

INFOWATCH

InfoWatch Traffic Monitor 6.9

Руководство по установке

27/09/2019

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Введение 4
1.1 Аудитория 4
1.2 Комплект документов 4
1.3 Техническая поддержка пользователей 4
2 Подготовка к установке 5
2.1 Схемы развертывания Системы и выбор типа установки 5
2.2 Аппаратные и программные требования 7
3 Установка Системы 15
3.1 Установка сервера Traffic Monitor и Базы данных 16
3.1.1 Общие сведения по этапам установки серверных компонентов 16
3.1.1.1 Стартовое окно 17
3.1.1.2 Выбор базы данных 18
3.1.1.3 Выбор режима установки 18
3.1.1.4 Выбор часового пояса 19
3.1.1.5 Установка пароля суперпользователя Системы 20
3.1.1.6 Выбор способа разбиения дискового пространства 20
3.1.1.7 Настройка сети 24
3.1.1.8 Настройка синхронизации времени (NTP-server) 27
3.1.1.9 Настройка локализации 28
3.1.1.10 Настройка автоматического удаления событий из БД 30
3.1.1.11 Завершение установки 32
3.1.2 Установка TM Enterprise и TM Standard в режиме "Все-в-одном" 33
3.1.3 Распределенная установка TM Enterprise 39
3.1.3.1 Установка Базы данных 40
3.1.3.2 Установка Сервера Traffic Monitor 44
3.2 Установка подсистемы Краулер 46
3.3 Установка InfoWatch Device Monitor 52
3.3.1 Установка серверной части InfoWatch Device Monitor 53
3.3.1.1 Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server 53
3.3.1.2 Рекомендации по развертыванию базы данных под управлением СУБД Oracle 54
3.3.1.3 Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL 55
3.3.1.4 Рекомендации по установке Сервера InfoWatch Device Monitor 55
3.3.1.5 Порядок установки серверной части InfoWatch Device Monitor 56
3.3.2 Установка Агента InfoWatch Device Monitor 68
3.3.2.1 Локальная установка Агента 69

3.3.2.2 Установка Агента с помощью средств распространения программного обеспечения 70
3.3.3 Схема развертывания InfoWatch Device Monitor 73
3.4 Предустановленные серверные параметры 76
4 Обновление Системы 79
4.1 Обновление ТМ Все-в-одном (All-in-one) Enterprise и Standard 83
4.2 Обновление ТМ при распределенной установке 96
4.3 Обновление подсистемы Краулер 119
4.4 Обновление InfoWatch Device Monitor 119
4.4.1 Обновление серверной части InfoWatch Device Monitor 120
4.4.2 Обновление Агента InfoWatch Device Monitor 122
4.5 Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew 123
4.5.1 Объединение конфигурационных файлов в Midnight Commander 123
4.5.2 Объединение конфигурационных файлов с помощью vimdiff 125
5 Удаление Системы 126
5.1 Удаление схемы базы данных 126
5.2 Удаление подсистемы Краулер 128
5.3 Удаление InfoWatch Device Monitor 128
5.3.1 Удаление Агента, установленного с помощью средств распространения программного обеспечения 129
6 Приложение А. Рекомендации по составлению имен и паролей . 131
7 Приложение В. Лицензии на стороннее программное обеспечение . 133

1 Введение

В настоящем руководстве вы можете найти сведения по установке, обновлению и удалению системы InfoWatch Traffic Monitor (IW TM).

1.1 Аудитория

Документ предназначен для специалистов службы технической поддержки компании InfoWatch, а также для инженеров компаний-партнеров компании InfoWatch.

1.2 Комплект документов

В комплект документации по InfoWatch Traffic Monitor входят:

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

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

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

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

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

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

- «*InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*».

Содержит пояснения к часто используемым конфигурационным файлам.

1.3 Техническая поддержка пользователей

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

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

Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ.
Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/support.
Перед обращением в службу технической поддержки рекомендуется посетить раздел База знаний на нашем сайте: https://kb.infowatch.com/. Возможно, там уже содержится ответ на интересующий вас вопрос или описано решение возникшей у вас проблемы.

2 Подготовка к установке

В этой главе вы можете найти информацию о:

- схемах развертывания системы и возможных типах установки;
- программных и аппаратных требованиях.

2.1 Схемы развертывания Системы и выбор типа установки

Система InfoWatch Traffic Monitor может поставляться в нескольких вариантах. При этом имеет значение режим установки Системы, используемая база данных (Oracle / PostgreSQL) и редакция системы (Standard / Enterprise).

Можно выделить следующие типичные варианты решений:

- **InfoWatch Traffic Monitor Standard** – решение для компаний размером до 300 сотрудников. Имеет ряд ограничений по сравнению с Enterprise-версией (подробнее см. таблицу ниже и https://www.infowatch.ru/products/traffic_monitor/versions). Разворачивается на едином сервере.
- **InfoWatch Traffic Monitor Enterprise** – полное масштабируемое решение с гибким конфигурированием компонентов. В максимально развернутой конфигурации может выглядеть следующим образом:
  - **Сервер Traffic Monitor**. Обеспечивает работу перехватчиков (IW_SNIFFER, IW_ICAP и IW_SMTPD), подсистемы анализа и подсистемы применения политик. В ряде случаев рекомендуется использовать несколько серверов Traffic Monitor: это позволяет обеспечивать более эффективную работу нагруженных процессов. При этом необходимо учитывать, что некоторые процессы должны быть запущены только на одном сервере (подробнее см. статью "Проверка автозапуска процессов" в Руководстве администратора).
  - **База данных**. Сервер СУБД Oracle или PostgreSQL.

    > **Примечание:**
    >
    > На сервере Traffic Monitor и Базе данных не рекомендуется устанавливать и запускать приложения (особенно серверные) или использовать компьютер в качестве файл-сервера.

  - **Device Monitor**. Модуль перехвата, реализованный в виде серверной части с управлением через Консоль и Агентов, распространяемых на компьютеры и мобильные устройства компании.
  - **Краулер**. Модуль перехвата, реализованный в виде служб сервера и сканера.
  - **Коннекторы**. Набор модулей перехвата для интеграции со сторонними системами.
  - **Консоль управления**. Веб-интерфейс управления Системой. Реализован в виде набора процессов, которые должны быть запущены только на одном сервере Traffic Monitor (подробнее см. статью " Проверка автозапуска процессов " в Руководстве администратора).

В следующей таблице описывается функциональная разница между редакциями системы, с учетом используемой базы данных.

Функция	TM Enterprise		TM Standard
	TM Enterprise Oracle	TM Enterprise PostgreSQL	TM Standard PostgreSQL
Срок хранения перехваченных данных	Ограничивается только размером хранилища		Ограничивается только размером хранилища
Контроль рабочих станций	Контроль использования съемных устройств и коммуникационных портов; контроль печати		Опционально (Возможность подключения модуля контроля рабочих станций InfoWatch Device Monitor зависит от объема данных и требуемых сроков хранения)
Масштабируемость	Решение может быть адаптировано для обслуживания большого количества сотрудников (десятки тысяч) при росте компании. Может использоваться в территориально распределенных филиалах, соединенных любыми каналами связи		Рассчитано на компании с числом сотрудников до 300 человек
Блокирование передачи трафика при выявлении нарушения	Да		Опционально (внедрение проводится силами сертифицированных инженеров)
Схема интеграции	Несколько вариантов на выбор: интеграция «в разрыв», поддержка ICAP, перехват в режиме копии трафика (SPAN, port mirroring и др.)		Работа в режиме копии трафика (интеграция «в разрыв» - опционально)

Существуют следующие типы установки:

- *Все-в-одном Standard* – все компоненты Системы (с СУБД PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor.
- *Все-в-одном Enterprise* – все компоненты Системы (с СУБД Oracle Enterprise или PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor.
- *Сервер Traffic Monitor* + *База данных* – сервер Traffic Monitor и СУБД Oracle Enterprise или PostgreSQL устанавливаются на разные машины. Такая установка используется, если с учетом предполагаемой нагрузки сервисы Traffic Monitor и СУБД не смогут производительно работать на одной машине.

Важно

После установки администратор настраивает Систему в зависимости от целей внедрения (см. документ "Infowatch Traffic Monitor. Руководство администратора", статья "Настройка Системы после установки").

2.2 Аппаратные и программные требования

Требования к аппаратной конфигурации сервера для InfoWatch Traffic Monitor определяются на основании типа установки, предполагаемой нагрузки на Систему и параметров сети, в которой происходит развертывание Системы. Поэтому спецификация оборудования для каждого случая рассчитывается отдельно.

Варианты схем развертывания Системы описаны в статье "Схемы развертывания Системы и выбор типа установки". Согласно статье, может выполняться установка следующих элементов:

- **Сервер для установки "Все-в-одном"** – используется для редакции TM Enterprise – установка Enterprise-решения в режиме "Все-в-одном". *См. требования для отдельностоящего сервера TM Enterprise.*
- **Сервер Traffic Monitor** – отдельностоящий сервер или кластер серверов TM Enterprise. *Требования см. ниже.*
- **Сервер базы данных** – сервер СУБД Oracle или PostgreSQL. На этом компьютере не рекомендуется устанавливать и запускать приложения (особенно серверные) или использовать его в качестве файл-сервера. *Требования см. ниже.*
- **Сервер Краулер и сканер Краулер** – службы, работающие на Windows-системах. *Требования см. ниже.*
- **Коннекторы** – требования к этим компонентам описаны в документации, поставляемой вместе с программным обеспечением коннекторов.
- **Сервер Device Monitor с Агентами Device Monitor** – модуль, базирующийся на Windows-системах и имеющий агенты на Windows- и Linux-системах, а также на мобильных устройствах. *Требования см. ниже*.
- **Консоль управления** – автоматически устанавливается вместе с сервером Traffic Monitor и не предъявляет дополнительных программно-аппаратных требований к серверу. Для доступа к Консоли следует использовать браузер Google Chrome актуальной версии.

Для сервера Traffic Monitor аппаратно-программные требования варьируются в очень большом диапазоне. Так, минимальная конфигурация подразумевает следующие ограничения:

- для всех перехватчиков отключено использование OCR;
- сервер не принимает данные от Device Monitor и Краулера.

Также на количество и назначение серверов Traffic Monitor может влиять существенная разница в нагрузке на те или иные каналы перехвата: например, для эффективной обработки трафика и с Device Monitor, и с Краулера, может потребоваться использовать отдельный сервер для процесса **iw_xapi_xapi**.

Примерные минимальные программно-аппаратные требования приведены в следующей таблице. Подробный расчет конфигурации настоятельно рекомендуется проводить с участием специалистов InfoWatch или компании-партнера, у которой вы приобретаете продукт.

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Сервер TM Standard				
RAID-массив с fault tolerance: 300 GB	2CPU 6xC, 2,6 GHz	24 GB	Не предъявляются *	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков**
Сервер TM Enterprise, менее 10 GB трафика в день				
RAID-массив с fault tolerance: 600 GB	2CPU 8xC + Hyper-threading (Intel® Xeon® Processor E5-2640 v3 - частота 2,6 Hz)	24 GB	Не предъявляются *	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков**
Сервер TM Enterprise, от 10 до 50 GB трафика в день				
RAID-массив с fault tolerance	2SRVx2CPU 10xC	32-48 GB на каждый из серверов	Не предъявляются *	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков**
Сервер TM Enterprise, более 50 GB трафика в день				
RAID-массив с fault tolerance	Рассчитывается по запросу	От 32GB на каждый из серверов	Не предъявляются *	
Сервер БД Oracle или PostgreSQL (Обеспечивает хранение трафика для 1-2 тыс. пользователей, сроком до 3 месяцев; в случае использования OCR и Device Monitor требования рассчитываются по запросу)				

RAID-массив с fault tolerance: 500 GB	2CPU от 6xC, 2,6 GHz	От 16GB и более в зависимости от объема данных, интенсивности вставки и обработки	• PostgreSQL 9.4.12; • Oracle Database 11.2.0.1.0.	
Сервер Crawler и сканер Crawler				
30 GB свободного пространства - для сервера и для сканера: необходимо для временного хранения файлов, скопированных с проверяемых ресурсов и для установки	От 2-х ядер	От 2 GB	ОС: • Microsoft Windows Vista 7 Service Pack 1/2; • Microsoft Windows Vista 8 Service Pack 2; • Microsoft Windows Server 2008 R2 Service Pack 1; • Microsoft Windows Server 2012 R2 Service Pack P2. Платформа: • Microsoft .Net Framework 4.5.1.	• На сервере TM должен быть включен автозапуск процесса **iw_xapi_xapi** • И сервер, и сканер Crawler должны быть установлены на компьютеры, находящиеся в одном домене: в том, к которому принадлежат компьютеры, которые предполагается сканировать. • Рекомендуется выбирать расположение компьютера, на котором будет работать сканер Crawler, так, чтобы он находился в сегменте сети, максимально близком к тем сегментам, которые будут подлежать сканированию. Удаленность может существенно увеличить нагрузку на сеть. • Если сегменты сети, где развернута система InfoWatch Traffic Monitor с Crawler, разделены между собой межсетевыми экранами, для корректной работы Crawler должны быть открыты порты 1337 (подключение Traffic Monitor к серверу Crawler) и 6556 (подключение сканера Crawler к серверу Crawler).
Сервер Device Monitor				

Не менее 3 GB свободного пространства для установки. Также понадобится свободное пространство для анализа данных, объем зависит от нагрузки на сервер.	От 2-х ядер	От 2 GB	ОС (поддерживаются платформы x86 и x64): • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2. Платформа: • Microsoft .Net Framework 4.5.1 Клиент СУБД: • Oracle Database 11; В случае установки Device Monitor на серверную ОС разрядностью x64, необходимо использовать приложение Oracle Client разрядностью также x64;	• На сервере TM должен быть включен автозапуск процесса **iw_xapi_xapi** • Наличие локального DNS для перевода доменных имен в адреса • Режим FIPS должен быть отключен

			• Microsoft SQL Server 2005, 2008, 2012, 2014 (Express, Developer, Workgroup, Standard, Enterprise) • PostgreSQL версии 9.	
Агент Device Monitor для рабочих станций				
Не менее 1 GB свободного пространства для установки. Также понадобится свободное пространство для временного хранения файлов, предназначенных для передачи на анализ.	От 2-х ядер	От 2.5 GB	ОС: • Microsoft Windows XP Professional Service Pack 3 со всеми обновлениями; • Microsoft Windows Vista Service Pack 2; • Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 и 8.1; • Microsoft Windows 10; • Microsoft Windows Server 2003; • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2;	Наличие локального DNS для перевода доменных имен в адреса

Агент Device Monitor для мобильных устройств				

Не предъявляются: агент устанавливается на мобильное устройство определенной конфигурации, список поддерживаемых устройств приведен.	Не предъявляются: агент устанавливается на мобильное устройство определенной конфигурации, список поддерживаемых устройств приведен.	Не предъявляются: агент устанавливается на мобильное устройство определенной конфигурации, список поддерживаемых устройств приведен.	Не предъявляются: агент устанавливается на мобильное устройство определенной конфигурации, список поддерживаемых устройств приведен.	Поддерживаются следующие конфигурации устройств:
				• InfoWatch Taigaphone (доверенная прошивка)
				• на платформе Android:
				  • ASUS Nexus 7 2013 LTE (K009), версия Android 4.4.4 (версия прошивки KTU84P)
				  • ASUS Nexus 7 2013 LTE (K009), версия Android 5.1.1 (версия прошивки LMY47V)
				  • ASUS ZenFone 2 (ASUS_Z00ED), версия Android 5.0.2 (версия прошивки 12.8.5.222)
				  • Samsung Galaxy A3 (SM-A310F), версия Android 5.1.1 (версия прошивки LMY47X.A310FXXU1AOL7)
				  • Samsung Galaxy A5 (SM-A510F), версия Android 5.1.1 (версия прошивки LMY47X.A510FXXU0AOK8)
				  • Samsung Galaxy J1 (SM-J120F), версия Android 5.1.1 (версия прошивки LMY47X.J120FXXU1AOL2)
				  • Samsung Galaxy S4 (I9500), версия Android 4.4.2 (версия прошивки I9500XXUGNF6)
				  • Samsung Galaxy S4 (I9505), версия Android 4.4.2 (версии прошивки KOT49H.I9505XXUGNG8, KOT49H.I9505XXUFNC9)
				  • Samsung Galaxy S5 (SM-G900F), версия Android 4.4.2 (версии прошивки KOT49H.G900FXXU1ANE2, KOT49H.G900FXXU1ANK7)

				• Samsung Galaxy Tab A6 (SM-T585), версия Android 6.0.1 (версии прошивки MMB29K.T585XXU2AQA2) - Для перехвата трафика Skype на данной прошивке необходимо обновить его мобильное приложение.
Консоль управления Device Monitor				
Не менее 35 MB	Как у используемой ОС	Как у используемой ОС	ОС: • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Vista Service Pack 2; • Microsoft Windows 7 Service Pack 1 • Microsoft Windows 8 и 8.1; • Microsoft Windows 10.	

Примечание:

Допустима установка Системы в виртуальную среду: VMware, MS Hyper-V или других систем виртуализации.

Работа агентов Device Monitor поддержана в среде виртуализации Citrix 7.13 и 7.14.

* Требования к ПО для серверов не предъявляются: программа-инсталлятор (kickstart) форматирует жесткий диск и устанавливает необходимое ПО.

** На сервере Traffic Monitor могут использоваться перехватчики, которые предъявляют дополнительные требования:

- **iw_sniffer** может получать копию трафика от управляемого коммутатора с поддержкой функции SPAN/Port Mirroring (рекомендованная модель - Cisco Catalyst 2960 Series) с портом, настроенным на режим TRx (BOTH - получение и передача в одном подключении);
- **iw_icap** работает с ICAP-клиентом, встроенным в любой прокси-сервер, соответствующий стандарту RFC 3507 (например, SQUID версии не ниже 3.4.x, Cisco IronPort S10 и Blue Coat SG Series). Перед тем, как использовать конкретную модель устройства рекомендуется уточнить совместимость с модулем IW ICAP в службе технической поддержки компании InfoWatch. На прокси-сервере должна присутствовать лицензия на ICAP; включение поддержки ICAP выполняется согласно сопроводительной документации к выбранному прокси-серверу.

3 Установка Системы

Примечание:

После установки Системы будет автоматически загружена пробная лицензия на технологии Traffic Monitor (более подробную информацию о лицензировании см. в документе «InfoWatch Traffic Monitor. Руководство администратора»).

В данном разделе приведены инструкции для каждого из типов установки Системы.

О выборе типа установки см. "Схемы развертывания Системы и выбор типа установки".

Реализация схем развертывания в имеющейся инфраструктуре описана в документе «InfoWatch Traffic Monitor. Руководство администратора».

Важно!

До начала установки убедитесь, что среда, в которой будет развернута Система, удовлетворяет аппаратным и программным требованиям (см. "Аппаратные и программные требования").

Установка серверных компонентов системы InfoWatch Traffic Monitor выполняется с помощью программы-инсталлятора.

В зависимости от целевого назначения сервера, будет различаться набор устанавливаемых компонентов:

Назначение сервера	Ключ	Компоненты, устанавливаемые инсталлятором
Все компоненты InfoWatch Traffic Monitor (Enterprise или Standard) устанавливаются на один компьютер	**TME All-in-one**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка и настройка СУБД Oracle (только для **TME All-in-one**) или PostgreSQL • Установка схемы базы данных IW Traffic Monitor • Установка RPM пакетов сервера IWTM • Установка подсистемы мониторинга • Установка консоли управления
Установка сервера СУБД со схемой БД Traffic Monitor на отдельный компьютер	**TME DB server**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка и настройка СУБД Oracle Enterprise или PostgreSQL • Установка схемы базы данных IW Traffic Monitor

Установка сервера Traffic Monitor на отдельный компьютер	**TME Node server**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка RPM пакетов сервера IWTM • Установка подсистемы мониторинга • Установка консоли управления

Вы можете найти информацию по интересующему Вас типу установки в статьях:

Вы можете найти информацию по интересующему Вас типу установки в статьях:

- Установка сервера Traffic Monitor и Базы данных
- Общие сведения по этапам установки серверных компонентов
- Установка TM Enterprise и TM Standard в режиме "Все-в-одном"
- Распределенная установка TM Enterprise
  - Установка Базы данных
  - Установка Сервера Traffic Monitor
- Установка подсистемы Crawler (опционально)
- Установка InfoWatch Device Monitor (опционально)

Сведения о предустановленных учетных записях приведены в статье "Предустановленные серверные параметры".

После окончания установки серверных компонентов работа в консоли управления доступна через окно браузера, при этом требуется ввести URL-адрес:

- сервера Traffic Monitor – если выполнена установка «Все-в-одном»;
- основного сервера Traffic Monitor (сервера, где установлен пакет `web-gui`) – если компоненты Системы установлены на разные компьютеры.

О выделении основного сервера при распределенной установке см. документ «*InfoWatch Traffic Monitor. Руководство администратора*», статья "*Дополнительные настройки при установке с ключами TME DB Server и TME Node Server*".

3.1 Установка сервера Traffic Monitor и Базы данных

Сведения по установке системы Traffic Monitor на операционную систему Red Hat Enterprise Linux приведены в следующих разделах:

- Общие сведения по этапам установки серверных компонентов
- Установка TM Enterprise и TM Standard в режиме "Все-в-одном"
- Распределенная установка TM Enterprise

3.1.1 Общие сведения по этапам установки серверных компонентов

В этом разделе содержится подробное описание шагов инсталлятора kickstart, являющихся общими для всех типов установки серверных компонентов Системы:

- Стартовое окно
- Выбор базы данных
- Выбор режима установки
- Выбор часового пояса
- Установка пароля суперпользователя Системы
- Выбор способа разбиения дискового пространства
- Настройка сети

- Настройка синхронизации времени (NTP-server)
- Настройка локализации
- Настройка автоматического удаления событий из БД
- Завершение установки

Стартовое окно



Первый экран мастера установки (**kickstart**) позволяет выбрать одно из следующих действий:

- **TM Enterprise** – начнется установка InfoWatch Traffic Monitor Enterprise.
- **TM Standard** – начнется установка InfoWatch Traffic Monitor Standard.

> **Важно!**
>
> Для редакции **TM Standard** доступна установка только в режиме **TMS All-in-one: TM+DB server - PostgreSQL**. Шаги "Выбор базы данных" и "Выбор режима установки" в этом случае будут пропущены.
> О выборе редакции установки см. "Схемы развертывания Системы и выбор типа установки".

- **Boot from local drive** – выполняется загрузка с локального диска компьютера.
- **Rescue installed system** – выполняется аварийное восстановление системы InfoWatch Traffic Monitor. Ввиду сложности данная опция используется только инженерами компании InfoWatch.
- **Memory test** – выполняется тест оборудования компьютера (может занять некоторое время). Используется как вспомогательная функция при необходимости.

> **Примечание**
>
> Для просмотра дополнительных опций загрузки нажмите **F1**. Ввиду сложности дальнейших работ вызов дополнительных опций используются только инженерами компании InfoWatch.

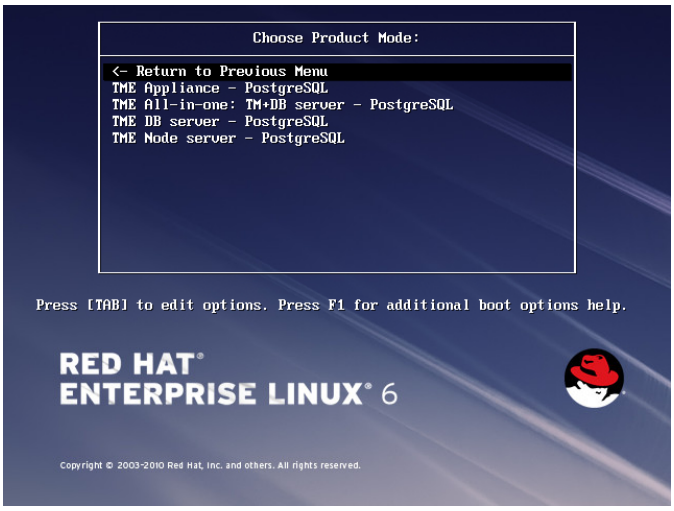
Выбор базы данных



Для редакции **Enterprise** инсталлятор предложит выбрать СУБД, которая должна быть установлена:

- **DB - Oracle Enterprise**;
- **DB - PostgreSQL**.

Выбор режима установки



После выбора СУБД потребуется выбрать режим установки. Набор режимов зависит от выбора, сделанного, на предыдущих шагах установки. Могут быть предложены следующие режимы:

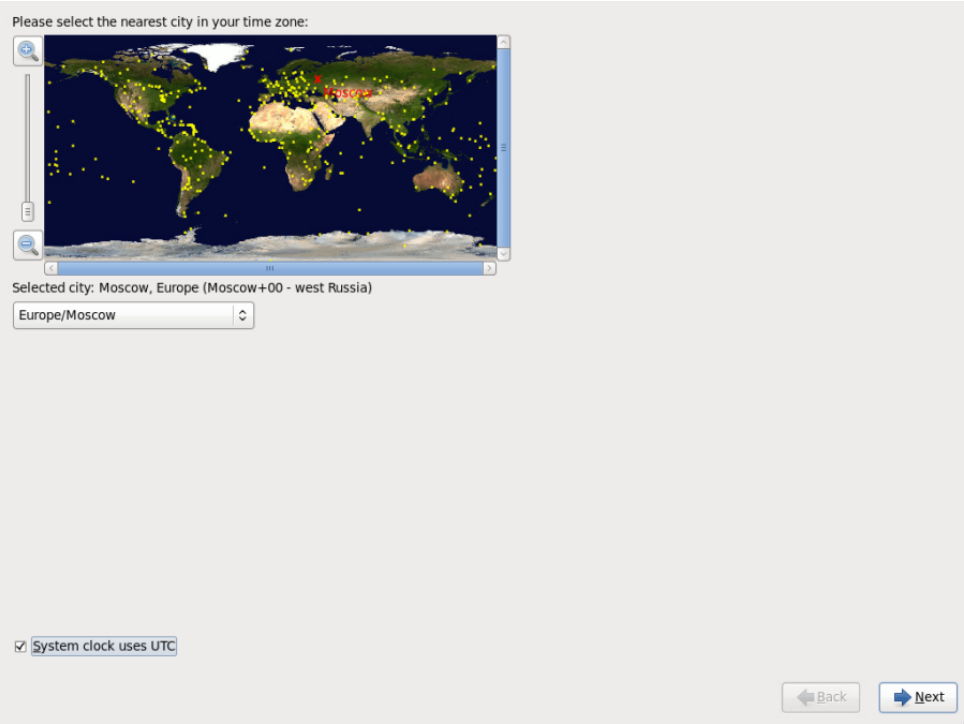
- **TME All-in-one: TM+DB server - PostgreSQL**,
  TME All-in-one: TM+DB server - Oracle,
  TMS All-in-one: TM+DB server - PostgreSQL – все компоненты Системы (с СУБД Oracle или

PostgreSQL) устанавливаются на один сервер. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor. Подробнее см. "Установка TM Enterprise и TM Standard в режиме "Все-в-одном"".

- **TME DB server (PostgreSQL** или **Oracle**) – установка базы данных вместе с выбранной СУБД на отдельный компьютер. Подробнее об этой установке см. "Установка Базы данных".
- **TME Node server (PostgreSQL** или **Oracle**) – установка сервера Traffic Monitor на отдельный компьютер. Подробнее об этой установке см. "Установка Сервера Traffic Monitor".

Подробнее о выборе режима установки см. "Схемы развертывания Системы и выбор типа установки".

Выбор часового пояса



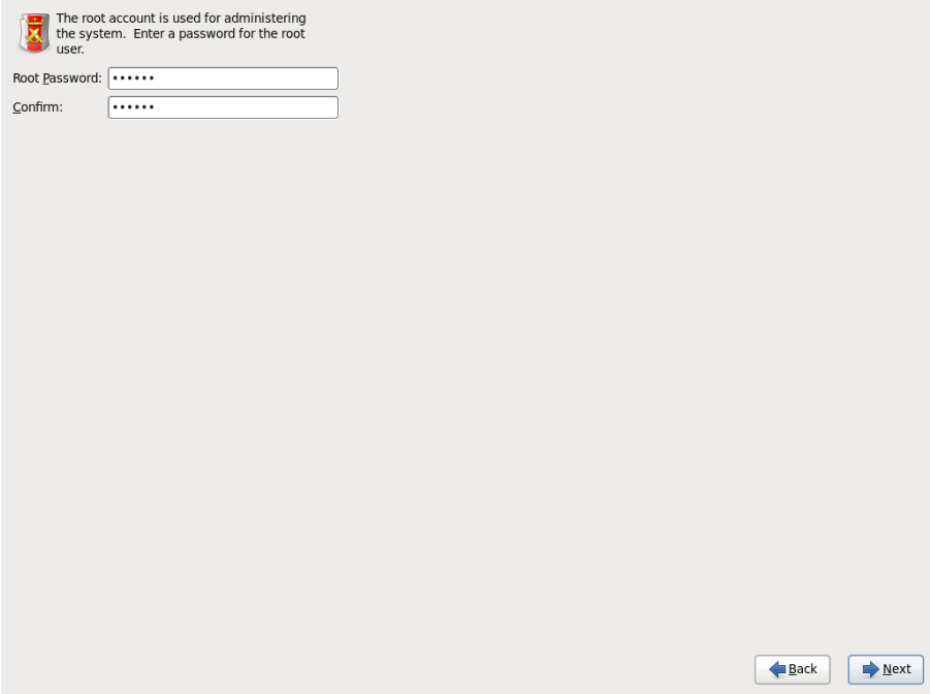
Затем инсталлятор предложит указать часовой пояс сервера.

Нужный город можно выбрать:

- в раскрывающемся списке. Города отсортированы по принадлежности к той или иной части света: например, Москва входит в группу Европа;
- на карте. Для навигации по карте используйте полосы прокрутки и инструменты изменения масштаба).

Поле **System clock uses UTC** показывает, будет ли системное время установлено по Гринвичу (UTC).

Установка пароля суперпользователя Системы



Пользователь *root* – это суперпользователь в Системе. Для пользователя *root* требуется указать пароль.

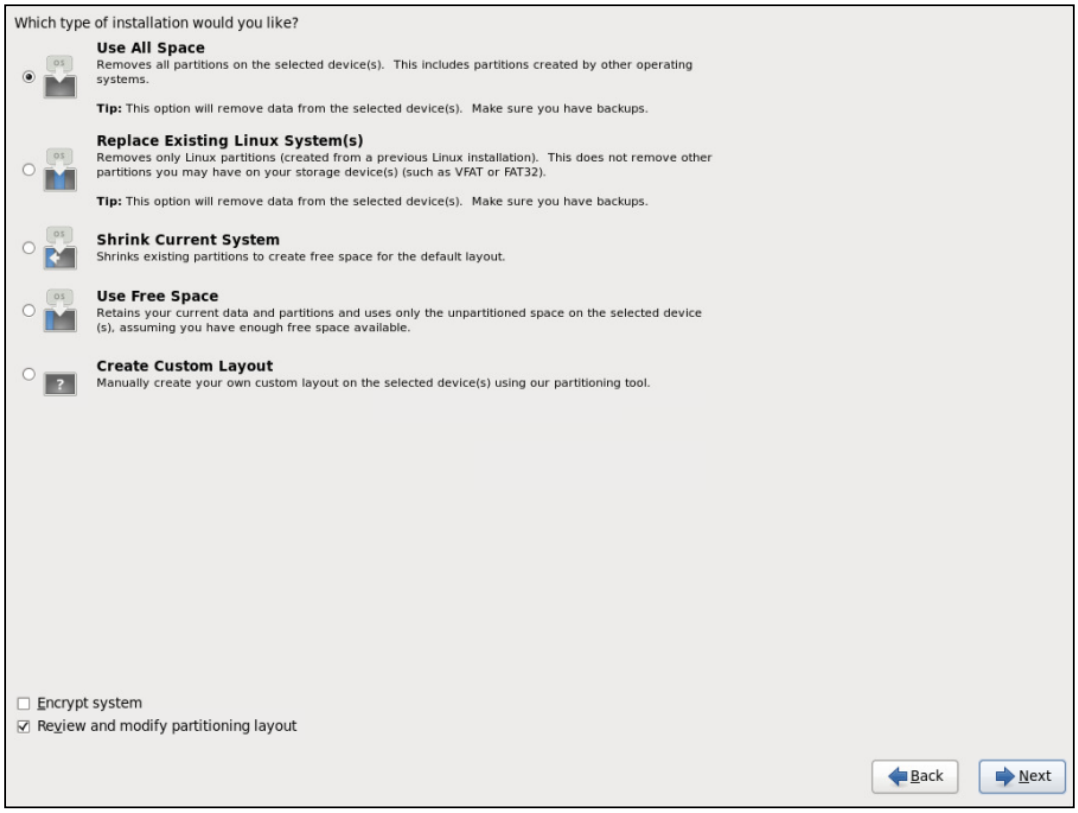
> **Примечание**
>
> Рекомендации по составлению паролей приведены в разделе Приложение А.

