр. 63)	Обработка SMTP-сообщений, полученных от Sniffer

Название секции, ссылка на раздел	Область настройки, которую конфигурирует секция
Секция [*CAS]* (п. 5.2.15 на стр. 63)	Работа подсистемы Контентного анализа
Секция [*ENCODE_DETECTOR]* (п. 5.2.16 на стр. 66)	Определение кодировки текста, извлеченного из объектов
Секция [*DBLOADER]* (п. 5.2.17 на стр. 66)	Процесс `iw_dbloader`, обеспечивающий загрузку объектов в базу данных
Секция [*FILTER]* (п. 5.2.18 на стр. 67)	Соединение с подсистемой Контентного анализа
Секция [*ORACLE]* (п. 5.2.19 на стр. 67)	Соединение с сервером базы данных
Секция [*EXPRESSD]* (п. 5.2.20 на стр. 67)	Процесс `iw_expressd`, обеспечивающий обработку объектов, полученных от систем InfoWatch Device Monitor и DeviceLock
Секция [*EXTRACTOR*] (п. 5.2.21 на стр. 69)	Извлечение файлов из архивов и вложений
Секция [*UPDATER]* (п. 5.2.22 на стр. 69)	Загрузка конфигурации из базы данных на сервер Traffic Monitor
Секция [*WARPD]* (п. 5.2.23 на стр. 70)	Извлечение данных из файлов, вложенных в перехваченные объекты
Секция [*ADLIBITUM]* (п. 5.2.24 на стр. 70)	Получение актуальных данных с сервера Active Directory

5.2.1. Секция [*GENERAL*]

В секции `[GENERAL]` заданы общие параметры:

Параметр	Описание
`User`	Имя пользователя – владельца InfoWatch Traffic Monitor (от имени которого запускаются процессы Traffic Monitor Server). Значение по умолчанию `iwtm`. **Важная информация!** Настоятельно не рекомендуется менять значение параметра `User`, так как это может привести к неработоспособности системы. Если необходимость в смене данного параметра все же возникла, то лучше переустановить Traffic Monitor Sever с помощью инсталлятора (см. *документ «InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*)
`Group`	Группа, членом которой является владелец InfoWatch Traffic Monitor. Значение по умолчанию `oinstall`
`Root`	Путь к корневому каталогу Системы. Значение по умолчанию `/usr/local/infowatch/tm3`
`VersionFile`	Путь к файлу, содержащему информацию о версии конфигурации, загруженной на сервер Traffic Monitor. Значение по умолчанию `etc/tmserver_version.dat`
`UserScript`	Путь к файлу сценария, в соответствии с которым подсистема анализа и принятия решения выполняет анализ и обработку объектов данного типа. Сценарий находится в каталоге `etc/scripts/user.lua` (путь задается относительно текущего каталога, которым является корневой каталог Системы)

Параметр	Описание
`SystemScript`	Путь к файлу системного сценария. Нарушение указанного значения или самого файла может привести к потере работоспособности системы.
`ContextRules`	Путь к файлу, содержащему правила изменения контекста сообщений. Значение по умолчанию: `/etc/rules.xml`
`ContextCustomRules`	Путь к файлу, содержащему правила дополнительные правила изменения контекста сообщений. Значение по умолчанию: etc/custom_rules.xml
`SampleDocumentsSync`	Признак того, выполняет ли данный сервер компиляцию эталонных документов (работа скрипта `db_CA.pl`): `Off`/`On`. Значение по умолчанию: `Off`. Значение `On` должно быть установлено только на одном сервере Системы.

5.2.2. Секция [*AUTO_RESTART*]

В секции `[AUTO_RESTART]` перечислены параметры, необходимые для автозапуска процессов. Автозапуск возможен для процессов:

- iw_warpd;
- iw_adlibitum;
- iw_sniffer;
- iw_messed;
- iw_deliverd;
- iw_smtpd;
- iw_expressd;
- iw_proxy ICQ;
- iw_proxy HTTP;
- iw_proxy SMTP;
- iw_dbloader,
- iw_updater;
- iw_icap;
- iw_qmover_client;
- iw_qmover_server.

> **Примечание:**
>
> Процесс `iw_icap` отображается в секции автозапуска только если установлен модуль интеграции с ICAP.
>
> Процессы `iw_qmover_client` и `iw_qmover_server` отображаются в секции автозапуска только если установлен модуль взаимодействия с удаленной базой данных. Причем отображается процесс, соответствующий типу модуля (client или server).

Для каждого процесса имеется одинаковый набор параметров:

Параметр	Описание
`autorestart`	Автоматическое управление запуском процесса (значение `On`). Если управлять запуском процесса не требуется, установите значение `Off`
`command`	Команда для запуска процесса

Параметр	Описание
args	Аргументы команды

Правила настройки параметров автозапуска:

1. Включите автозапуск для всех процессов, которые будут функционировать на данном экземпляре сервера Traffic Monitor. Например, если требуется запускать процессы iw_smtpd, iw_messed и iw_dbloader, то эти процессы обязательно должны быть настроены на автозапуск (autorestart = On).

   > **Примечание:**
   >
   > Первоначально настройка автозапуска процессов выполняется при установке Traffic Monitor Server. Список процессов, которые нужно запускать различается в зависимости от схемы внедрения. Основные схемы внедрения и списки процессов приведены в документе *«InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*.

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

   > **Важная информация!**
   >
   > Перед изменением параметров автозапуска остановите серверные процессы Traffic Monitor:
   >
   > `service iw-trafmon stop`
   >
   > Это необходимо для корректной смены параметров

3. Если для каких-либо перехватчиков используется OCR (подробнее см. *«InfoWatch OCR для IWTM* 4.1. *Руководство по установке»*), то для процессов iw_messed, iw_expressd и iw_warpd необходимо в параметре args изменить ссылку на конфигурационный файл tm.conf – ссылкой на конфигурационный файл tm_ocr.conf (подробнее см. п. 5.3 на стр. 70). То есть вместо

   ```
   args="-c /usr/local/infowatch/tm3/etc/tm.conf"
   ```

   должно быть указано

   ```
   args="-c /usr/local/infowatch/tm3/etc/tm_ocr.conf"
   ```

   В результате для параметров, указанных в tm_ocr.conf, будут использоваться значения из файла tm_ocr.conf.

5.2.3. Секция [*SMTPD*]

В секции [SMTPD] указаны параметры настройки процесса **iw_smtpd** (перехват SMTP-трафика с почтового relay-сервера):

Параметр	Описание
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования: от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 3.
MaxThreads	Максимальное количество потоков для параллельного выполнения процесса **iw_smtpd**. Значение по умолчанию 8. Увеличение числа потоков повысит производительность процесса, но повысит использование памяти.
MaxMsgSize	Максимальный размер письма (в байтах). Значение по умолчанию 10240000

Параметр	Описание
`Domain`	Полное доменное имя принимающего SMTP-сервера, использующееся для идентификации внутри почтового протокола. Рекомендуется использовать имя сервера TM, на котором работает процесс **iw_smtpd**.
`CoreDumpSize`	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение `-1` (отсутствие ограничений на размер дампа памяти). Значение `0` указывают, если запись не ведется. Значение по умолчанию `-1`
`ListenAddr`	Адрес сетевого интерфейса сервера, на котором запущен процесс прослушивания. Задаётся при установке.
`ListenPort`	Порт сервера, на котором запущен процесс прослушивания. Задаётся при установке.

5.2.4. Секция [*MESSED*]

В секции `[MESSED]` заданы настройки параметров процесса **iw_messed** (доставка SMTP-писем при интеграции с почтовым relay-сервером):

Параметр	Описание
`Daemon`	Запуск в режиме демона (значение `On`) или в режиме обычного процесса (значение `Off`). Значение по умолчанию `On`
`LogLevel`	Уровень протоколирования от `0`(протоколируются только ошибки) до `8` для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию `3`.
`MaxThreads`	Максимальное количество потоков для параллельного выполнения процесса **iw_messed**. Значение по умолчанию `8`. Увеличение числа потоков повысит производительность процесса, но повысит использование памяти.
`CoreDumpSize`	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение `-1` (отсутствие ограничений на размер дампа памяти). Значение `0` указывают, если запись не ведется. Значение по умолчанию `-1`
`Relay`	Полное доменное имя почтового relay-сервера, которому перенаправляется письмо, используется для идентификации внутри почтового протокола. Задаётся при установке.
`RelayPort`	Порт почтового relay-сервера, которому перенаправляется письмо. Задаётся при установке.
`HeloDomain`	Значение команды `HELLO` SMTP-диалога. Значение по умолчанию `smtp.company.com`
`Timeout`	Время, в течение которого предпринимаются попытки доставки SMTP-писем, в секундах. По истечении указанного времени письмо передается в базу данных. Значение по умолчанию `1200`
`OCR`	Неиспользуемый параметр. Настройка распознавания текста в растровых изображениях (OCR) для SMTP-писем выполняется в файле `tm_ocr.conf` (см. п. 5.3 на стр. 70). Подробнее об OCR см. документ *«InfoWatch OCR для InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*.

5.2.5. Секция [*DELIVERD*]

В секции [DELIVERD] заданы параметры процесса **iw_deliverd** (доставка SMTP-писем адресатам при интеграции с почтовым relay-сервером):

Параметр	Описание
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 3.
MaxRetries	Максимальное число попыток доставить сообщение. Значение по умолчанию 3
RetryTimeout	Время ожидания (в сек), по истечении которого предпринимается очередная попытка доставить сообщение (значение по умолчанию 10)
CoreDumpSize	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение -1 (отсутствие ограничений на размер дампа памяти). Значение 0 указывают, если запись не ведется. Значение по умолчанию -1
CheckPeriod	Интервал времени (в сек) между проверками на поступление новых сообщений. Значение по умолчанию 5
HeloDomain	Значение команды HELLO SMTP-диалога. Значение по умолчанию smtp.company.com
Relay	Полное доменное имя почтового relay-сервера, использующееся для идентификации внутри почтового протокола. Задаётся при установке. Рекомендуется использовать имя сервера TM, на котором работает процесс **iw_deliverd**.
RelayPort	Порт почтового relay-сервера. Задаётся при установке
Timeout	Время, в течение которого предпринимаются попытки доставки SMTP-писем, в секундах. Значение по умолчанию 1200

5.2.6. Секция [*QUEUE*]

В секции [QUEUE] заданы параметры очередей объектов:

Параметр	Описание
Db	Путь к очереди объектов, загружаемых в базу данных; очередь используется процессом iw_dbloader. Значение по умолчанию ./queue/db (путь указан относительно текущего каталога, которым является корневой каталог Системы)
Smtp	Путь к очереди SMTP-писем, используемой процессами iw_smtpd и iw_messed. Значение по умолчанию ./queue/smtp (путь указан относительно текущего каталога, которым является корневой каталог Системы)
Error	Путь к очереди объектов, обработка которых была прекращена вследствие ошибки, делающей невозможной дальнейшую обработку. В эту очередь попадают объекты с ошибками, произошедшими на этапах получения объектов процессами Traffic Monitor Server и загрузки полученных объектов в базу данных. Значение по умолчанию ./queue/error (путь указан относительно текущего каталога, которым является корневой каталог Системы)

Параметр	Описание
CheckPeriod	Период ожидания (в мсек) между проверками на поступление новых писем в очередь входящих SMTP-писем. Значение по умолчанию 1000

5.2.7. Секция [*SNIFFER*]

В секции [SNIFFER] заданы параметры процесса **iw_sniffer**:

Параметр	Описание
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 3.
Host	IP-адрес хоста, ожидающего подсоединения proxy
Port	Порт хоста, ожидающего подсоединения proxy
Clusters	Перечисление типов перехватчиков, описанных в следующих секциях. Значение по умолчанию: http,icq,smtp
LibraryPath	Путь к путь к динамическим библиотекам перехвата. Значение по умолчанию /usr/local/infowatch/tm3/lib
InterceptorLib	Путь к библиотеке перехватчика. Значение по умолчанию libtmcap_interceptor.so

5.2.8. Секция [HTTP]

В секции [HTTP] заданы параметры перехвата http-трафика с помощью sniffer:

Параметр	Описание
Interface	Сетевой интерфейс, от которого будут поступать копии сообщений. Вы можете задать одно из следующих значений: eth0, eth1 и т. д. Значение по умолчанию eth0. **Примечание:** допускается прием разных видов трафика от одного сетевого интерфейса
OpenTimeout	Время сохранения соединения (в сек) при отсутствии пакетов. Значение по умолчанию 600.
LiveTimeout	Время ожидания (в сек), в течение которого соединение должно перейти в состояние *ESTABLISHED*. Если состояние не изменилось, то соединение автоматически прекращается. Значение по умолчанию 86400
CloseTimeout	Время сохранения соединения (в сек) при переходе в состояние *TIME_WAIT*. Значение по умолчанию 300
QueueMemorySize	Объем памяти (в байтах), используемой для приема пакетов. При высокой загруженности канала, можно увеличить значение. Диапазон значений: от 1 до 500 Мб. Значение по умолчанию 4194304

Параметр	Описание
Balancer	Тип распределения трафика, между несколькими экземплярами Traffic Monitor Server. Возможные значения: • Connection. Для каждого нового TCP-соединения выбирается экземпляр Traffic Monitor Server. Таким образом, поочередно задействуются все экземпляры Traffic Monitor Server. • SrcIp. Распределение трафика между несколькими экземплярами Traffic Monitor Server выполняется на основании IP-адреса клиента. Это значит, что все данные с одинаковым IP-адресом клиента будут передаваться на один экземпляр Traffic Monitor Server Значение по умолчанию SrcIp
RulesTableFile	Путь к файлу, в котором заданы параметры фильтрации http-трафика с помощью sniffer (подробнее см. п. 5.8 на стр. 77). Значение по умолчанию etc/http.rules

5.2.9. Секция [ICQ]

В секции [ICQ] заданы параметры перехвата icq-трафика с помощью sniffer:

Параметр	Описание
Interface	Сетевой интерфейс, от которого будут поступать копии сообщений. Вы можете задать одно из следующих значений: eth0, eth1 и т. д. Значение по умолчанию eth0. **Примечание:** допускается прием разных видов трафика от одного сетевого интерфейса
OpenTimeout	Время сохранения соединения (в сек) при отсутствии пакетов. Значение по умолчанию 600.
LiveTimeout	Время ожидания (в сек), в течение которого соединение должно перейти в состояние *ESTABLISHED*. Если состояние не изменилось, то соединение автоматически прекращается. Значение по умолчанию 86400
CloseTimeout	Время сохранения соединения (в сек) при переходе в состояние *TIME_WAIT*. Значение по умолчанию 300
QueueMemorySize	Объем памяти (в байтах), используемой для приема пакетов. При высокой загруженности канала, можно увеличить значение. Диапазон значений: от 1 до 500 Мб. Значение по умолчанию 4194304
Balancer	Тип распределения трафика, между несколькими экземплярами Traffic Monitor Server. Возможные значения: • Connection. Для каждого нового TCP-соединения выбирается экземпляр Traffic Monitor Server. Таким образом, поочередно задействуются все экземпляры Traffic Monitor Server. • SrcIp. Распределение трафика между несколькими экземплярами Traffic Monitor Server выполняется на основании IP-адреса клиента. Это значит, что все данные с одинаковым IP-адресом клиента будут передаваться на один экземпляр Traffic Monitor Server Значение по умолчанию SrcIp
RulesTableFile	Путь к файлу, в котором заданы параметры фильтрации icq-трафика с помощью sniffer (подробнее см. п. 5.8 на стр. 77). Значение по умолчанию etc/icq.rules

5.2.10. Секция [SMTP]

В секции `[SMTP]` заданы параметры перехвата smtp-трафика с помощью sniffer:

Параметр	Описание
`Interface`	Сетевой интерфейс, от которого будут поступать копии сообщений. Вы можете задать одно из следующих значений: eth0, eth1 и т. д. Значение по умолчанию `eth0`. **Примечание:** допускается прием разных видов трафика от одного сетевого интерфейса
`OpenTimeout`	Время сохранения соединения (в сек) при отсутствии пакетов. Значение по умолчанию `600`.
`LiveTimeout`	Время ожидания (в сек), в течение которого соединение должно перейти в состояние *ESTABLISHED*. Если состояние не изменилось, то соединение автоматически прекращается. Значение по умолчанию `86400`
`CloseTimeout`	Время сохранения соединения (в сек) при переходе в состояние *TIME_WAIT*. Значение по умолчанию `300`
`QueueMemorySize`	Объем памяти (в байтах), используемой для приема пакетов. При высокой загруженности канала, можно увеличить значение. Диапазон значений: от 1 до 500 Мб. Значение по умолчанию `4194304`
`Balancer`	Тип распределения трафика, между несколькими экземплярами Traffic Monitor Server. Возможные значения: • `Connection`. Для каждого нового TCP-соединения выбирается экземпляр Traffic Monitor Server. Таким образом, поочередно задействуются все экземпляры Traffic Monitor Server. • `SrcIp`. Распределение трафика между несколькими экземплярами Traffic Monitor Server выполняется на основании IP-адреса клиента. Это значит, что все данные с одинаковым IP-адресом клиента будут передаваться на один экземпляр Traffic Monitor Server Значение по умолчанию `Connection`
`RulesTableFile`	Путь к файлу, в котором заданы параметры фильтрации smtp-трафика с помощью sniffer (подробнее см. п. 5.8 на стр. 77). Значение по умолчанию `etc/smtp.rules`

5.2.11. Секция [*PROXY*]

В секции `[PROXY]` заданы общие параметры настройки процесса **iw_proxy**:

Параметр	Описание
`Daemon`	Запуск в режиме демона (значение `On`) или в режиме обычного процесса (значение `Off`). Значение по умолчанию `On`
`LogLevel`	Уровень протоколирования от `0` (протоколируются только ошибки) до `8` для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию `3`.
`CoreDumpSize`	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение `-1` (отсутствие ограничений на размер дампа памяти). Значение `0` указывают, если запись не ведется. Значение по умолчанию `-1`

Параметр	Описание
MaxThreads	Максимальное количество потоков для параллельного выполнения процесса **iw_proxy**. Значение по умолчанию 32. Увеличение числа потоков повысит производительность процесса, но повысит использование памяти.
MaxFiles	Число открытых файлов. По умолчанию 0 – в этом случае используется значение, установленное в настройках операционной системы (по умолчанию 1024). Для повышения производительности при большом объеме трафика можно увеличить это значение. При изменении параметра нужно устанавливать значение больше системного. Для нагруженных систем рекомендуемое значение – 8000.
Module	Тип перехватчика (icq, http или smtp). Значение по умолчанию не задано (void)

5.2.12. Секция [*PROXY_ICQ*]

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

Параметр	Описание
MessageWindow	Количество сообщений диалога, по достижении которого ICQ-диалог сохраняется в файловую очередь. Значение по умолчанию 10
ListenPort	Порт сервера, на который передаются получаемые сообщения. Значение по умолчанию 5191
DialogTimeout	Интервал времени (в минутах), по истечению которого с момента перехвата последнего ICQ-сообщения необходимо сохранить диалог в файловую очередь. Значение по умолчанию 5
DialogBytesCount	Размер диалога (в байтах), по достижении которого ICQ-диалог сохраняется в файловую очередь. Значение по умолчанию 500
FakeFileTransferPort	Порт, с помощью перенаправления на который блокируются попытки передачи файлов. Значение по умолчанию 62225
DataPoolPageCount	Максимальное количество страниц данных (4 Кб) для обработки соединений. Значение по умолчанию 65536

Параметры, необходимые для приема данных от Sniffer:

Параметр	Описание
SnifferClusterID	Идентификатор кластера, в который будет включен данный экземпляр Traffic Monitor Server. Задается в виде строки. Например, icq
SnifferHost	IP-адрес экземпляра Traffic Monitor Server, на котором запущен процесс iw_sniffer
SnifferPort	Порт, через который процесс iw_sniffer принимает входящие соединения

5.2.13. Секция [*PROXY_HTTP*]

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

Параметр	Описание
`MinText`	Минимальный объем текста (в байтах), для которого будет проводиться контентный анализ. Значение по умолчанию 10 байт. Настройка данного параметра позволяет снизить нагрузку на сервер контентного анализа. Это может быть достигнуто путем отказа от контентного анализа текста, размер которого настолько мал, что не позволяет передавать значимые сообщения
`MinHeader`	Минимальный объем текста (в байтах) для одного блока переменной в кодировке URL, который будет передан на сервер контентного анализа. Значение по умолчанию `10`.
`SetCp1251`	Использование кодовой таблицы windows-1251 вместо mac-cyrillic при автоматическом определении кодировки текста в HTTP-запросе. Значение по умолчанию `On`. Если в вашей организации применяется программное обеспечение, использующее кодировку windows-1251, то рекомендуется оставить этот параметр включенным (значение `On`). Автоматическое определение кодовой таблицы в ряде случаев может происходить некорректно. В частности, при недостаточно большом объёме русскоязычного текста возможен выбор кодировки mac-cyrillic вместо windows-1251
`SkipNegotiate`	Отключает сохранение в очередь HTTP-запросов с NTLM Type 1 (необходимо для исключения дубликатов запросов). Значение по умолчанию `On`. При реализации схемы внедрения, когда перехват копии HTTP-трафика выполняется через Sniffer, должен принимать значение `Off`.
`MaxMemoryBlock`	Максимальный объем данных POST-запроса (в килобайтах), которые могут храниться в оперативной памяти. Блоки большего размера будут выгружаться во временные файлы. Значение по умолчанию 4096 Кб
`LogBlock`	Запись в системный журнал сообщений о блокировке перехваченных HTTP-запросов. Запись ведется, если установлено значение `On`. По умолчанию запись отключена – значение `Off`
`CharsetDetection`	Метод определения кодировки текста. Значение по умолчанию `0`. При этом кодировка определяется обычным методом. После извлечения в контекст, тексты некоторых POST-запросов могут отображаться некорректно. Для исправления проблемы можно установить значение `1`
`StatusCheck`	Установка состояния доставки HTTP-запроса (отображается в Management Console) в зависимости от статус-кода, возвращенного веб- или прокси-сервером. Если установлено значение `On`, то анализ кода выполняется, что позволяет более точно показывать состояние доставки HTTP-запроса. Значение по умолчанию `On`

Параметр	Описание
AuthContext	Отключает сохранение в очередь HTTP-запросов без аутентификации. Возможные значения: • 0 – производится сохранение запросов без аутентификации; • 1 – не сохраняются запросы с ответом прокси-сервера "*407*", • 2 – не сохраняются запросы с NTLM Type 1, либо без заголовка *Proxy-Authorization.* При этом значении значение параметра SkipNegotiate не имеет значения: Система работает так, как если бы он имел значение On. Значение по умолчанию 1
SkipStat4XX	Отключает сохранение в очередь HTTP-запросов с ответом прокси-сервера вида "*4XX*", где *XX* – любые цифры. Значение по умолчанию On.
IcqFilter	Возможность перехвата ICQ-сообщений (если установлено значение On), передаваемых через прокси-сервер (поверх HTTP). По умолчанию возможность отключена – установлено значение On
IcqKnownServers	Диапазоны IP для ICQ серверов при перехвате ICQ поверх HTTP. Несколько диапазонов перечисляются через запятую, например: "205.188.251.0/24:443, 64.12.30.0/24:443, 205.188.8.8:443"
MessageWindow	Количество сообщений диалога, по достижении которого ICQ-диалог (при перехвате ICQ поверх HTTP) сохраняется в файловую очередь. Значение по умолчанию 10
DecodeHttpContent	Включение распаковки содержимого запроса в случае наличия заголовка Content-Encoding со значением gzip, deflate или compress. Значение по умолчанию On
ExtractHttpEntity	Включение процедуры извлечения текста из кодированного содержимого запроса с помощью внешних распаковщиков. Эта процедура применяется при сбоях внутренней процедуры декодирования с использованием zlib. Значение по умолчанию Off
DialogTimeout	Временной интервал (в минутах), по истечении которого с момента перехвата последнего сообщения происходит сохранение ICQ-диалога (при перехвате ICQ поверх HTTP) в файловую очередь. Значение по умолчанию 5
DialogBytesCount	Размер диалога (в байтах), по достижении которого ICQ-диалог (при перехвате ICQ поверх HTTP) сохраняется в файловую очередь. Значение по умолчанию 500
FakeFileTransferPort	Порт, с помощью перенаправления на который блокируются попытки передачи файлов. Значение по умолчанию 62225
DataPoolPageCount	Максимальное количество страниц данных (4 Кб) для обработки соединений. Значение по умолчанию 65536
WCGAuthCache	Признак того, включена ли функция кэширования авторизационной информации, необходимая для интеграции с WebSense WSG. Чтобы включить кэширование, установите значение On. Значение по умолчанию Off
WCGAuthTTL	Время кэширования авторизационной информации, если включен параметр WCGAuthCache, в секундах. Значение по умолчанию 900