Если введенный пароль не соответствует правилам безопасности, на экране отобразится предупреждающее окно **Weak Password**. Используйте кнопки:

- **Use anyway** – если вы хотите использовать введенный пароль без учета рекомендаций;
- **Cancel** – если вы хотите изменить введенный пароль.

Выбор способа разбиения дискового пространства

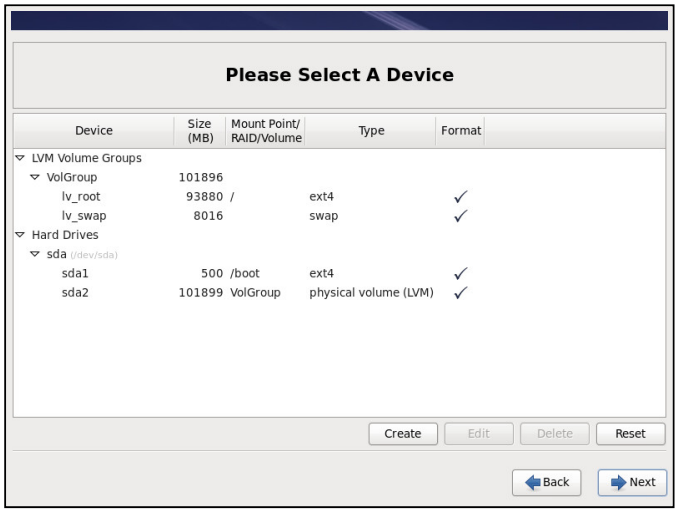
> **Важно**
>
> По завершении установки Системы компоненты будут установлены в следующие директории:
>
> - InfoWatch Traffic Monitor – в каталог `/opt/iw`;
> - БД – в каталоги `/u01` и `/u02`.



Далее необходимо будет указать инсталлятору, как разбить дисковое пространство. Поскольку дисковое место на сервере InfoWatch Traffic Monitor используется только для самой Системы, на данном шаге нужно выбрать **Use All Space**.

> **Важно!**
>
> Удалятся все разделы устройства (устройств), включая разделы, созданные другими операционными системами. *Позаботьтесь о резервном копировании нужных вам данных!*

Чтобы настроить разбивку дисков или просто удостовериться в том, что указанные по умолчанию настройки корректны, нужно установить флажок в поле **Review and modify partitioning layout** и нажать **Next**.

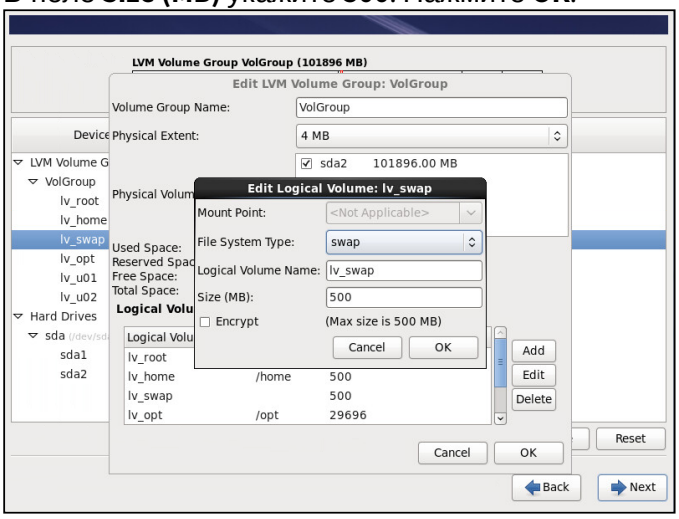


Для большинства случаев достаточно разбиения по умолчанию. Если Система установлена распределенно, и используется СУБД Oracle, рекомендуется отводить для раздела */root* минимум 100 ГБ дискового пространства.

Если необходимо внести изменения, используйте стандартные средства работы с дисками, доступные в инсталляторе.

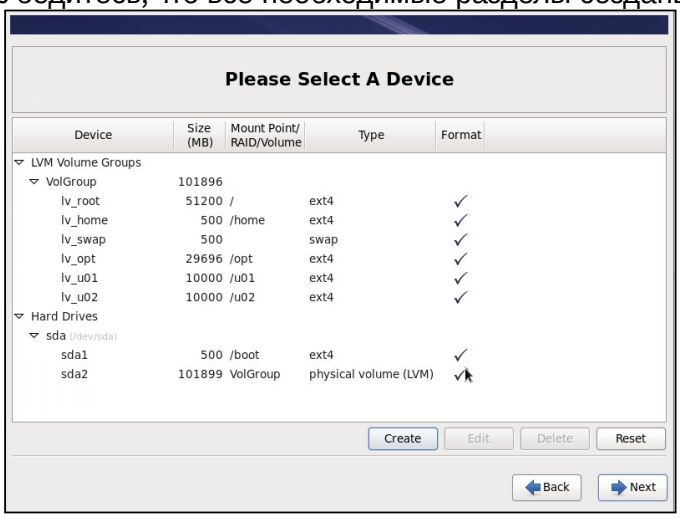
Рекомендуется разбить диск размером не менее 150Gb следующим образом:

1. В окне **Please Select A Device** выберите раздел **lv_root** и нажмите **Edit**.
2. В поле **Size (MB)** укажите **70000**. Нажмите **OK**.
3. В окне **Please Select A Device** выберите раздел **lv_swap** и нажмите **Edit**.
4. В поле **Size (MB)** укажите **500**. Нажмите **OK**.



5. В окне **Please Select A Device** нажмите **Create**.
6. В окне **Create Storage** выберите **LVM Logical Volume** и нажмите **Create.**
7. В поле **Mount Point** укажите: `/home`
8. В поле **Logical Volume Name** укажите: `lv_home`
9. В поле **Size (MB)** укажите **500**. Нажмите **OK.** Убедитесь, что новый раздел **lv_home** создан.
10. В окне **Please Select A Device** нажмите **Create**.
11. В окне **Create Storage** выберите **LVM Logical Volume** и нажмите **Create.**
12. В поле **Mount Point** укажите: `/opt`
13. В поле **Logical Volume Name** укажите: `lv_opt`
14. В поле **Size (MB)** укажите **30000**. Нажмите **OK.** Убедитесь, что новый раздел **lv_opt** создан.
15. Чтобы создать разделы для хранения табличных пространств, в окне **Please Select A Device** нажмите **Create.**
16. В окне **Create Storage** выберите **LVM Logical Volume** и нажмите **Create.**
17. В поле **Mount Point** укажите: `/u01`
18. В поле **Logical Volume Name** укажите: `lv_u01`
19. В поле **Size (MB)** укажите **10000**. Нажмите **OK.** Убедитесь, что новый раздел **lv_u01** создан.
20. Повторите действия 16-19 для создания раздела **u02.**

21. Убедитесь, что все необходимые разделы созданы:

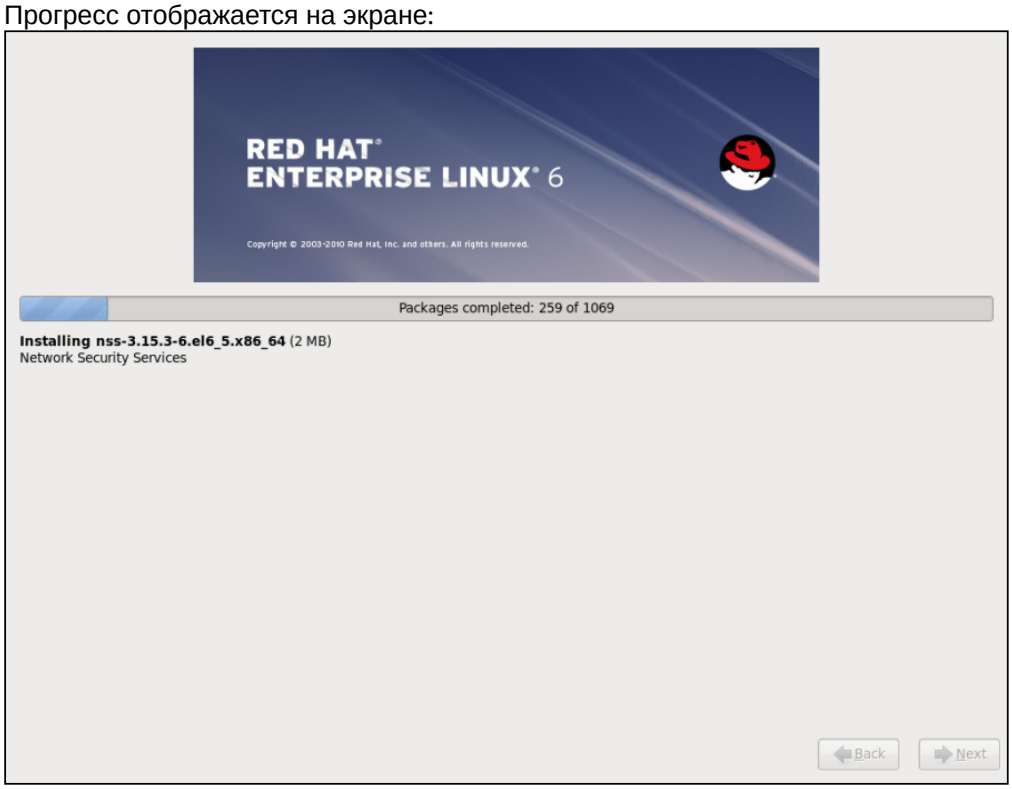


22. Нажмите **Next** в окне **Please Select A Device** .

После завершения разбивки и нажатия кнопки **Next** начнется процесс разбиения диска, а затем – установки операционной системы.

> **Примечание:**
>
> На экран может быть выведено окно **Format Warnings**, свидетельствующее о том, что требуется отформатировать разделы жесткого диска, которые будут использоваться для установки. Для продолжения установки нажмите **Format**.

Прогресс отображается на экране:

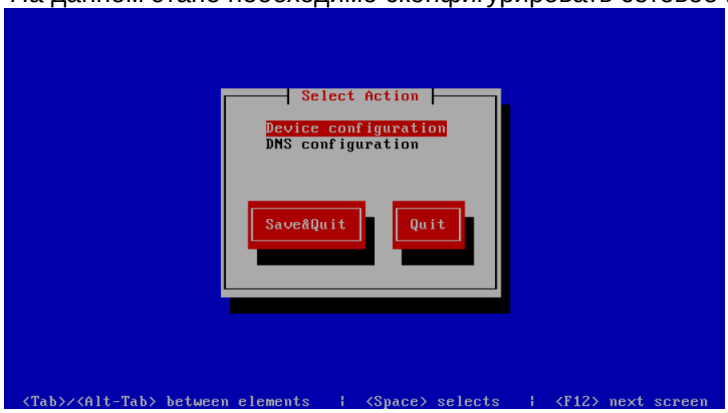


Процесс может занять некоторое время.

По окончании установки операционной системы выполнится перезагрузка, и будет предложено настроить сетевые параметры (см. "Настройка сети").

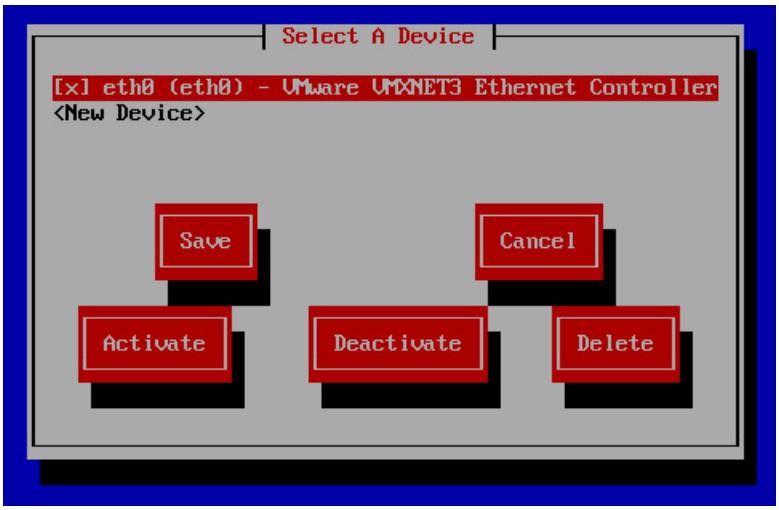
Настройка сети

На данном этапе необходимо сконфигурировать сетевое подключение.



Настройка сети имеет две составляющие:

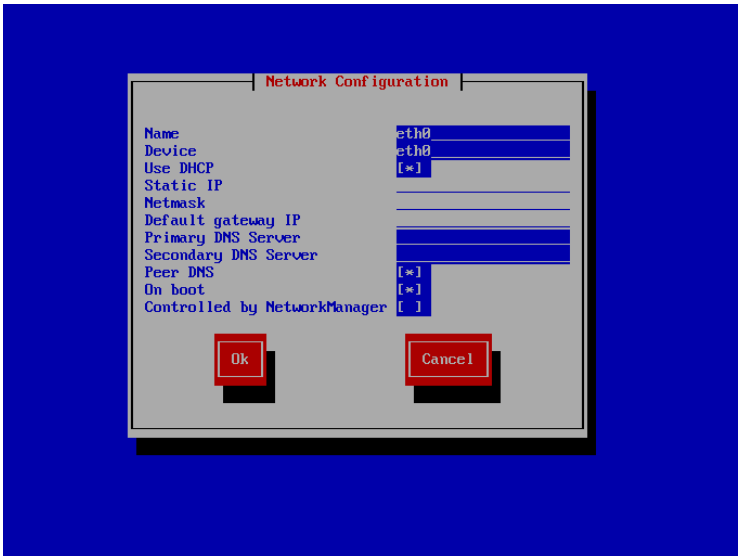
- **Device configuration** - настройка сетевой карты.
  При настройке **Device configuration** будет предложено выбрать сетевой интерфейс из имеющихся (**eth0** и другие) или создать новый (**<New Device>**).



Признак выбора расположен в начале строки с названием интерфейса и выглядит как **[X]**. Обычно используется **eth0**.

Чтобы активировать или деактивировать интерфейс, нужно установить на нем курсор (строка с названием будет выделена красным), затем по нажатию **Tab** перейти на кнопки управления, расположенные в нижней части экрана, и нажать **Activate** или **Deactivate**, соответственно.

Чтобы настроить интерфейс, нужно установить на нем курсор (строка с названием будет выделена красным) и нажать **Enter**.



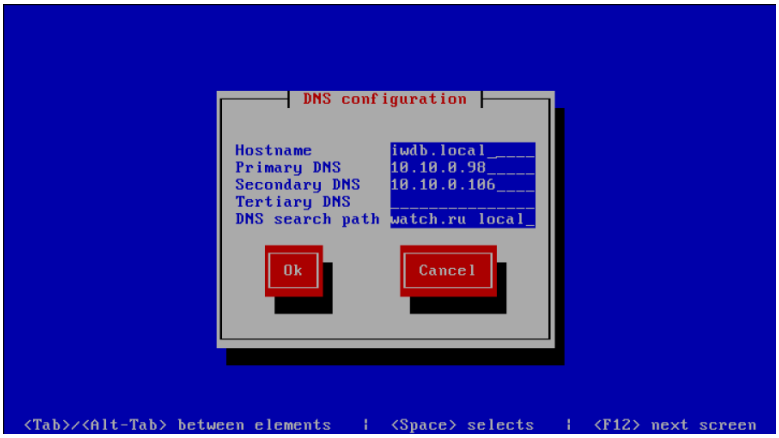
Для включения и выключения опций используйте пробел.

Для использования сетевого интерфейса нужно указать его сетевые настройки (статический IP-адрес машины и прочее). Если Система будет получать данные настройки от DHCP-сервера, нужно включить опцию **Use DHCP** (с помощью клавиши пробел).

> **Важно!**
>
> При использовании настройки **Use DHCP** Система будет использовать только данные, полученные от указанных серверов DHCP. Данные, введенные в окне **DNS configuration** (см. далее) будут игнорироваться. Если вручную изменить файл `/etc/resolv.conf`, то его данные при следующей перезагрузке сервера будут заменены на полученные от сервера DHCP.

> **Важно!**
>
> Опция **Controlled by NetworkManager** должна быть выключена.

- **DNS configuration** - настройка DNS-конфигурации.
  При настройке **DNS configuration** будет предложено указать необходимые параметры сервера.



> **Важно!**
>
> Если в окне **Network Configuration** был отмечен пункт **Use DHCP**, то вместо этих параметров будут использоваться полученные от указанных серверов DHCP.

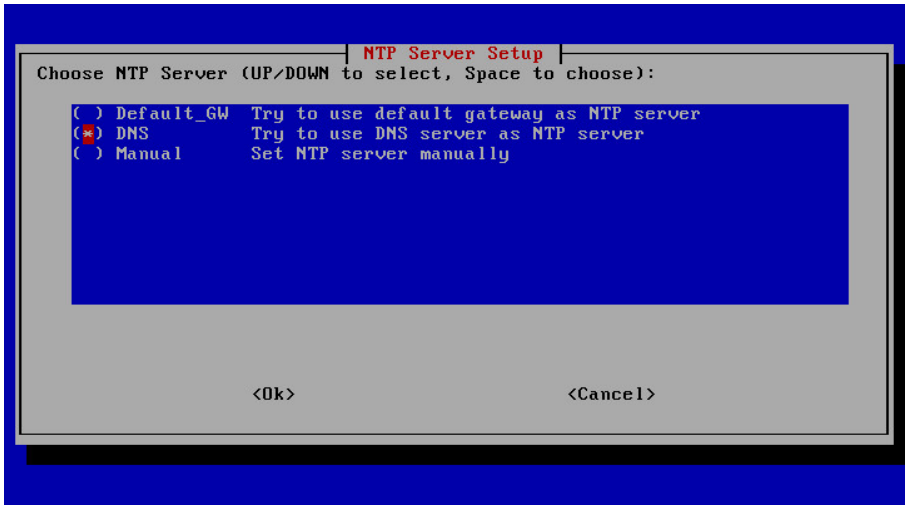
По завершении настроек потребуется нажать **Save&Quit**, чтобы подтвердить изменения.

Система обработает введенные данные и попросит подтверждения настроек.

```
/etc/hosts:
127.0.0.1       localhost.localdomain   localhost
10.60.20.71     iw-VMware-4224e9959.local       iw-VMware-4224e9959

DNS configuration (/etc/resolv.conf):
; generated by /sbin/dhclient-script
search infowatch.ru local
nameserver 10.10.50.90
nameserver 10.60.11.23

IP configuration (ip addr show):
1: lo:
    inet 127.0.0.1/8 scope host lo
2: eth0:
    inet 10.60.70.80/24 brd 10.60.70.255 scope global eth0

IP ROUTE configuration (ip route show):
10.60.70.0/24 dev eth0  proto kernel  scope link  src 10.60.70.80
169.254.0.0/16 dev eth0  scope link  metric 1002
HOSTNAME: iw-VMware-4224e9959.local
Are the network settings correct (Y/n)? y
```

На данном этапе необходимо проверить указанные сетевые настройки. Если настройки некорректны, введите **N** и укажите правильные параметры (см. предыдущие шаги). Если настройки корректны, введите **Y** для подтверждения и нажмите **Enter**.

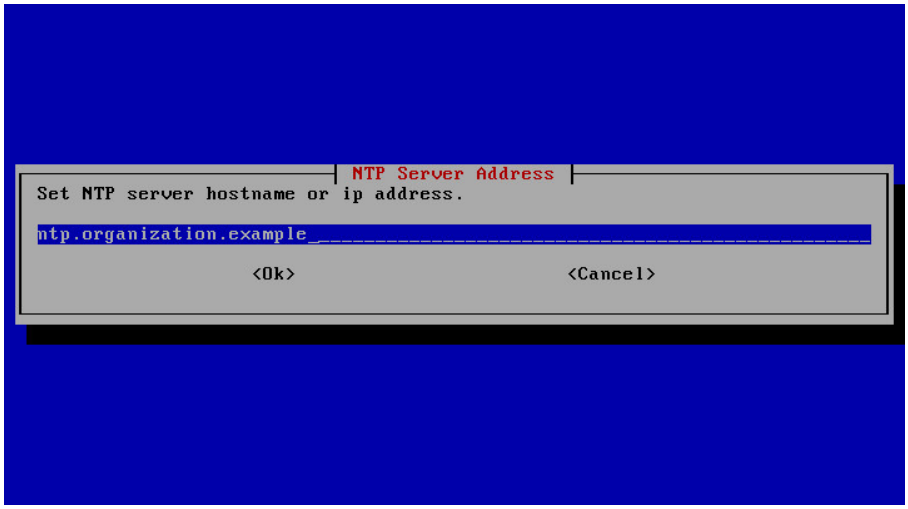
Настройка синхронизации времени (NTP-server)



На данном этапе требуется выбрать одну из следующих опций настройки сервера для синхронизации времени (NTP-server):

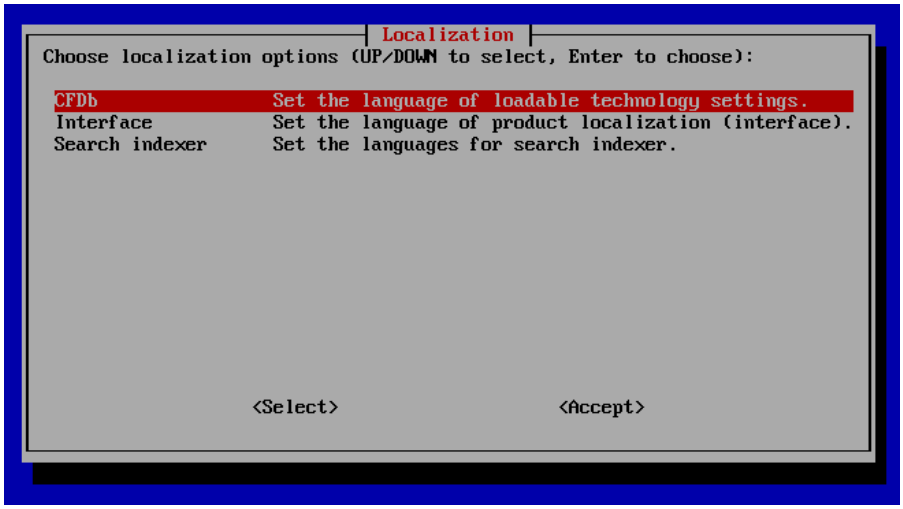
- **Default_GW** - шлюз, используемый компьютером по умолчанию;
- **DNS** - контроллер домена: обычно используется в организациях в качестве сервера времени;
- **Manual** - возможность вручную указать имя сервера или его IP-адрес.

Для выбора опции нужно установить знак астериска (*) в необходимом поле и нажать пробел, затем - **OK**.



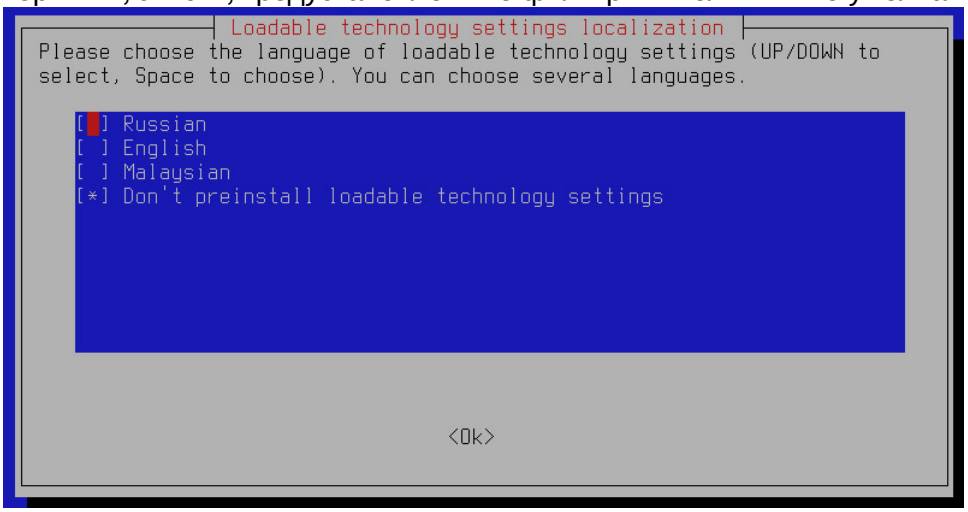
Если по каким-либо причинам указать NTP-сервер не удается, нажмите **Cancel** и выполните данную настройку позднее (подробнее см. в документе «*InfoWatch Traffic Monitor. Руководство администратора*»).

Настройка локализации



Система имеет несколько языков локализации. На данном этапе предлагается выбрать:

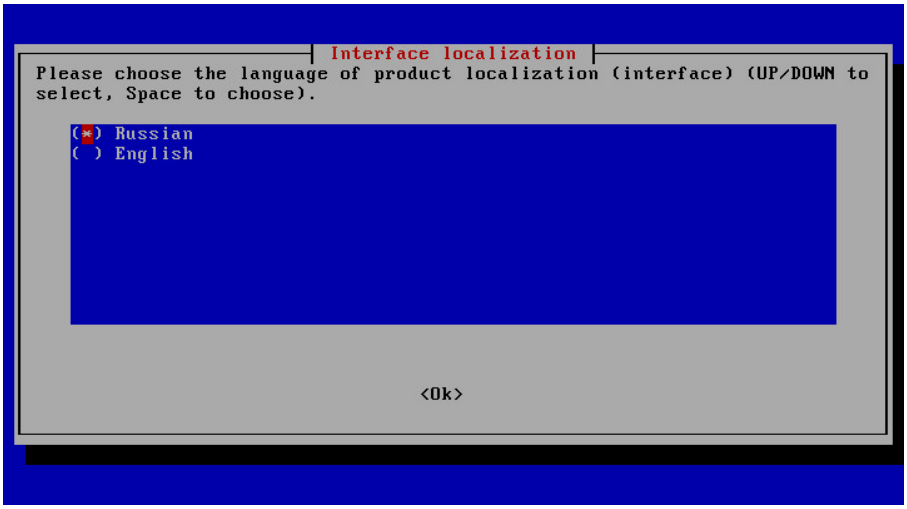
- **CFDb** - языковые настройки для таких предустановленных сущностей, как категории и термины, списки, предустановленные фильтры и политики по умолчанию.



  Предлагаются три языка:

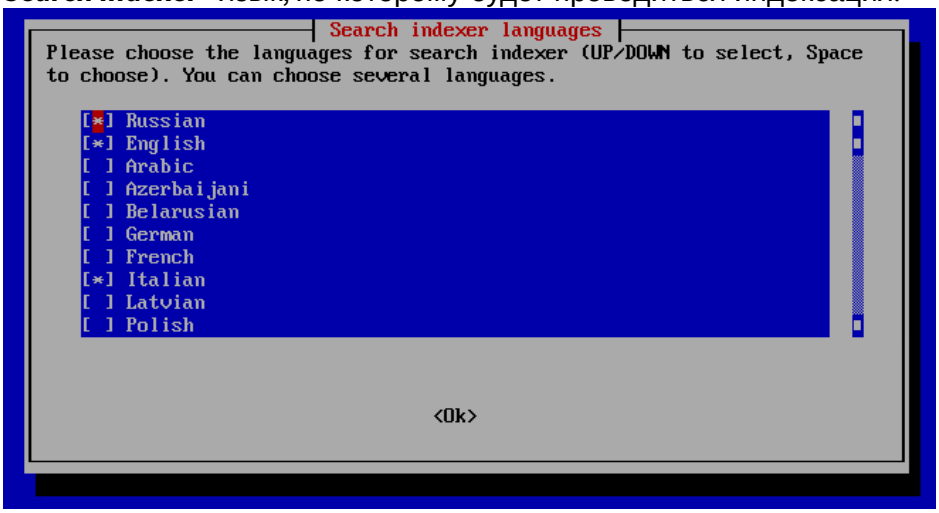
  - *Russian* – русский;
  - *English* – английский;
  - *Malaysian* – малайский.

  Также есть возможность не создавать предустановленных сущностей - опция **Don't preinstall loadable technology settings**.
  Для выбора нужно установить знак астериска (*) в необходимом поле и нажать пробел, затем - **OK**. Вы можете выбрать один, два или три языка.
- **Interface** - язык, на котором будет установлена консоль управления. На выбор предлагаются два языка:
  - *Russian* – для русскоязычного интерфейса;
  - *English* – для англоязычного интерфейса.



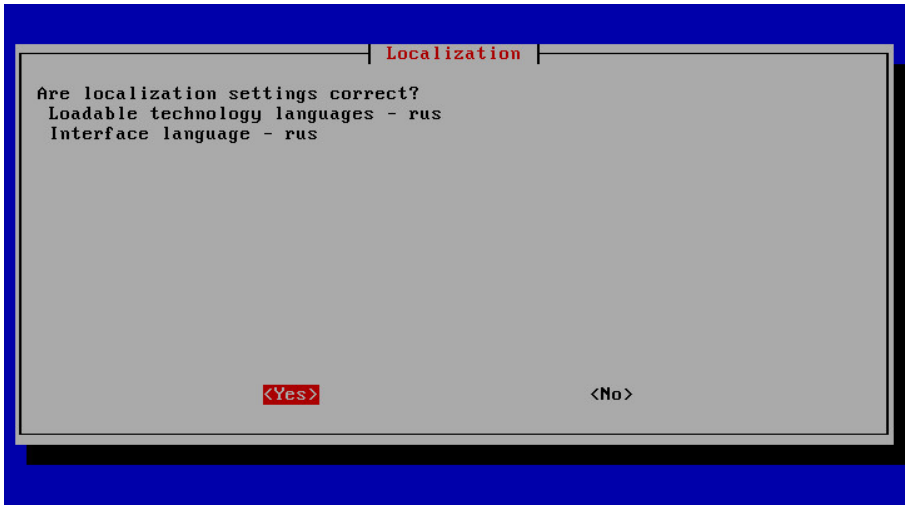
Для выбора нужно установить знак астериска (*) в необходимом поле и нажать пробел, затем - **OK**.

- **Search Indexer** - язык, по которому будет проводиться индексация.



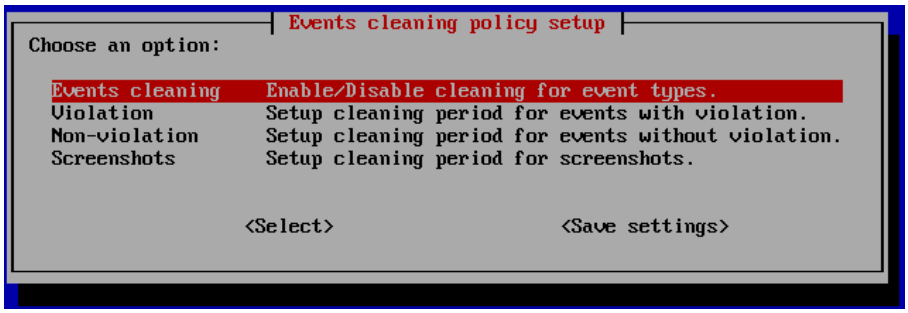
Доступны многие языки. Для выбора нужно установить знак астериска (*) в необходимом поле и нажать пробел, затем - **OK**. Вы можете выбрать один, два или несколько языков.

После выбора параметров локализации требуется нажать **Accept**.



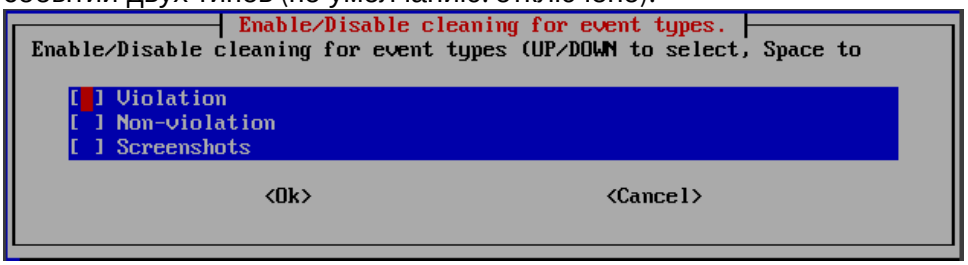
В открывшемся окне требуется проверить, что выбранные языки для предустановленных сущностей, интерфейса и индексации указаны правильно, затем нажать **Yes**.