Параметр	Описание
`DataPoolSize`	Максимальный объём выделенной памяти для обработки соединений, в Мб. Значение по умолчанию `1024`

Параметры, необходимые для приема данных от Sniffer:

Параметр	Описание
`SnifferClusterID`	Идентификатор кластера, в который будет включен данный экземпляр Traffic Monitor Server. Задается в виде строки. Например, `http`
`SnifferHost`	IP-адрес экземпляра Traffic Monitor Server, на котором запущен процесс iw_sniffer
`SnifferPort`	Порт, через который процесс iw_sniffer принимает входящие соединения

5.2.14. Секция [*PROXY_SMTP*]

В секции `[PROXY_SMTP]` задаются параметры, необходимые для обработки SMTP-сообщений, полученных от Sniffer:

Параметр	Описание
`MaxMsgSize`	Размер SMTP-сообщения (в байтах), при превышении которого сообщение не обрабатывается Системой. Значение по умолчанию – `52428800`.
`DataPoolPageCount`	Максимальное количество страниц данных (4 Кб) для обработки соединений. Значение по умолчанию `65536`

Параметры, необходимые для приема данных от Sniffer:

Параметр	Описание
`SnifferClusterID`	Идентификатор кластера, в который будет включен данный экземпляр Traffic Monitor Server. Задается в виде строки. Например, `smtp`
`SnifferHost`	IP-адрес экземпляра Traffic Monitor Server, на котором запущен процесс iw_sniffer
`SnifferPort`	Порт, через который процесс iw_sniffer принимает входящие соединения

5.2.15. Секция [*CAS*]

В секции `[CAS]` задаются параметры сервера контентного анализа:

Параметр	Описание
`Daemon`	Запуск в режиме демона (значение `On`) или в режиме обычного процесса (значение `Off`). Значение по умолчанию `On`
`LogLevel`	Уровень протоколирования от `0`(протоколируются только ошибки) до `8` для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию `3`.

Параметр	Описание
CoreDumpSize	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение -1 (отсутствие ограничений на размер дампа памяти). Значение 0 указывают, если запись не ведется. Значение по умолчанию -1
ListenAddr	Адрес сетевого интерфейса сервера контентного анализа, на котором запущен процесс прослушивания запросов на обработку текста, поступающих от подсистемы анализа и принятия решения. Значение по умолчанию 127.0.0.1
ListenPort	Порт сервера контентного анализа, на котором запущен процесс прослушивания. Значение по умолчанию 4201
SocketBacklog	Максимальное количество процессов, которые могут одновременно содержаться в очереди на обработку. Значение по умолчанию 32.
BaseVerFile	Путь файлу, содержащему информацию о конфигурации, используемой сервером контентного анализа в текущий момент. Значение по умолчанию cas/cas_version.dat (путь указан относительно текущего каталога, которым является корневой каталог Системы)
LangDetOntoloy	Путь к файлу с онтологией классификатора. Значение по умолчанию cas/lang.ont.bin

Параметры технологии лингвистического анализа (*Classifier*):

Параметр	Описание
CLLib	Путь к библиотеке лингвистического анализа. Значение по умолчанию lib/libclassifier.so
CLSrcXmlBase	Путь к XML-базе данных. Значение по умолчанию cas/base.xml
CLSearchLimit	Максимальное количество терминов, возвращаемых в результате поиска. 0 - отключение; -1 - отсутствие ограничений на количество возвращаемых терминов. Значение по умолчанию 10.
CLNiokrOntologyPrefix	Префикс файлов в онтологии классификатора. Значение по умолчанию cas/onto.
CLSpellingCorrector	Включение (значение On) или отключение (значение Off) возможности детектировать термины, присутствующие в тексте с ошибками или опечатками: определяются расхождения с термином в один символ (замена, перестановка, отсутствие, лишний символ). По умолчанию функция выключена (значение *Off*)
CLTransliteration	Включение (значение On) или отключение (значение Off) возможности детектировать термины, написанные транслитом. По умолчанию нормализация текста согласно правилам транслитерации не производится (значение *Off*)
CLTransliterationTable	Путь к таблице транслитерации, согласно которой производится нормализация текста; значение, указанное по умолчанию, и сам файл, менять не следует.

Параметры технологии цифровых отпечатков (*Copyright Analysis*):

Параметр	Описание
CALib	Путь к библиотеке цифровых отпечатков. Значение по умолчанию lib/libch_copyanalysis.so
CADB	Путь к базе данных цифровых отпечатков. Значение по умолчанию cas/ca_db
CATempDB	Путь к временной базе данных цифровых отпечатков. Значение по умолчанию cas/ca_temp_db
CASearchLimit	Максимальное количество терминов, возвращаемых в результате поиска. 0 - отключение; -1 - отсутствие ограничений на количество возвращаемых терминов. Значение по умолчанию 10.
CATextRelLimit	Порог релевантности: доля совпадения текстовых данных из анализируемого объекта с эталонным документом, достаточная для того, чтобы считать, что объект соответствует этому эталонному документу. Возможные значения - от 0 до100. Значение по умолчанию 10.
CABinRelLimit	Порог релевантности: доля совпадения бинарных данных из анализируемого объекта с эталонным документом, достаточная для того, чтобы считать, что объект соответствует этому эталонному документу. Возможные значения - от 0 до100. Значение по умолчанию 10.
CABinLMin	Минимальная длина фрагмента бинарных данных, на которых может срабатывать детектирование цифровых отпечатков. Значение по умолчанию 23.
CABinLMax	Максимальная длина фрагмента бинарных данных, на которых может срабатывать детектирование цифровых отпечатков. Значение по умолчанию 111.
CAMinTextSize	Минимальное количество текста, из которого может быть создан текстовый цифровой отпечаток, в байтах. Значение по умолчанию 100.
IMEnabled	Включение (значение On) и выключение (значение Off) детектора печатей. Значение по умолчанию – Off.

Параметры технологии детектирования текстовых объектов:

Параметр	Описание
TOSearchLimit	Максимальное количество текстовых объектов, возвращаемых в результате поиска. 0 - отключение; -1 - отсутствие ограничений на количество возвращаемых текстовых объектов. Значение по умолчанию 10
TONiokrSrcActiveList	Путь к файлу, содержащему список активных текстовых объектов.
TOUsrObjs	Путь к файлу, содержащему список пользовательских текстовых объектов.
TOLib	Путь к библиотеке текстовых объектов. Значение по умолчанию lib/libch_tobjdetector.so
TOPhoneCountryCodes	Путь к файлу со списком телефонных кодов различных стран. Значение по умолчанию cas/do_phone_country.txt
TOPhoneCityCodes	Путь к файлу со списком телефонных кодов различных городов. Значение по умолчанию cas/do_phone_city.txt

Параметр	Описание
TOSkillaObjects	Путь к папке, содержащей ссылки на места расположения скомпилированных текстовых объектов
TOSkillaSource	Путь к папке, содержащей ссылки на места расположения исходных текстовых объектов
TOAllSource	Путь к папке, содержащей ссылки на места расположения всех исходных текстовых объектов, включая пользовательские
TOAllObjects	Путь к папке, содержащей ссылки на места расположения всех скомпилированных текстовых объектов, включая пользовательские
ICEnabled	Включение (значение On) и выключение (значение Off) детектора паспортов Российской федерации. Значение по умолчанию – Off.
FAEnabled	Включение (значение On) и выключение (значение Off) детектора заполненных форм. Значение по умолчанию – Off.
TAEnabled	Включение (значение On) и выключение (значение Off) детектора выгрузок из БД. Значение по умолчанию – Off.

5.2.16. Секция [*ENCODE_DETECTOR*]

В секции [ENCODE_DETECTOR] заданы параметры определения кодировки текста

Параметр	Описание
NIOKR	Выбор использования детектора кодировки InfoWatch вместо детектора Mozilla. Значение On – технология InfoWatch; Off – Mozilla. Значение по умолчанию Off.

5.2.17. Секция [*DBLOADER*]

В секции [DBLOADER] заданы параметры для настройки процесса **iw_dbloader**:

Параметр	Описание
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 3.
CoreDumpSize	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение -1 (отсутствие ограничений на размер дампа памяти). Значение 0 указывают, если запись не ведется. Значение по умолчанию -1
MaxThreads	Максимальное количество потоков для параллельного выполнения процесса **iw_dbloader**. Значение по умолчанию 8. В результате увеличения числа потоков возрастет производительность процесса, но увеличится использование памяти.
CacheSize	Количество идентификаторов объектов БД для кэширования (на один экземпляр процесса). Значение по умолчанию 32.

Параметр	Описание
XMLValidityCheck	Параметр, определяющий необходимость проверки правильности формирования контекста: Yes - проверка проводится; No – проверка не проводится. Значение по умолчанию No
XMLSchemaFile	Путь к файлу с правилами формирования контекста. Значение по умолчанию etc/message.xsd
MaxTextinContext	Максимальное количество текстов в одном объекте. Если количество текстов превышает значение параметра, объект не сохраняется в базе данных, а передаётся в очередь ошибок. Значение по умолчанию 65535.

5.2.18. Секция [*FILTER*]

В секции [FILTER] указаны общие параметры подсистемы Контентного Анализа:

Параметр	Описание
Server	Адрес сетевого интерфейса, к которому подключаются все процессы, взаимодействующие с сервером контентного анализа. Значение по умолчанию 127.0.0.1
Port	Порт, к которому подключаются все процессы, взаимодействующие с сервером контентного анализа. Значение по умолчанию 4201

5.2.19. Секция [*ORACLE*]

Параметры соединения с сервером базы данных заданы в секции [ORACLE]:

Параметр	Описание
Username	Имя учетной записи пользователя Linux части
Password	Пароль учетной записи пользователя Linux части
Connstr	Строка соединения с сервером базы данных (псевдоним сервера из файла tnsnames.ora)
OraHome	Значение переменной окружения ORACLE_HOME

5.2.20. Секция [*EXPRESSD*]

В секции [EXPRESSD] заданы параметры процесса **iw_expressd**:

Параметр	Описание
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 3.

Параметр	Описание
CoreDumpSize	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение -1 (отсутствие ограничений на размер дампа памяти). Значение 0 указывают, если запись не ведется. Значение по умолчанию -1
MaxThreads	Максимальное количество потоков для параллельного выполнения процесса **iw_expressd**. Значение по умолчанию 4. Увеличение числа потоков повысит производительность процесса, но повысит использование памяти. **Важная информация!** Для корректного приема объектов от систем InfoWatch Device Monitor и DeviceLock, укажите то же число обрабатывающих потоков, которое задано на сервере InfoWatch Device Monitor (или в настройках DeviceLock Adapter). За настройку числа обрабатывающих потоков InfoWatch Device Monitor и DeviceLock Adapter отвечает параметр NumberOfConnections в конфигурационном файле InfoWatch.DeviceMonitor.Server.exe.config и InfoWatch.DeviceLockAdapter.exe.config соответственно (подробнее см. «*InfoWatch Device Monitor. Руководство по установке и конфигурированию*» и «*InfoWatch DeviceLock Adapter. Руководство администратора*»).
ListenAddr	Адрес сетевого интерфейса сервера, на котором запущен процесс прослушивания объектов, поступающих от систем InfoWatch Device Monitor и DeviceLock. Значение по умолчанию 0.0.0.0
ListenPort	Порт сервера, на котором запущен процесс прослушивания. Значение по умолчанию 4101
MaxLoadAvg	Максимальная нагрузка на систему, в которой запущен процесс **iw_expressd** (пороговое значение, выраженное в условных единицах). Если загрузка системы равна указанному пороговому значению или превышает его, процесс **iw_expressd** прекращает прием писем. Когда нагрузка на систему будет снижена, прием писем возобновляется. Значение по умолчанию 10
CheckPrintMonitor	Включение (On) или отключение (Off) извлечения текста из теневых копий заданий на печать, полученных от Device Monitor. Значение по умолчанию Off. Настройка распознавания текста в растровых изображениях (OCR) выполняется в файле tm_ocr.conf (см. п. 5.3 на стр. 70). Подробнее об OCR см. документ *«InfoWatch OCR для InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*. **Важная информация!** При интеграции с Infowatch Device Monitor версии 3.4 необходимо указать CheckPrintMonitor = On независимо от использования OCR.
OCR	Настройка распознавания текста в растровых изображениях (OCR) выполняется в файле tm_ocr.conf (см. п. 5.3 на стр. 70). Подробнее об OCR см. документ *«InfoWatch OCR для InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*. **Важная информация!** Если OCR = Off, то txt-файлы сразу передаются на контентный анализ. Этот вариант необходим, если OCR-экстракторы не используются, или требуется уменьшение нагрузки на сервер Traffic Monitor
DmOCR, DlaOCR, CrawlerOCR, SkypeOCR, XmppOCR, MmpOCR, FtpOCR	Настройка распознавания текста в растровых изображениях (OCR) для различных типов перехватчиков настраивается в файле tm_ocr.conf (см. п. 5.3 на стр. 70). Подробнее об OCR см. документ *«InfoWatch OCR для InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*.