Настройка автоматического удаления событий из БД



Настройте параметры автоматического удаления событий из БД. Для этого выберите одну из трех опций, затем нажмите **Select**:

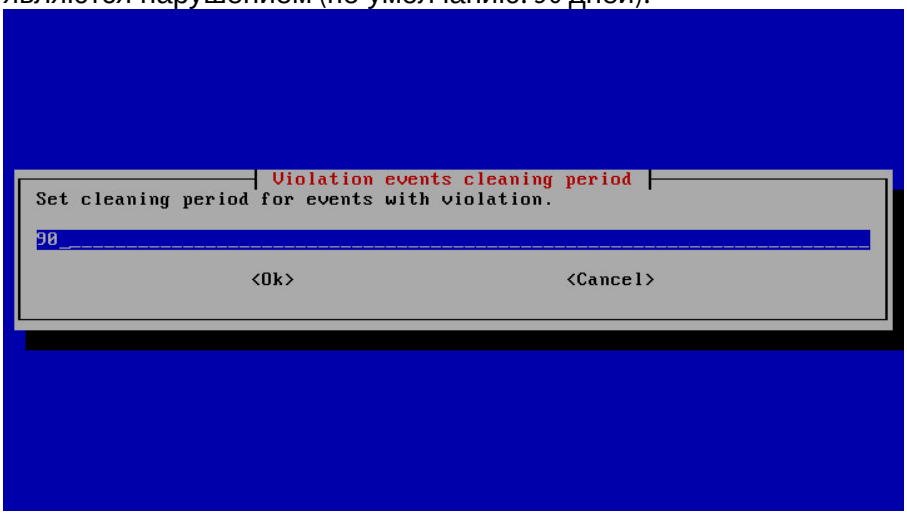
- **Events cleaning** – настраивает включение и выключение автоматического удаления событий двух типов (по умолчанию: отключено).

  Чтобы выбрать пункт, установите курсор в нужное поле и нажмите пробел до появления в поле значка астериска (*):
  - **Violation** – включить автоматическое удаление событий, которые являются нарушением (подробнее о нарушениях см. «*InfoWatch Traffic Monitor. Руководство пользователя*»);
  - **Non-violation** – включить автоматическое удаление событий, которые не являются нарушением;
  - **Screenshots** – включить автоматическое удаление снимков экрана, полученных с Агентов Device Monitor.

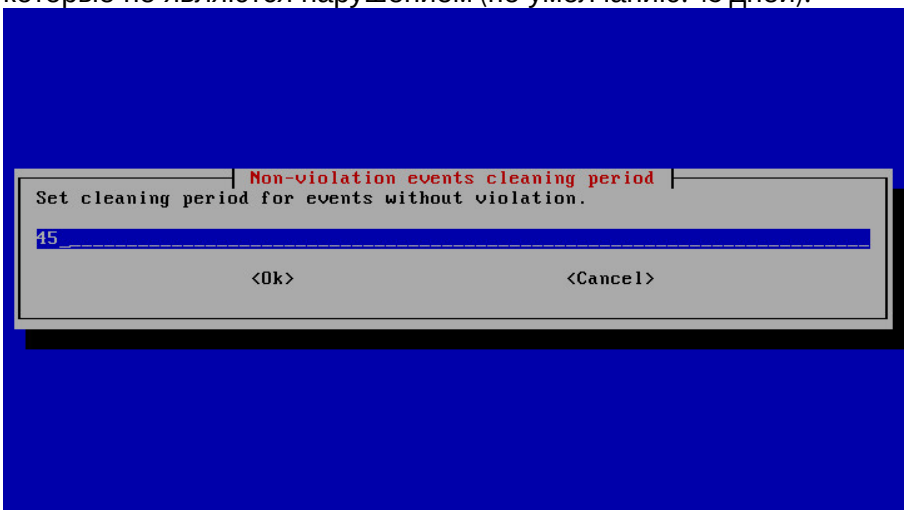
При необходимости вы можете выбрать несколько пунктов.
Нажмите **Ok**.

- **Violation** – настраивает периодичность автоматического удаления событий, которые являются нарушением (по умолчанию: 90 дней).



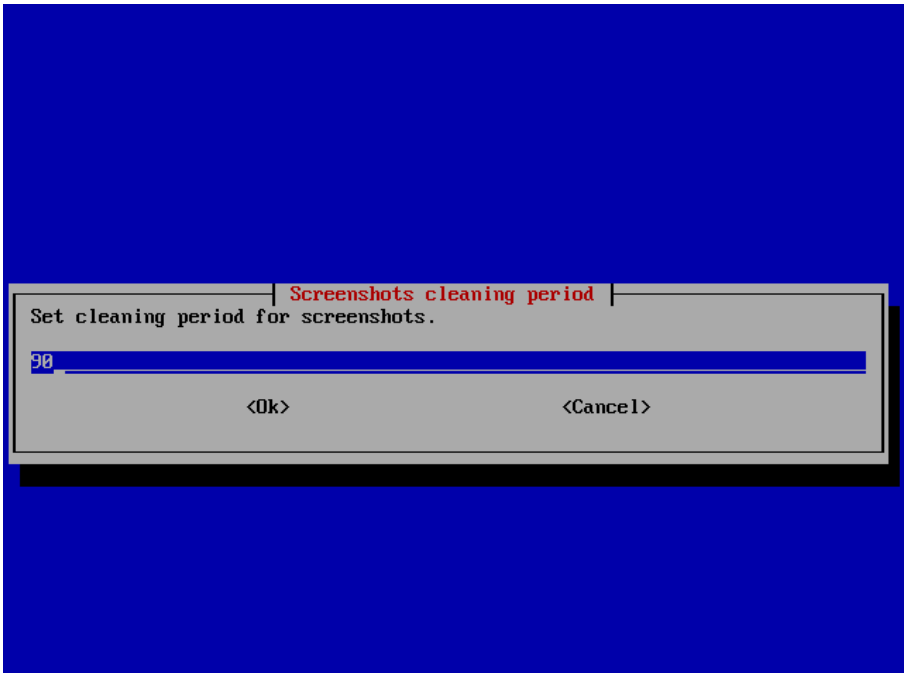
Введите периодичность удаления в днях. Нажмите **Ok**.

- **Non-violation** – настраивает периодичность автоматического удаления событий, которые не являются нарушением (по умолчанию: 45 дней).



Введите периодичность удаления в днях. Нажмите **Ok**.

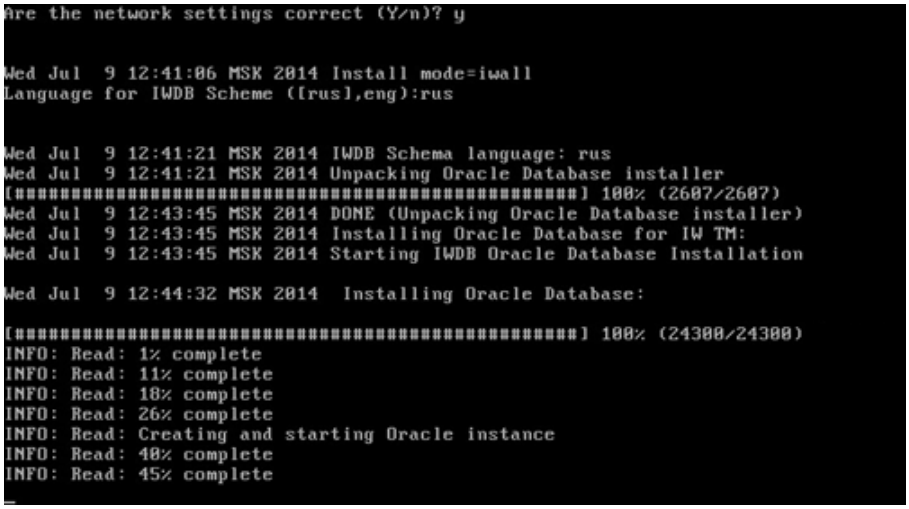
- **Screenshots** – настраивает периодичность автоматического удаления снимков экрана, полученных с Клиентов Device Monitor.



Введите периодичность удаления в днях. Нажмите **Ok**.
По завершении настроек нажмите **Save settings**.

Завершение установки

По завершении настроек начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране:



В результате установки в Системе будут созданы учетные записи, приведенные в статье "Предустановленные серверные параметры".

Имя сервера (hostname) будет иметь следующий формат:
`iwtm-xxxxxxxxxxxxxxx.local`
где xxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

О порядке настройки Системы см. документ «*InfoWatch Traffic Monitor. Руководство администратора*».

3.1.2 Установка TM Enterprise и TM Standard в режиме "Все-в-одном"

Установка «все-в-одном» позволяет установить все компоненты Системы на один компьютер.

> **Важно!**
>
> В данной статье приведена инструкция без подробного описания экранов установки. Дополнительная информация содержится в разделе «Общие сведения по этапам установки серверных компонентов».

Чтобы установить Traffic Monitor Enterprise или Traffic Monitor Standard в режиме «Все-в-одном», выполните следующие действия:

1. Подключите диск с дистрибутивом: программа-инсталлятор (**kickstart**) запустится автоматически.
2. В окне приветствия выберите:
   - **TM Enterprise** – для установки редакции Enterprise;
   - **TM Standard** – для установки редакции Standard.

   > **Важно!**
   >
   > При установке редакции **TM Standard**, в качестве базы данных доступна только PostgreSQL.

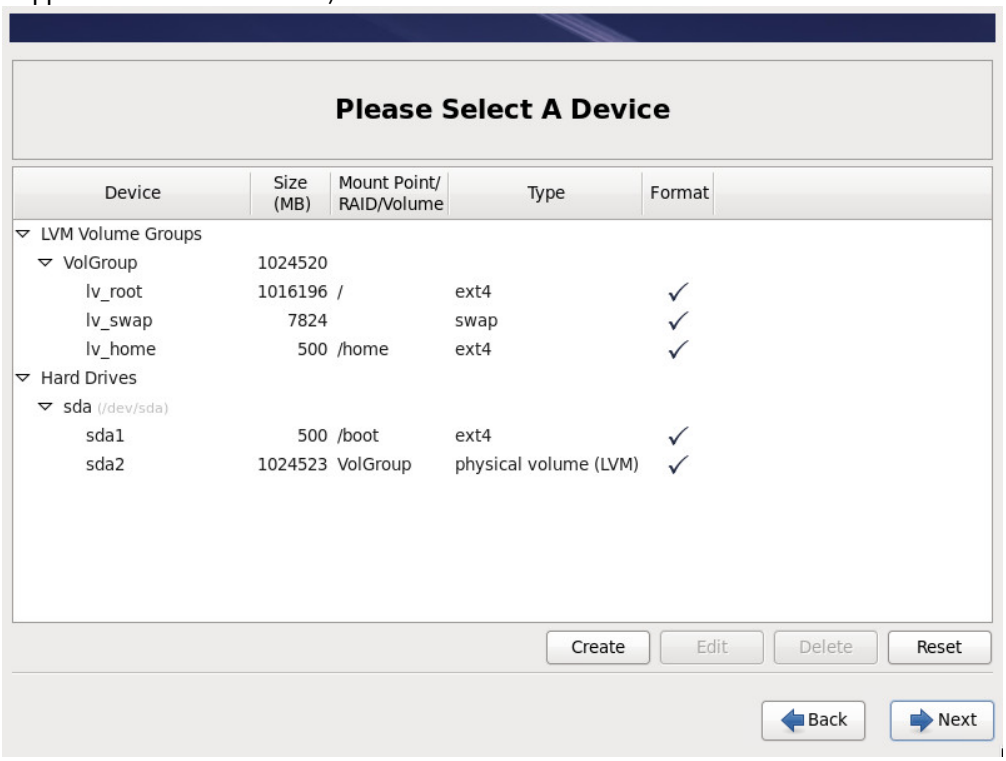
   Нажмите **Enter**.
3. В окне выбора базы данных укажите, какая СУБД должна быть установлена (опция доступна только для **TM Enterprise**):
   a. **Oracle Enterprise**;
   b. **PostgreSQL**.

   Нажмите **Enter**.
4. В окне выбора режима установки выберите **TME All-in-one** или **TMS All-in-one** в зависимости от выбранной редакции, нажмите **Enter**.

   > **Важно!**
   >
   > После выбора режима установки на экран может быть выведено предупреждение «*The storage device below may contain data*». Чтобы очистить диск и начать установку, нажмите **Yes, discard any data**, оставив без изменений поле **Apply my choice to all devices with undetected partitions of file systems**.

5. Укажите настройки часового пояса для сервера (если системное время установлено по Гринвичу (UTC), установите флажок в поле **System clock uses UTC**), нажмите **Next**.
6. Задайте пароль пользователя *root*, подтвердите его и нажмите **Next**. Рекомендации по составлению паролей приведены в разделе "Приложение А".
7. Определите способ разбиения дискового пространства (детальное описание см. в статье "Выбор способа разбиения дискового пространства"):

a. Выберите **Use All Space**.
b. Отметьте опцию **Review and modify partitioning layout**, расположенную внизу окна.
c. Нажмите **Next**.
d. В окне **Please Select A Device** выберите раздел **lv_home** и нажмите **Edit**.
e. В поле **Size (MB)** укажите **5000**. Нажмите **OK**.
f. В окне **Please Select A Device** выберите раздел **lv_root** и нажмите **Edit**.
g. В поле **Size (MB)** укажите все оставшееся свободное пространство (отображается под полем - **Max size is...**) . Нажмите **OK**.



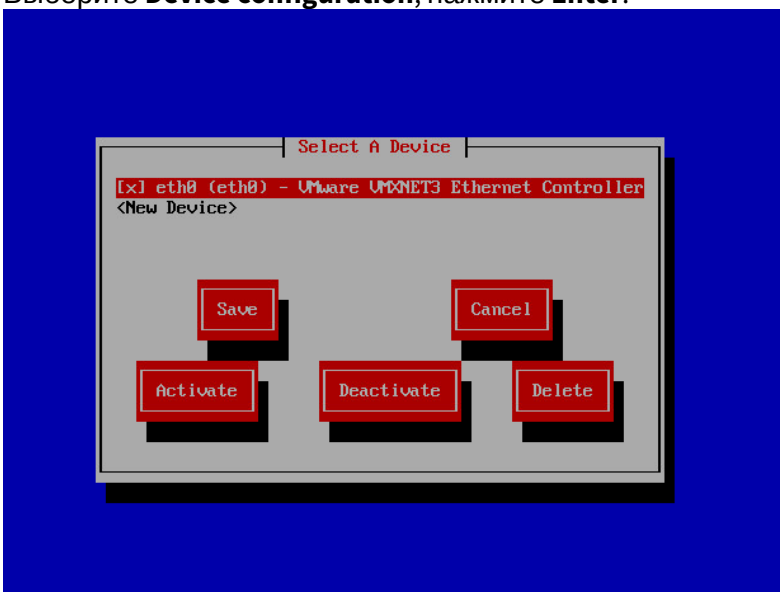
h. Нажмите **Next**.

> **Примечание:**
>
> На экран может быть выведено окно **Format >Warnings**, свидетельствующее о том, что требуется отформатировать разделы жесткого диска, которые будут использоваться для установки. Для продолжения установки нажмите **Format**.

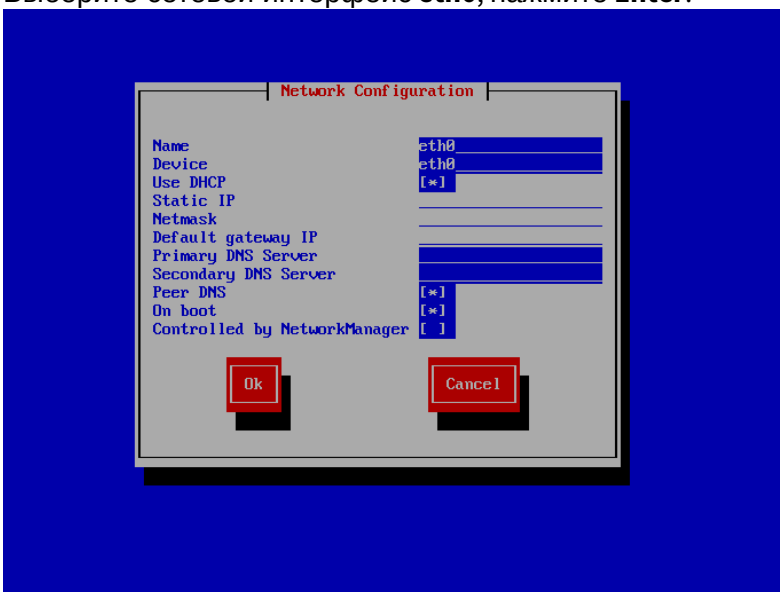
Начнется процесс разбиения диска, а затем – установки операционной системы.
Прогресс выполнения обоих процессов будет отображаться на экране.
Это может занять некоторое время.
По окончании установки операционной системы выполнится перезагрузка, и будет предложено настроить сетевые параметры.

8. Для настройки параметров сетевой карты:

a. Выберите **Device configuration**, нажмите **Enter**.



b. Выберите сетевой интерфейс **eth0**, нажмите **Enter**.



> **Важно!**
>
> Не включайте опцию **Controlled by Network Manager**.

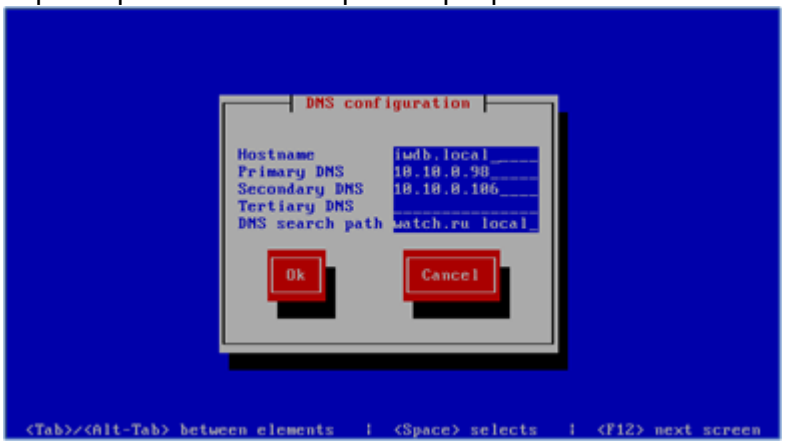
> **Важно!**
>
> При конфигурировании **eth0** убедитесь, что опция **On boot** включена.

c. Если вы хотите, чтобы Система использовала сетевые настройки от DHCP сервера, переведите курсор в поле **Use DHCP** и нажмите пробел. В противном

случае вручную введите сетевые настройки сервера (статический IP-адрес машины и прочее). По завершении конфигурирования нажмите **OK**.

d. Нажмите **Save**, чтобы сохранить сделанные настройки.

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



10. Нажмите **Save&Quit**.
11. Проверьте указанные сетевые настройки. Если настройки некорректны, нажмите **N** на клавиатуре и укажите правильные параметры (см. предыдущие шаги). Если настройки корректны, нажмите **Y** на клавиатуре для подтверждения и нажмите **Enter**.
12. Настройте адрес сервера для синхронизации времени (NTP-server). Для этого установите знак астериска (*) в поле **DNS** и нажмите пробел, затем - **OK**.

> **Примечание:**
>
> Если по каким-либо причинам указать NTP-сервер не удается, нажмите **Cancel** и выполните данную настройку позднее (подробнее о настройке NTP-сервера см. в документе "InfoWatch Traffic Monitor. Руководство администратора", статья "Настройка синхронизации времени").

13. Настройте параметры локализации:
    a. Укажите язык предустановленных сущностей:
        i. Выберите **CFDB**, нажмите **Enter** .
        ii. Выберите требуемый язык.
        При выборе опции **Don't preinstall loadable technology settings** стандартная конфигурация Системы не устанавливается.
        iii. Нажмите **OK**.
        На выбранном языке будут созданы такие предустановленные сущности, как классификатор, фильтры, политики по умолчанию.

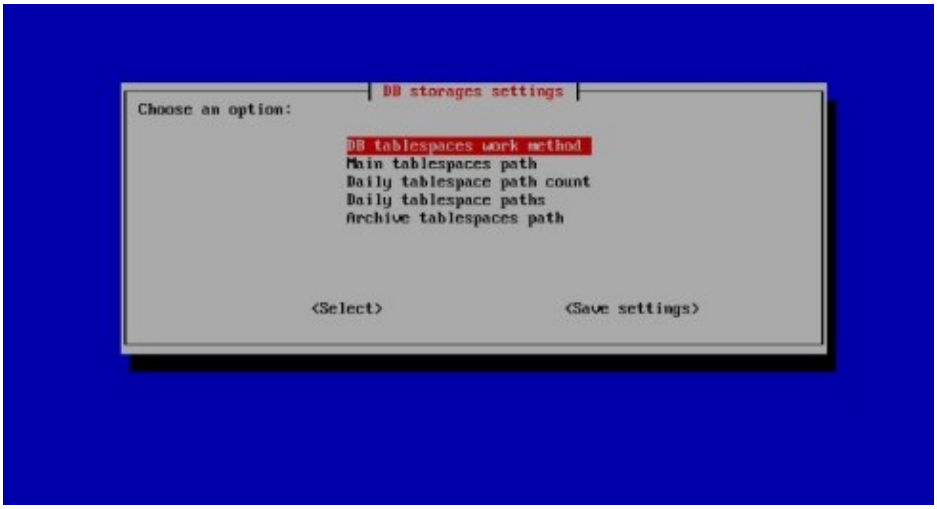
    b. Укажите язык интерфейса:
        i. Выберите **Interface**, нажмите **Enter**.
        ii. Выберите требуемый язык.
        На выбранном языке будет установлена консоль управления.
        iii. Нажмите **OK**.

    c. Укажите язык для индексатора поиска:

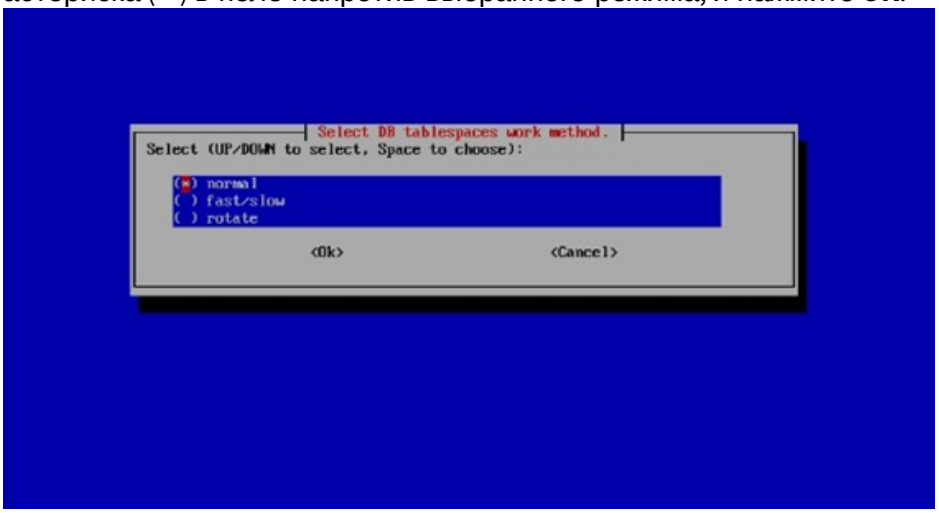
i. Выберите **Search indexer**, нажмите **Enter**.
ii. Выберите один или несколько языков.
iii. Нажмите **OK**.

d. Нажмите **Accept**.
e. В открывшемся окне проверьте, что выбранные языки указаны правильно, затем нажмите **Yes**.

14. Настройте параметры хранения данных в БД Системы:
    a. Выберите тип табличного пространства: **DB tablespaces work method** и нажмите **Enter**.



    b. Определите режим хранения файлов табличного пространства, установив знак астериска (*) в поле напротив выбранного режима, и нажмите **OK**.



- **Normal** (обычный) – режим переноса данных, при котором переключение на следующий раздел (если он указан) происходит при переполнении предыдущего.
- **Fast/slow** (быстрые и медленные диски) – режим переноса данных с разделением пулов на быстрый и медленный. Свежие данные сохраняются в быстром разделе и через указанное количество дней перемещаются на медленные разделы (медленный пул работает при этом в режиме normal).

- **Rotate** (ежедневное переключение) – режим переноса данных, при котором переход к следующему разделу происходит ежедневно и при переполнении предыдущего.

> **Примечание:**
>
> Особенности режимов хранения данных (**normal**, **fast/slow** и **rotate**) описаны в статье базы знаний "Настройка режима хранения данных в ТП. Хранение данных на разных дисках".

c. Выберите **Main tablespaces path** и укажите путь к диску хранения данных основного табличного пространства (по умолчанию указан путь **/u02/oradata** для СУБД Oracle и **/u02/pgdata** для СУБД PostgreSQL).
d. Нажмите **Enter**.
e. Выберите **Daily tablespace path count** и укажите количество путей для файлов ежедневных табличных пространств (число от 1 до 10, по умолчанию указано 1).
f. Нажмите **Enter**.
g. Выберите **Daily tablespace paths** и укажите путь к диску хранения данных ежедневного табличного пространства (по умолчанию указан путь **/u02/oradata1** для СУБД Oracle и **/u02/pgdata1** для СУБД PostgreSQL).
h. Нажмите **Enter**.
i. Выберите **Number of days to store in fast tablespaces for fast/slow method** и укажите период хранения файлов табличных пространств в быстром разделе в режиме **fast/slow** (число от 1 до 1000, по умолчанию указано 7 дней). Файлы старше указанного периода автоматически переносятся на медленные диски (только для режима **fast/slow**).
j. Нажмите **Enter**.
k. Выберите **Fast daily tablespaces path for fast/slow method** и укажите путь к диску хранения файлов ежедневных табличных пространств в быстром разделе в режиме **fast/slow** (по умолчанию указан путь **/u03/pgdata** - только для режима **fast/slow**).
l. Нажмите **Enter**.
m. Выберите **Archive tablespaces path** и укажите путь к диску хранения файлов архивированных табличных пространств (по умолчанию указан путь **/u02/arch**).
n. Нажмите **Enter**.
o. Нажмите **Save settings**, чтобы сохранить выбранные настройки.
p. В открывшемся окне проверьте, что выбранные параметры указаны правильно, затем нажмите **Yes**.

15. Настройте параметры автоматического удаления событий из БД (по умолчанию автоматическое удаление отключено):
    a. Выберите **Events cleaning** и нажмите **Select**:
        i. Установите курсор в нужное поле и нажмите пробел до появления в поле значка астериска (*):
            - **Violation** – включить автоматическое удаление событий, которые являются нарушением (подробнее о нарушениях см. «*InfoWatch Traffic Monitor. Руководство пользователя*»);

- **Non-violation** – включить автоматическое удаление событий, которые не являются нарушением;
- **Screenshots** – включить автоматическое удаление снимков экрана, полученных от Агентов Device Monitor.
  При необходимости вы можете выбрать несколько пунктов.

ii. Нажмите **Ok**.

b. Если включено автоматическое удаление событий с нарушением, укажите период их хранения до удаления:
   i. Выберите **Violation** и нажмите **Select**:
   ii. В открывшемся окне введите количество дней, по прошествии которых событие будет автоматически удаляться (по умолчанию: 90 дней).
   iii. Нажмите **Ok**.

c. Если включено автоматическое удаление событий без нарушения, укажите период их хранения до удаления:
   i. Выберите **Non-violation** и нажмите **Select**:
   ii. В открывшемся окне введите количество дней, по прошествии которых событие будет автоматически удаляться (по умолчанию: 45 дней).
   iii. Нажмите **Ok**.

d. Если включено автоматическое удаление снимков экрана, полученных от Агентов Device Monitor, укажите период их хранения до удаления:
   i. Выберите **Screenshots** и нажмите **Select**:
   ii. В открывшемся окне введите количество дней, по прошествии которых снимки экрана будут автоматически удаляться (по умолчанию: 90 дней).
   iii. Нажмите **Ok**.

e. По завершении настроек нажмите **Save settings**.
f. В открывшемся окне проверьте, что все настройки указаны правильно, затем нажмите **Yes**.

Начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране. Процесс может занять некоторое время.

В результате установки в системе будут созданы учетные записи, приведенные в статье "Предустановленные серверные параметры".

Имя сервера (hostname) будет иметь следующий формат:
`iwtm-xxxxxxxxxxxxxxx.local`
где xxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

Установка Веб-консоли управления происходит в автоматическом режиме с помощью программы-инсталлятора (**kickstart**). После окончания установки серверных компонентов работа в консоли управления доступна через окно браузера, при этом требуется ввести URL-адрес сервера Traffic Monitor.

О порядке дальнейшей настройки Системы см. документ «InfoWatch Traffic Monitor. Руководство администратора».

3.1.3 Распределенная установка TM Enterprise

Traffic Monitor в редакции Enterprise позволяет развернуть Систему так, чтобы сервер Traffic Monitor и СУБД (Oracle Enterprise или PostgreSQL) были установлены на разные компьютеры. Такая установка используется, если с учетом предполагаемой нагрузки сервисы Traffic Monitor и СУБД не смогут производительно работать на одном компьютере.

Установка серверов должна производиться в следующем порядке:

1. Установка Базы данных (TME DB server);
2. Установка Сервера Traffic Monitor (TME Node server).

> **Важно!**
>
> Установка в другом порядке (сервер Traffic Monitor устанавливается раньше, чем База данных) не поддерживается и приводит к возникновению ошибок в процессе установки.

Вы можете установить несколько серверов Traffic Monitor. При этом необходимо логически разделить их на основной и второстепенный (второстепенные). Основным сервером называется сервер, на котором будут запущены процессы, необходимые Системе в единственном экземпляре.

Установка Базы данных

> **Важно!**
>
> В данном разделе приведена инструкция без подробного описания экранов установки. Дополнительная информация содержится в разделе " Общие сведения по этапам установки серверных компонентов".

Чтобы установить Базу данных, выполните следующие действия:

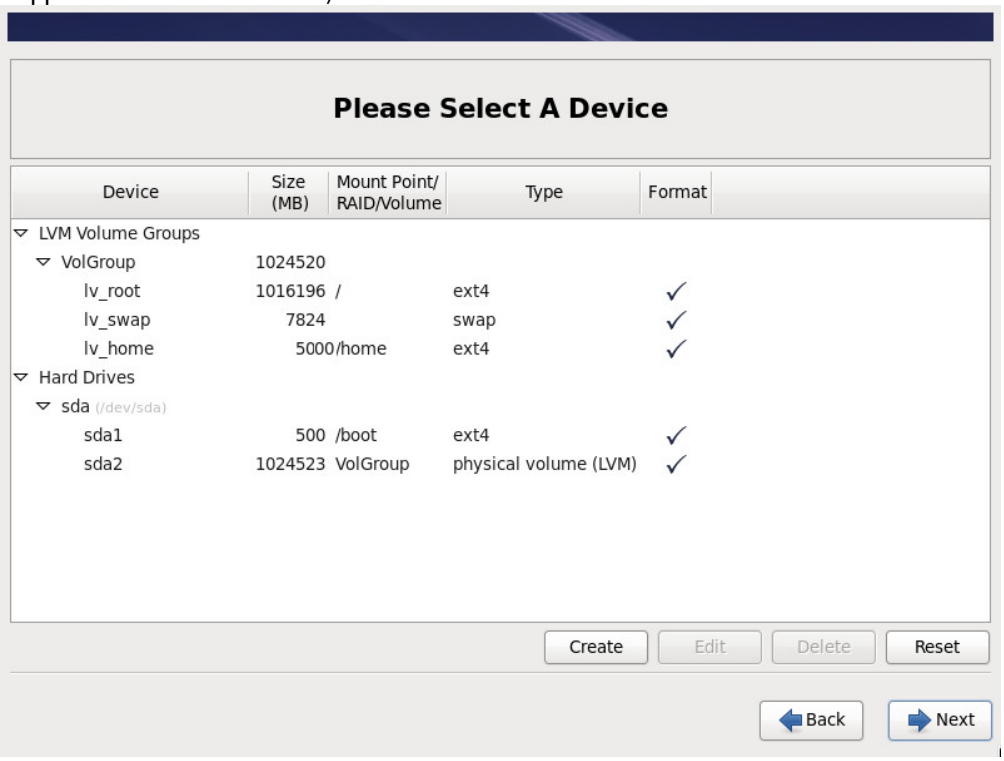
1. В окне приветствия выберите **TM Enterprise**, нажмите **Enter**.
2. В окне выбора базы данных укажите, какая СУБД должна быть установлена:
   a. Oracle Standard;
   b. PostgreSQL.