5.2.21. Секция [*EXTRACTOR*]

В секции `[EXTRACTOR]` указаны параметры, используемые при извлечении файлов из архивов и вложений:

Параметр	Описание
`DetectorPath`	Путь к файлу, в котором хранятся настройки, необходимые для определения и обработки архивов и вложений. Значение по умолчанию `etc/detector.conf` (путь задается относительно текущего каталога, которым является корневой каталог Системы)
`PrintDetectorPath`	Путь к файлу, в котором хранятся настройки экстракторов Print Monitor для `expressd`. Значение по умолчанию `etc/detector_prn.conf` (путь задается относительно текущего каталога, которым является корневой каталог Системы)
`TempDir`	Путь к каталогу, в который временно сохраняются извлеченные файлы. Значение по умолчанию `tmp` (путь указан относительно текущего каталога, которым является корневой каталог Системы)

5.2.22. Секция [*UPDATER*]

В секции `[UPDATER]` указаны параметры, необходимые для загрузки конфигурации из базы данных на Traffic Monitor Server:

Параметр	Описание
`Daemon`	Запуск в режиме демона (значение `On`) или в режиме обычного процесса (значение `Off`). Значение по умолчанию `On`
`LogLevel`	Уровень протоколирования от `0`(протоколируются только ошибки) до `8` для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию `3`.
`CoreDumpSize`	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение `-1` (отсутствие ограничений на размер дампа памяти). Значение `0` указывают, если запись не ведется. Значение по умолчанию `-1`
`cas_script`	Путь к файлу сценария, в соответствии с которым выполняется перезагрузка сервисов, выполняющих контентный анализ. Сценарий находится в файле `etc/cas_reload.sh` (путь задается относительно текущего каталога, которым является корневой каталог Системы)
`tmserver_script`	Путь к файлу сценария, в соответствии с которым выполняется перезагрузка всех сервисов сервера ТМ, кроме сервисов контентного анализа и синхронизации с Active Directory. Сценарий находится в файле `etc/tmserver_reload.sh` (путь задается относительно текущего каталога, которым является корневой каталог Системы)
`activedirectory_script`	Путь к файлу сценария, в соответствии с которым выполняется перезагрузка сервисов, выполняющих синхронизацию с Active Directory. Сценарий находится в файле `etc/tmserver_reload.sh` (путь задается относительно текущего каталога, которым является корневой каталог Системы)

5.2.23. Секция [*WARPD*]

В секции [*WARPD*] заданы параметры процессов извлечения данных из архивов, вложенных в перехваченные объекты:

Параметр	Описание
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 3.
CoreDumpSize	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение -1 (отсутствие ограничений на размер дампа памяти). Значение 0 указывают, если запись не ведется. Значение по умолчанию -1
MaxThreads	Максимальное количество потоков для параллельного выполнения процессов. Значение по умолчанию 1. Увеличение числа потоков повысит производительность процесса, но повысит использование памяти.

5.2.24. Секция [*ADLIBITUM*]

В секции [*ADLIBITUM*] заданы параметры процессов получения актуальных данных с сервера Active Directory:

Параметр	Описание
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 3.
ErrorDelay	Время задержки после неудачной попытки синхронизации, до следующей попытки синхронизации, в секундах

5.3. Настройка использования OCR для различных перехватчиков (файл tm_ocr.conf)

Конфигурационный файл tm_ocr.conf, расположенный в каталоге /usr/local/infowatch/tm3/etc/, определяет распознавание текста в растровых изображениях (OCR) для различных перехватчиков. Если в файле tm.conf для необходимых процессов (iw_messed, iw_expressd и iw_warpd) указана ссылка на файл tm_ocr.conf (подробнее см. п. 5.2.2 на стр. 53), то при обработке перехваченных изображений будут применяться настройки из файла tm_ocr.conf вместо аналогичных параметров из файла tm.conf.

Подробную информацию о порядке установки и настройки OCR см. документ *«InfoWatch OCR для InfoWatch Traffic Monitor. Руководство по установке и конфигурированию»*.

5.3.1. Секция [*MESSED*]

Секция `[MESSED]` файла `tm_ocr.conf` содержит параметр `OCR`, с помощью которого вы можете включить (значение `On`) или отключить (значение `Off`) использование OCR для файлов, полученных от SMTP Monitor. Значение по умолчанию `On`.

5.3.2. Секция [*EXPRESSD*]

В секции `[EXPRESSD]` определяется, для каких мониторов будет использоваться OCR. Значение по умолчанию для всех параметров, кроме `CheckPrintMonitor` и `OCR` , - `Off`. Чтобы включить использование OCR для файлов, полученных от того или иного перехватчика, измените значение соответствующего параметра на `On`.

Параметр	Описание
`CheckPrintMonitor`	Использование OCR для файлов, полученных от Print Monitor. **Важная информация!** При интеграции с Infowatch Device Monitor версии 3.4 необходимо указать `CheckPrintMonitor = On` независимо от использования OCR.
`OCR`	Использование OCR для файлов, полученных от Print Monitor. В зависимости от используемой версии InfoWatch Device Monitor, перехватчик Print Monitor может передавать задания на печать в формате txt (извлечение текста выполняется средствами Device Monitor) или в формате pdf, либо передаёт оба файла (txt+pdf). В первых двух случаях значение параметра OCR не влияет на работу системы. **Важная информация!** Если `OCR = Off`, то txt-файлы сразу передаются на контентный анализ. Рекомендуется, если требуется уменьшение нагрузки на сервер Traffic Monitor
`DmOCR`	Использование OCR для файлов, полученных от Device Monitor
`DlaOCR`	Использование OCR для файлов, полученных от DeviceLock Adapter
`CrawlerOCR`	Использование OCR для файлов, полученных от перехватчика Crawler
`SkypeOCR`	Использование OCR для файлов, полученных от Skype Monitor
`XmppOCR`	Использование OCR для файлов, полученных от XMPP Monitor
`MmpOCR`	Использование OCR для файлов, полученных от MMP Monitor
`FtpOCR`	Использование OCR для файлов, полученных от FTP Monitor

5.3.3. Секция [*EXTRACTOR*]

В секции [EXTRACTOR] указаны параметры, используемые при извлечении файлов из архивов и вложений:

Параметр	Описание
DetectorPath	Путь к файлу, в котором хранятся настройки, необходимые для определения и обработки архивов и вложений. Значение по умолчанию etc/detector_ocr.conf. О порядке настройки этого файла см. документ «*InfoWatch OCR для InfoWatch Traffic Monitor. Руководство по установке и конфигурированию*»
TempDir	Путь к каталогу, в который временно сохраняются извлеченные файлы. Значение по умолчанию tmp (путь указан относительно текущего каталога, которым является корневой каталог Системы)

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

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

В файле /usr/local/infowatch/tm3/etc/icap.conf, секция [ICAP] задаются параметры взаимодействия с ICAP сервером:

Параметр	Описание и примеры настройки
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования: от 0(протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 3.
CoreDumpSize	Размер (в байтах) дампа памяти. Данный параметр используется для разбора ошибочных ситуаций. Рекомендуется указывать значение -1 (отсутствие ограничений на размер дампа памяти). Значение 0 указывают, если запись не ведется. Значение по умолчанию -1
MaxFiles	Число открытых файлов. По умолчанию 0 – в этом случае используется значение, установленное в настройках операционной системы (по умолчанию 1024). Для повышения производительности при большом объеме трафика можно увеличить это значение. При изменении параметра нужно устанавливать значение больше системного. Для нагруженных систем рекомендуемое значение – 8000.
ListenPort	Порт, на котором ICAP-сервер прослушивает HTTP-запросы, поступающие от прокси-сервера с ICAP-клиентом. Допускается использование портов с номерами от 1025. Значение по умолчанию 1344

Параметр	Описание и примеры настройки
`PathTemporary`	Путь к хранилищу временных файлов ICAP-сервера (по умолчанию `/usr/local/infowatch/tm3/temp/icap`)
`error_html`	Путь к HTML-файлу, в котором содержится сообщение, выводимое в окне интернет-обозревателя, если запрос пользователя был заблокирован Системой. Значение по умолчанию `etc/error.html`. (путь указан относительно текущего каталога, которым является корневой каталог Системы)
`min_text_length`	Минимальный объем текста (в байтах), для которого будет проводиться контентный анализ. Значение по умолчанию 5 байт. Настройка данного параметра позволяет снизить нагрузку на сервер контентного анализа. Это может быть достигнуто путем отказа от контентного анализа текста, размер которого настолько мал, что не позволяет передавать значимые сообщения
`min_data_length`	Минимальный объем (в байтах) URL-переменной, который будет включен в текстовый блок для передачи на контентный анализ. Значение по умолчанию 10 байт.
`LogBlock`	Настройка для уровня протоколирования не меньше 4 (`LogLevel=4`). Запись в системный журнал сообщений о блокировке перехваченных HTTP-запросов. Значение по умолчанию - `0`: запись не ведется
`LogTimer`	Запись в системный журнал сообщений о времени обработки HTTP-запросов. Запись ведется, если установлено значение `1`. По умолчанию имеет значение `0` – запись не ведется
`disable_ipv6`	Отключение (`disable_ipv6 = 1`) и включение (`disable_ipv6 = 0`) поддержки подключений по протоколу IPv6. По умолчанию поддержка включена. Если на сервере ICAP поддержка IPv6 отключена, то служба `iw_icap` будет запускаться и работать в штатном режиме только при включенной опции, то есть когда `disable_ipv6 = 1`.

5.5. Настройка параметров обработки архивов вложений (файл detector.conf)

В файле `/usr/local/infowatch/tm3/etc/detector.conf` хранится база данных сигнатур, с помощью которых определяется тип файлов при распаковке архивов и вложений.

Секция `[common]` предназначена для настройки общих параметров:

Параметр	Описание и примеры настройки
`Timeout`	Время ожидания (в секундах) до завершения обработки файла. Значение по умолчанию: `Timeout = 1800`
`Minfilesize`	Минимальный размер файла (в байтах), подлежащего распаковке. Это ограничение позволяет увеличить производительность Системы, за счет отказа от распаковки небольших файлов. Значение по умолчанию: `MinFileSize = 10`

Параметр	Описание и примеры настройки
FilenameCharsets	Если кодировка имени файла отличается от стандартной (ANSI, UTF), то файл будет обрабатываться как соответствующий кодировкам, указанным в данном параметре. Несколько значений перечисляются через запятую; Система будет последовательно пытаться обработать файл в перечисленных кодировках, пока не найдёт похожую. Значение по умолчанию: `FilenameCharsets = "UTF-8,cp1251,cp866"`
DefaultTextCharset	Если кодировка содержимого файла отличается от стандартной (ANSI, UTF), то файл будет обрабатываться как соответствующий кодировкам, указанным в данном параметре. Несколько значений перечисляются через запятую; Система будет последовательно пытаться обработать файл в перечисленных кодировках, пока не найдёт похожую. Значение по умолчанию "`UTF-8`"
Speed	Предположительная скорость работы экстрактора, в Кб/с, в расчете на 1 ГГц частоты процессора. Значение по умолчанию "`100`"
NeedLogLevel	Уровень протоколирования - от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 0.