   Нажмите **Enter**.
3. В окне выбора режима установки выберите **TME DB server**, нажмите **Enter**.

   > **Важно!**
   >
   > После выбора режима установки на экран может быть выведено предупреждение "*The storage device below may contain any data*". Чтобы очистить диск и начать установку, нажмите **Yes, discard any data**, оставив без изменений поле **Apply my choice to all devices with undetected partitions of filesystems**.

4. Укажите настройки часового пояса для сервера (если системное время установлено по Гринвичу (UTC), установите флажок в поле **System clock uses UTC**), нажмите **Next**.
5. Задайте пароль пользователя *root*, подтвердите его и нажмите **Next**. Рекомендации по составлению паролей приведены в разделе Приложение А.
6. Определите способ разбиения дискового пространства (детальное описание см. в статье "Выбор способа разбиения дискового пространства"):
   a. Выберите **Use All Space**.
   b. Отметьте опцию **Review and modify partitioning layout**, расположенную внизу окна.

c. Нажмите **Next**.
d. В окне **Please Select A Device** выберите раздел **lv_home** и нажмите **Edit**.
e. В поле **Size (MB)** укажите **5000**. Нажмите **OK**.
f. В окне **Please Select A Device** выберите раздел **lv_root** и нажмите **Edit**.
g. В поле **Size (MB)** укажите все оставшееся свободное пространство (отображается под полем - **Max size is...**) . Нажмите **OK**.



h. Нажмите **Next**.

Начнется процесс разбиения диска, а затем – установки операционной системы.
Прогресс выполнения обоих процессов будет отображаться на экране.
Процесс может занять некоторое время.
По окончании установки операционной системы выполнится перезагрузка, и будет предложено настроить сетевые параметры.

7. Выполните настройку параметров сетевой карты и DNS конфигурации как описано в статье "Настройка сети". Нажмите **Save&Quit**.
8. Проверьте указанные сетевые настройки. Если настройки некорректны, нажмите **N** на клавиатуре и укажите правильные параметры. Если настройки корректны, нажмите **Y** на клавиатуре для подтверждения и нажмите **Enter**.
9. Настройте адрес сервера для синхронизации времени (NTP-server). Для этого установите знак астериска (*) в поле **DNS** и нажмите пробел, затем - **OK**.
10. Настройте параметры локализации:
    a. Укажите язык настроек классификации:
        i. Выберите **CFDB**, нажмите **Enter** .
        ii. Выберите требуемый язык настроек классификации, нажмите **OK**.
        На выбранном языке будут созданы такие предустановленные сущности, как классификатор, фильтры, политики по умолчанию.
    b. Укажите язык интерфейса:
        i. Выберите **Interface**, нажмите **Enter**.

ii. Выберите требуемый язык интерфейса, нажмите **OK**.
На выбранном языке будет установлена консоль управления.

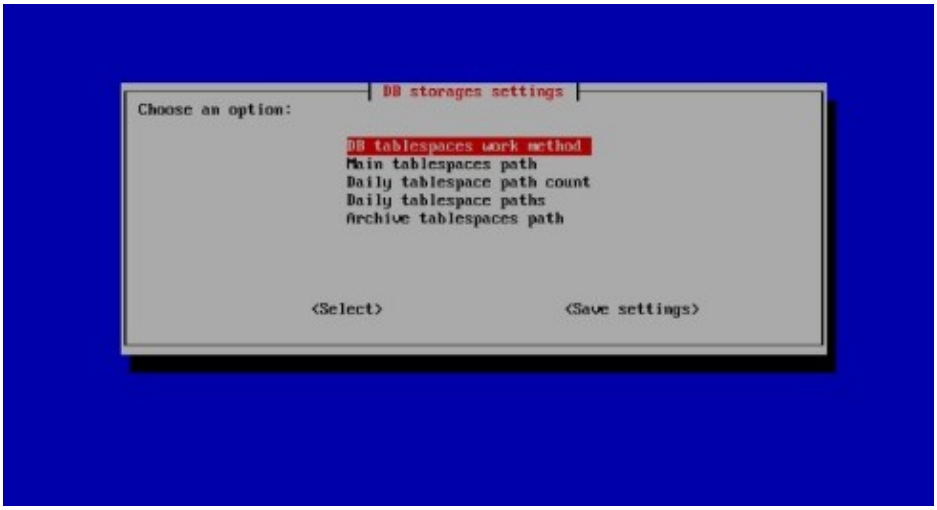
c. Укажите язык для индексатора поиска:
   i. Выберите **Search indexer**, нажмите **Enter**.
   ii. Выберите один или несколько языков.
   iii. Нажмите **OK**.

d. Нажмите **Accept**.

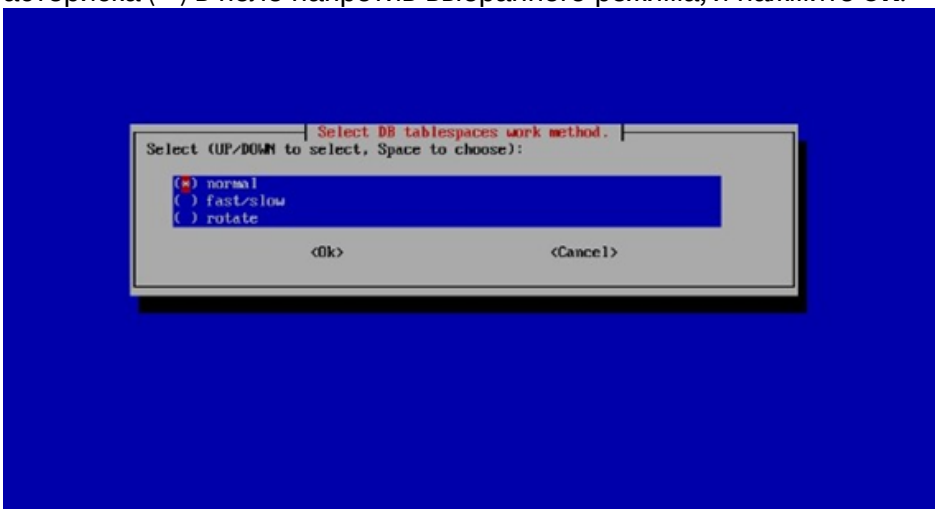
e. В открывшемся окне проверьте, что выбранные языки для настроек классификации и для интерфейса указаны правильно, затем нажмите **Yes**.

11. Настройте параметры хранения данных в БД Системы:

a. Выберите тип табличного пространства: **DB tablespaces work method** и нажмите **Enter**.



b. Определите режим хранения файлов табличного пространства, установив знак астериска (*) в поле напротив выбранного режима, и нажмите **OK**.



- **Normal** (обычный) – режим переноса данных, при котором переключение на следующий раздел (если он указан) происходит при переполнении предыдущего.

- **Fast/slow** (быстрые и медленные диски) – режим переноса данных с разделением пулов на быстрый и медленный. Свежие данные сохраняются в быстром разделе и через указанное количество дней перемещаются на медленные разделы (медленный пул работает при этом в режиме normal).
- **Rotate** (ежедневное переключение) – режим переноса данных, при котором переход к следующему разделу происходит ежедневно и при переполнении предыдущего.

> **Примечание:**
>
> Особенности режимов хранения данных (**normal**, **fast/slow** и **rotate**) описаны в статье базы знаний "Настройка режима хранения данных в ТП. Хранение данных на разных дисках".

c. Выберите **Main tablespaces path** и укажите путь к диску хранения данных основного табличного пространства (по умолчанию указан путь **/u02/oradata** для СУБД Oracle и **/u02/pgdata** для СУБД PostgreSQL).
d. Нажмите **Enter**.
e. Выберите **Daily tablespace path count** и укажите количество путей для файлов ежедневных табличных пространств (число от 1 до 10, по умолчанию указано 1).
f. Нажмите **Enter**.
g. Выберите **Daily tablespace paths** и укажите путь к диску хранения данных ежедневного табличного пространства (по умолчанию указан путь **/u02/oradata1** для СУБД Oracle и **/u02/pgdata1** для СУБД PostgreSQL).
h. Нажмите **Enter**.
i. Выберите **Number of days to store in fast tablespaces for fast/slow method** и укажите период хранения файлов табличных пространств в быстром разделе в режиме **fast/slow** (число от 1 до 1000, по умолчанию указано 7 дней). Файлы старше указанного периода автоматически переносятся на медленные диски (только для режима **fast/slow**).
j. Нажмите **Enter**.
k. Выберите **Fast daily tablespaces path for fast/slow method** и укажите путь к диску хранения файлов ежедневных табличных пространств в быстром разделе в режиме **fast/slow** (по умолчанию указан путь **/u03/pgdata** - только для режима **fast/slow**).
l. Нажмите **Enter**.
m. Выберите **Archive tablespaces path** и укажите путь к диску хранения файлов архивированных табличных пространств (по умолчанию указан путь **/u02/arch**).
n. Нажмите **Enter**.
o. Нажмите **Save settings**, чтобы сохранить выбранные настройки.
p. В открывшемся окне проверьте, что выбранные параметры указаны правильно, затем нажмите **Yes**.

12. Настройте параметры автоматического удаления событий из БД.
Выберите одну из трех опций, затем нажмите **Select**:
    - **Events cleaning** – настраивает включение и выключение автоматического удаления событий двух типов (по умолчанию: отключено).
    Включите автоматическое удаление событий, которые являются нарушением и/

или не являются нарушением. Для этого поставьте маркер напротив поля **Violation** и/или **Non - violation**. Нажмите **Ok**.

- **Violation** – настраивает периодичность автоматического удаления событий, которые являются нарушением (по умолчанию: 90 дней).
  Установите периодичность удаления в днях. Нажмите **Ok**.
- **Non - violation** – настраивает периодичность автоматического удаления событий, которые не являются нарушением (по умолчанию: 45 дней).
  Установите периодичность удаления в днях. Нажмите **Ok** .
- **Screenshots** – настраивает периодичность автоматического удаления снимков экрана, полученных с Клиентов Device Monitor.

13. По завершении настроек нажмите **Save settings** .

Начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране. Процесс может занять некоторое время.

В результате установки в Системе будут созданы учетные записи, перечисленные в статье "Предустановленные серверные параметры".

Имя сервера (hostname) будет иметь следующий формат:
`iwtm-xxxxxxxxxxxxxxx.local`
где xxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

О порядке дальнейшей настройки Системы см. документ «*InfoWatch Traffic Monitor. Руководство администратора*».

Установка Сервера Traffic Monitor

> **Важно!**
>
> В данной статье приведена инструкция без подробного описания экранов установки. Дополнительная информация содержится в разделе «Общие сведения по этапам установки серверных компонентов».

Чтобы установить Сервер Traffic Monitor, выполните следующие действия:

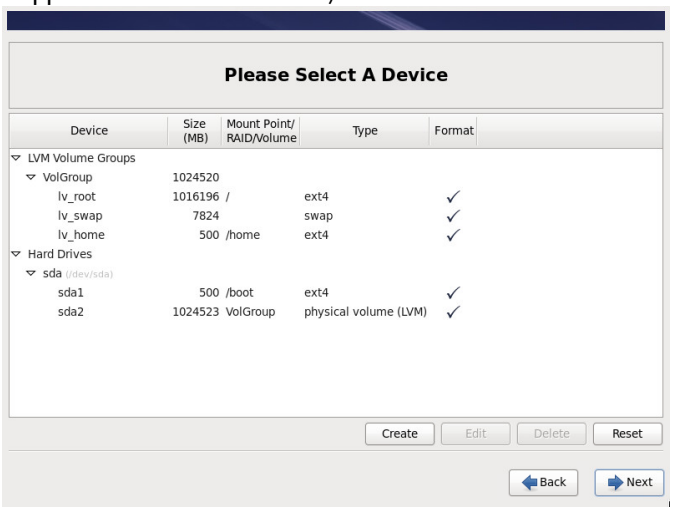
1. Подключите диск с дистрибутивом: программа-инсталлятор (**kickstart**) запустится автоматически.
2. В окне приветствия выберите **TM Enterprise**.
3. В окне выбора базы данных в укажите, какая СУБД должна быть установлена:
   a. **Oracle Standard**;
   b. **PostgreSQL**.

   Нажмите **Enter**.
4. В окне выбора режима установки выберите **TME Node server**, нажмите **Enter**.

> **Важно!**
>
> После выбора режима установки на экран может быть выведено предупреждение «*The storage device below may contain any data*». Чтобы очистить

диск и начать установку, нажмите **Yes, discard any data**, оставив без изменений поле **Apply my choice to all devices with undetected partitions of file systems**.

5. Укажите настройки часового пояса для сервера (если системное время установлено по Гринвичу (UTC), установите флажок в поле **System clock uses UTC**), нажмите **Next**.
6. Задайте пароль суперпользователя *root*, подтвердите его и нажмите **Next**. Рекомендации по составлению паролей приведены в разделе Приложение А. Рекомендации по составлению имен и паролей.
7. Определите способ разбиения дискового пространства (детальное описание см. в статье "Выбор способа разбиения дискового пространства"):
   a. Выберите **Use All Space**.
   b. Отметьте опцию **Review and modify partitioning layout**, расположенную внизу окна.
   c. Нажмите **Next**.
   d. В окне **Please Select A Device** выберите раздел **lv_home** и нажмите **Edit**.
   e. В поле **Size (MB)** укажите **5000**. Нажмите **OK**.
   f. В окне **Please Select A Device** выберите раздел **lv_root** и нажмите **Edit**.
   g. В поле **Size (MB)** укажите все оставшееся свободное пространство (отображается под полем - **Max size is...**) . Нажмите **OK**.



   h. Нажмите **Next**.

> **Примечание:**
>
> На экран может быть выведено окно **Format >Warnings**, свидетельствующее о том, что требуется отформатировать разделы жесткого диска, которые будут использоваться для установки. Для продолжения установки нажмите **Format**.

8. Начнется процесс разбиения диска, а затем – установки операционной системы. Прогресс выполнения обоих процессов будет отображаться на экране. Процесс может занять некоторое время. По окончании установки операционной системы выполнится перезагрузка, и будет предложено настроить сетевые параметры.
9. Выполните настройку параметров сетевой карты и DNS конфигурации как описано в статье "Настройка сети". Нажмите **Save&Quit**.

10. Проверьте указанные сетевые настройки. Если они некорректны, нажмите **N** на клавиатуре и укажите правильные параметры. Если настройки корректны, нажмите **Y** на клавиатуре для подтверждения и нажмите **Enter**.
11. Настройте адрес сервера для синхронизации времени (NTP-server). Для этого установите знак астериска (*) в поле **DNS** и нажмите пробел, затем - **OK**.
12. Укажите статический IP-адрес сервера БД, нажмите **Enter**.

    > **Примечание.**
    >
    > Если используется DHCP, необходимо привязать выдачу определенного IP-адрес к MAC-адресу.

13. Проверьте правильность настроек. Если они некорректны, нажмите **N** на клавиатуре и укажите правильные параметры. Если настройки корректны, нажмите **Y** на клавиатуре для подтверждения и нажмите **Enter**.

В результате установки в Системе будут созданы учетные записи, приведенные в статье "Предустановленные серверные параметры".

Имя сервера (hostname) будет иметь следующий формат:
`iwtm-xxxxxxxxxxxxxxx.local`
где xxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

Установка Веб-консоли управления происходит в автоматическом режиме с помощью программы-инсталлятора (**kickstart**). После окончания установки серверных компонентов работа в консоли управления доступна через окно браузера, при этом требуется ввести URL-адрес сервера Traffic Monitor.

О порядке дальнейшей настройки Системы см. документ «*InfoWatch Traffic Monitor. Руководство администратора*».

3.2 Установка подсистемы Краулер

Перехватчик Краулер 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;

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

Перед установкой ознакомьтесь с требованиями к аппаратному и программному обеспечению компьютеров, на которые будет выполняться установка компонентов. Для установки обоих компонентов подсистемы Краулер (сервер и сканер) используется единый дистрибутив.

Важно!

И сервер, и сканер Краулер должны быть установлены на компьютеры, находящиеся в одном домене: в том, к которому принадлежат компьютеры, которые предполагается сканировать.

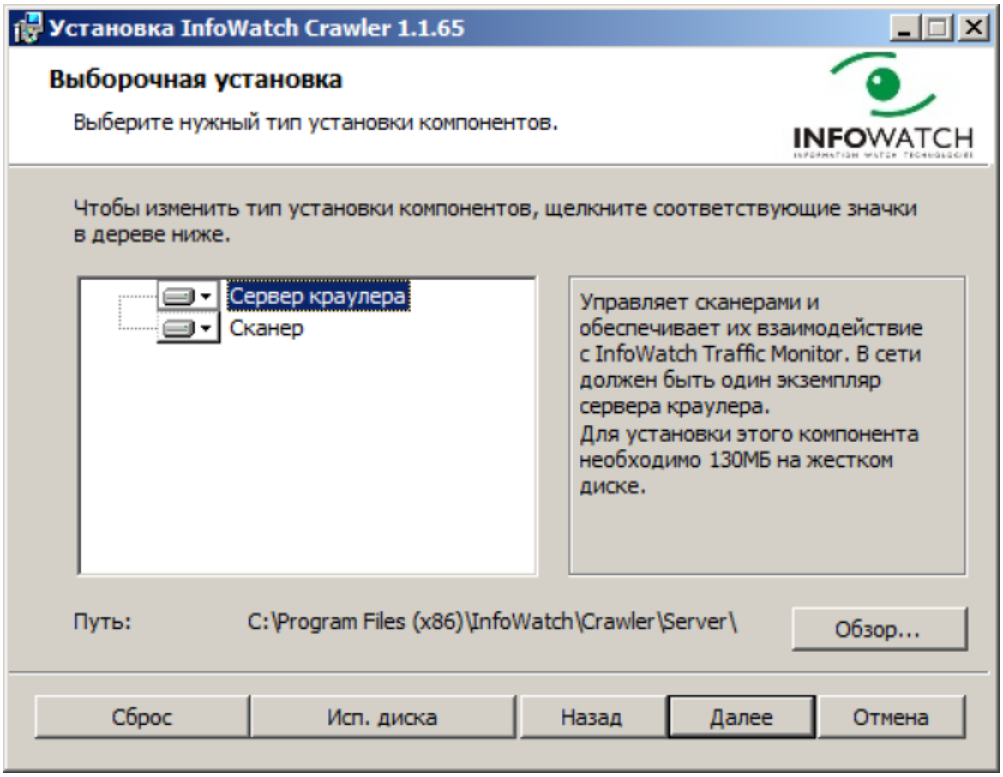
Чтобы установить Краулер:

1. Запустите установочный пакет `Crawler_vx.x.xxx.msi`, где x.x.xxx – номер версии.

   Примечание:

   Язык мастера установки определяется автоматически и зависит от выбранного формата (см. **Пуск -> Панель управления -> Язык и региональные стандарты**, вкладка **Форматы**).

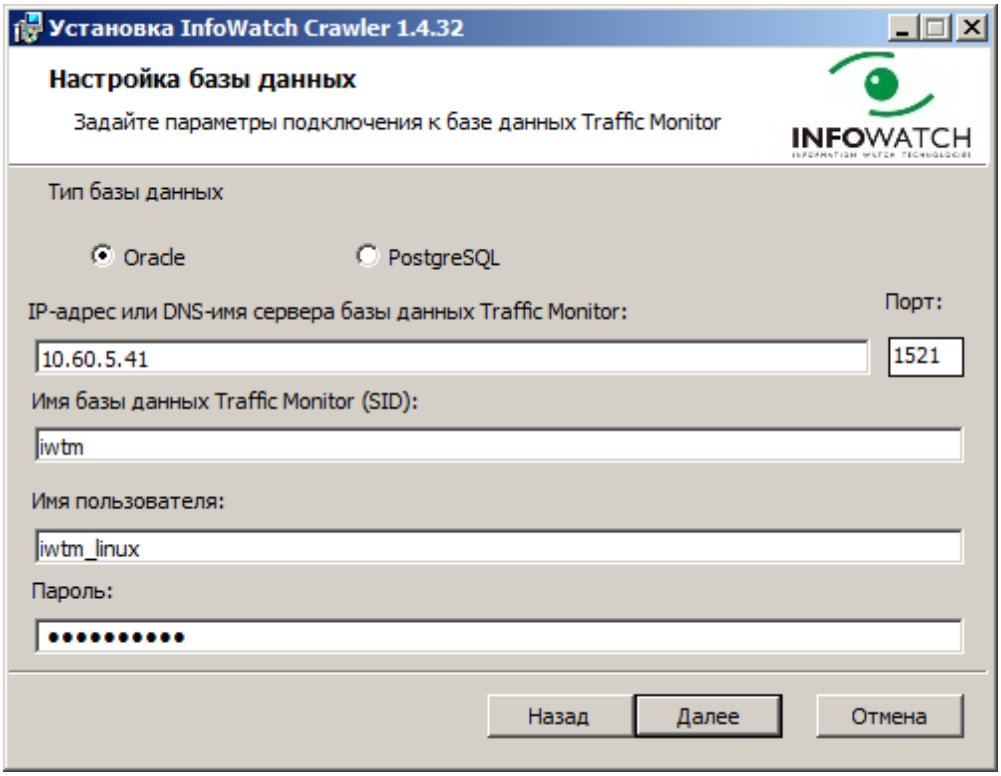
2. В окне приветствия мастера установки InfoWatch Crawler нажмите **Далее**.
3. В окне выбора области установки нажмите **Далее**.
4. На шаге **Выборочная установка** определите, какие компоненты Crawler нужно установить и укажите директорию, в которую будет установлен компонент:
   - **Сервер краулера** – установка службы InfoWatch.Crawler.Server, управляющей заданиями сканирования и обеспечивающей взаимодействие с сервером, базой данных и Консолью управления Traffic Monitor.
   - **Сканер** – установка службы InfoWatch.Crawler.Scaner, осуществляющей сканирование сетевых папок и файловых хранилищ согласно заданным пользователем параметрам.



Если Вы не хотите устанавливать какой-либо из компонентов, выберите его и в раскрывшемся списке отметьте пункт ✕ **Этот компонент будет полностью недоступен**.

Укажите путь к директориям, в которые будут установлены компоненты, и нажмите **Далее**.

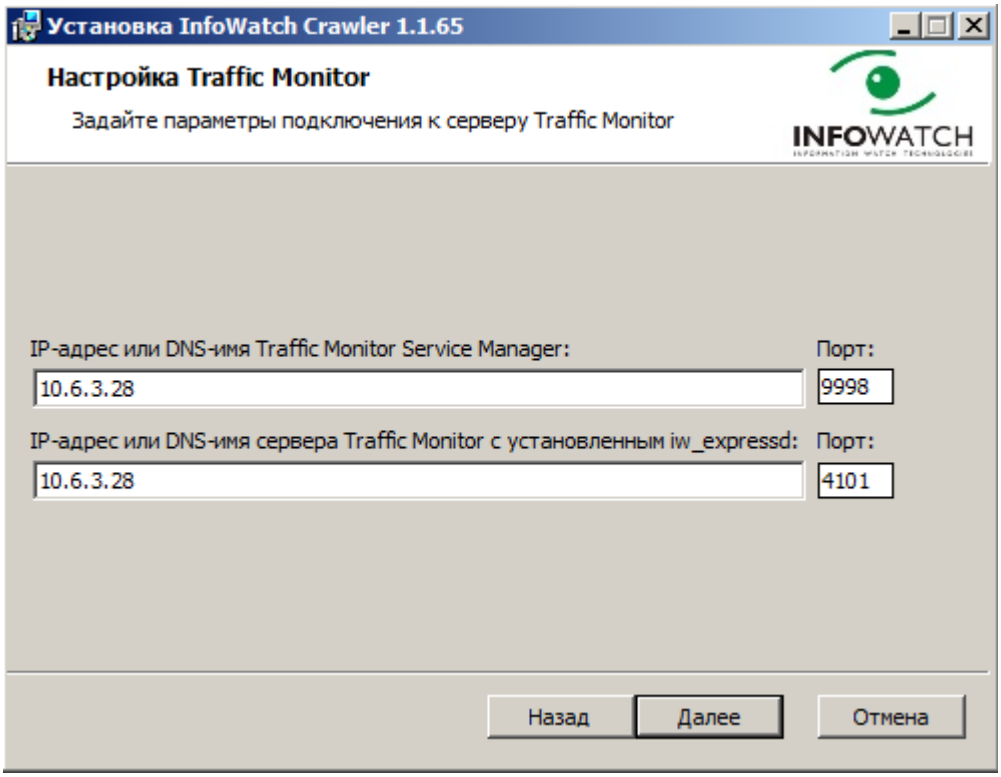
5. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сервер краулера**:
   a. Укажите параметры соединения службы `InfoWatch.Crawler.Server` с базой данных Traffic Monitor, нажмите **Далее**.



В зависимости от используемой СУБД параметры подключения могут различаться:

Параметр	Oracle	PostgreSQL	Пояснения
IP-адрес или DNS-имя	Соответственно используемому серверу БД TM		
Порт	1521	5433	
Имя базы данных	iwtm	postgres	Для PostgreSQL указывается SID или service name.
Имя пользователя	iwtm_linux	iwtm_linux	Пользователь Linux-части СУБД, от имени которого перехваченные объекты будут загружаться в базу данных.
Пароль	xxXX1234	xxXX1234	Если не изменялся после установки серверной части Traffic Monitor.

b. Укажите параметры соединения службы `InfoWatch.Crawler.Server` с сервером Traffic Monitor, нажмите **Далее**.

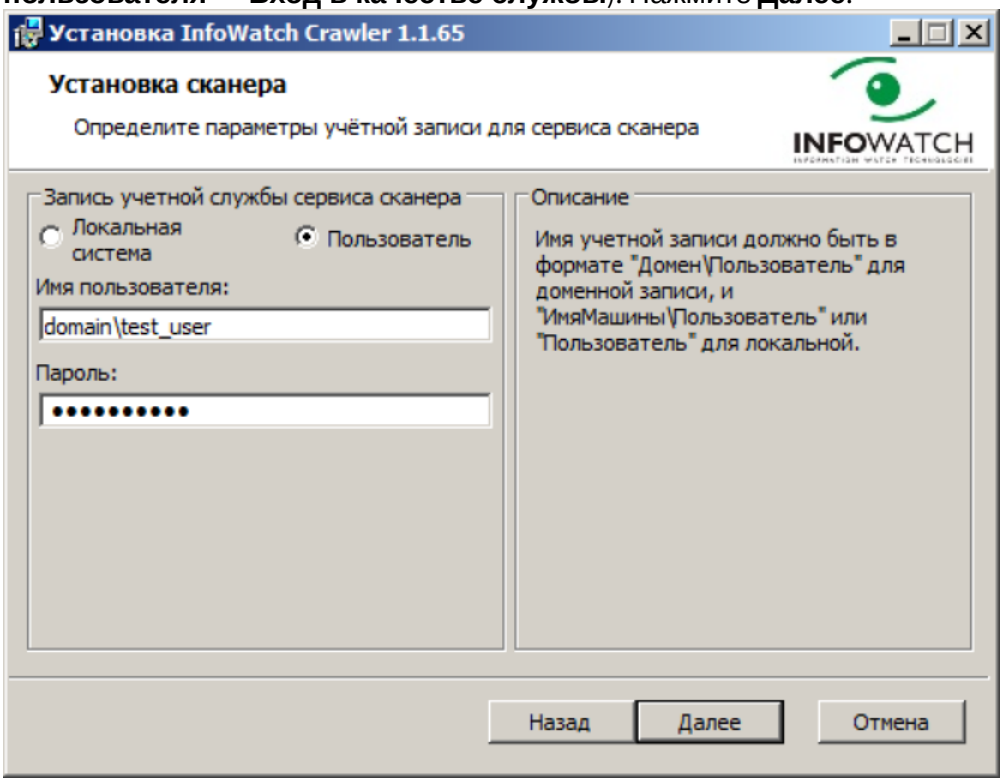


В случае распределенной установки укажите следующие значения:
- в поле **IP-адрес или DNS-имя Traffic Monitor Service Manager** укажите IP-адрес или DNS-имя сервера TM с установленным **iw_serman**;
- в поле **IP-адрес или DNS-имя сервера Traffic Monitor с установленным iw_expressed** укажите IP-адрес или DNS-имя сервера TM (TME Node Server).

После окончания установки запустите сервер Краулера. Для этого выполните следующие действия:

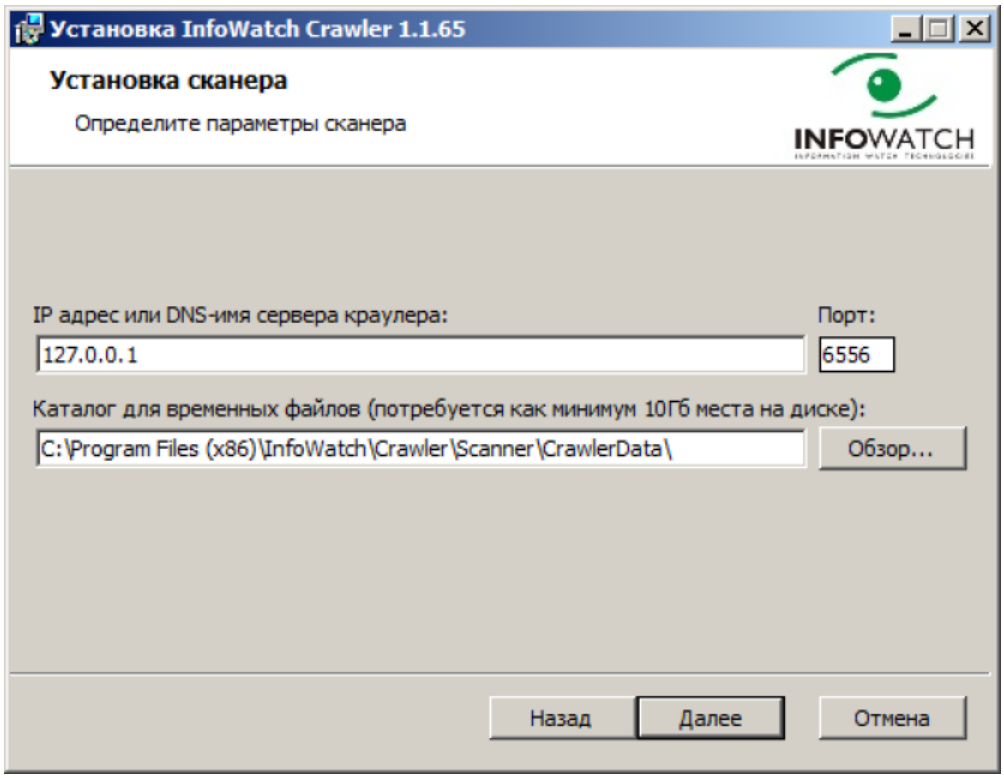
6. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сканер**:
   a. укажите, от имени какой учетной записи будет запускаться служба InfoWatch.Crawler.Scaner. Вы можете выбрать стандартную учетную запись Local System (рекомендуется) или ввести параметры учетной записи, имеющей право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

пользователя –> Вход в качестве службы). Нажмите **Далее**.



b. укажите:
   - IP адрес или DNS имя компьютера, куда установлен компонент **Сервер**;
   - номер порта сервера Краулер;
   - путь к директории, куда сканер будет временно сохранять файлы, скопированные с проверяемых ресурсов.

> **Примечание:**
>
> Если поле **Каталог для временных файлов** оставить пустым, то установщик автоматически выберет последнее использованное в операционной системе значение пути.



7. Нажмите **Далее**.
8. Нажмите **Установить**, чтобы начать установку Краулер. По окончании установки нажмите **Готово**.
9. После установки компонента Сервер запустите его, выполнив следующие действия:
    a. подключитесь к серверу, на котором установлен пакет **iwtm-webgui**;
    b. в файле **web.conf**, расположенном в директории `/opt/iw/tm5/etc`, измените значение параметра `enabled` секции `crawler` с "0" на "1";
    c. выполните команду `service iwtm restart kicker`.

3.3 Установка InfoWatch Device Monitor

Процесс установки выполняется в следующей последовательности:

1. Установка серверной части InfoWatch Device Monitor.
   В состав серверной части входят следующие компоненты:
    - база данных,
    - сервер InfoWatch Device Monitor,
    - консоль управления InfoWatch Device Monitor.
2. Установка агента InfoWatch Device Monitor.
   Агент устанавливается на каждый компьютер, который необходимо контролировать с помощью InfoWatch Device Monitor.

До начала установки убедитесь, что среда, в которой будет развернут InfoWatch Device Monitor, удовлетворяет аппаратным и программным требованиям (см. "Аппаратные и программные требования").

3.3.1 Установка серверной части InfoWatch Device Monitor

Серверная часть InfoWatch Device Monitor устанавливается при помощи универсальной программы установки.
Универсальная программа установки находится на диске с дистрибутивом Device Monitor (каталог `Setup.Unified`). При помощи данной программы можно установить все компоненты, за исключением Агента: базу данных, Сервер Device Monitor и Консоль управления.
Для управления базой данных может использоваться СУБД Microsoft SQL Server, Oracle или PostgreSQL.
Консоль управления может подключаться к основному Серверу.
Подробнее об установке читайте в следующих разделах:

- Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server;
- Рекомендации по развертыванию базы данных под управлением СУБД Oracle;
- Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL;
- Рекомендации по установке Сервера InfoWatch Device Monitor;
- Порядок установки серверной части InfoWatch Device Monitor.

Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server

На компьютере, с которого будет запущен процесс создания базы данных, предварительно должен быть установлен пакет Microsoft .NET Framework 2.0 Service Pack 1, Microsoft .NET Framework 4.0 или выше.
Учетная запись, от имени которой будет создаваться база данных, должна быть подготовлена заранее.
Выбор типа учетной записи зависит от того, какой способ аутентификации вы планируете использовать для подключения к серверу базы данных. В СУБД Microsoft SQL Server поддерживаются два способа аутентификации:

- **Аутентификация Windows**. Аутентификация выполняется с использованием учетных записей, принадлежащих к домену Windows. Данные аутентификации обрабатываются системой безопасности Microsoft Windows.
- **Встроенная в SQL Server**. Используются учетные записи СУБД Microsoft SQL Server. Аутентификация выполняется средствами СУБД.

> **Важно!**
>
> Для обеспечения приемлемого уровня безопасности настоятельно рекомендуется использовать способ **Аутентификация Windows**.

Если вы планируете использовать способ Аутентификация Windows:

1. Убедитесь, что в домене Windows существует учетная запись, от имени которой будет создаваться база данных. Эта учетная запись должна иметь права локального администратора на том компьютере, с которого будет запущен процесс создания базы данных. При необходимости создайте новую учетную запись.
2. Включите учетную запись в состав учетных записей СУБД Microsoft SQL Server, выбрав при этом **Аутентификация Windows**.
3. Назначьте учетной записи роль **dbcreator**.

Если вы планируете использовать способ Встроенная в SQL Server:

1. Создайте новую учетную запись Microsoft SQL Server. При настройке параметров записи: выберите **Встроенная в SQL Server**, задайте имя и пароль.

2. Назначьте учетной записи роль **dbcreator**.

> **Примечание:**
>
> Имя и пароль встроенной учетной записи указывают при настройке параметров базы данных (см. "Порядок установки серверной части InfoWatch Device Monitor", шаг 6).

Рекомендации по развертыванию базы данных под управлением СУБД Oracle

На компьютере, с которого будет запущен процесс создания схемы базы данных, предварительно должны быть установлены:

- пакеты Microsoft .NET Framework 2.0 и Microsoft .NET Framework 4.5
- клиент СУБД Oracle (только после установки пакетов Microsoft .NET Framework 2.0 и Microsoft .NET Framework 4.5)
- провайдер Oracle Database Provider for .NET (ODP.NET)

> **Важно!**
>
> Выбор данного компонента рекомендуется производить путем отметки соответствующего поля при пользовательском типе установки (Custom). Проводить установку необходимо от имени администратора.

Перед тем как начать создание схемы базы данных, убедитесь, что идентификатор соединения с сервером базы данных прописан в файле tnsnames.ora (см. "Настройка параметров соединения с сервером СУБД ORACLE").

Настройка параметров соединения InfoWatch Device Monitor с сервером СУБД Oracle

Для корректного соединения с сервером СУБД Oracle на каждом компьютере, на котором установлен клиент СУБД Oracle, необходимо выполнить настройку файла tnsnames.ora, расположенного в каталоге `[ORACLE_HOME]\network\admin`.

Настройка файла tnsnames.ora

Укажите параметры подключения к серверу СУБД Oracle. Для этого добавьте в файл tnsnames.ora запись следующего вида:

```
tns_name =
 (DESCRIPTION =
 (ADDRESS = (PROTOCOL = TCP)(HOST = host_name)(PORT = port_number))
 (CONNECT_DATA =
 (SERVER = DEDICATED)
 (SERVICE_NAME = service_name)
 )
 )
```

Здесь нужно подставить действительные значения для следующих параметров:

- `tns_name` – псевдоним сервера СУБД Oracle;
- `host_name` – доменное имя или IP-адрес сервера СУБД Oracle;
- `port_number` – порт сервера, на котором запущен процесс прослушивания клиентских подключений;
- `service_name` – имя сервиса базы данных.

Пример записи в файле **tnsnames.ora**:

```
IWDM =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = iwdm.example.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)
```

Важно!

Файл **tnsnames.ora** чувствителен к форматированию. Поэтому, если вы редактируете его, копируя приведенный пример, обратите внимание: в скопированном фрагменте не должно быть пустых строк.

Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL

На компьютере, с которого будет запущен процесс создания базы данных, предварительно должны быть установлены:

- ОС Microsoft Windows Server 2008 R2/2012/2012 R2;
- пакет Microsoft .NET Framework 4.5.2.

Скачайте на официальном сайте PostgreSQL 9.5 и установите с параметрами по умолчанию.

При установке будет создан супер-пользователь postgres, для которого нужно прописать пароль. Информация о нем будет доступна во входящей в комплект установки утилите pgAdmin III в секции "Роли входа".

Примечание:

Для увеличения быстродействия системы рекомендуется устанавливать ОС, серверную часть InfoWatch Device Monitor и СУБД PostgreSQL на разные физические жесткие диски.

Рекомендации по установке Сервера InfoWatch Device Monitor

Для повышения производительности InfoWatch Device Monitor рекомендуется развертывать Сервер и базу данных на отдельных компьютерах.

Сервер Device Monitor и Агент Device Monitor необходимо устанавливать в одном часовом поясе. Это обеспечит отображение корректного времени перехвата события.

Важно!

При развертывании пула из нескольких серверов, на каждом из них должна быть установлена одинаковая версия серверного приложения InfoWatch Device Monitor, соответствующая актуальной версии базы данных.

Чтобы сервер InfoWatch Device Monitor мог устанавливать свои Агенты на мобильные устройства, сервер должен иметь длинное имя. Если используемый сервер не введен в домен Windows, для него требуется настроить FQDN. Для этого:

1. В свойствах системы, на вкладке **Имя компьютера**, нажмите **Изменить**.
2. В диалоговом окне **Изменение имени компьютера или домена** нажмите **Дополнительно**.
3. В поле **Основной DNS суффикс этого компьютера** введите имя домена.
4. Нажмите **ОК**.
5. Убедитесь, что в поле **Полное имя компьютера** отображается длинное имя.

В процессе настройки параметров Сервера (см. "Порядок установки серверной части InfoWatch Device Monitor") необходимо указать учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor. Возможны следующие варианты:

- **Local System**. Запуск службы от имени системной учетной записи.
- **Пользователь**. Запуск службы от имени учетной записи домена Windows.

Для базы данных под управлением СУБД Microsoft SQL Server. Если для аутентификации пользователя, создающего базу данных, выбран способ Аутентификация Windows (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server"), а база данных и Сервер будут находиться на разных компьютерах, то выберите вариант Пользователь.

> **Важно!**
>
> Не рекомендуется выбирать вариант Local System. В этом случае пользователь может получить неограниченные права, что противоречит принципам создания политики безопасности.
>
> Создайте сервисную учетную запись и предоставьте ей права записи в каталог установки сервера DM: `\Program Files\InfoWatch\Device Monitor\Server`

Учетная запись домена Windows (вариант **Пользователь**) должна быть подготовлена заранее. Для этого выполните следующие действия:

1. Разрешите учетной записи запускать процесс как службу. Для этого:
   - В **Панели управления** откройте компонент **Администрирование > Локальная политика безопасности**.
   - В открывшемся диалоговом окне выберите узел **Локальные политики > Назначение прав пользователя**.
   - Справа в области сведений дважды щелкните право **Вход в качестве службы**.
   - На вкладке **Параметр локальной безопасности** добавьте подготовленную учетную запись.

- Включите учетную запись в состав учетных записей СУБД Microsoft SQL Server.
  По окончании установки предоставьте учетной записи доступ к созданной базе данных. При выборе разрешения на доступ к базе данных укажите роль **db_owner**.

Порядок установки серверной части InfoWatch Device Monitor

> **Важно!**
>
> Перед началом установки ознакомьтесь с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor".

Важно!

При развертывании пула из нескольких серверов, на каждом из них должна быть установлена одна и та же версия серверного приложения InfoWatch Device Monitor, соответствующая актуальной версии базы данных.

1. **Запуск мастера установки**
   Вставьте диск с дистрибутивом Device Monitor в дисковод. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы.
   В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите **Далее**.
2. **Принятие лицензионного соглашения**
   Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите **Далее**.
3. **Выбор устанавливаемого компонента**
   На шаге **Выборочная установка** по умолчанию выбраны все компоненты:
   - Сервер
   - Консоль управления
   - Модуль MSM (Тайга) - компонент, обеспечивающий возможность установки Агента Device Monitor на мобильные устройства (подробнее см. " *Infowatch Traffic Monitor. Руководство пользователя* ", раздел "Мобильные устройства"). Может быть установлен и использован только вместе с Консолью управления.

   Если необходимо, измените состав устанавливаемых компонентов. Так, например, если вы рассчитываете использовать Консоль управления на другой рабочей станции, то вам не нужно устанавливать этот компонент: нажмите **Консоль управления** и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**.
   Вы также можете изменить папку, куда будет установлен тот или иной компонент: выберите компонент в списке, нажмите и укажите другое местоположение.
   Нажмите **Далее**.
4. **Определение параметров сервера**
   На шаге **Тип устанавливаемого сервера** выберите:
   - **Основной сервер** – должен быть установлен первым. К нему будут подключаться Агенты и Консоль управления.
   - **Вспомогательный сервер** – дополнительный сервер, обеспечивающий балансировку нагрузки от Агентов.

     Важно!

     Изменение имени сервера Device Monitor после установки может привести к перебоям в работе Системы.

> **Примечание**
>
> Установка вспомогательного сервера возможна только после установки основного на отдельный компьютер. Установка вспомогательного сервера описана в пункте 14.

Для обеспечения быстрой актуализации информации о серверах, рекомендуется отметить **Опубликовать сервер в Active Directory**.

> **Важно!**
>
> Актуализируя политики безопасности, компьютеры периодически взаимодействуют с сервером Device Monitor. Поэтому, чтобы вновь добавленный сервер мог сразу же приступить к обслуживанию компьютеров, а также для своевременного уведомления Агентов о возможных изменениях портов серверов, рекомендуется при установке сервера публиковать его данные в домене.
> Для публикации данных сервера Device Monitor в домене, учетной записи, от имени которой выполняется установка сервера, требуются права на создание и удаление точек подключения.

Если у вас есть СУБД со схемой БД Device Monitor того же номера версии, что устанавливается на сервер, снимите отметку **Установить новую базу данных** . Нажмите **Далее** .

5. **Файл для импорта элементов конфигурации**

   Если установка новой базы данных не производится, этот шаг будет пропущен. Чтобы использовать ранее экспортированный файл конфигурации сервера (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Импорт/экспорт настроек и схемы безопасности"), нажмите **Выбрать** и укажите место расположения файла конфигурации.

   > **Важно!**
   >
   > Файл конфигурации должен быть расположен на локальном диске или внешнем носителе. Расположение в сетевой папке программой установки не поддерживается.

   Нажмите **Далее** .
6. **Выбор сервера базы данных**
   Укажите СУБД, под управлением которой будет находиться база данных Device Monitor, выбрав один из следующих вариантов:
   - Microsoft SQL Server

- Oracle
- PostgreSQL

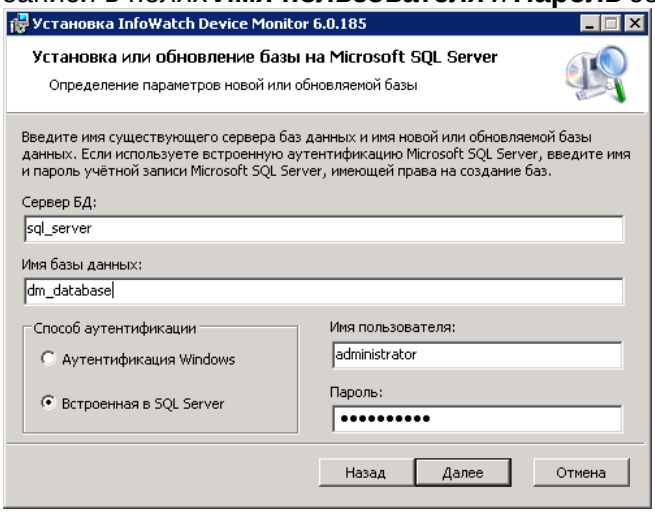
Если на Шаге 4 вы решили использовать уже существующую базу данных (опция **Установить новую базу данных** не была выбрана), то вам будет необходимо дополнительно указать параметры соединения с существующей базой данных Device Monitor.
Нажмите **Далее**.

7. **Настройка базы данных**
Этот шаг будет пропущен, если на Шаге 4 вы решили использовать уже существующую базу данных.
Принцип настройки базы данных зависит от типа используемой СУБД.
При использовании СУБД Microsoft SQL Server укажите следующие параметры:
   - **Сервер БД**. NetBIOS имя сервера СУБД Microsoft SQL Server, на котором будет создана база данных.

Не задавайте в поле **Сервер БД** IP-адрес, так как в этом случае вы не сможете подключиться к серверу базы данных.
Если на сервере базы данных есть именованные экземпляры, то имя сервера нужно указывать в следующем виде: `<имя_сервера>\<имя_экземпляра>`.
   - **Имя базы данных**. Имя создаваемой базы данных.

Может содержать буквы латинского алфавита, цифры и прочие символы, за исключением пробелов и специальных символов: «*», «?», «/», «\», «|», «^», «:», «"». Должно начинаться с латинской буквы.
Длина имени может составлять от 1 до 123 символов.
   - **Способ аутентификации**. Способ аутентификации пользователя, от имени которого создается база данных и который будет использоваться для работы с БД. В качестве значения данного параметра укажите способ аутентификации, выбранный при подготовке учетной записи (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server").

Если учетной записи назначена аутентификация Windows, то выберите значение **Аутентификация Windows**. В этом случае процесс создания БД будет выполняться от имени доменного пользователя, выполняющего установку.
Если учетной записи назначена встроенная в SQL Server аутентификация, выберите значение Встроенная в SQL Server. Затем укажите имя и пароль подготовленной учетной записи в полях **Имя пользователя** и **Пароль** соответственно.



При использовании СУБД Oracle настройте следующие параметры:

a. В области **Сервер БД** задайте параметры соединения с сервером базы данных:
- **Сервер**. Имя сервера базы данных. В качестве значения данного параметра указывают псевдоним сервера из файла tnsnames.ora.
- **Пароль для 'SYSTEM'**. Пароль учетной записи пользователя SYSTEM.

b. В области **Данные о схеме** укажите параметры учетной записи владельца создаваемой схемы базы данных:

> **Важно!**
>
> Не рекомендуется указывать параметры существующей схемы базы данных.

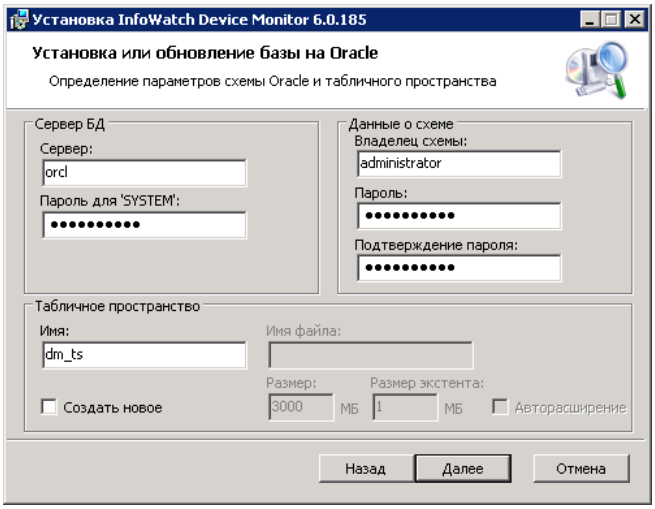
- **Владелец схемы**. Имя учетной записи владельца схемы базы данных.
- **Пароль, Подтверждение пароля**. Пароль учетной записи владельца схемы базы данных.

Назначение пароля выполняется в соответствии с требованиями, указанными в документации к СУБД Oracle.

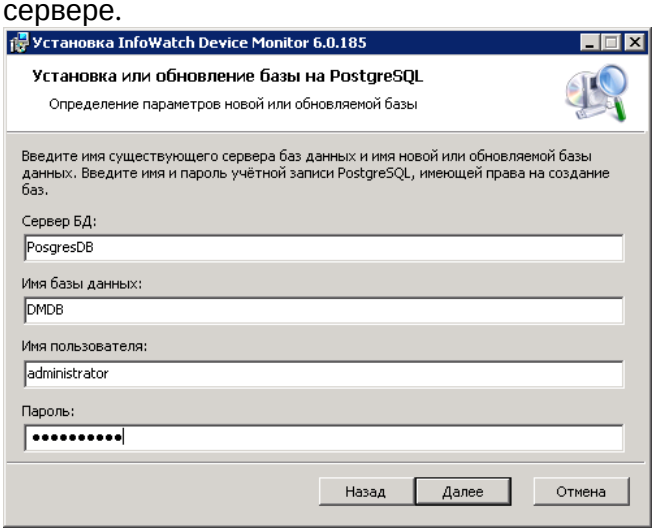
c. Настройте параметры табличного пространства в области **Табличное пространство**.

Вы можете использовать существующее табличное пространство или создать новое. При использовании существующего табличного пространства, укажите имя табличного пространства в поле **Имя**.

Чтобы создать новое табличное пространство, отметьте поле **Создать новое**. Затем укажите параметры табличного пространства:
- **Имя**. Имя нового табличного пространства.
- **Имя файла**. Имя файла данных, в котором будет храниться новое табличное пространство.
- **Размер**. Максимальный размер (в МБ) файла данных (значение по умолчанию - 3000 МБ).
- **Размер экстента**. Максимальный размер (в МБ) непрерывного фрагмента пространства в файле данных (значение по умолчанию - 1 МБ).
- **Авторасширение**. Возможность автоматического расширения файла данных средствами СУБД Oracle. Если отмечено поле **Авторасширение**, то функция авторасширения будет включена (по умолчанию данная функция отключена).



При использовании СУБД PostgreSQL укажите следующие параметры:
- **Сервер БД**. Имя сервера СУБД PostgreSQL, на котором будет создана база данных. Порт по умолчанию - 5432. Если будет использовать другой порт, необходимо его задать в формате `host:port`.
- **Имя базы данных**. Имя создаваемой базы данных.Может содержать буквы латинского алфавита, цифры и прочие символы, за исключением пробелов и специальных символов: «*», «?», «/», «\», «|», «^», «:», «"». Должно начинаться с латинской буквы.Длина имени может составлять от 1 до 123 символов.
- **Имя пользователя** - имя учетной записи, имеющей права на создание БД на PostgreSQL сервере.
- **Пароль** - пароль учетной записи, имеющей права на создание БД на PostgreSQL сервере.



После того как все необходимые параметры будут заданы, нажмите **Далее**.

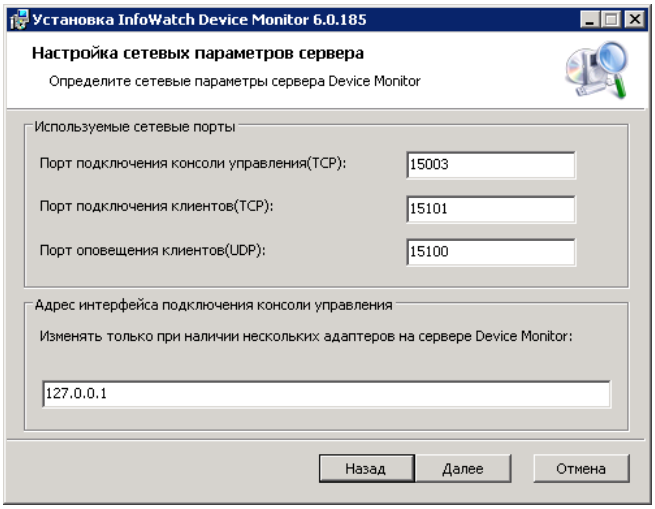
8. **Настройка сетевых параметров сервера**

   Настройте параметры Сервера:
   a. В области **Используемые сетевые порты** задайте номера TCP и UDP портов, используемые для:
      - **подключения Консоли управления**;
      - **подключения Агентов** для передачи схем безопасности на контролируемые

компьютеры, отправки информации о событиях и теневых копий на сервер;
- **оповещения Агентов** об изменениях схем безопасности.

b. В области **Адрес интерфейса подключения консоли управления** укажите IP-адрес, через который будет осуществляться взаимодействие между Сервером и Консолью управления.

> **Важно!**
>
> Изменять значение данного параметра следует, только если Сервер будет установлен на компьютер с несколькими сетевыми адаптерами, подключенными к разным сетям. При наличии одного сетевого адаптера не допускается изменение данного параметра, иначе подключение Консоли управления к Серверу будет невозможно.
> Если в процессе работы на компьютер с установленным Сервером будут добавлены дополнительные сетевые адаптеры, то изменить настройку данного параметра можно в конфигурационном файле Сервера.



После того как все необходимые параметры будут указаны, нажмите **Далее**.

9. **Настройка защищенного канала**

Укажите порт, по которому будут передаваться трафик между Агентом и Сервером InfoWatch Device Monitor.

Если на Шаге 4 вы выбрали **Установить новую базу данных**, то в области **Ключ защищенного канала** выберите:

- если установка выполняется впервые - оставьте настройку **Создать новый ключ**;
- если вы использовали сервер версии 6.0 и выше и удалили его, а затем хотите опять установить, то для того, чтобы Агенты Device Monitor смогли подключиться и привязаться к новому серверу, необходимо указать ключ шифрования, который использовался на старом сервере. Рекомендации о сохранении ключа шифрования даны в разделе "Удаление InfoWatch Device Monitor". Выберите **Использовать существующий ключ** и укажите путь к файлу с имеющимся ключом шифрования.

Нажмите **Далее**.

Если была выбрана настройка **Создать новый ключ**, укажите путь, куда Система сохранит файл со сгенерированным ключом.

10. **Настройка учетной записи сервера**

    Выберите учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor, в соответствии с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor". При выборе варианта **Пользователь** укажите имя и пароль подготовленной учетной записи домена Windows. Имя задается в формате `DOMAIN\USERNAME`.
    Нажмите **Далее**.
11. **Настройка учетной записи администратора сервера**

    Укажите данные (имя и пароль) учетной записи администратора сервера. Данной учетной записи будет присвоена роль **Суперпользователь** (подробнее см. " *Infowatch Traffic Monitor. Руководство пользователя* ", статья "Управление учетными записями Консоли управления"): она используется при первом подключении к Серверу с помощью Консоли управления.
    Нажмите **Далее** .

12. **Настройка параметров соединения с сервером InfoWatch Traffic Monitor**

    Если на Шаге 4 вы решили использовать уже существующую базу данных (опция **Установить новую базу данных** не была выбрана), то этот шаг будет пропущен.
    Укажите параметры для взаимодействия с сервером InfoWatch Traffic Monitor:
    - Адрес сервера TM. Адрес сервера InfoWatch Traffic Monitor. Запись адреса должна иметь следующий формат:
      `host:port`
      Параметр host должен содержать доменное имя или IP-адрес сервера InfoWatch Traffic Monitor. Адрес сервера является стандартным URI-адресом (Uniform Resource Identifier), формальный синтаксис которого описан в RFC 3986 http://tools.ietf.org/html/rfc3986.
      В качестве параметра *port* указывается порт сервера InfoWatch Traffic Monitor, через который будет осуществляться доставка событий. По умолчанию, порт сервера InfoWatch Traffic Monitor – 9100.

      > **Важно!**
      >
      > Если планируется интеграция с Traffic Monitor версии 5.5 или ниже, используйте формат `host:port`, где `port` - 4101.

    - Количество соединений. Количество соединений с сервером InfoWatch Traffic Monitor. Вы можете задать значение от 1 до 32 соединений.
      - **Токен авторизации**. Токен для подключения к API. Необходимо указывать при работе с Traffic Monitor версии 6.0 и выше. Получите актуальный токен от администратора Traffic Monitor.
      - если в схеме развертывания Device Monitor не планируется интеграция с InfoWatch Traffic Monitor, отметьте поле **Работать в автономном режиме**. В этом случае вы можете, отметив поле **Сохранять теневые копии**, сохранять перехваченные теневые копии файлов в директорию установки сервера.

Нажмите **Далее**.

13. **Завершение установки**

Нажмите **Установить**, чтобы начать установку Сервера.
В процессе установки будет запрошено разрешение на установку программного обеспечения Taiga System. Разрешение необходимо для установки драйверов, обеспечивающих поддержку контроля мобильных устройств. Нажмите **Установить**: в противном случае работа мастера установки будет завершена и произойдет полный откат установки.

> **Примечание.**
>
> Данное сообщение будет выведено, если на Шаге 3 "Выбор устанавливаемого компонента" был выбран компонент Модуль MSM (Тайга).

Следуйте указаниям для завершения установки.

> **Важно!**
>
> При установке на Microsoft Windows Server 2012 и Microsoft Windows Server 2012 R2, на экран будет выведено диалоговое окно **Windows Security**, которое устанавливает виртуальный принтер InfoWatch, необходимый для обработки печати из metro-приложений. Для установки виртуального принтера нажмите **Install**.

> **Примечание.**
>
> Этап установки сигнатур может занимать существенное время (до получаса).

14. **Установка вспомогательного сервера**

Работа вспомогательного сервера связана с основным, и настройки основного распространяются на вспомогательный сервер, что гарантирует принцип соединения серверов Device Monitor.

a. Запуск мастера установки
   Вставьте диск с дистрибутивом Device Monitor в дисковод. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы. В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите **Далее**.
b. Принятие лицензионного соглашения
   Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите **Далее**.

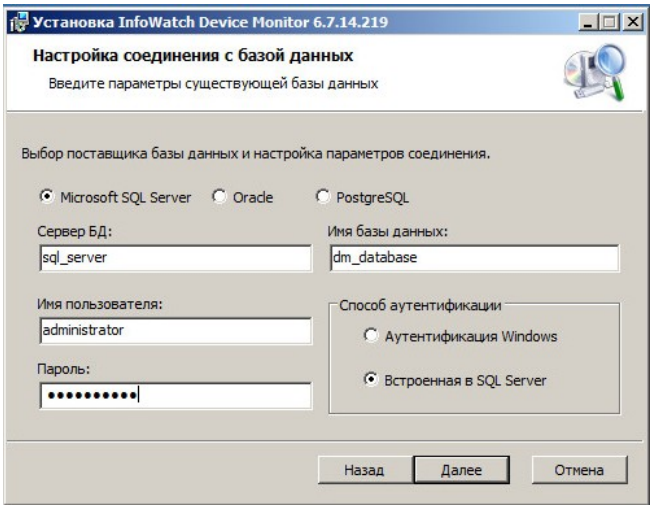
c. Выбор устанавливаемого компонента
На шаге **Выборочная установка** по умолчанию выбраны все компоненты:
- Сервер
- Консоль управления
- Модуль MSM (Тайга) - компонент, обеспечивающий возможность установки Агента Device Monitor на мобильные устройства (подробнее см. "*Infowatch Traffic Monitor . Руководство пользователя*", раздел "Мобильные устройства"). Может быть установлен и использован только вместе с Консолью управления.

Если необходимо, измените состав устанавливаемых компонентов. Так, например, если вы рассчитываете использовать Консоль управления на другой рабочей станции, то вам не нужно устанавливать этот компонент: нажмите **Консоль управления** и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**.
Вы также можете изменить папку, куда будет установлен тот или иной компонент: выберите компонент в списке, нажмите и укажите другое местоположение.
Нажмите **Далее**.

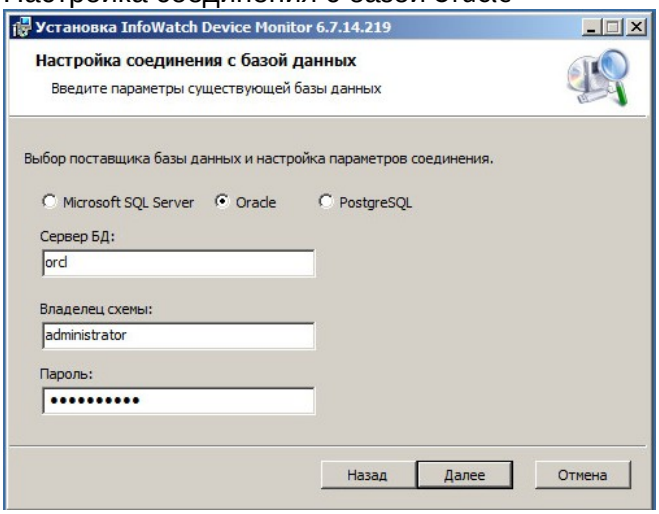
d. Определение параметров сервера
На шаге **Тип устанавливаемого сервера** выберите **Вспомогательный сервер**.

> **Важно!**
>
> Установка вспомогательного сервера не позволяет установить новую базу данных, поэтому следует указать параметры существующей базы данных.

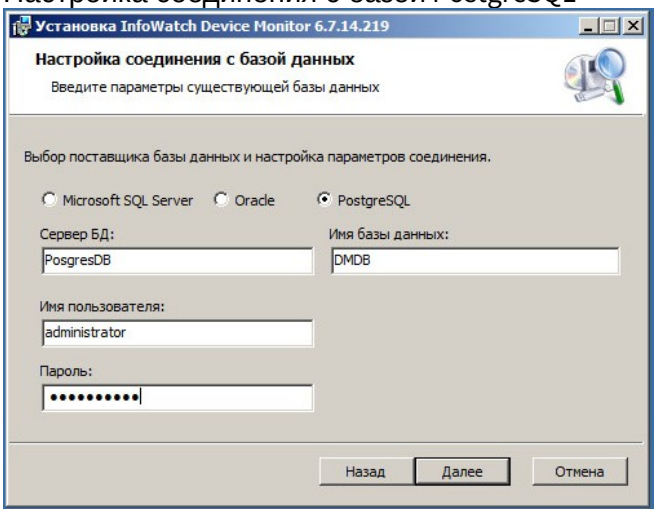
e. Настройка соединения с базой данных
Укажите СУБД, под управлением которой находится база данных Device Monitor и введите оставшиеся параметры соединения такими же, которые были использованы при установке основного сервера:
Настройка соединения с базой Microsoft SQL Server
Если учетной записи назначена аутентификация Windows, и база данных была создана от имени доменного пользователя, то выберите значение **Аутентификация Windows .** Если учетной записи назначена встроенная в SQL Server аутентификация, выберите значение **Встроенная в SQL Server** :



Настройка соединения с базой Oracle



Настройка соединения с базой PostgreSQL



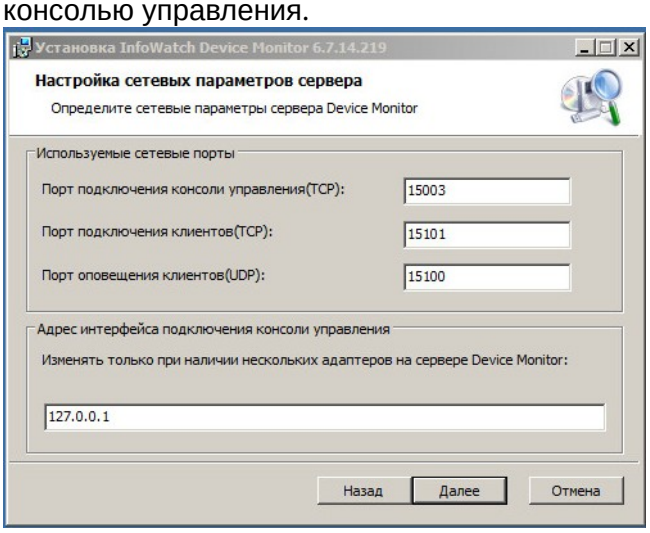
После того как все необходимые параметры будут указаны, нажмите **Далее**.

f. Настройка сетевых параметров сервера

Настройте параметры сервера:

В области **Используемые сетевые порты** задайте номера TCP и UDP портов,

используемых для:
- подключения Консоли управления;
- подключения Агентов для передачи схем безопасности а контролируемые компьютеры, отправки информации о событиях и теневых копий на сервер;
- оповещения Агентов об изменениях схем безопасности.
В области **Адрес интерфейса подключения консоли управления** укажите IP-адрес, через который будет осуществляться взаимодействие между сервером и консолью управления.