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

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

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

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

Параметр	Описание и примеры настройки

`Sign`	Сигнатура формата, которая представляет собой «образцовую» последовательность значений (байтов) с начальным смещением и масками. Эта последовательность необходима для однозначного определения формата файлов по их содержимому
	Сигнатура может включать до 16 триад вида:
	`[OFFSET]:BYTE_VALUE/[MASK]`
	Допускается также и строковая сигнатура, например, `"BZh"`, для BZIP2. Эта сигнатура означает указанную последовательность байтов от смещения `0`. Поиск строковых сигнатур выполняется без учета регистра символов.
	Параметр `OFFSET` является необязательным. Для первого байта этот параметр по умолчанию равен `0`, для всех последующих – увеличивается на единицу. Смещение можно задать с символом «`?`» – поиск образца в первых N байтах файла. Например, для поиска образца в первых 500 байтах файла, нужно задать смещение `'500?'`.
	Параметр `MASK`, также является необязательным и равен `0xFF` по умолчанию.
	Пример (сигнатура заголовка WAV-формата):
	`Sign = "'RIFF', 0x8: 'WAVEfmt'"`
	Начиная от смещения `0`, расположена последовательность `'R'`, `'I'`, `'F'`, `'F'`, далее от смещения `8` должно следовать `'W'`, `'A'`, `'V'`, `'E'`, `'f'`, `'m'`, `'t'`

`Comment`	Комментарий с пояснениями, например, указание используемой версии архиватора: `Comment = "bzip2 v. 1.0.x"`
`Extract`	Строка команды для извлечения файлов. Например, `Extract = "/usr/bin/bzip2 -f -dc ${SRC} > ${OUTDIR}/${SRC}"` где `${OUTDIR}` – каталог, в который будет распакован архив, а `${SRC}` – имя файла, который нужно распаковать
`Exclude`	Если параметр включен (`On`), то распаковка объекта выполняется, но информация об архиваторе не добавляется в XML-контекст объекта. Это позволяет не отображать в контексте объекта фиктивные контейнеры типа MS-TNEF. По умолчанию параметр отключен (`Off`)
`CaseInsensitive`	Признак того, что при обработке файла не будет учитываться регистр символов.
`CreatesTags`	Признак того, что при обработке с помощью экстракторов Traffic Monitor происходит извлечение метаинформации из файла.

5.6. Синхронизация базы отпечатков эталонных документов между несколькими серверами

> **Важная информация!**
>
> Синхронизация базы отпечатков эталонных документов производится, если используются два и более сервера Traffic Monitor.

Если в Системе используются два и более сервера Traffic Monitor, для них предусмотрена разная логика обновления базы отпечатков эталонных документов:

- сервер *Master* – главный сервер, обновляющий базу отпечатков эталонных документов (выполняет скрипт **db_CA.pl**). Сервером *Master* в Системе может являться только один сервер;

- сервер *Slave* – второстепенный сервер, копирующий отпечатки эталонных документов с сервера *Master*. Взаимодействие сервера *Slave* с базой отпечатков эталонных документов состоит в обмене служебной информацией, подтверждающей актуальность настроек базы эталонных документов на сервере *Slave* (выполнение скрипта **db_CA_lite.pl**). Серверами *Slave* в Системе могут являться один или несколько серверов.

По умолчанию все серверы в Системе настроены для работы, как главные (*Master*), поэтому необходимо выполнить синхронизацию базы отпечатков эталонных документов между несколькими серверами.

Чтобы синхронизировать базу отпечатков эталонных документов между несколькими серверами, выполните следующие действия:

1. Произвольно выберите, какой из серверов будет использоваться как *Master*.

> **Примечание:**
>
> Остальные сервера будут использоваться как *Slave*.
>
> Предполагается, что выбор логики работы сервера (*Master* или *Slave*) зависит от предпочтений администратора Системы и не требует дополнительных действий по настройке логики работы, кроме указанных в пределах данного подраздела.

2. На сервере (серверах) *Slave*:
   a) Войдите в систему от имени пользователя **root**.
   b) В файле **/etc/crontab** удалите строку

```
* * * * * root /usr/local/infowatch/tm3/bin/scripts/db_CA.pl&>/dev/null
```

   Скрипт **db_CA.pl** перестанет выполняться сервером *Slave*.

   c) Выполните команду:

```
service crond restart
```

   Произойдет обновление запланированных на сервере задач.

3. На сервере *Master*:
   a) Войдите в систему от имени пользователя **root**.
   b) Выполните команды:

```
ssh-keygen
```

```
ssh-copy-id -i /root/.ssh/id_rsa <адрес_сервера_Slave>,
```

   где `<адрес_сервера_Slave>` - IP-адрес сервера *Slave*.

> **Важная информация!**
>
> Если в Системе используются более одного сервера *Slave*, команда `ssh-copy-id <адрес_сервера_Slave>` должна быть выполнена отдельно для каждого из серверов *Slave*.

   c) Выполните команду:

```
/usr/local/infowatch/tm3/bin/scripts/db_CA.pl
```

5.7. Настройка максимального размера добавляемого эталонного документа (файл casdbcfg.conf)

Файл `/usr/local/infowatch/tm3/etc/casdbcfg.conf` содержит значение максимального размера файла эталонного документа, из которого может быть создан цифровой отпечаток (подробнее об эталонных документах см. «*InfoWatch Traffic Monitor. Руководство пользователя*»).

По умолчанию максимальный размер файла – 128 Мб:

```
CAMaxFileSize = 128
```

Однако изменить данный параметр возможно только через базу данных.

Чтобы изменить максимально допустимый размер загружаемого эталонного документа:

1. Подключитесь к серверу базы данных от имени владельца схемы базы данных:

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

   где `db_login` и `db_password` – имя и пароль владельца схемы базы данных, а `tns_name` – имя службы TNS.

   Если проверка пройдена успешно, то в ответ на выполнение команды будет выведено приглашение SQL *Plus:

   ```
   SQL>
   ```

2. Выполните следующий сценарий:

   ```
   begin
     sp_ca_max_file_size_set(128);
   commit;
   end;
   /
   ```

   где вместо 128 укажите требуемый допустимый размер файла, в мегабайтах. Для снятия ограничения укажите «-1».

3. Выполнить загрузку конфигурации на серверы (см. документ «*InfoWatch Traffic Monitor. Руководство пользователя*»)

В результате значение параметра `CAMaxFileSize` в файле `casdbcfg.conf` также будет изменено.

5.8. Настройка правил фильтрации для Sniffer

При использовании схемы со Sniffer, вы можете настроить Систему так, что на обработку в Traffic Monitor будут отправляться только пакеты, отправленные на определенные адреса и порты. Эти правила задаются в отдельности для каждого типа трафика и содержатся в файлах `icq.rules`, `http.rules` и `smtp.rules` каталога `/usr/local/infowatch/tm3/etc/`.

Содержимое файлов представляет собой набор правил, на соответствие которым проверяется пакет.

Каждое правило имеет следующий формат:

```
aaa.bbb.ccc.ddd[/число_бит] *|порт1,порт2,порт3-порт4 ACCEPT|DROP
```

где:

- `aaa.bbb.ccc.ddd` – IP-адрес узла или подсети
- `число_бит` – число бит; если не указано, то принимается равным 32 (то есть для выполнения правила IP-адрес пакета должен быть точно равен указанному).
- `порт1,порт2,порт3-порт4` – перечень портов: перечисление через запятую, диапазоны указываются через дефис. Если вместо перечня портов указан символ «*», то принимаются пакеты для всех портов.

- `ACCEPT` – при выполнении условия пакет принимается и отправляется на дальнейшую обработку.
- `DROP` – при выполнении условия дальнейшая обработка пакета прекращается, он не передается ни на сервер Traffic Monitor, ни в базу данных.

Строки с комментариями начинаются с символа '#'.

Фильтрация производится в следующем порядке:

IP-адрес и порт пакета проверяются на соответствие правилам: от первой строки к последней.

Если IP-адрес совпадает по маске и порт попадает в указанный диапазон, то выполняется указанное в правиле действие: пакет принимается и отправляется на дальнейшую обработку (ACCEPT) или его обработка прекращается (DROP).

Если IP-адрес либо порт не соответствуют условию, то выполняется проверка по следующей строчке.

Если пакет не соответствует ни одному условию из приведенных в файле правил, то его дальнейшая обработка прекращается, он не передается ни на сервер Traffic Monitor, ни в базу данных.

Пример:

Пусть пакет, отправленный на адрес 10.1.0.1, порт 22, проверяется по следующим правилам:

```
# Получение пакетов, отправленных на порт 3128 на сервер 10.0.1.128
10.0.1.128 3128 ACCEPT
# Отбрасывать всё остальное, что идёт в подсеть 10.0.1.*
10.0.1.0/24 * DROP
# Получение всего, отправленного на стандартные порты и прокси в подсети 10.*.*.*
10.0.0.0/8 1-1023,3128,8080 ACCEPT
# Все остальные пакеты отбрасываются
```

В результате для пакета будет выполнено третье правило, и пакет будет передан на дальнейшую обработку в Traffic Monitor.

5.9. Управление загрузкой объектов в удаленную базу данных

Загрузка объектов в удаленную базу данных используется, когда у организации имеется один или несколько филиалов, и трафик, перехватываемый в филиалах, нужно хранить в центральном офисе. Тогда после анализа объекты из филиалов передаются в базу данных центрального офиса. Передача данных происходит по медленным каналам связи (от 128 кбит/с).

Для реализации схемы взаимодействия с удаленной базой данных на Traffic Monitor Server устанавливается дополнительный модуль. В филиалах устанавливается клиентская часть, в центральном офисе устанавливается серверная часть модуля взаимодействия с удаленной базой данных.

Основные схемы развертывания при работе с удаленной базой данных описаны в документе «*Руководство по установке и конфигурированию*».

Далее в этом разделе:

- *Параметры приема объектов на стороне сервера (п. 5.9.1 на стр. 78).*
- *Параметры отправки объектов на стороне клиента (п. 5.9.2 на стр. 79).*
- *Настройка ширины полосы пропускания для канала передачи данных (клиент) (п. 5.9.3 на стр. 80).*
- *Просмотр статистической информации по загрузке объектов в удаленную базу данных (п. 5.9.4 на стр. 80).*

5.9.1. Параметры приема объектов на стороне сервера

В файле `/usr/local/infowatch/tm3/etc/qmover.conf` на стороне сервера (загрузчика объектов) в секции `[QMOVER_SERVER]` задаются параметры приема объектов от клиентов:

Параметр	Описание
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования: от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 1.
ListenerPort	Порт, на котором будут прослушиваться поступающие объекты. Значение по умолчанию 16888
Clients	Список удаленных клиентов, передающих объекты на сервер: Clients = "client_1 client_2 … client_N" Параметры каждого клиента заданы в отдельной секции [client_N]: • IP. IP-адрес клиента N. • QueuePath. Путь к очереди, в которую будут поступать файлы, полученные от клиента N. По умолчанию – общая очередь /usr/local/infowatch/tm3/queue/db.

5.9.2. Параметры отправки объектов на стороне клиента

В файле /usr/local/infowatch/tm3/etc/qmover.conf на стороне клиента (перехватчика объектов) в секции [QMOVER_CLIENT] задаются параметры передачи очереди объектов в удаленную базу данных:

Параметр	Описание
Daemon	Запуск в режиме демона (значение On) или в режиме обычного процесса (значение Off). Значение по умолчанию On
LogLevel	Уровень протоколирования: от 0 (протоколируются только ошибки) до 8 для отладочной информации. Соответствует уровням протоколирования syslog. Значение по умолчанию 1.
ListenerIP	IP-адрес сервера-загрузчика, на котором будут прослушиваться поступающие объекты. Значение по умолчанию 127.0.0.1
ListenerPort	Порт сервера-загрузчика, на котором на котором будут прослушиваться поступающие объекты. Значение по умолчанию 16888
Window	Размер окна (во фреймах). Значение по умолчанию 100
MaxFrameSize	Максимальный размер фрейма (в байтах). Значение по умолчанию 1400 Примечание: не рекомендуется устанавливать размер фрейма больше, чем максимальный размер фрейма (MTU) маршрутизаторов, находящихся между клиентом и сервером.
QueuePath	Путь к локальной очереди объектов, которую надо пересылать на удаленный сервер. Значение по умолчанию - queue/db/

5.9.3. Настройка ширины полосы пропускания для канала передачи данных (клиент)

По умолчанию полоса пропускания имеет ширину 128 Кбит/с. Но вы можете настроить автоматическое изменение полосы пропускания в различные периоды времени. Настройка выполняется на стороне клиента (перехватчика объектов) при помощи утилиты:

```
/usr/local/infowatch/tm3/bin/iw_qmover_channel__width_setter
```

Допускается изменение ширины полосы пропускания в диапазоне от 128 Кбит/с до 2 Мбит/с.