После того как все необходимые параметры будут указаны, нажмите **Далее**.

g. Настройка учетной записи сервера
Выберите учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor, в соответствии с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor". При выборе варианта **Пользователь** укажите имя и пароль подготовленной учетной записи домена Windows. Имя задается в формате `DOMAIN\USERNAME`.
Нажмите **Далее**.

h. Завершение установки
Нажмите **Установить**, чтобы начать установку сервера. В процессе установки будет запрошено разрешение на установку программного обеспечения Taiga System. Разрешение необходимо для установки драйверов, обеспечивающих поддержку контроля мобильных устройств. Нажмите **Установить**: в противном случае работа мастера установки будет завершена и произойдет полный откат установки.

> **Примечание**
>
> Данное сообщение будет выведено, если на шаге 3 "Выбор устанавливаемого компонента" был выбран компонент Модуль MSM (Тайга).

Следуйте указаниям для завершения установки. Этап установки сигнатур может занять некоторое время.

3.3.2 Установка Агента InfoWatch Device Monitor

Агент Device Monitor и Сервер Device Monitor необходимо устанавливать в одном часовом поясе. Это обеспечит отображение корректного времени перехвата события.

> **Важно!**
>
> Не допускается установка Агента InfoWatch Device Monitor и сервера Device Monitor на один компьютер, это может привести к неработоспособности сервера.

Агент InfoWatch Device Monitor может быть установлен на рабочие станции одним из следующих способов:

- Локальная установка. Выполняется при помощи универсальной программы установки непосредственно на каждом компьютере.
- Удаленная установка с помощью стороннего ПО. Осуществляется с использованием средств распространения программного обеспечения: например, посредством механизма групповых политик Microsoft Active Directory.
- Удаленная, через задачи распространения в Консоли управления InfoWatch Device Monitor (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", раздел "Удаленная установка, обновление и удаление Агентов").

Установка Агента InfoWatch Device Monitor на мобильные устройства выполняется при добавлении этого устройства в схему безопасности (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", статьи "Добавление мобильного устройства через назначение сотруднику" и "Добавление мобильного устройства в группу компьютеров").

Чтобы успешно установить или обновить Агент InfoWatch Device Monitor, следуйте рекомендациям:

1. Исключите параллельное использование сторонних DLP-систем;
2. Добавьте в исключения антивируса процессы Агента InfoWatch Device Monitor (список файлов см. в статье "Список файлов Агента InfoWatch для добавления в исключения антивирусов");
3. Отключите самозащиту антивируса;
4. По возможности отключите или удалите антивирус на время установки, обновления и удаления Агента InfoWatch Device Monitor;
5. Обеспечьте доступ к портам, необходимым для работы Агента InfoWatch Device Monitor (список портов см. в "*Infowatch Traffic Monitor. Руководство администратора*", раздел "Настройка Сервера InfoWatch Device Monitor");
6. Если не требуется использовать компонент контроля сетевых соединений, отключите его при создании дистрибутива Агента InfoWatch Device Monitor;
7. Установите Агенты InfoWatch Device Monitor сначала тестовые машины или на небольшую группу рабочих станций;
   Если на тестовой группе в течение 2-3 дней не возникало ошибок, снижения производительности, зависания приложений, продолжайте установку на рабочие станции.

Важно!

Выключение питания компьютера в процессе установки/удаления Агента может привести к ошибкам, ведущим к нестабильной работе операционной системы.

Важно!

В процессе установки Агента будут закрыты (если они были запущены) программы Mozilla Firefox и Mozilla Thunderbird.

Локальная установка Агента

Важно!

Настоятельно не рекомендуется устанавливать Агенты InfoWatch Device Monitor на компьютеры с одинаковыми именами. Такие компьютеры будут зарегистрированы как один компьютер и, соответственно, на них будет распространяться одна политика, будет вестись единая регистрация событий и т.д.

Установку Агента может выполнять пользователь, имеющий права локального администратора на том компьютере, на который выполняется установка.

1. **Запуск мастера установки**

   Вставьте диск с дистрибутивом Системы в дисковод для компакт-дисков. Затем откройте каталог `Client`. В данном каталоге найдите и запустите файл установки для требуемой платформы.
   В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor Client. Нажмите на кнопку **Далее**, чтобы перейти к следующему окну мастера установки.

2. **Выбор каталога для установки**

   Укажите путь к каталогу, в который будет установлен **Агент**.

   Важно!

   Путь к каталогу может содержать следующие символы: 0-9,a-z,A-Z, ":", ".", "_", "-", "\", " ". При наличии в пути других символов, установка Агента будет некорректной.

   Нажмите кнопку **Далее**.

3. **Настройка параметров**

   Укажите параметры соединения с Сервером InfoWatch Device Monitor:

- **Сервер**. Имя сервера InfoWatch Device Monitor.
- **Порт**. Номер порта, используемого для соединения между Агентом и Сервером InfoWatch Device Monitor (по умолчанию задан порт 15101).

Нажмите кнопку **Далее**.

4. **Завершение установки**

   После перехода к окну **Подтверждение установки**, нажмите кнопку **Далее,** чтобы начать установку Агента. Следуйте дальнейшим указаниям мастера для завершения установки. По окончании установки перезагрузите компьютер.

Установка Агента с помощью средств распространения программного обеспечения

Установка Агента на компьютеры может выполняться администратором корпоративной сети централизованно, с помощью средств распространения программного обеспечения. В настоящем разделе описывается пример такой установки посредством Microsoft Active Directory.

Установка Агента через Microsoft Active Directory осуществляется посредством механизма групповых политик. Для установки необходимо выбрать такую групповую политику, которая распространяется на все компьютеры, подлежащие контролю при помощи Агента. Это может быть политика, назначенная:

- контейнеру Active Directory, содержащему все компьютеры, на которые будет выполняться установка Агента.
- всему домену Active Directory, но не являющаяся доменной политикой по умолчанию (*Default Domain Policy*). Распространение этой политики должно быть назначено только той группе, которая включает в себя все компьютеры, подлежащие контролю при помощи Агента.

1. **Создание инсталляционного комплекта**

   Создайте установочный msi-пакет `Setup.Client.ru.msi` (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Создание пакета установки"). Разместите установочный пакет в сетевом каталоге, доступном для чтения всем компьютерам домена, на которые будет установлен Агент.

2. **Отключение быстрого входа в систему Microsoft Windows XP Professional**

   Перед установкой Агента через механизм групповых политик необходимо отключить оптимизацию быстрого входа в систему для компьютеров, на которых установлена операционная система Microsoft Windows XP Professional (так называемый асинхронный режим входа в систему). Подробная информация об этой функции доступна в базе знаний Microsoft (см. KB305293).

   Чтобы отключить функцию оптимизации быстрого входа в систему:
   a. Откройте редактор используемой групповой политики.
   b. В дереве консоли выберите каталог **Computer Configuration** > **Administrative templates** > **System** > **Logon**. В области сведений выберите параметр **Always wait for the network at computer startup and logon**. Затем в окне свойств данного параметра установите значение **Enabled**.

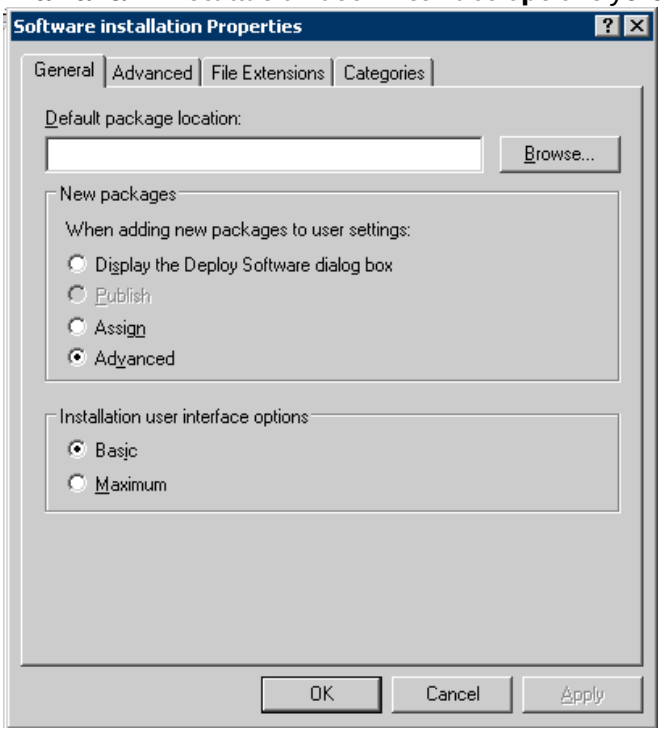
> **Примечание:**
>
> Если данная функция не отключена, то для установки Агента потребуется еще одна дополнительная перезагрузка, связанная с механизмом распространения групповой политики Windows.

3. **Редактирование групповой политики**

   Перед установкой Агента средствами Active Directory необходимо отредактировать используемую групповую политику.

   Чтобы отредактировать групповую политику:

   a. Откройте оснастку **Active directory users and computers** (**Start** > **Settings** > **Control Panel** > **Administrative tools** > **Active directory users and computers**).
   b. В дереве консоли выберите контейнер Active Directory, содержащий все компьютеры, на которые будет выполняться установка Агента.
   c. Откройте оснастку **Group Policy**. Для этого в контекстном меню контейнера Active Directory выберите команду **Properties**. Затем в открывшемся диалоговом окне перейдите на вкладку **Group policy**. На данной вкладке выберите объект групповой политики и нажмите на кнопку **Edit**.
   d. В дереве консоли выберите расширение **Software Installation** (**Computer Configuration** > **Software Settings**).
   e. В контекстном меню расширения **Software Installation** выберите команду **Properties**. В открывшемся диалоговом окне на вкладке General выполните следующие настройки (см. рисунок):
   - на панели **New packages** установите значение **Advanced**;
   - на панели **Installation user interface options** установите значение **Basic**.



f. По окончании настройки нажмите на кнопку **OK**.

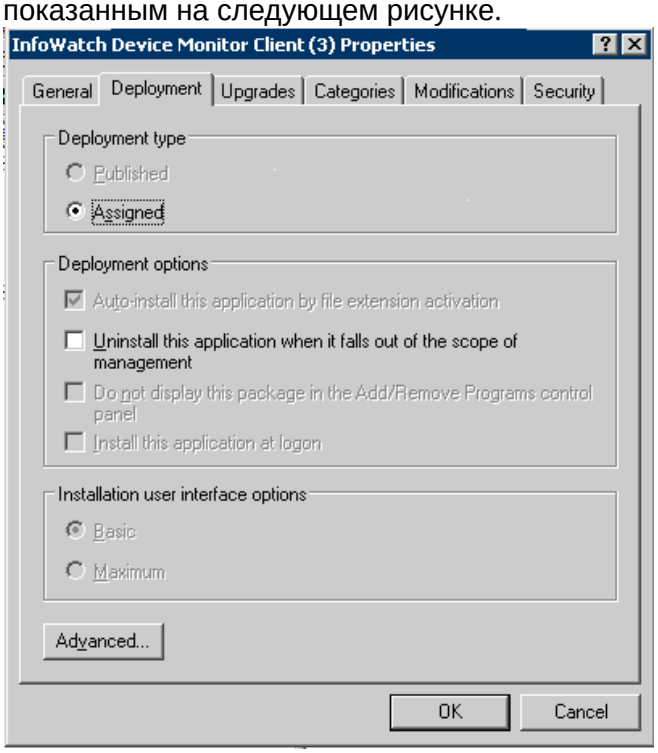
4. **Подготовка задания на установку Агента**

Создание и настройка задания на установку Агента выполняется в окне **Group Policy Object Editor**:

a. После того как окно **Group Policy Object Editor** будет открыто, в дереве консоли выберите расширение **Software Installation** (**Computer Configuration** > **Software Settings**). Щелкните правой кнопкой мыши по названию выделенного пункта и в раскрывшемся контекстном меню выберите пункт **New** > **Package**.

b. В открывшемся диалоговом окне **Open** укажите установочный msi-пакет клиентского модуля `Setup.Client.ru.msi` (установочный пакет должен быть предварительно размещен в сетевом каталоге, доступном для чтения всем компьютерам домена, на которые будет установлен Агент).

c. Выполните настройку свойств нового пакета:
- Убедитесь, что установки, заданные на вкладке **Deployment**, соответствуют показанным на следующем рисунке.



- После того как все необходимые настройки будут заданы, нажмите на кнопку **OK**.

d. В дереве консоли выберите каталог **Computer Configuration** > **Administrative templates** > **System** > **Scripts**. В области сведений выберите параметр **Run logon scripts synchronously**. Затем в окне свойств данного параметра установите значение **Enabled**.

5. **Выполнение установки**

Добавленное задание отображается в списке заданий оснастки **Software Installation**. Задание выполняется при первой перезагрузке компьютера, на который должен быть установлен Агент. Запуск службы InfoWatch Device Monitor Client осуществляется автоматически сразу после установки.

Способ установки отображается в столбце **Deployment state**. Состояние **assigned** означает, что установка осуществляется принудительно, т.е. без учета мнения пользователя, работающего за компьютером, на который выполняется установка Агента. Состояние **published** соответствует установке с запросом согласия от пользователя.

Важно!

Вы можете проверить успешность установки Агента в Консоли управления InfoWatch Device Monitor. Все компьютеры, на которые Агент был успешно установлен, должны отображаться в списке раздела **Группы компьютеров**. Чтобы просмотреть список всех контролируемых компьютеров, воспользуйтесь кнопкой **Показать все компьютеры**, расположенной в верхней части Панели навигации. Чтобы получить актуальные сведения об установленных Агентах, воспользуйтесь кнопкой **Обновить**, расположенной на панели инструментов.

Примечание:

При отключении протокола SMB1 на компьютерах с ОС Windows XP централизованное обновление Агента возможно лишь путем создания пакетов установки с их последующей инсталляцией средствами групповых политик, либо при помощи агента распространения.

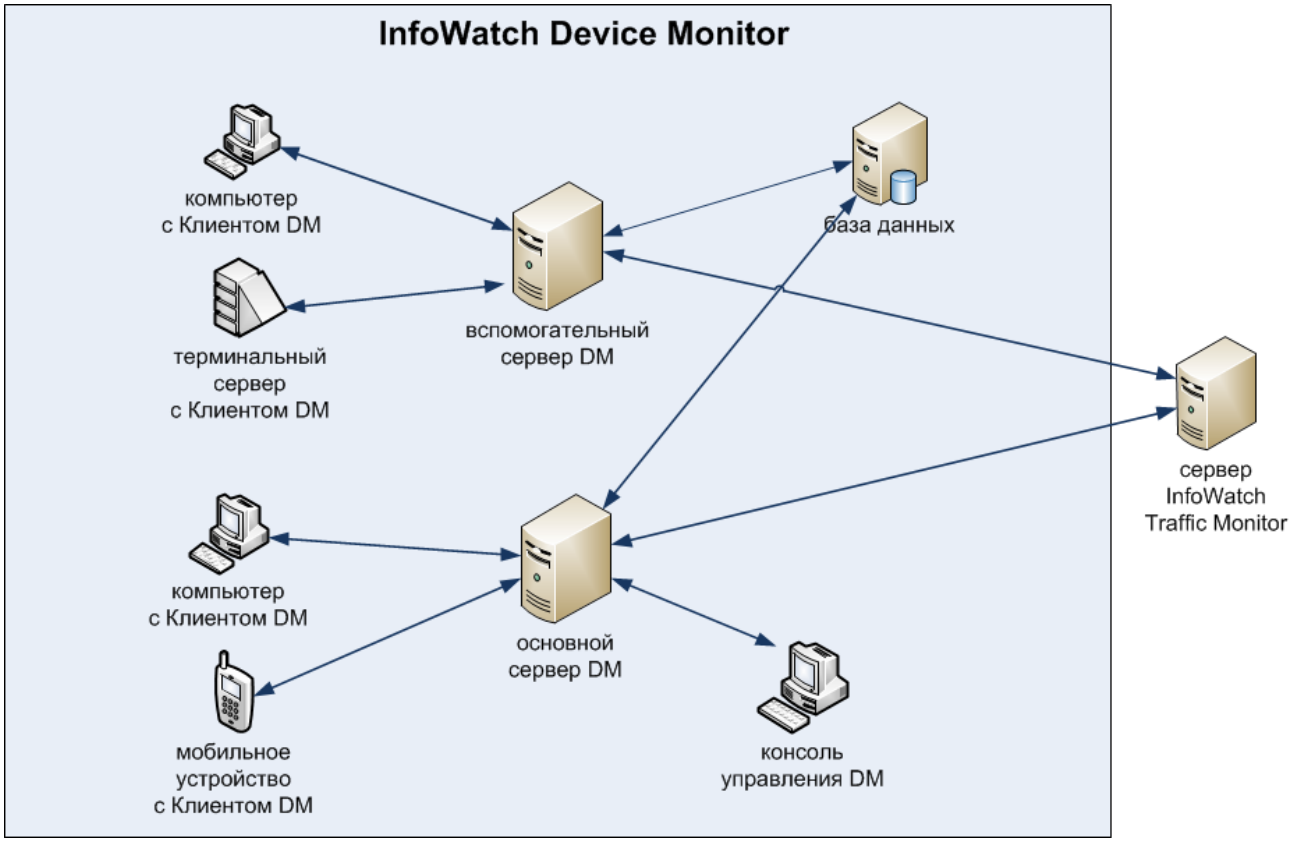
3.3.3 Схема развертывания InfoWatch Device Monitor

Компоненты, входящие в состав InfoWatch Device Monitor, перечислены в следующей таблице:

Компонент	Назначение
InfoWatch Device Monitor Client (клиентское приложение InfoWatch Device Monitor, Агент)	Перехват действий сотрудников на контролируемых рабочих станциях и мобильных устройствах
InfoWatch Device Monitor Server (сервер InfoWatch Device Monitor, Сервер)	Конфигурирование клиентских приложений, сбор данных от клиентских приложений и передача этих данных системе InfoWatch Traffic Monitor
InfoWatch Device Monitor Database (база данных)	Хранение информации, необходимой для работы Device Monitor
Консоль управления InfoWatch Device Monitor (Консоль управления)	Управление модулем Device Monitor

Менеджер управления серверами	Изменение ролей и других атрибутов серверов Device Monitor

Взаимодействие компонентов Device Monitor показано на рисунке:



Для повышения производительности Device Monitor, можно использовать кластеризацию. При этом одна схема базы данных будет использоваться несколькими серверами для хранения и распространения общей схемы безопасности.

Сервер и база данных могут находиться на одном компьютере. Однако для увеличения производительности рекомендуется размещать базу данных и сервер на разных компьютерах.

Консоль управления может подключаться только к основному серверу. Используя Консоль управления можно управлять всеми серверами в кластере.

Система разворачивается и работает следующим образом:

1. Первым устанавливают **основной сервер** (см. "*Infowatch Traffic Monitor 6.0. Руководство пользователя*", статья "Работа с Менеджером управления серверами").
2. При установке основного сервера определяют используемый сервер **базы данных**: СУБД может располагаться как отдельно, так и на том же компьютере, что и основной сервер.
3. При установке основного сервера создается **схема базы данных**, где будет храниться **схема безопасности** и другие параметры Device Monitor.
4. При необходимости, можно установить **вспомогательные серверы**, которые будут обеспечивать балансировку нагрузки.
5. **Консоль управления** может устанавливаться на любую рабочую станцию. Консоль управления подключается к основному серверу. Из Консоли управления выполняется настройка схемы безопасности в соответствии с требованиями корпоративной политики безопасности.

6. На **рабочие станции** и **мобильные устройства** устанавливаются **Агенты Device Monitor**. Агенты выполняют подключение к серверу Device Monitor по зашифрованному каналу, с привязкой к серверу на основании ключа, используемого для шифрования трафика. Агенты Device Monitor обеспечивают реализацию схемы безопасности, а также получение теневых копий и их отправку на сервер Device Monitor.
7. Серверы Device Monitor получают из базы данных обновленные версии схемы безопасности и распространяют их на контролируемые рабочие станции и мобильные устройства. С контролируемых рабочих станций и мобильных устройств на сервер передается информация о событиях, подпадающих под действие правила схемы безопасности, а также теневые копии файлов. Информация о событиях передается в базу данных. Теневые копии передаются в систему InfoWatch Traffic Monitor.

Пример 1

1. Сотрудник, работающий на контролируемой рабочей станции, обращается к контролируемому периферийному устройству (например, дает команду распечатать документ через USB принтер).
2. Агент проверяет, имеет ли сотрудник право на работу с периферийным устройством. Если такого разрешения нет, то сотруднику будет отказано в доступе к устройству (в рассматриваемом случае документ не будет отправлен на печать).

Печать документов на локальных и сетевых принтерах отслеживается перехватчиком Print Monitor. Копия задания на печать передается в InfoWatch Traffic Monitor для анализа. Отправка документов на печать возможна при условии, что сотруднику разрешен доступ к принтеру (проверяется перехватчиком Device Monitor).

Пример 2

В Device Monitor задано правило, отслеживающее запись в PDF-файл на съемном устройстве. В правиле указано, что при выполнении этой операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к записи в файл на съемном устройстве (например, копирует файл на USB Flash Drive).
2. Если операция записи в файл на съемном устройстве успешно завершена, то Агент InfoWatch Device Monitor генерирует событие и создает теневую копию файла.
3. Если создать теневую копию файла невозможно (например, при отсутствии свободного места на жестком диске), операция записи в файл на съемном устройстве будет произведена без создания теневой копии, о чем будет указано в информации о событии.
4. Агент передает данные (событие и теневую копию файла) на Сервер InfoWatch Device Monitor. Если соединение с Сервером отсутствует, то данные сохраняются на контролируемом компьютере. После восстановления связи данные будут доставлены на Сервер.
5. Сервер отправляет данные в систему InfoWatch Traffic Monitor для анализа. Если соединение с сервером InfoWatch Traffic Monitor отсутствует, то данные сохраняются на компьютере. После восстановления связи данные будут доставлены в систему InfoWatch Traffic Monitor.

Попытки записи в файлы на съемных устройствах отслеживаются перехватчиком File Monitor. Полученные сведения передаются затем в InfoWatch Traffic Monitor для анализа. В то же время доступ к съемному устройству контролируется перехватчиком Device Monitor. Поэтому сотрудник может выполнять операцию записи в файл только на тех съемных устройствах, к которым у него есть доступ.

Пример 3

В Device Monitor задано правило, отслеживающее печать DOC-файлов. В правиле указано, что при выполнении подобной операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к отправке документа на печать.
2. Если задание на печать сформировано успешно, то Агент InfoWatch Device Monitor генерирует событие и создает теневую копию документа, отправленного на печать.
3. В случае если создать теневую копию документа невозможно (например, при отсутствии свободного места на жестком диске), операция печати будет произведена без создания теневой копии, о чем будет указано в информации о событии.
4. Агент передает данные (событие и теневую копию документа) на Сервер InfoWatch Device Monitor. Если соединение с Сервером отсутствует, то данные сохраняются на контролируемом компьютере. После восстановления связи данные будут доставлены на Сервер.
5. Сервер отправляет данные в систему InfoWatch Traffic Monitor для анализа. Если соединение с сервером InfoWatch Traffic Monitor отсутствует, то данные сохраняются в базе данных. После восстановления связи данные будут доставлены в систему InfoWatch Traffic Monitor.

3.4 Предустановленные серверные параметры

В результате установки Системы создается ряд параметров, обращение к которым может потребоваться при настройке и эксплуатации Системы.

Имя сервера (hostname): **iwtm-xxxxxxxxxxxxxxxx.local**, где xxxxxxxxxxxxxxxx – серийный номер (Serial Number) сервера.

Директории установки Системы (могут располагаться на разных серверах):

- сервер Traffic Monitor – **/opt/iw**
- БД – **/u01** и **/u02**

> **Важно!**
>
> Смените пароли пользователей **oracle** и **postgres** сразу после установки Системы.

Параметры базы данных Traffic Monitor:

Параметр	Oracle	PostgreSQL
Порт подключения к БД	**1521**	**5433**
Имя базы данных / SID или service name	**iwtm**	**postgres**

oinstall - группа владельца инсталляции клиента СУБД, в состав которой включены пользователи **iwtm**, **oracle** для базы данных Oracle и **iwtm, root** для базы данных PostgreSQL.

Учетные записи Linux:

Назначение	Имя	Пароль
Суперпользователь OS Linux (root)	**root**	Задается при установке
Пользователь Linux, от имени которого будут запускаться серверные процессы Traffic Monitor	**iwtm**	Без пароля
Владелец схемы базы данных	**iwtm**	xxXX1234
Пользователь, от имени которого будут запускаться серверные процессы базы данных Oracle **Примечание:** При установке базы данных PostgreSQL, данная учетная запись не создается	**oracle**	xxXX1234
Пользователь, от имени которого будут запускаться серверные процессы базы данных PostgreSQL **Примечание:** При установке базы данных Oracle, данная учетная запись не создается	**postgres**	xxXX1234

Учетные записи баз данных:

> **Примечание:**
>
> Учетные записи доступны после запуска **sqlplus** для Oracle и **psql** для PostgreSQL.

Назначение	Имя учетной записи Oracle	Имя учетной записи PostgreSQL	Пароль
Учетные записи для администрирования базы данных	**sys**	**postgres**	xxXX1234
	system		
Учетная запись для доступа Linux-процессов к базе данных	**iwtm_linux**		xxXX1234
Учетная запись для доступа Веб-консоли управления к базе данных	**iwtm_web**		xxXX1234
Учетная запись для доступа подсистемы мониторинга (Nagios) к базе данных	**iwtm_nagios**		xxXX1234

Учетные записи Веб-консоли управления:

Назначение	Имя	Пароль
Администратор пользователей	**administrator**	xxXX1234
Офицер безопасности	**officer**	xxXX1234

Директория индексов Sphinx: **/var/lib/sphinx**

Назначение	Имя	Пароль
Пользователь Linux, от имени которого будут запускаться бинарные файлы и индексы Sphinx	**iwtm**	Без пароля

4 Обновление Системы

Важно!

Обновление до требуемой версии поддерживается с любой из 2 предыдущих версий. До версии 6.9 обновление может быть установлено с версий 6.7 и/или 6.5. Порядок выпуска версий Системы указан в статье "Traffic Monitor: Главная".

Примечание:

Установка Системы происходит с использованием подключаемого репозитория.

Репозиторий - это папка, содержащая файлы и другие папки и предоставляющая их по запросу операционной системе. Другими словами, репозиторий - это хранилище, из которого устанавливаются и обновляются программы. Перед использованием необходимо подключить репозиторий, чтобы операционная система могла к нему обращаться (процедура подключения описана ниже).

Важно!

Перед обновлением необходимо применить конфигурацию. Если не применить конфигурацию перед обновлением, она будет применена принудительно.

Важно!

Во время обновления Системы перехват и анализ событий работать не будут.

Перед обновлением убедитесь в наличии:

- дистрибутивного диска InfoWatch Traffic Monitor той версии, до которой планируется обновление;
- доступа к физическому или виртуальному серверу (серверам), которые необходимо обновить;
- пароля пользователя *root*.

Также до начала обновления требуется выяснить:

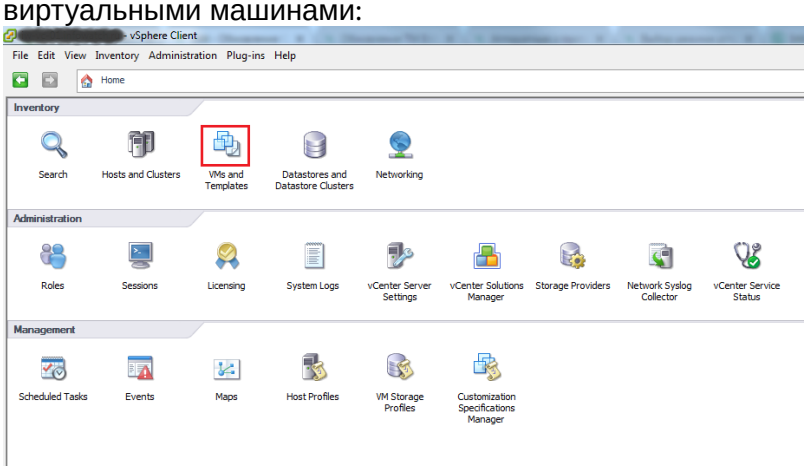
- какой тип установки в Системе (могут быть типы *Все-в-одном (All-in-one)* и *Распределенная установка (Node Server + Database Server)*) - данная информация понадобится для выбора инструкции по обновлению;
- какая СУБД используется (Oracle или PostgreSQL) - данная информация понадобится при обновлении схемы БД и серверных компонентов;
- планируется ли установить новую стандартную БКФ - данная информация понадобится при установке репозитория. Установка новой стандартной БКФ удалит прежнюю БКФ (стандартную или нестандартную) со всеми внесенными в нее доработками;
- на каком сервере установлен пакет `web-gui` - данная информация понадобится для очистки кеша сервера после обновления схемы БД. **Подсказка:** пакет установлен на том сервере, к которому подключается консоль управления Traffic Monitor.

До начала обновления выполните следующие действия:

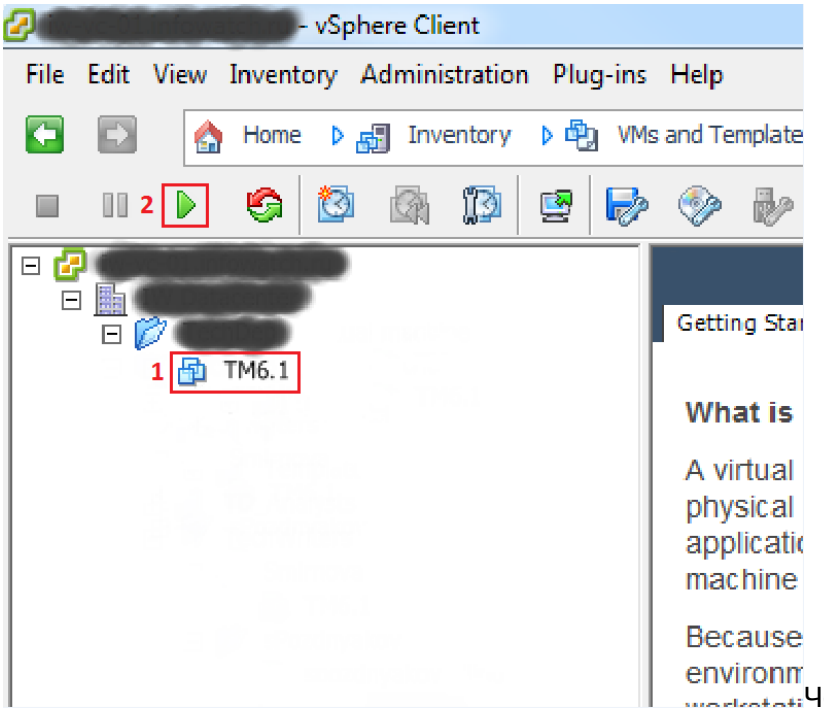
1. Включите (если он был выключен) каждый сервер, предназначенный для обновления:
   - в случае физического сервера - нажмите кнопку включения, расположенную на корпусе сервера (подробнее см. в инструкции к серверу);
   - в случае виртуального сервера - выполните команду **Power On** (см. пример ниже).

> **Примечание:**
>
> В настоящей инструкции приводятся примеры по работе с виртуальным сервером в клиентском приложении одной из наиболее часто используемых сред виртуализации - VMware vSphere (VMware vSphere Client). Рамками на рисунках выделены области интерфейса, которые нужно последовательно выделять щелчком мыши для достижения требуемых результатов.