Чтобы настроить ограничения на ширину полосы пропускания:

на стороне сервера отправителя (*client*) 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 (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 cron команды:

```
00 9 * * * /usr/local/infowatch/tm3/bin/iw_qmover_channel_width_setter 128
00 18 * * * /usr/local/infowatch/tm3/bin/iw_qmover_channel_width_setter 256
```

5.9.4. Просмотр статистической информации по загрузке объектов в удаленную базу данных

Просматривать статистическую информацию по загрузке объектов в удаленную базу данных можно на клиенте и на сервере.

Чтобы вывести статистическую информацию по работе клиента,

выполните команду:

```
killall -SIGUSR2 iw_qmover_client
```

После выполнения команды в системный журнал протоколирования на клиенте будет записана следующая информация:

Запись в журнале	Значение
stat: started at	Время запуска демона `iw_qmover_client`
stat: works on … file queue	Путь к очереди объектов, подготовленных к передаче на сервер

Запись в журнале	Значение
stat: bytes sent: … objects sent: …	Объем (в байтах) отправленных объектов Количество отправленных объектов
stat: bytes recv: … file ACKs recv: … object NAKs recv: …	Объем подтверждений (в байтах) от сервера Количество объектов успешно принятых сервером-загрузчиком (*server*) Количество команд на повторную обработку объектов
stat: uses bandwidth … kbit/s	Полоса пропускания (kbit/s), занимаемая клиентом в текущий момент
stat: connected to server <IP-адрес> или stat: currently disconnected from server <IP-адрес>	Клиент подключился к серверу-загрузчику с указанным IP-адресом или отключился от сервера-загрузчика

Чтобы вывести статистическую информацию по работе сервера,

выполните команду:

```
killall –SIGUSR2 iw_qmover_server
```

После выполнения команды в системный журнал протоколирования будет записана следующая информация:

Запись в журнале	Значение
stat: started at	Время запуска сервиса (listener), прослушивающего объекты, поступающие от клиента
Для каждого клиента	
stat: client <IP-адрес> work on … file queue	Путь к файловой очереди, в которую загружаются объекты, полученные от клиента с данным IP-адресом
stat: status is CONNECTED или stat: status is DISCONNECTED	Состояние соединения с клиентом (*client*): подключен (CONNECTED) или отключен (DISCONNECTED)
stat: bytes recv … objects recv …	Объем (в байтах) принятых объектов Количество принятых объектов
stat: bytes sent … file ACKs sent … file NAKs sent …	Объем подтверждений (в байтах), отправленных клиенту Количество объектов успешно принятых сервером-загрузчиком (*server*) Количество запросов на повторную передачу объекта

5.10. Архивирование каталога очереди сообщений

При ошибках в очереди входящих SMTP-писем заархивируйте каталог очереди SMTP-писем и сохраните его для последующего анализа. Затем удалите каталог. Местоположение каталога очереди сообщений

указано в конфигурационном файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[Queue]` как значение параметра `Smtp` (подробнее о параметрах `tm.conf` см. п. 5.2 на стр. 51).

5.11. Протоколирование работы Системы

Протоколирование в InfoWatch Traffic Monitor Server ведется средствами системы протоколирования syslog. Подсистема протоколирования соответствует *local1*.

За подробной информацией по работе с системой протоколирования syslog вы можете обратиться к документации syslog.

Настройка расширенного протоколирования

> **Важная информация!**
>
> Следует учитывать, что повышение уровня протоколирования (`LogLevel`) может значительно снизить производительность Системы.

Чтобы настроить расширенное протоколирование для одного или нескольких процессов Traffic Monitor Server:

1. В файле `tm.conf` установите для параметра `LogLevel` необходимое значение, не ниже `3`.
2. Разрешите запись сообщений с соответствующим уровнем протоколирования в системный журнал `/etc/rsyslog.conf`. Для этого нужно добавить в строку для `/var/log/messages` значение:

   ```
   *.debug;
   ```
3. После внесения изменений в системный журнал, перезапустите службу syslog:

   ```
   service rsyslog restart
   ```

Файлы журналов

Файлы журналов расположены по следующим путям:

- `/var/log/messages` (основной журнал)
- `/var/log/maillog` (анализ запросов и ответов от серверов SMTP)
- `/var/log/tm.log` (только если система интегрирована с Tivoli)

Также полная информация о работе Системы может быть доступна через БД Oracle: таблица **v_sys_log**.

Использование утилиты Sosreport для сбора информации о системе

Утилита **sosreport** - это стандартная утилита Linux, предназначенная для сбора подробной информации о системе: характеристики оборудования, список установленных пакетов, произведенные настройки и т.п.

Чтобы собрать информацию о системе:

1. Закройте все запущенные приложения.
2. От имени root выполните:

   ```
   [root@iwdb ~]# sosreport --batch
   ```

   До окончания процесса сбора информации не запускайте никаких приложений и не производите никаких настроек.

В результате в каталоге `/tmp` будет создан файл `вида /tmp/sosreport-iwdb.777777777-57831-7fee1d.tar.bz2`. Этот файл можно, например, отправить в службу технической поддержки.

5.12. Перемещение объектов между очередями (утилита iw_qtool)

Необходимость перемещения объектов из одной очереди в другую может возникнуть, когда:

- Объекты из филиалов загружаются в базу данных центрального офиса по медленному каналу связи (используется модуль загрузки в удаленную базу данных), и для каждого филиала существует отдельная очередь объектов (локальная очередь), поэтому для загрузки в базу данных нужно переместить объекты в общую очередь сервера (глобальная очередь).
- Объекты не загружаются в базу данных (см. Приложение С на стр. 96).

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

> **Примечание:**
>
> Утилиту iw_qtool нужно запускать от имени владельца InfoWatch Traffic Monitor. Имя владельца задано в файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[GENERAL]`, параметр `user`.

Команды для работы с утилитой iw_qtool:

Название команды	Описание, синтаксис, примеры
`stat`	Показывает количество объектов в очереди. *Синтаксис*: `iw_qtool stat` *`имя_очереди`* *Пример (просмотр статистики по очереди объектов, загружаемых в базу данных):* `/usr/local/infowatch/bin/iw_qtool stat /usr/local/infowatch/queue/db`

`move`	Перемещает объекты из одной очереди в другую.
	Важная информация! В процессе перемещения объектов утилита создает временные файлы в текущем каталоге. Поэтому в данном случае рекомендуется запускать утилиту iw_qtool из каталога `/usr/local/Infowatch/tm3`.
	Синтаксис:
	`iw_qtool move очередь_источник очередь_приемник [количество_объектов]`
	Параметры:
	• `очередь_источник` – полное имя очереди, из которой нужно переместить объекты. Если указанной очереди не существует, то работа утилиты завершится ошибкой;
	• `очередь_приемник` – полное имя очереди, в которую нужно переместить объекты. Если указанная очередь не существует, то она будет создана в процессе работы утилиты.
	• `количество_объектов` – ограничение на количество перемещаемых объектов (необязательный параметр). Если этот параметр не задан, то будут перемещены все объекты, находящиеся в очереди-источнике.
	Пример (перенос объектов из очереди errors в очередь db):
	`iw_qtool move /usr/local/infowatch/tm3/queue/errors /usr/local/infowatch/tm3/queue/db`

`put`	Помещает одиночный объект в очередь. **Важная информация!** Для выполнения команды необходимо иметь права на запись в текущий каталог. *Синтаксис*: `iw_qtool put очередь_получатель xml_файл_объекта файл_объекта` *Параметры*: • `очередь_получатель` – полное имя очереди, в которую нужно поместить объект. Если указанной очереди не существует, то работа утилиты завершится ошибкой;

Название команды	Описание, синтаксис, примеры
	• `xml_файл_объекта` – полное имя XML файла объекта. Если указанного файла не существует, то работа утилиты завершится ошибкой. • `файл_объекта` – полное имя файла с данными объекта. Если указанного файла не существует, то работа утилиты завершится ошибкой. *Пример (помещение объекта в очередь db):* `iw_qtool put /usr/local/infowatch/tm3/queue/db /home/iwtm/000000000.dat.xml /home/iwtm/000000000.dat`

5.13. Загрузка очередей объектов

Чтобы обеспечить загрузку имеющихся очередей объектов:

1. Остановите процессы Traffic Monitor:

   ```
   OS:root> service iw-trafmon stop
   ```

2. Для процессов перехватчиков **iw_proxy**, **iw_smtpd**, **iw_expressd** и **iw_icap** отключите автозапуск в файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[AUTO_RESTART]`:

   ```
   autorestart = Off
   ```

3. Запустите процессы Traffic Monitor

   ```
   service iw-trafmon start
   ```

4. Дождитесь, пока будут обработаны все объекты в файловой очереди. Для этого можно проследить содержимое каталогов с очередями (о расположении этих каталогов см. п. 5.2.6 на стр. 56, *«Секция [*QUEUE]*»*).

Примечание:

По окончании обновления Системы убедитесь, что перехватчики запущены, и в конфигурационном файле включен автозапуск процессов.

5.14. Восстановление работоспособности системы в аварийных ситуациях

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

1. Остановите процессы Traffic Monitor Server, выполнив команду:

   ```
   service iw-trafmon stop
   ```

2. Закройте все экземпляры Management Console.
3. Переместите объекты из ошибочных очередей в обычные. Процедура выполняется при помощи утилиты iw_qtool (см. п. 5.12 на стр. 82).
4. По окончании работ проверьте соединение с СУБД Oracle, выполнив команду:

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

   где `db_login` и `db_password` – имя и пароль владельца схемы базы данных, а `tns_name` – имя службы TNS.

   Если проверка пройдена успешно, то в ответ на выполнение указанной команды будет выведено приглашение SQL *Plus:

   ```
   SQL>
   ```

5. Запустите процессов Traffic Monitor Server, выполнив команду:

```
service iw-trafmon start
```

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

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

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

ПРИЛОЖЕНИЕ А. ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ УТИЛИТЫ АВТОАРХИВИРОВАНИЯ

Утилита автоархивирования предназначена для архивирования табличных пространств в схеме базы данных версии 3.4.1 и выше.

> **Важная информация!**
>
> Во время работы утилиты автоархивирования не запускайте вручную задания базы данных: IWADDPARTS, IWTM_SYNC_INDEXES, IWDROP. Это может привести к потере данных.

Настоящая инструкция содержит описание следующих действий:

- *Настройка параметров архивирования (см. п. А.1 на стр. 86).*
- *Запуск автоархивирования (см. п. А.2 на стр. 87).*
- *Определение переменных окружения (см. п. А.3 на стр. 88).*
- *Повторное автоматическое архивирование восстановленного табличного пространства (см. п. А.4 на стр. 89).*
- *Сообщения об ошибках (см. п. А.5 на стр. 89).*

А.1. Настройка параметров архивирования

Настройка автоархивирования производится с помощью конфигурационного файла autoarchive.conf. Конфигурационный файл состоит из строк вида `параметр=значение`.

А.1.1. Параметры конфигурационного файла

Параметр	Описание
`database`	Строка подключения к БД (tnsname).
`username`	Имя владельца схемы данных. Обязательный параметр. **Примечание:** в случае установки с использованием kickstart, значение параметра должно быть `iwtm`.
`password`	Пароль. Обязательный параметр.
`age`	Возраст табличных пространств, в днях: табличные пространства, созданные раньше, подлежат архивации. Обязательный параметр. **Пример:** если параметр указан равным 5, то архивируются табличные пространства, созданные 5 дней назад и ранее. **Примечание:** если параметр указан равным 0, то архивируются все табличные пространства, включая табличные пространства за текущий день.

Параметр	Описание
`dest_dir`	Директория для архивирования. Обязательный параметр. **Примечание:** • указываемая директория должна быть создана самим администратором (например, в директории, созданной в результате распаковки архива, добавим каталог `catalog`); • после распаковки архива скрипту необходимо задать права запуска с помощью команды `chmod` (для скрипта `autoarchive` команда будет иметь вид: `chmod +x autoarchive`).
`log_info`, `log_errors`	Параметры вывода сообщений информационных сообщений и сообщений об ошибках. Чтобы настроить вывод сообщений в файл, в качестве значения параметра укажите имя файла. Если параметр не задан или отсутствует, сообщения будут выводиться на консоль. Чтобы отключить вывод какого-либо типа сообщений, укажите в качестве значения параметра `/dev/null`, например: `log_info=/dev/null`
`job_timeout`	Таймаут ожидания завершения заданий БД в секундах. По умолчанию равен `7200` (т.е. 2 часа).

Пример файла конфигурации:

```
database=
username=iwtm
password=xx1234
age=3
dest_dir=./catalog/
```

A.2. Запуск автоархивирования

Для запуска автоархивирования необходимы следующие права:

- права владельца схемы БД (требуется для работы с job и получения табличных пространств с их файлами).
- unix-пользователь должен иметь право чтения и записи файлов табличных пространств и каталогов архива. Вы можете использовать учетную запись Oracle или создать отдельного пользователя с соответствующими правами.

A.2.1. Запуск вручную

Чтобы запустить сценарий вручную, введите следующую команду:

```
$ perl autoarchive autoarchive.conf [simulate]
```

где:

- `autoarchive.conf` - файл конфигурации (обязательный параметр);
- `simulate` - необязательный параметр, запускающий сценарий в режиме проверки: реальных изменений в БД сделано не будет, но будет выполнена остановка, поиск табличных пространств и файлов, подлежащих архивации, а затем - разрешено выполнение заданий.

A.2.2. Автоматический запуск

Чтобы настроить автоматический запуск автоархивирования по расписанию, создайте задание с указанием времени автозапуска в cron (подробнее см. man 5 crontab).

Сценарий должен запускаться ночью, не ранее чем через 1 час после запуска последнего из ежедневных заданий Oracle. К числу этих заданий относятся `IWADDPARTS` и `IWDROP`.

A.3. Определение переменных окружения

В некоторых случаях для доступа к БД сценарий может потребовать указать переменные окружения. На это могут указать сообщения об ошибках, отображающиеся при попытке запуска сценария (см. п. A.5 на стр. 89). В таком случае вам необходимо указать переменные окружения в строке запуска сценария.

В общем виде командная строка для запуска сценария выглядит так:

```
ORACLE_HOME=<значение для ORACLE_HOME> LD_LIBRARY_PATH=<значение для SO-библиотеки> perl
-I<значение для pm-модуля 1> -I<значение для pm-модуля 2> ./autoarchive autoarchive.conf
```

О том, как получить значения переменных окружения, см. п. A.3.1 на стр. 88 и п. A.3.2 на стр. 88.

Пример строки запуска автоархивирования с указанием переменных окружения:

```
ORACLE_HOME=/u01/app/oracle/product/11.2.0/db_1
LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib"                    -
I/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi                        -
I/u01/app/oracle/product/11.2.0/db_1/lib ./autoarchive autoarchive.conf
```

A.3.1. Поиск путей к модулям

Для работы DBI perl-модуля доступа к БД при запуске автоархивирования может оказаться необходимым указать местоположение pm-модулей и SO-библиотек.

Для поиска и отображения путей к модулям воспользуйтесь специальным сценарием autoarchive-autodetect.

Примечание: если в поиск необходимо включить файлы, появившиеся после последней индексации, то перед запуском сценария выполните индексацию вручную (см. man updatedb).

Пример результата работы сценария autoarchive-autodetect:

```
Using locate to find modules...
{
  LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib"
}
  perl
{
  -I/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi
{
  -I/u01/app/oracle/product/11.2.0/dbhome_1/lib
```

С помощью путей к модулям, отображенных в результате работы сценария, вы можете составить командную строку для запуска сценария:

Пример 1:

```
LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib"                    -
I/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi                        -
I/u01/app/oracle/product/11.2.0/dbhome_1/lib ./autoarchive autoarchive.conf
```

Пример 2 (на машине установлена переменная окружения $ORACLE_HOME):

```
LD_LIBRARY_PATH=$ORACLE_HOME/lib                          perl                   -
I$ORACLE_HOME/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi-I$ORACLE_HOME/lib
./autoarchive autoarchive.conf
```

A.3.2. Задание переменной окружения ORACLE_HOME

В некоторых случаях для работы DBI perl модулей также требуется задать переменную окружения ORACLE_HOME. Если она не задана, при попытке запуска автоархивирования появится соответствующее сообщение об ошибке (см. см. п. A.5 на стр. 89).

В этом случае в начале строки запуска автоархивирования необходимо указать значение переменной окружения ORACLE_HOME. Как правило, она равна LD_LIBRARY_PATH без последнего /lib (см. п. A.3.1 на стр. 88).

Пример:

```
ORACLE_HOME="/u01/app/oracle/product/11.2.0/dbhome_1"
LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib"                    -
I/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi                        -
I/u01/app/oracle/product/11.2.0/db_1/lib ./autoarchive autoarchive.conf
```

A.3.3. Быстрый запуск автоархивирования

Для удобства запуска вы можете создать shell-файл с полной командой запуска сценария `autoarchive`, либо задать переменные окружения заранее.

Пример 1 (в bash):

```
export ORACLE_HOME="/u01/app/oracle/product/11.2.0/dbhome_1"
export LD_LIBRARY_PATH="/u01/app/oracle/product/11.2.0/dbhome_1/lib"
export PERL5LIB="/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi"
```

Пример 2:

```
export ORACLE_HOME=/u01/app/oracle/product/11.2.0/dbhome_1
export LD_LIBRARY_PATH=$ORACLE_HOME/lib
export PERL5LIB="/usr/lib/perl5/vendor_perl/5.8.5/i386-linux-thread-multi"
```

После выполнения этих настроек автоархивирование можно запускать с помощью короткой строки:

```
./autoarchive autoarchive.conf
```

A.4. Повторное автоматическое архивирование восстановленного табличного пространства

Если табличное пространство, ранее заархивированное автоматически, было восстановлено (см. п. 4.3.4 на стр. 37), то повторное автоматическое архивирование этого ТП описанным выше способом выполняться не будет.

Для автоматического архивирования восстановленного ТП необходимо от имени владельца схемы базы данных выполнить следующий сценарий:

```
BEGIN
   update tbs_list
      set status = 1
      where part_date = дата_табличного_пространства;
COMMIT;
END;
/
```

A.5. Сообщения об ошибках

Ниже приведены описания возможных ошибок, отображающихся при работе сценария.

Если при запуске утилиты автоархивирования отображается следующая ошибка:

```
/u01/app/oracle/product/11.2.0/dbhome_1/perl/lib/site_perl/5.10.0/i686-linux-thread-
multi/auto/DBI/DBI.so: undefined symbol: Perl_Istack_sp_ptr
```

То проверьте версию perl DBI помощью следующей команды:

```
rpm –q perl-DBI
```

Если пакет отсутствует или имеет версию ниже 1.52, выполните установку с помощью следующей команды:

```
rpm –i perl-DBI
```

Если отображается следующая ошибка:

```
Can't locate DBI.pm in @INC (@INC contains: [тут длинный список]) at autoarchive
BEGIN failed--compilation aborted at ...
```

Это означает, что не заданы или заданы неправильно пути к pm-модулям.

Если отображается следующая ошибка:

```
install_driver(Oracle) failed: Can't load '[...]Oracle.so' for module
DBD::Oracle: libclntsh.so.11.1: cannot open shared object file:
No such file or directory at /usr/lib/perl5/5.8.8/i386-linux-thread-multi/DynaLoader.pm
line at (eval 1) line 3
Compilation failed in require at (eval 1) line 3.
Perhaps a required shared library or dll isn't installed where expected at autoarchive
line
```

Это означает, что не задан или задан неправильно `LD_LIBRARY_PATH`.

Если отображается следующая ошибка:

```
ORACLE_HOME environment variable not set!
DBI connect('database','username',...) failed: (UNKNOWN OCI STATUS 1804)
OCIInitialize. Check ORACLE_HOME and NLS settings etc. at autoarchive
DBI Connect error: (UNKNOWN OCI STATUS 1804) OCIInitialize. Check ORACLE_HOME and NLS
settings etc. at autoarchive
```

Это означает, что не задана переменная окружения `ORACLE_HOME`.

Если отображается следующая ошибка:

```
DBI connect('iwtm','iwtm_578',...) failed: (UNKNOWN OCI STATUS 1804)
OCIInitialize. Check ORACLE_HOME and NLS settings etc. at autoarchive
DBI Connect error: (UNKNOWN OCI STATUS 1804) OCIInitialize.
Check ORACLE_HOME and NLS settings etc. at autoarchive
```

Это означает, что переменная окружения `ORACLE_HOME` есть, но задана неверно.

Если отображается следующая ошибка:

```
DBI connect('iwtm','iwtm_578',...) failed: Error while trying to retrieve text for error
ORA-12154 (DBD ERROR: OCIServerAttach) at autoarchive
DBI Connect error: Error while trying to retrieve text for error ORA-12154 (DBD ERROR:
OCIServerAttach) at autoarchive
```

Переменная окружения `ORACLE_HOME` есть, но задана неверно.

ПРИЛОЖЕНИЕ В. ИНДИКАТОРЫ МОНИТОРИНГА

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

> **Важная информация!**
>
> Если производились изменения конфигурационных файлов, то пороговые значения и период проверки могут отличаться от указанных.

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

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

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

Название индикатора	Проверка	Значения	Период опроса	Порядок действий при достижении индикаторами пороговых значений
Конфигурационный файл iwmon-services				
PING	Доступность хоста с помощью команды `ping`	– хост недоступен – хост доступен	5 мин.	Проверьте сетевое оборудование (коммутацию и настройки) Проверьте настройки межсетевого экрана (firewall)
SSH	Доступность хоста по ssh	– ssh недоступен – ssh доступен	10 мин.	Проверьте сетевое оборудование (коммутацию и настройки) Проверьте настройки межсетевого экрана (firewall) Убедитесь, что сервис sshd запущен: `service sshd status`
Swap Usage	Занято SWAP на хосте. Указывает на нехватку оперативной памяти	– свободно < 10% SWAP – свободно от 10 до 20% SWAP – свободно >20% SWAP	5 мин.	В таблице процессов выявите процессы, занимающие больше всего памяти, и примите соответствующие меры.
Current Users	Количество пользователей, зарегистрированных на хосте	– >50 пользователей – от 20 до 50 – < 20 пользователей	30 мин.	С помощью команд `who` и `w` определите, какие пользователи зарегистрированы в системе, и отключите лишних пользователей.