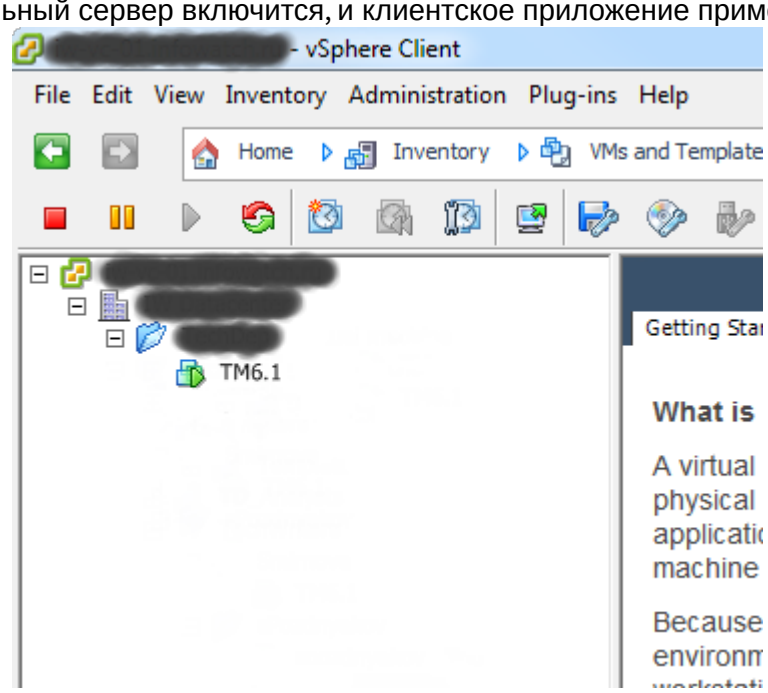
Запустите клиентское приложение VMware vSphere Client от имени администратора (щелкните правой кнопкой мыши на иконке приложения и выберите **Запуск от имени администратора**). Войдите в приложение, используя логин и пароль, выданные администратором вашей информационной сети. Перейдите в раздел с виртуальными машинами:



Последовательно раскройте все узлы в левой части рабочей области, пока не дойдете до нужного виртуального сервера.
Включите виртуальный сервер:



Через некоторое время виртуальный сервер включится, и клиентское приложение примет вид:



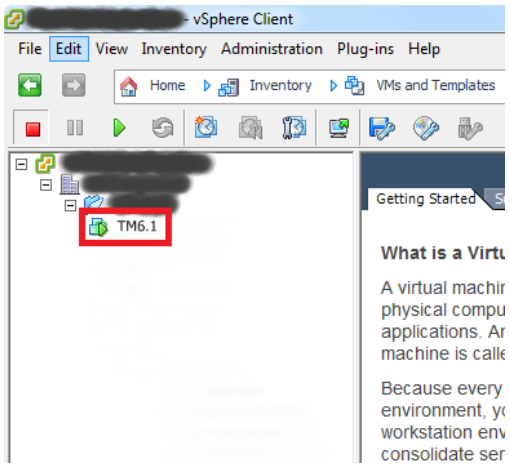
2. Подключите дистрибутивный диск InfoWatch Traffic Monitor к серверам, предназначенным для обновления:
   - в случае физического сервера:
     - если дистрибутив поставлен на оптическом диске - вставьте диск в cd- или dvd-привод сервера и дождитесь, пока сервер прочитает диск;
     - если диск поставлен в виде ISO-образа - смонтируйте образ средствами вашей операционной системы;
   - в случае виртуального сервера:

- если дистрибутив поставлен на оптическом диске - вставьте диск в cd- или dvd-привод компьютера, на котором ведете работу, а затем подключите диск к виртуальному серверу (см. пример ниже);
- если диск поставлен в виде ISO-образа, смонтируйте образ средствами вашей операционной системы, а затем подключите диск к виртуальному серверу (см. пример ниже).

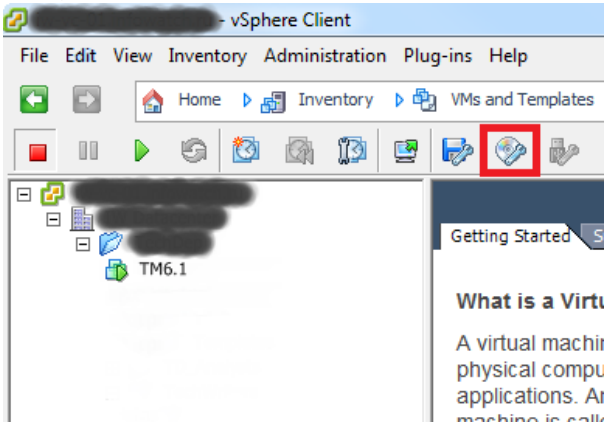
Примечание:

В примере предполагается, что дистрибутивный диск находится в устройстве **F** компьютера, с которого осуществляется обновление виртуального сервера ТМ (то есть компьютера, с которого выполнен вход в VMware vSphere Client).

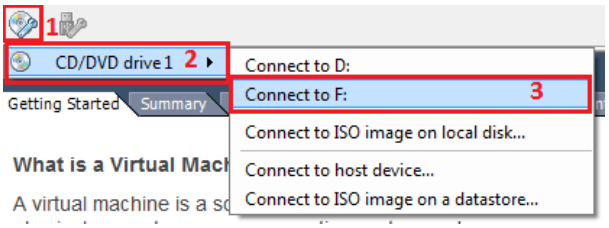
1)



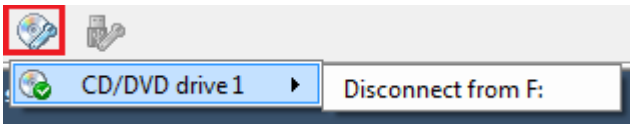
2)



3)



Практически сразу после нажатия **Connect to F:** диск подключится к виртуальному серверу, и меню примет вид:



После установки дистрибутивного диска все готово к обновлению. Обновите серверы согласно следующим инструкциям:

- Обновление ТМ Все-в-одном (All-in-one) Enterprise и Standard - обновление сервера с типом установки "Все-в-одном" (*Enterprise* или *Standard*);
- Обновление ТМ при распределенной установке - обновление сервера с распределенным типом установки (База данных отдельно, Серверы ТМ отдельно);

> **Примечание:**
>
> Сведения по обновлению подсистемы Device Monitor смотрите в статье "Обновление InfoWatch Device Monitor".

4.1 Обновление ТМ Все-в-одном (All-in-one) Enterprise и Standard

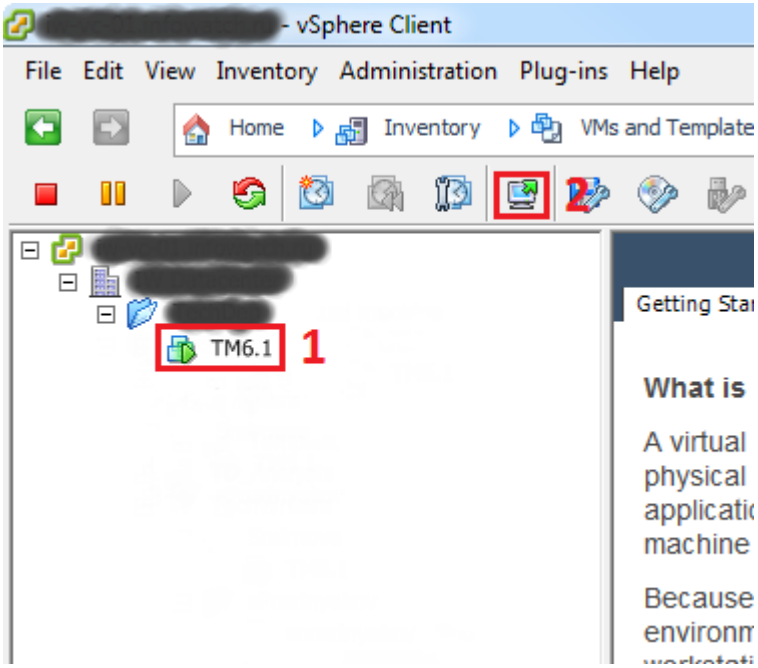
Обновление будет вестись в консоли обновляемого сервера. Консоль (или терминал) - это окно операционной системы семейства Linux, команды в котором вводятся в текстовом виде - строкой. В зависимости от разновидности сервера, в начале работы консоль может выводить общие сведения о сервере и приглашение войти или просто приглашение войти. В любом случае в самом начале потребуется ввести логин пользователя, от имени которого будет выполнен вход.

Консоль выглядит так:



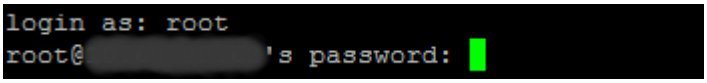
Чтобы обновить Систему, выполните следующие действия:

1. Откройте консоль обновляемого сервера:
   - в случае физического сервера - консоль отображается на экране монитора, подключенного к серверу;
   - в случае виртуального сервера - выполните команду **Launch Virtual Machine Console** (см. пример ниже).

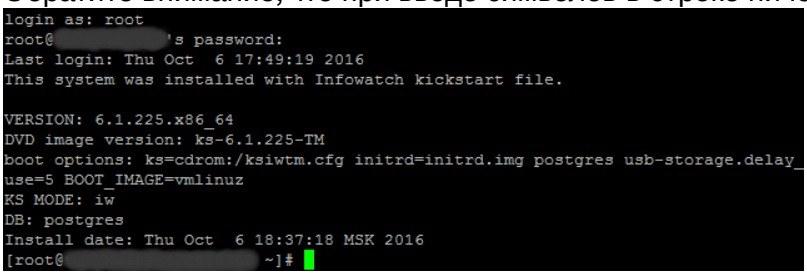


Откроется окно с консолью сервера.

2. В строке **Login as:** (или **login:** - в зависимости от разновидности сервера) введите *root* и нажмите **Enter**.



3. В строке **root@<адрес_сервера>'s password:** (или **Password:** - в зависимости от разновидности сервера) введите пароль пользователя *root* (суперпользователя) и нажмите **Enter**.
Обратите внимание, что при вводе символов в строке ничего не будет отображаться.



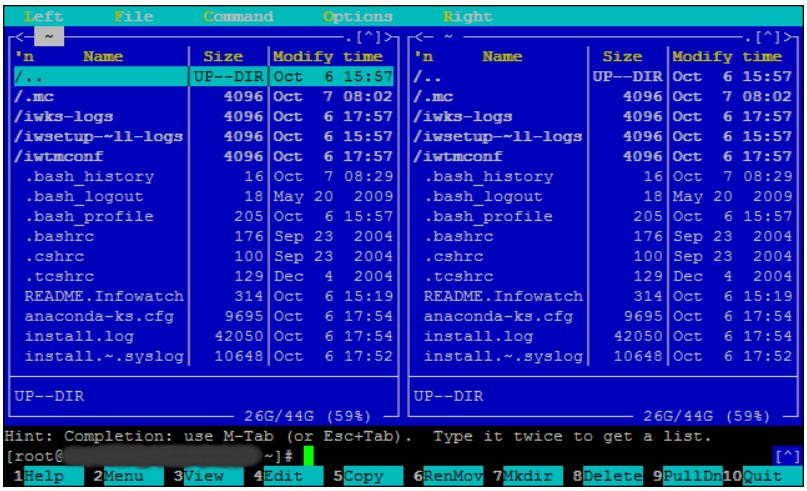
На экране отобразится служебная информация и - последней строкой - приглашение ввести команду (командная строка).

> **Подсказка:**
>
> Команды в консоли вводятся с помощью клавиатуры и обязательно подтверждаются нажатием клавиши **Enter**, поэтому в данной инструкции под "введите команду `command`" подразумевается "введите команду `command` и нажмите **Enter**". После выполнения команды снова отображается приглашение - оно заканчивается знаком # или $ (в зависимости от того, от имени какого

пользователя выполнен вход). Прежде чем вводить следующую команду, нужно убедиться, что в командной строке отображается приглашение.

4. Введите команду для вызова файлового менеджера:

```
mc
```

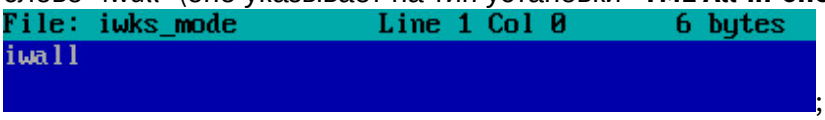


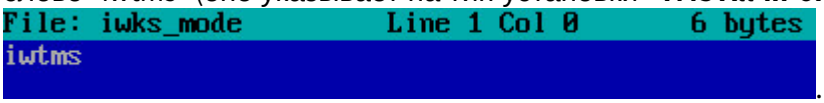
На экране отобразится окно файлового менеджера *Midnight Commander*, в котором удобно просматривать файлы.
Навигация в файловом менеджере осуществляется при помощи стрелок клавиатуры и клавиши **Enter** или при помощи мыши. При этом без дополнительных действий вы можете вводить команды в командной строке (она видна в нижней части экрана).
Для перехода на уровень выше установите курсор в поле **/..** (первая строка в файловом менеджере) и нажмите **Enter**.

5. Перейдите в директорию `/opt/iw/tm5` и убедитесь в наличии там файла **iwks_mode**.



> **Примечание:**
>
> Если файл **iwks_mode** отсутствует в директории, то его необходимо создать. Для этого введите команду:
> `touch iwks_mode`

6. Установите курсор на файл **iwks_mode** и нажмите клавишу **F3**.
   В зависимости от редакции Системы(*Enterprise* или *Standard*) на экране должно отобразится содержимое файла **iwks_mode**:
   - слово "iwall" (оно указывает на тип установки - **TME All-in-one: TM+DB server**)
     

     ;
   - слово "iwtms" (оно указывает на тип установки - **TMS All-in-one: TM+DB server**)
     

     .

   > **Примечание:**
   >
   > Если файл имеет другое содержимое:
   > 1. повторно нажмите **F3**.
   > 2. нажмите **F4**.
   > 3. в открывшемся окне удалите все символы и, в зависимости от редакции Системы, введите `iwall` или `iwtms`
   > 4. нажмите **F2**.
   > 5. в открывшемся окне подтвердите сохранение файла, нажав **Save**.
   > 6. нажмите **F10**.
   > 7. нажмите **F3** и убедитесь в корректности содержимого файла.

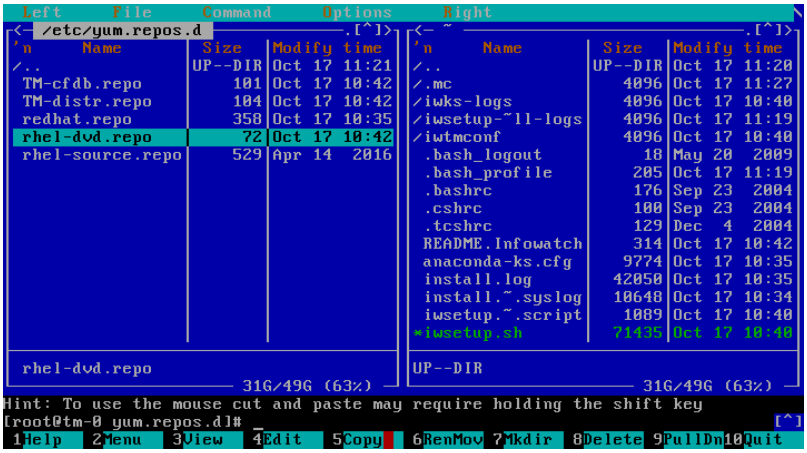
7. Нажмите **F3**.
8. Введите команду:
   ```
   mkdir -p /mnt/rhel-dvd
   ```
   Будет создана директория `/mnt/rhel-dvd`
9. Убедитесь, что диск с дистрибутивом InfoWatch Traffic Monitor подключен к серверу (см. статью "Обновление Системы", шаг 2).
10. Введите команду:
    ```
    mount /dev/cdrom /mnt/rhel-dvd
    ```

    > **Примечание:**
    >
    > Между частями команды "/dev/cdrom" и "/mnt/rhel-dvd" есть пробел.

    Дистрибутивный диск, находящийся в разделе `/dev/cdrom`, будет подключен в качестве репозитория в директории `/mnt/rhel-dvd`.
11. Перейдите в директорию `/mnt/rhel-dvd` и убедитесь в наличии там файлов и папок. Если директория пуста, повторите шаги 9 и 10.
12. Перейдите в директорию `/etc/yum.repos.d` и убедитесь в наличии там файла **rhel-dvd.repo** (этот файл потребуется для указания пути к файлам обновления).

Примечание:

Ввиду того, что в файловом менеджере алфавитная сортировка, папки стоят раньше файлов (поскольку имеют в начале префикс - дробную черту (**/** , *слеш*)). Поэтому директория **/yum.repos.d** стоит одной из последних в списке папок, начинающихся с символа дробной черты (/), но до первого файла.



Примечание:

Если файл **rhel-dvd.repo** отсутствует в директории, то его необходимо создать. Для этого введите команду:

```
touch rhel-dvd.repo
```

13. Установите курсор на файл **rhel-dvd.repo** и нажмите **F4**.
14. Убедитесь, что файл имеет следующее содержимое:

```
[rhel-dvd]
name=Red Hat Enterprise Linux $releasever - $basearch - DVD
baseurl=file:///mnt/rhel-dvd/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm]
name=DVD_IWTM
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/Linux/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm-cfdb]
name=DVD_IW-CFDB
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/cfdb/
enabled=0
gpgcheck=0
```

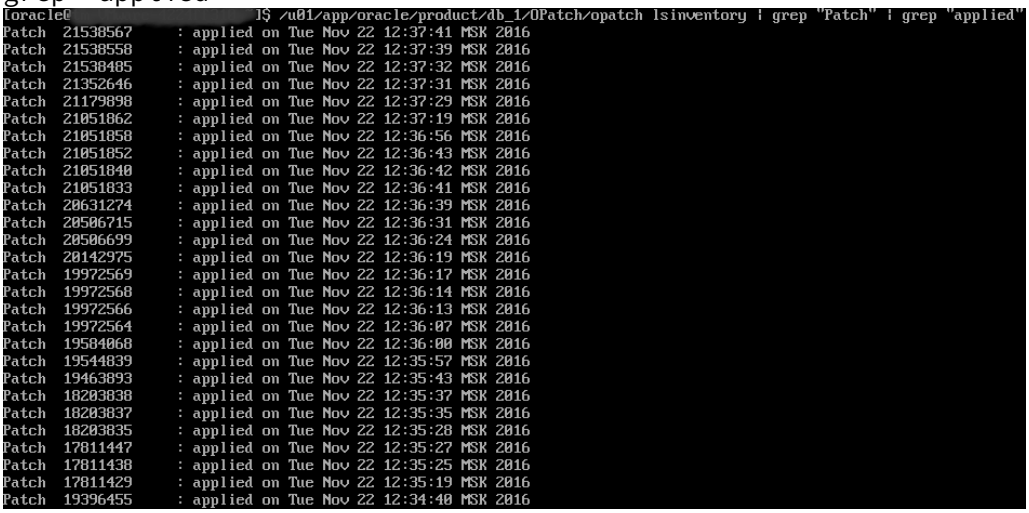
> **Важно!**
>
> Если текст файла отличается, замените его на указанный.

15. В параметрах `enabled` блоков `[rhel-dvd]` и `[rhel-dvd-iwtm]` замените значения с `0` на `1`.
16. Если вы хотите обновить стандартную БКФ, в параметре `enabled` блока `[rhel-dvd-iwtm-cfdb]` замените значение с `0` на `1`. Произведенные во время работы изменения БКФ будут сохранены.
17. Нажмите **F2**.
18. В открывшемся окне подтвердите сохранение файла, нажав **Save**.
19. Нажмите **F10**.
20. Нажмите **F3** и убедитесь в корректности содержимого файла, затем снова нажмите **F3** для закрытия файла.
21. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    ```
    exit
    ```
22. Введите команду для очищения кеша менеджера пакетов:
    ```
    yum clean all
    ```
23. Введите команды для остановки перехватчиков:
    ```
    service iwtm stop icap
    service iwtm stop smtpd
    service iwtm stop expressd
    service iwtm stop sniffer
    service iwtm stop xapi_xapi
    service iwtm stop xapi_puppy
    ```
24. Снова введите команду для вызова файлового менеджера:
    ```
    mc
    ```
25. Дождитесь, пока обработаются все события, стоящие в очереди на обработку. События, находящиеся в очереди, хранятся в следующих директориях:
    ```
    opt/iw/tm5/queue/analysis/.db/
    opt/iw/tm5/queue/analysis/.in/
    opt/iw/tm5/queue/analysis/.out/
    opt/iw/tm5/queue/db/.db/
    opt/iw/tm5/queue/db/.in/
    opt/iw/tm5/queue/db/.out/
    opt/iw/tm5/queue/smtp/.db/
    opt/iw/tm5/queue/smtp/.in/
    opt/iw/tm5/queue/smtp/.out/
    ```
    По завершении обработки событий данные директории должны стать пустыми.

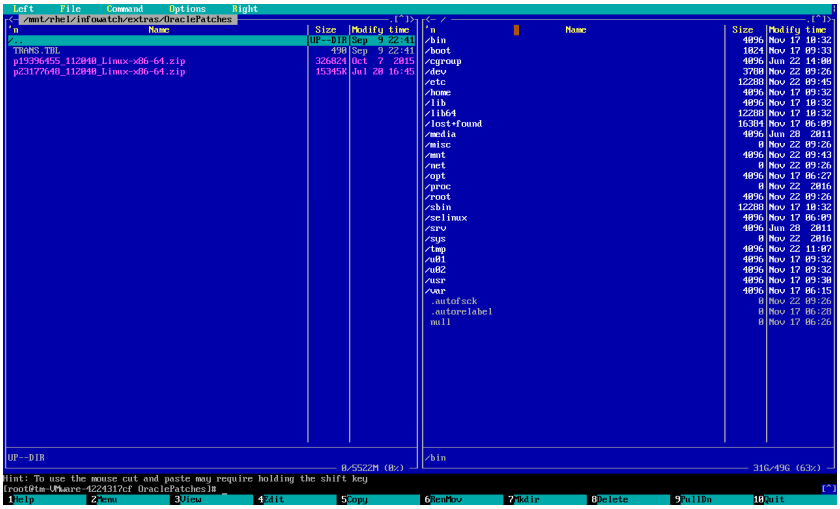
> **Важно!**
>
> До продолжения обновления настоятельно рекомендуется убедиться в том, что все указанные выше директории пусты . В противном случае нельзя

гарантировать успешное обновление и дальнейшую работоспособность Системы.
Если по какой-либо причине дождаться завершения обработки невозможно, вы можете удалить события из очереди, при этом такие события будут полностью удалены из Системы.
Чтобы удалить событие, перейдите в нужную директорию в файловом менеджере, установите курсор на планируемом к удалению событии и нажмите **F8**, затем подтвердите удаление, выбрав в открывшемся окне **Yes**.

26. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    `exit`
27. Введите команду для остановки сервисов сервера Traffic Monitor:
    `service iwtm stop`
28. Если в Системе используется СУБД Oracle, выполните следующие действия:
    a. Введите команду для остановки СУБД Oracle:
       `service oracle stop`
    b. Введите команду для переключения на нужного пользователя:
       `su - oracle`
    c. Введите команду для получения списка установленных в Системе патчей:
       `/u01/app/oracle/product/db_1/OPatch/opatch lsinventory | grep "Patch" | grep "applied"`



       на экране отобразится список патчей, установленных в Системе. Запишите все номера, указанные после слов "Patch" (в другой записи номер патча - это первые восемь цифр после буквы **p**. Например, номер патча **p19972569_112040_Linux-x86-64.zip** - это 19972569). Данные номера понадобятся для того, чтобы сверить установленные и необходимые для обновления патчи.
    d. Снова введите команду для вызова файлового менеджера:
       `mc`
    e. Перейдите в директорию `/mnt/rhel-dvd/infowatch/extras/OraclePatches` и убедитесь, что номера патчей, расположенных в директории, входят в список номеров патчей, установленных в Системе (которые вы записали).



Примечание:

Если какого-либо патча из директории `/mnt/rhel-dvd/infowatch/extras/OraclePatches` нет в списке установленных, потребуется установить данный патч.
Перед установкой патча может потребоваться обновить утилиту OPatch. Для это выполните следующие действия:

i. Если файловый менеджер *Midnight Commander* работает, для выхода (требуется для лучшего контроля выполнения команд) введите команду:
   `exit`
ii. Введите команду для перехода в нужную директорию
   `cd /mnt/rhel-dvd/infowatch/extras/OraclePatches`
iii. Для создания резервной копии введите команду:
   `mv /u01/app/oracle/product/db_1/OPatch /u01/app/oracle/product/db_1/OPatch_backup`
iv. Введите команду для извлечения архива с новой версией:
   `unzip p6880880_112000_Linux-x86-64.zip -d /tmp/`
v. Для предоставления пользователю oracle прав на работу с директорией и файлами введите команду:
   `chown oracle:oinstall -R /tmp/OPatch`
vi. Для переноса новой версии введите команду:
   `mv /tmp/OPatch /u01/app/oracle/product/db_1`

Для установки патча выполните следующие действия (пример приведен для патча с номером 12345678 - p12345678_112040_Linux-x86-64.zip):

i. Если файловый менеджер *Midnight Commander* работает, для выхода (требуется для лучшего контроля выполнения команд) введите команду:
   `exit`

ii. Введите команду для извлечения патча:
`unzip /mnt/rhel-dvd/infowatch/extras/OraclePatches/p12345678_112040_Linux-x86-64.zip -d /tmp/`
iii. Введите команду для перехода в нужную директорию:
`cd /tmp/12345678/`
iv. В зависимости от типа патча введите команду для установки:
- `/u01/app/oracle/product/db_1/OPatch/opatch napply . -silent -ocmrf /mnt/rhel-dvd/infowatch/extras/OraclePatches/ocm0.rsp` (в случае композитного (составного) патча);
- `/u01/app/oracle/product/db_1/OPatch/opatch apply -silent -ocmrf /mnt/rhel-dvd/infowatch/extras/OraclePatches/ocm0.rsp` (в случае одиночного патча).

Когда патч установится, на экран будет выведено сообщение:

```
OPatch completed with warnings.
Press any key to continue..._
```

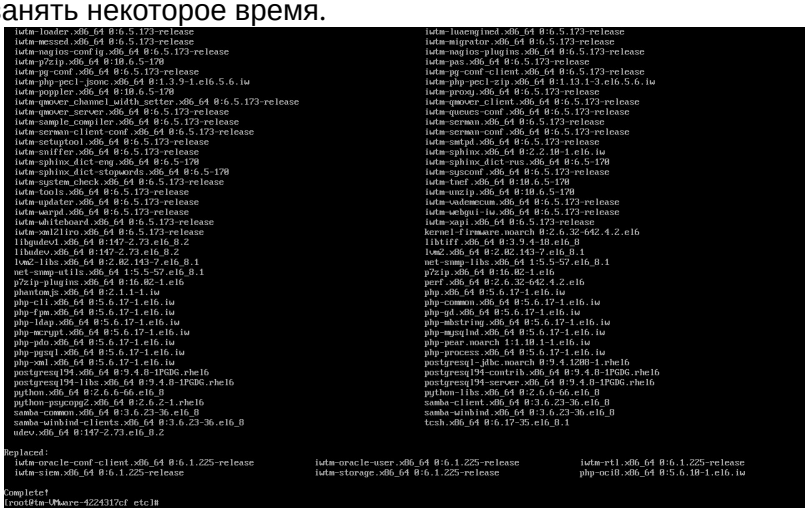
v. Нажмите любую клавишу для продолжения.
vi. Введите команды для удаления более ненужных файлов:
`cd /tmp/ && rm -rf /tmp/12345678/ && rm -f /tmp/PatchSearch.xml`

f. если файловый менеджер *Midnight Commander* работает, для выхода (требуется для лучшего контроля выполнения команд) введите команду:
`exit`
g. введите команду для переключения обратно на пользователя *root*:
`logout`
h. введите команду для запуска СУБД Oracle:
`service oracle start`

29. **В зависимости от используемой СУБД и необходимости обновить БКФ введите команду для запуска процесса обновления пакетов:**
    a. Если в параметре `enabled` блока `[rhel-dvd-iwtm-cfdb]` установлено значение `0`:
    - `yum upgrade --exclude=iwtm-rtl-pg,iwtm-siem-pg,iwtm-policy*` (если используется **СУБД Oracle**)
    - `yum upgrade --exclude=iwtm-rtl-oracle,iwtm-siem-oracle,iwtm-policy*` (если используется **СУБД PostgreSQL**)

    b. Если в параметре `enabled` блока `[rhel-dvd-iwtm-cfdb]` установлено значение `1`
    - `yum upgrade --exclude=iwtm-rtl-pg,iwtm-siem-pg` (если используется **СУБД Oracle**)
    - `yum upgrade --exclude=iwtm-rtl-oracle,iwtm-siem-oracle` (если используется **СУБД PostgreSQL**)

30. Перед загрузкой нужных для установки пакетов будет выведен запрос вида
```
Total download size: 4.4 M
Is this ok [y/N]:
```
. Для продолжения наберите **Y** на клавиатуре и нажмите **Enter**.
Начнется скачивание пакетов из репозитория, а затем - установка пакетов. Это может занять некоторое время.

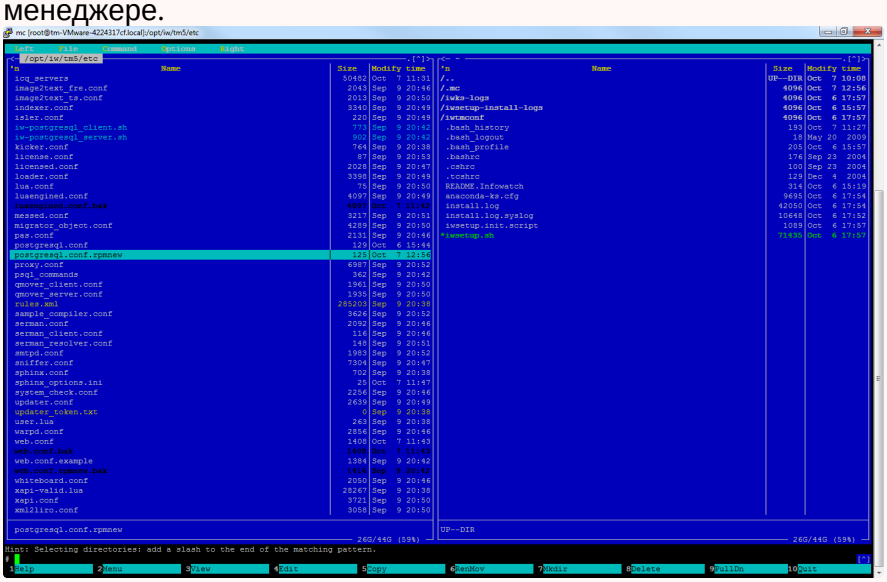


> **Примечание:**
>
> При обновлении пакетов Системы с **СУБД PostgreSQL** в лог `/root/iwsetup-install-logs/iwsetup-install.log` может быть записано следующее сообщение:
> `PHP Warning: PHP Startup: Unable to load dynamic library '/usr/lib64/php/modules/oci8.so'- libclntsh.so.11.1: cannot open shared object file: No such file or directory in Unknown on line 0`
> Такое поведение Системы является корректным.

31. Снова введите команду для вызова файлового менеджера:
`mc`
32. Если во время использования Системы в конфигурационные файлы с расширением **.conf** вносились изменения, перейдите в директории `/opt/iw/tm5/etc` и `/etc/nginx` и проверьте наличие файлов с расширением **conf.rpmnew**. Если такие файлы есть, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew").