Название индикатора	Проверка	Значения	Период опроса	Порядок действий при достижении индикаторами пороговых значений
Total Processes	Количество процессов, запущенных на хосте	– >400 процессов – от 250 до 400 – < 250 процессов	30 мин.	В таблице процессов, с помощью команд `ps` или `top` выявите, каких процессов больше всего, и примите соответствующие меры.
Root Partition	Наличие свободного места в корневой файловой системе	– свободно < 10% – свободно < 20% – свободно >= 20%	30 мин.	Проверьте содержимое файловой системы root, по возможности освободите место. В противном случае, подключите дополнительное дисковое пространство
/var Partition	Наличие свободного места в файловой системе `/var`	– свободно < 10% – свободно < 20% – свободно >= 20%	30 мин.	Проверьте содержимое файловой системы /var, по возможности освободите место. В противном случае, подключите дополнительное дисковое пространство

service ntpd state	Состояние системного сервиса ntpd	– сервис не запущен
		– сервис запущен
			30 мин.	Убедитесь, что сервис запущен:
				`service servicename status`
				Запустите сервис:
				`service servicename start`
				и включите его автоматический запуск:
				`chkconfig --list servicename`
				`chkconfig servicename on`
				где `servicename` – имя сервиса.
				В случае сбоя при запуске сервиса, устраните причину сбоя и запустите сервис снова.

service crond state	Состояние системного сервиса CRON	– сервис не запущен – сервис запущен	30 мин.	
local postfix smtp	Состояние системного сервиса Postfix	– сервис не запущен – сервис запущен	30 мин.	
service syslog state	Состояние системного сервиса syslog	– сервис не запущен – сервис запущен	30 мин.	
TM Licence	Валидность даты лицензии на перехватчики	– < 2 дней – <= 2 недель – > 2 недель	1 сутки	Обновите лицензию на подсистему анализа, как описано в документе «Руководство по установке и конфигурированию», раздел 3.3.3 «Установка лицензий на Подсистему Анализа»
TM queue SMTP	Количество объектов в очереди `smtp`	– >= 200 объектов – < 10	30 мин.	Проверьте доступность БД Проверьте, что запущен dbloader Просмотрите записи журнала alert_iwtm.log. messages - есть ли сообщения о том, что БД занята работающим джобом и не может вставить новые объекты (также симптомом является высокая нагрузка на CPU). В этом случае либо ждите, когда джоб отработает, либо (если джоб висит боле суток), выясните и устраните причины его зависания, затем принудительно остановите его работу.
TM queue Errors	Количество объектов в очереди `errors`	– >= 200 объектов – < 10	30 мин.	
TM queue DB	Количество объектов в очереди `db`	– >= 200 объектов – < 10	30 мин.	

Название индикатора	**Проверка**	**Значения**	**Период опроса**	**Порядок действий при достижении индикаторами пороговых значений**
TM coredump files	Наличие файлов coredump в директории TM	– присутствует хотя бы один файл coredump – отсутствуют файлы coredump	4 часа	Выгрузите файлы coredump и отправьте их в службу поддержки InfoWatch для дальнейших консультаций
TM daemons state	Статус сервисов TM	– хотя бы один сервис не запущен – все сервисы запущены	30 мин.	Устраните причину сбоя и запустите сервисы
CAS Licence	Валидность даты лицензии на подсистему анализа	– < 2 дней – <= 2 недель – > 2 недель	1 сутки	Обновите лицензию на подсистему анализа, как описано в документе «Руководство по установке и конфигурированию», раздел 3.3.2 «Установка и замена лицензии на перехватчики»
Syslog Errors	Наличие записей об ошибках в системном журнале По умолчанию индикатор отключен (параметр в конфигурационном файле закомментирован)	– присутствует хотя бы одна запись –записи об ошибках отсутствуют	10 мин.	Просмотрите ошибки в системном журнале, определите и устраните их причины.
Конфигурационный файл iwmon-services-db				
Oracle Database Status	Доступность требуемой БД. По умолчанию БД=`iwtm`	– БД доступна – БД недоступна	10 мин.	Если серверная часть Traffic Monitor и БД установлены на разных компьютерах, то на сервере TM проверьте сетевое оборудование (коммутацию и настройки), а также настройки межсетевого экрана (firewall). Если БД установлена на том же компьютере, что и серверная часть Traffic Monitor, то запустите сервис oracle: `service oracle start`
Oracle TNS Status	Работа TNS listener	– TNS listener не запущен – TNS listener запущен	10 мин.	Убедитесь, что листенер стартован Убедитесь, что оракловый сервис зарегистрирован на листенере Убедитесь, что нет сетевых проблем между сервером мониторинга и сервером БД.
DB Alert Log Errors	Наличие записей об ошибках в журнале `alert_iwtm.log` базы данных	– присутствует хотя бы одна запись –записи об ошибках отсутствуют	5 мин.	Просмотрите ошибки в журнале `alert_iwtm.log`, определите и устраните их причины.

Название индикатора	Проверка	Значения	Период опроса	Порядок действий при достижении индикаторами пороговых значений
DB Alert Log Size	Размер лог-файла Oracle (`alert_iwtm.log`)	– > 100 Mb – >= 50 Mb – < 50 Mb	5 мин.	Если файл растёт слишком быстро, выясните и устраните причины его роста. Сделайте копию лог-файла и заархивируйте её. Обнулите файл: `> alert_iwtm.log`
DB v_sys_log Errors	Наличие записей об ошибках в представлении `v_sys_log` базы данных	– присутствует хотя бы одна запись –записи об ошибках отсутствуют	30 мин.	Выполнить следующий SQL запрос: `select CONTENT, DATE_INSERT from v_sys_log where SEVERITY=('WARNING','ERROR');` Результаты запроса передайте в службу поддержки InfoWatch для дальнейших консультаций
/u01 partition	Наличие свободного места в файловой системе `/u01`	– свободно менее 10% – свободно более 20%	10 мин.	Проверьте значение интервала удаления ежедневных ТП (параметр `drop_interval` для настройки `drop_part_date_lag`) – см. п. 4.3.5 на стр. 38. При необходимости, уменьшите это значение. Проверьте содержимое файловой системы, по возможности освободите место. В противном случае, подключите дополнительное дисковое пространство
/u02 partition	Наличие свободного места в файловой системе `/u02`	– свободно менее 10% – свободно более 20%	10 мин.	
Конфигурационный файл iwmon-services-ntp				

NTP time	Расхождение времени на сервере с эталоном	– расхождение > 1 с.
		– расхождение от 0,5 с. до 1 с.
		– время синхронизировано
			30 мин.	Выполните синхронизацию:
				`service ntpd stop`
				`ntpdate <ip ntp сервера>`
				`hwclock --systohc`
				В файле /etc/ntp.conf для параметра server в качестве значения укажите IP-адрес ntp сервера.
				Запустите ntpd:
				`service ntpd start`

Название индикатора	Проверка	Значения	Период опроса	Порядок действий при достижении индикаторами пороговых значений
Конфигурационный файл iwmon-services-loadavg				
Current Load	Нагрузка на соответствующую группу хостов. Количество процессов, ожидающих scheduling, в расчете на 4 физических ядра CPU При расчёте порога срабатывания для другого количества ядер, рассчитывайте значения пропорционально указанным.	– > 20.0,16.0,12.0 – от 10.0,8.0,6.0 до 20.0,16.0,12.0 – < 10.0,8.0,6.0	30 мин.	Уточните пороговые значения с учетом количества ядер на хосте.
Конфигурационный файл iwmon-services-traffic				
Check Traffic	Наличие в БД объектов с SOURCE_IP из подсетей, указанных в параметре `check_command`. По умолчанию индикатор отключен (параметр в конфигурационном файле закомментирован)	– объекты из указанных подсетей отсутствуют – присутствует хотя бы один объект из указанных подсетей	1 час	Проверьте наличие этих сетей в копии трафика: 1. Отправьте тестовые сообщения из этих подсетей 2. Проверьте отправку, например, с помощью команды `tcp dump`. 3. Убедитесь, что индикатор свидетельствует о появлении объекта в БД. Если проверка прошла успешно, для исключения избыточных уведомлений увеличьте период опроса для индикатора
Конфигурационный файл iwmon-services-dm				
Device Monitor Status	Состояние сервиса InfoWatch Device Monitor. По умолчанию индикатор отключен (параметр в конфигурационном файле закомментирован)	– сервис не работает – сервис работает	10 мин.	Непосредственно на сервере InfoWatch Device Monitor проверьте работу сервиса.

ПРИЛОЖЕНИЕ C. РАЗРЕШЕНИЕ ПРОБЛЕМ

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

В сценарии автостарта `iw-trafmon` неверно задана переменная окружения `ORACLE_HOME`.

Решение

Откройте сценарий автостарта 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 Traffic Monitor Server.

Решение

Включите пользователя – владельца InfoWatch Traffic Monitor (от имени которого запускаются процессы Traffic Monitor Server) – в группу `oinstall` (группа владельца инсталляции клиента СУБД Oracle). Группа владельца InfoWatch Traffic Monitor указана в файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[GENERAL]` (см. п. 5.2.1 на стр. 52).

Значительно снижается производительность Системы или обработка трафика полностью прекращается

Возможны следующие причины:

Причина возникновения проблемы	Решение
При работе сценария logwatch операционной системы повышается нагрузка на процессы Системы. В результате значительно снижается скорость обработки трафика.	Возможны два варианта решения проблемы: • Установите для всех процессов Traffic Monitor Server уровень логирования (параметр `LogLevel` в файле `tm.conf`) равным 0. • Отключите запуск сценария logwatch в crond (по умолчанию сценарий запускается ежедневно в 4 часа)
На Traffic Monitor Server установлен высокий уровень протоколирования для одного или нескольких процессов	Рекомендуется для всех процессов оставлять уровень протоколирования по умолчанию (см. п. 5.2 на стр. 51). Чтобы проверить уровень протоколирования, посмотрите значение параметра LogLevel в файлах: • `usr/local/infowatch/tm3/etc/tm.conf` (секции SMTPD, MESSED, DELEVERD, SNIFFER, PROXY, CAS, DBLOADER, EXPRESSD, UPDATER); • `usr/local/infowatch/tm3/etc/qmover.conf` (секции `[QMOVER_server]`, `[QMOVER_client]`) • `usr/local/infowatch/tm3/etc/icap.conf` (секция ICAP) Если для одного или нескольких процессов уровень протоколирования был повышен, уменьшите его, рекомендуется вернуть значение по умолчанию

При загрузке объекта в базу данных неожиданно прервана работа базы данных

Если работа базы данных прерывается во время загрузки объекта в базу, то такой объект помещается в очередь `/usr/local/infowatch/tm3/queue/errors`. Впоследствии такой объект не будет автоматически загружен в базу данных.

Решение

При помощи утилиты iw_qtool скопируйте объект из очереди `/usr/local/infowatch/tm3/queue/errors` в очередь `/usr/local/infowatch/tm3/queue/db`.

Например:

```
iw_qtool move /usr/local/infowatch/tm3/queue/errors /usr/local/infowatch/tm3/queue/db
```

> **Примечание:**
>
> Утилиту `iw_qtool` нужно запускать от имени владельца InfoWatch Traffic Monitor. Имя владельца задано в файле `/usr/local/infowatch/tm3/etc/tm.conf`, секция `[GENERAL]`, параметр `user`.

ГЛОССАРИЙ

Active Directory

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

BCC

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

Crawler

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

DeviceLock

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

DeviceLock Adapter

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

Device Monitor

Модуль подсистемы перехвата трафика. ПО, предназначенное для контроля доступа пользователей к периферийным устройствам и мониторинга операций по копированию данных на съемные носители и отправкой данных на печать

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

LUN

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

Management Console

См. Консоль управления

OCR

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

OSCAR

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

Postfix

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

Relay-сервер

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

Sniffer

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

SPAN

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

SPAN-копия

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

Traffic Monitor Enterprise

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

Traffic Monitor Standard

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

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

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

init.ora 42

P

Postfix 47, 48

S

SMTP-конверт 47

SMTP-письмо 47

очередь входящих писем 57

T

trace –файл 42

Traffic Monitor Server

параметры загрузки конфигурации 70

сервер контентного анализа 64

X

XML-контекст 47

К

Контентный анализ 48

Конфигурация

параметры загрузки на Traffic Monitor Server 70

Л

Лицензионный ключ

iw_customer.dat 22

iw_license.dat 22

О

Обработка архивов и вложений

настройка tm.conf 70, 73

П

Пользователь

владелец InfoWatch Traffic Monitor 53

Процессы Traffic Monitor Server

iw_cas2d 48

iw_dbloader 67

iw_deliverd 48, 57

iw_expressd 48, 68

iw_icap 49

iw_messed 48, 56

iw_proxy 60

iw_proxy (HTTP) 48, 62

iw_proxy (ICQ) 48, 61

iw_proxy (PRINTER) 48

iw_proxy (SMTP) 48

iw_qmover_client 49

iw_qmover_server 49

iw_smtpd 47, 55

проверка запуска 50

управление работой процессов 50

Р

Резервное копирование БД 40

восстановление 45

копирование 44

размер бэкапа 41

создание 41

С

Сервер контентного анализа

настройка параметров 68

СУБД Oracle

параметры соединения 68

Сценарий автозапуска

iw-caserv 50

iw-trafmon 50

Ф

Файл

iw-caserv 50

iw-trafmon 50