> **Важно!**
>
> Если в Системе используется СУБД PostgreSQL, при обновлении с версии 6.0 или 6.1 до 6.5 и более новых обязательно выполните следующие действия:
> a. Перейдите в директорию `/opt/iw/tm5/etc`

b. Установите курсор на файл **postgresql.conf.rpmnew** в файловом менеджере.



c. Нажмите **F4**.

d. Замените значения секций файла значениями соответствующих секций файла **postgresql.conf**. Получится так:

```
{
    "DB": "postgres",
    "Password": "xxXX1234",
    "Username": "iwtm_linux",
    "Port": 5433,
    "Host": "localhost"
}
```

> **Примечание:**
>
> При распределенном типе установки значением поля "Host" будет IP-адрес сервера, на котором установлена СУБД. Например:
> `"Host": "10.60.23.6",`

e. Нажмите **F2**.

f. В открывшемся окне подтвердите сохранение файла, нажав **Save**.

g. Нажмите **F10**.

h. Установите курсор на файл **postgresql.conf** в файловом менеджере.

i. Нажмите **F8** для удаления файла **postgresql.conf**.

j. В открывшемся окне подтвердите удаление файла, нажав **Yes**.

k. Выделите файл **postgresql.conf.rpmnew** в файловом менеджере.

l. Нажмите **F6**.

m. В поле **to** введите `/opt/iw/tm5/etc/postgresql.conf` и нажмите **Enter**.
Теперь в Системе есть только один конфигурационный файл PostgreSQL - **postgresql.conf**. Он имеет структуру файла новой версии и нужное

наполнение:

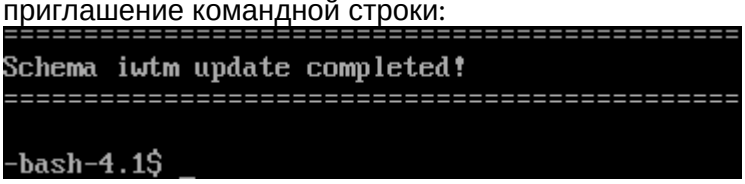
```
{
    "DB": "postgres",
    "Password": "xxXX1234",
    "Username": "iwtm_linux",
    "Port": 5433,
    "Host": "localhost"
}
```

33. Если во время использования Системы в конфигурационные файлы с расширением **.cfg** (служба Nagios) вносились изменения, перейдите в директории `/etc/nagios/iwmon` и `/etc/nagios` и проверьте наличие файлов с расширением **cfg.rpmnew**. Если такие файлы есть, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew").
34. Если во время использования Системы в файлы сценариев LUA (файлы с расширением **.lua**) вносились изменения, перейдите в директорию `/opt/iw/tm5/etc/scripts/` и проверьте наличие файлов с расширением **.lua.rpmnew**. Если такие файлы есть, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew").
35. **В зависимости от используемой СУБД** перейдите в директорию:
    - `/opt/iw/tm5/csw/oracle` (если используется **СУБД Oracle**);
    - `/opt/iw/tm5/csw/postgres` (если используется **СУБД PostgreSQL**).
36. Выделите файл **database.conf**.



37. Нажмите **F3**.
38. Убедитесь, что для параметра `\set schema_version` указана версия, до которой происходит обновление. Если указана старая версия, повторите шаги 27 - 36.
39. Нажмите **F3**.
40. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    ```
    exit
    ```
41. Последовательно введите команды для остановки служб:
    ```
    service iwtm stop
    service php-fpm stop
    service nagios stop
    ```

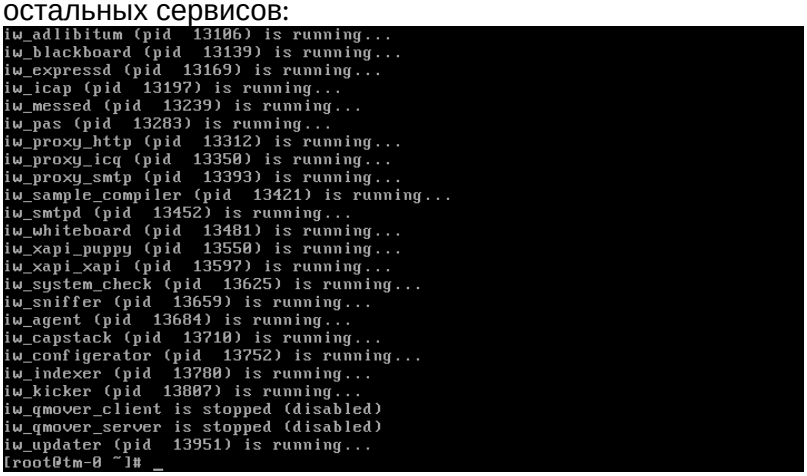
> **Примечание:**
>
> При наличии в Системе подсистемы Краулер потребуется приостановить службы указанной подсистемы (на сервере Краулер). Данная процедура выполняется на сервере, где установлена подсистема, стандартными средствами ОС Windows: **Пуск** - **Панель управления** - **Администрирование** - **Службы**, затем потребуется выделить службу в списке служб и нажать **Приостановка службы**.

42. **В зависимости от используемой СУБД** введите команду для переключения на нужного пользователя:
    - `su - oracle` - для переключения на пользователя *oracle* (если в Системе используется **СУБД Oracle**)
    - `su - postgres` - для переключения на пользователя *postgres* (если в Системе используется **СУБД PostgreSQL**)
43. **В зависимости от используемой СУБД** введите команду для перехода в нужную директорию:
    - `cd /opt/iw/tm5/csw/oracle` - (если в Системе используется **СУБД Oracle**)
    - `cd /opt/iw/tm5/csw/postgres` - (если в Системе используется **СУБД PostgreSQL**)
44. Введите команду для запуска скрипта (сценария) обновления БД:
    `./update.sh`
    Начнется процесс обновления схемы данных. Это может занять некоторое время. По окончании обновления на экране отобразятся информационное сообщение и приглашение командной строки:
    

45. Введите команду для очистки кеша:

    `redis-cli flushall`
46. Введите команду для переключения обратно на пользователя *root*:
    `logout`
47. Введите команду для перезагрузки сервера:
    `reboot`
48. Дождитесь загрузки сервера и повторите шаги **2** и **3** данной инструкции для входа в консоль.
49. Введите команду для проверки запуска процессов:
    `service iwtm status`
    На экране отобразится список процессов и их статус. Обычно сервисы `iw_qmover_client` и `iw_qmover_server` бывают остановлены, а все остальные сервисы - запущены, при этом строки должны заканчиваться фразой "**is stopped (disabled)...**" для сервисов `iw_qmover_client` и `iw_qmover_server` и фразой "**is running...**" для всех

остальных сервисов:



Примечание:

При наличии в Системе подсистемы Краулер потребуется запустить службы указанной подсистемы (на сервере Краулер). Данная процедура выполняется на сервере, где установлена подсистема, стандартными средствами ОС Windows: **Пуск** - **Панель управления** - **Администрирование** - **Службы**, затем потребуется выделить службу в списке служб и нажать **Запуск службы**.

Обновление сервера Traffic Monitor "Все-в-одном" (All-in-one) завершено. Номер версии Системы в окне **О системе** Консоли управления Traffic Monitor должен измениться на новый. Если в Системе есть другие серверы или подсистемы, подлежащие обновлению, воспользуйтесь инструкциями данного раздела.

Примечание:

Для корректного отображения консоли управления до начала работ удалите кеш в вашем браузере. Данное действие выполняется стандартными средствами браузера.

4.2 Обновление TM при распределенной установке

Обновление будет вестись в консоли обновляемого сервера. Консоль (или терминал) - это окно операционной системы семейства Linux, команды в котором вводятся в текстовом виде - строкой. В зависимости от разновидности сервера, в начале работы консоль может выводить общие сведения о сервере и приглашение войти или просто приглашение войти. В любом случае в самом начале потребуется ввести логин пользователя, от имени которого будет выполнен вход.

Консоль выглядит так:



Обновлению подлежат все серверы ТМ (тип установки TME Node Server) и сервер СУБД (тип установки TME DB Server).

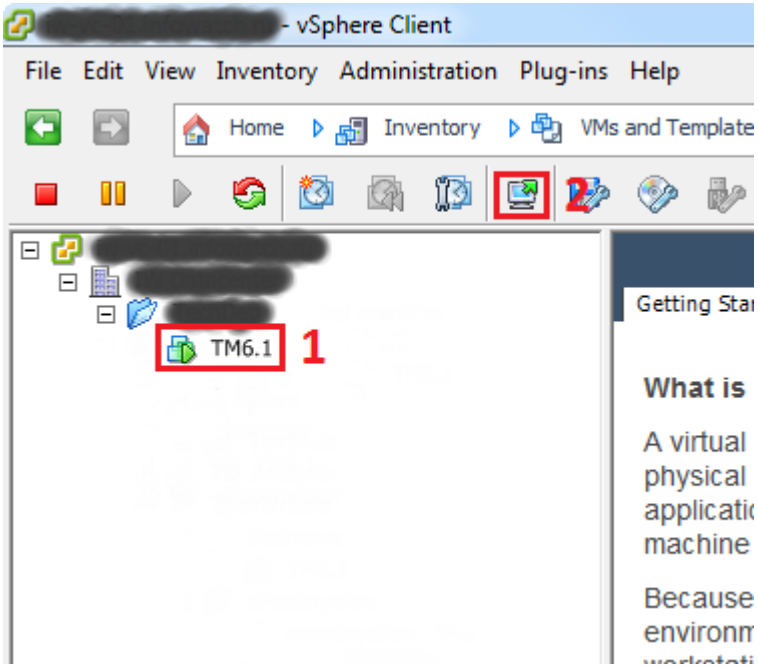
Порядок обновления следующий:

Шаг 1. Обновление всех серверов ТМ (TME Node Server).
Шаг 2. Обновление сервера СУБД (TME DB Server).
Шаг 3. Проверка работоспособности внутренних сервисов Системы.
Шаг 4. Завершение обновления на сервере СУБД (TME DB Server).
Шаг 5. Перезапуск всех серверов ТМ (TME Node Server).

ШАГ 1. ОБНОВЛЕНИЕ ВСЕХ СЕРВЕРОВ ТМ (TME Node Server)

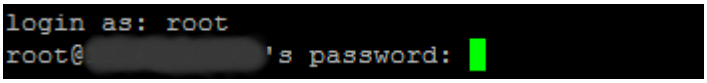
Чтобы обновить Серверы ТМ (TME Node Server), на каждом из них выполните следующие действия:

1. Откройте консоль обновляемого сервера:
    - в случае физического сервера - консоль отображается на экране монитора, подключенного к серверу;
    - в случае виртуального сервера - выполните команду **Launch Virtual Machine Console** (см. пример ниже).

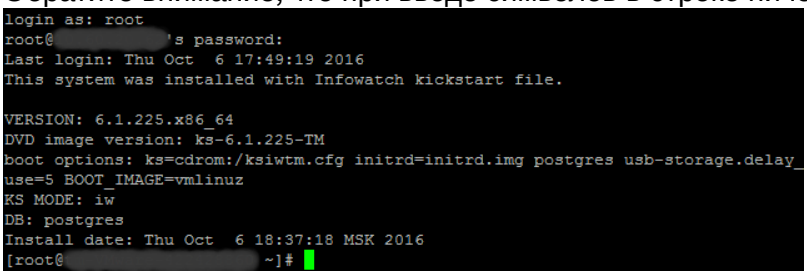


Откроется окно с консолью сервера.

2. В строке **Login as:** (или **login:** - в зависимости от разновидности сервера) введите *root* и нажмите **Enter**.



3. В строке **root@<адрес_сервера>'s password:** (или **Password:** - в зависимости от разновидности сервера) введите пароль пользователя *root* (суперпользователя) и нажмите **Enter**.
Обратите внимание, что при вводе символов в строке ничего не будет отображаться.



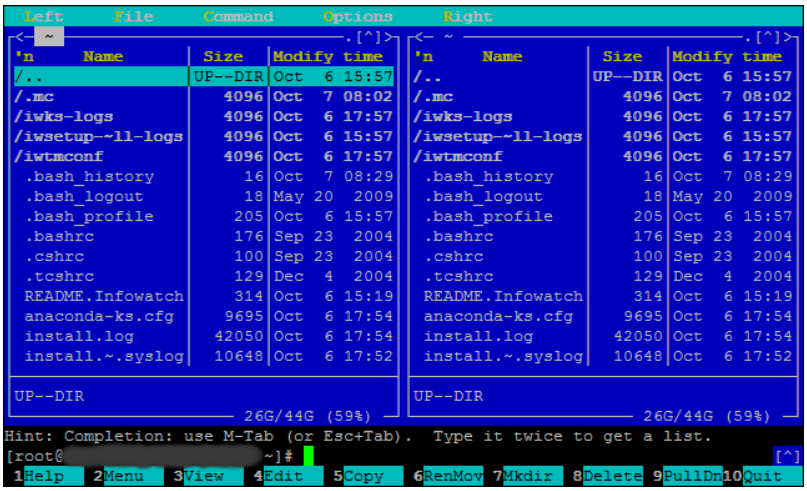
На экране отобразится служебная информация и - последней строкой - приглашение ввести команду (командная строка).

> **Подсказка:**
>
> Команды в консоли вводятся с помощью клавиатуры и обязательно подтверждаются нажатием клавиши **Enter**, поэтому в данной инструкции под "введите команду `command`" подразумевается "введите команду `command` и нажмите **Enter**". После выполнения команды снова отображается приглашение - оно заканчивается знаком # или $ (в зависимости от того, от имени какого

пользователя выполнен вход). Прежде чем вводить следующую команду, нужно убедиться, что в командной строке отображается приглашение.

4. Введите команду для вызова файлового менеджера:

```
mc
```



На экране отобразится окно файлового менеджера *Midnight Commander*, в котором удобно просматривать файлы.
Навигация в файловом менеджере осуществляется при помощи стрелок клавиатуры и клавиши **Enter** или при помощи мыши. При этом без дополнительных действий вы можете вводить команды в командной строке (она видна в нижней части экрана).
Для перехода на уровень выше установите курсор в поле **/..** (первая строка в файловом менеджере) и нажмите **Enter**.

5. Перейдите в директорию `/opt/iw/tm5` и убедитесь в наличии там файла **iwks_mode**.



> **Примечание:**
>
> Если файл **iwks_mode** отсутствует в директории, то его необходимо создать. Для этого введите команду:
> `touch iwks_mode`

6. Установите курсор на файл **iwks_mode** и нажмите клавишу **F3**.
   На экране должно отобразится содержимое файла **iwks_mode**: слово "iwtm" (оно указывает на тип установки - **TME Node server**).

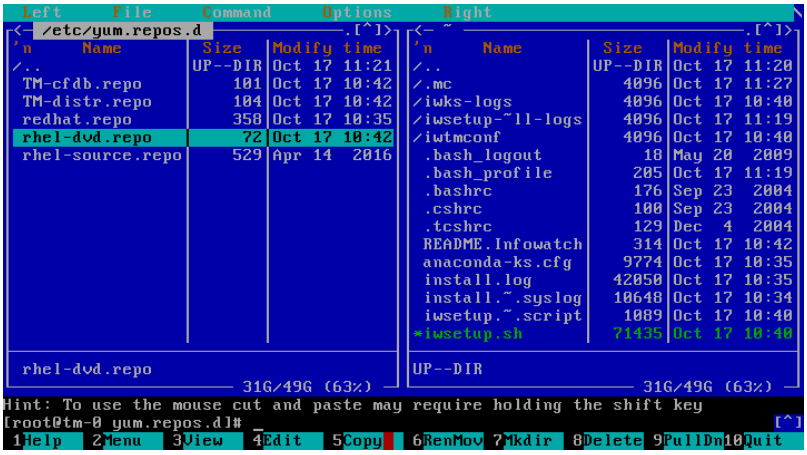
   > **Примечание:**
   >
   > Если файл имеет другое содержимое:
   > 1. повторно нажмите **F3**.
   > 2. нажмите **F4**.
   > 3. в открывшемся окне удалите все символы и введите: `iwtm`
   > 4. нажмите **F2**.
   > 5. в открывшемся окне подтвердите сохранение файла, нажав **Save**.
   > 6. нажмите **F10**.
   > 7. нажмите **F3** и убедитесь в корректности содержимого файла.

7. Нажмите **F3**.
8. Введите команду:
   ```
   mkdir -p /mnt/rhel-dvd
   ```
   Будет создана директория `/mnt/rhel-dvd`
9. Убедитесь, что диск с дистрибутивом InfoWatch Traffic Monitor подключен к серверу (см. статью "Обновление Системы", действие 2).
10. Введите команду:
    ```
    mount /dev/cdrom /mnt/rhel-dvd
    ```

    > **Примечание:**
    >
    > Между частями команды "/dev/cdrom" и "/mnt/rhel-dvd" есть пробел.

    Дистрибутивный диск, находящийся в разделе `/dev/cdrom`, будет подключен в качестве репозитория в директории `/mnt/rhel-dvd`.
11. Перейдите в директорию `/mnt/rhel-dvd` и убедитесь в наличии там файлов и папок. Если директория пуста, повторите действия 9 и 10.
12. Перейдите в директорию `/etc/yum.repos.d` и убедитесь в наличии там файла **rhel-dvd.repo** (этот файл потребуется для указания пути к файлам обновления).

    > **Примечание:**
    >
    > Ввиду того, что в файловом менеджере алфавитная сортировка, папки стоят раньше файлов (поскольку имеют в начале префикс - дробную черту (**/** , *слеш*)). Поэтому директория **/yum.repos.d** стоит одной из последних в списке папок, начинающихся с символа дробной черты (**/**), но до первого файла.



> **Примечание:**
>
> Если файл **rhel-dvd.repo** отсутствует в директории, то его необходимо создать. Для этого введите команду:
> `touch rhel-dvd.repo`

13. Установите курсор на файл **rhel-dvd.repo** и нажмите **F4**.
14. Убедитесь, что файл имеет следующее содержимое:

```
[rhel-dvd]
name=Red Hat Enterprise Linux $releasever - $basearch - DVD
baseurl=file:///mnt/rhel-dvd/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm]
name=DVD_IWTM
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/Linux/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm-cfdb]
name=DVD_IW-CFDB
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/cfdb/
enabled=0
gpgcheck=0
```

> **Важно!**
>
> Если текст файла отличается, замените его на указанный.

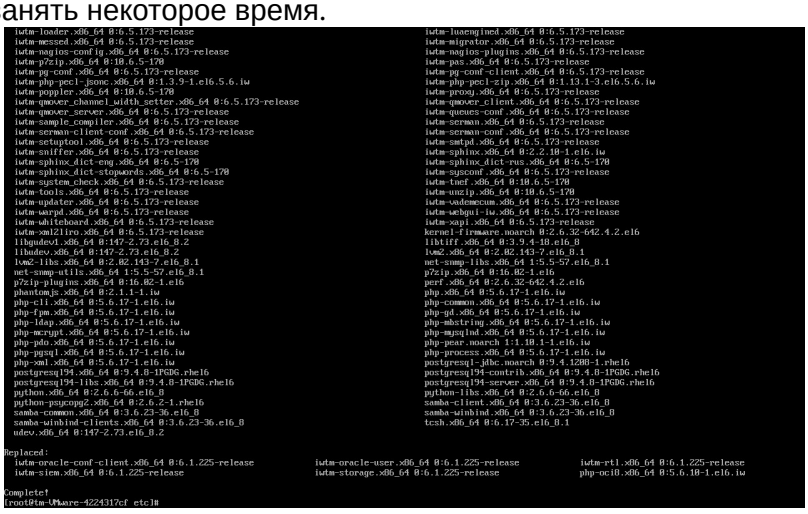
15. В параметрах `enabled` блоков `[rhel-dvd]` и `[rhel-dvd-iwtm]` замените значения с `0` на `1`.
16. Нажмите **F2**.
17. В открывшемся окне подтвердите сохранение файла, нажав **Save**.
18. Нажмите **F10**.

19. Нажмите **F3** и убедитесь в корректности содержимого файла, затем снова нажмите **F3** для закрытия файла.
20. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    ```
    exit
    ```
21. Введите команду для очищения кеша менеджера пакетов:
    ```
    yum clean all
    ```
22. Выполните команды для остановки перехватчиков:
    ```
    service iwtm stop icap
    service iwtm stop smtpd
    service iwtm stop expressd
    service iwtm stop sniffer
    service iwtm stop xapi_xapi
    service iwtm stop xapi_puppy
    ```

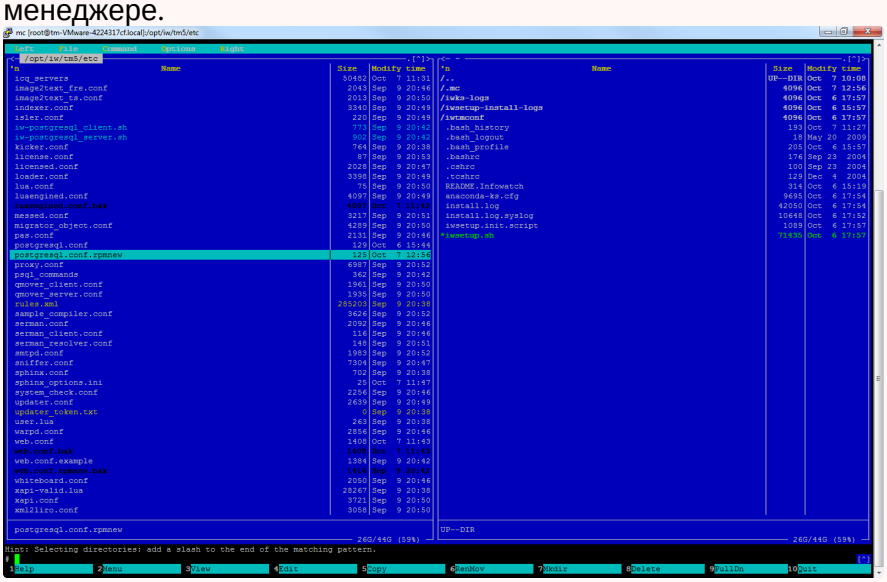
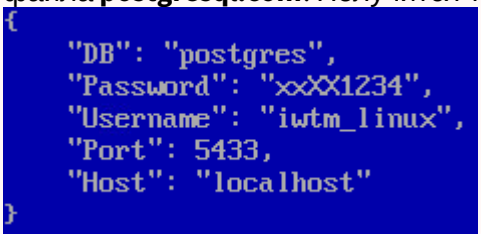
    > **Примечание:**
    >
    > Если в Системе используются два и более серверов перехвата, то к следующему действию следует переходить после выполнения указанных действий на каждом из этих серверов.

23. Снова введите команду для вызова файлового менеджера:
    ```
    mc
    ```
24. Дождитесь, пока обработаются все события, стоящие в очереди на обработку. События, находящиеся в очереди, хранятся в следующих директориях:
    ```
    opt/iw/tm5/queue/analysis/.db/
    opt/iw/tm5/queue/analysis/.in/
    opt/iw/tm5/queue/analysis/.out/
    opt/iw/tm5/queue/db/.db/
    opt/iw/tm5/queue/db/.in/
    opt/iw/tm5/queue/db/.out/
    opt/iw/tm5/queue/smtp/.db/
    opt/iw/tm5/queue/smtp/.in/
    opt/iw/tm5/queue/smtp/.out/
    ```
    По завершении обработки событий данные директории должны стать пустыми.

> **Важно!**
>
> До продолжения обновления настоятельно рекомендуется убедиться в том, что все указанные выше директории пусты . В противном случае нельзя гарантировать успешное обновление и дальнейшую работоспособность Системы.
> Если по какой-либо причине дождаться завершения обработки невозможно, вы можете удалить события из очереди, при этом такие события будут полностью удалены из Системы.
> Чтобы удалить событие, перейдите в нужную директорию в файловом менеджере, установите курсор на планируемом к удалению событии и нажмите **F8**, затем подтвердите удаление, выбрав в открывшемся окне **Yes**.

25. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    `exit`
26. Введите команды для остановки сервисов сервера Traffic Monitor:
    ```
    service iwtm stop
    service php-fpm stop
    service nagios stop
    ```
27. **В зависимости от используемой СУБД** введите команду для запуска процесса обновления пакетов:
    - `yum upgrade --exclude=iwtm-rtl-pg,iwtm-siem-pg,iwtm-policy*` (если используется **СУБД Oracle**)
    - `yum upgrade --exclude=iwtm-rtl-oracle,iwtm-siem-oracle,iwtm-policy*` (если используется **СУБД PostgreSQL**)
28. Перед загрузкой нужных для установки пакетов будет выведен запрос вида
    ```
    Total download size: 4.4 M
    Is this ok [y/N]:
    ```
    . Для продолжения наберите **Y** на клавиатуре и нажмите **Enter**.
    Начнется скачивание пакетов из репозитория, а затем - установка пакетов. Это может занять некоторое время.
    
29. Введите команду для повторной остановки сервиса `php-fpm`:
    ```
    service php-fpm stop
    ```

30. Снова введите команду для вызова файлового менеджера:
    `mc`
31. Если во время использования Системы в конфигурационные файлы с расширением **.conf** вносились изменения, перейдите в директории `/opt/iw/tm5/etc` и `/etc/nginx` и проверьте наличие файлов с расширением **conf.rpmnew**. Если такие файлы есть, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew").

> **Важно!**
>
> При обновлении Traffic Monitor с версии 6.0 или 6.1 до 6.5 и более новых обязательно выполните следующие действия:
>
> a. Перейдите в директорию `/opt/iw/tm5/etc`
> b. Установите курсор на файл **postgresql.conf.rpmnew** в файловом менеджере.
>
> 
>
> c. Нажмите **F4**.
> d. Замените значения секций файла значениями соответствующих секций файла **postgresql.conf**. Получится так:
>
> 
>

> **Примечание:**
>
> При распределенном типе установки значением поля "Host" будет IP-адрес сервера, на котором установлена СУБД. Например:
> `"Host": "10.60.23.6",`

e. Нажмите **F2**.
f. В открывшемся окне подтвердите сохранение файла, нажав **Save**.
g. Нажмите **F10**.
h. Установите курсор на файл **postgresql.conf** в файловом менеджере.
i. Нажмите **F8** для удаления файла **postgresql.conf**.
j. В открывшемся окне подтвердите удаление файла, нажав **Yes**.
k. Выделите файл **postgresql.conf.rpmnew** в файловом менеджере.
l. Нажмите **F6**.
m. В поле **to** введите `/opt/iw/tm5/etc/postgresql.conf` и нажмите **Enter**. Теперь в Системе есть только один конфигурационный файл PostgreSQL - **postgresql.conf**. Он имеет структуру файла новой версии и нужное наполнение:

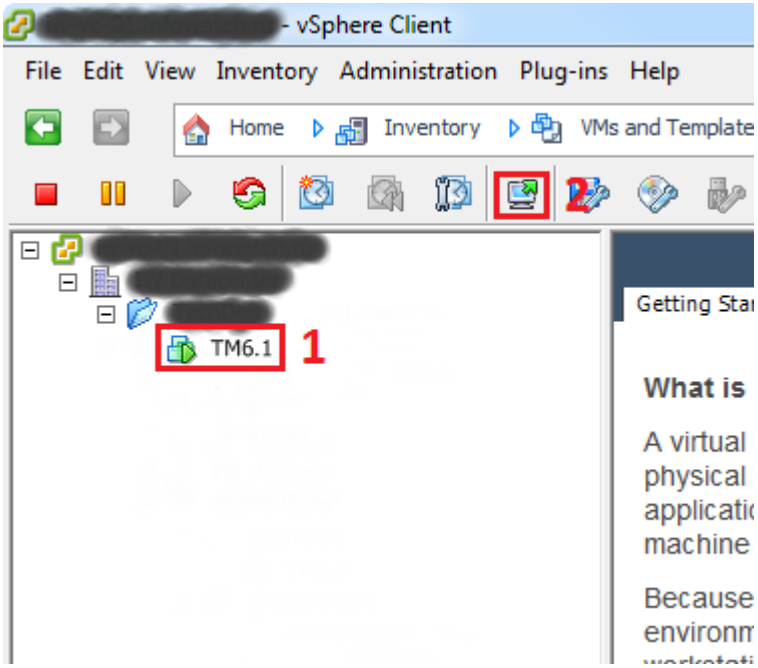
```
{
    "DB": "postgres",
    "Password": "xxXX1234",
    "Username": "iwtm_linux",
    "Port": 5433,
    "Host": "localhost"
}
```

32. Если во время использования Системы в конфигурационные файлы с расширением **.cfg** (служба Nagios) вносились изменения, перейдите в директории `/etc/nagios/iwmon` и `/etc/nagios` и проверьте наличие файлов с расширением **cfg.rpmnew**. Если такие файлы есть, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew").
33. Если во время использования Системы в файлы сценариев LUA (файлы с расширением **.lua**) вносились изменения, перейдите в директорию `/opt/iw/tm5/etc/scripts/` и проверьте наличие файлов с расширением **.lua.rpmnew**. Если такие файлы есть, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew").
34. Обновите сервер СУБД (TME DB Server) - описание смотрите ниже.

ШАГ 2. ОБНОВЛЕНИЕ СЕРВЕРА СУБД (TME DB Server)

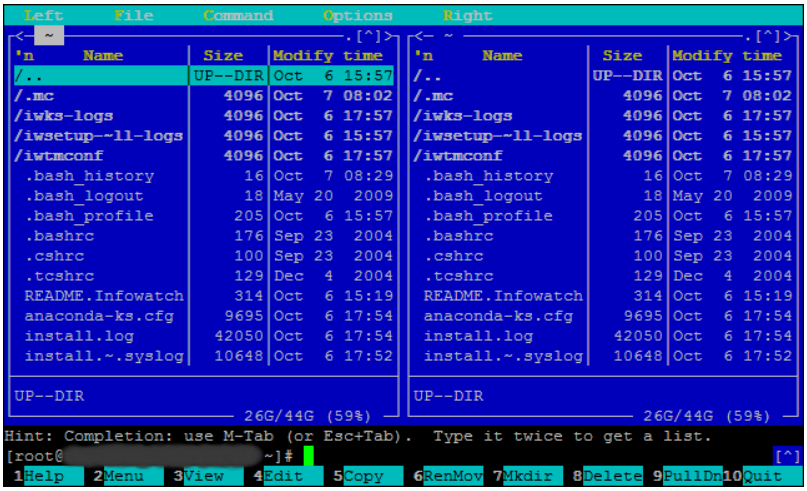
Чтобы обновить Сервер СУБД (TME DB Server), выполните следующие действия:

1. Откройте консоль обновляемого сервера:
   - в случае физического сервера - консоль отображается на экране монитора, подключенного к серверу;
   - в случае виртуального сервера - выполните команду **Launch Virtual Machine Console** (см. пример ниже).



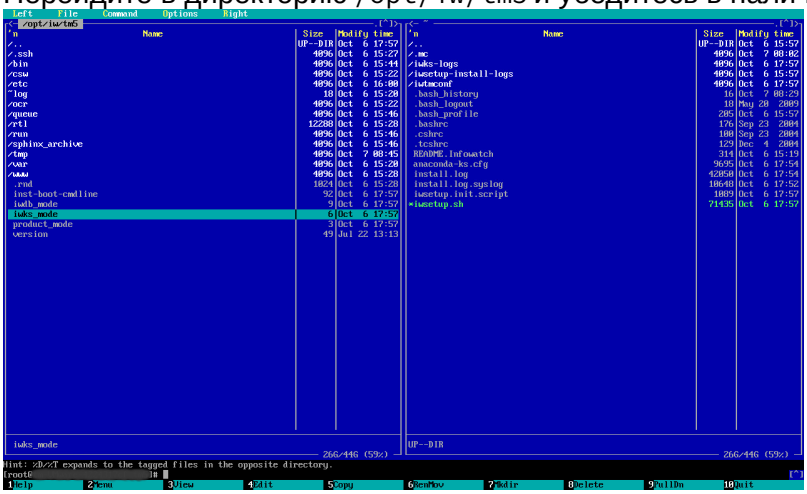
Откроется окно с консолью сервера.

2. В строке **Login as:** (или **login:** - в зависимости от разновидности сервера) введите *root* и нажмите **Enter**.
3. В строке **root@<адрес_сервера>'s password:** (или **Password:** - в зависимости от разновидности сервера) введите пароль пользователя *root* (суперпользователя) и нажмите **Enter**.
   На экране отобразится служебная информация и - последней строкой - приглашение ввести команду (командная строка).
4. Введите команду для вызова файлового менеджера:
   `mc`



На экране отобразится окно файлового менеджера *Midnight Commander*, в котором удобно просматривать файлы.
Навигация в файловом менеджере осуществляется при помощи стрелок клавиатуры и клавиши **Enter** или при помощи мыши. При этом без дополнительных действий вы можете вводить команды в командной строке (она видна в нижней части экрана).
Для перехода на уровень выше установите курсор в поле **/..** (первая строка в файловом менеджере) и нажмите **Enter**.

5. Перейдите в директорию `/opt/iw/tm5` и убедитесь в наличии там файла **iwks_mode**.



> **Примечание:**
>
> Если файл **iwks_mode** отсутствует в директории, то его необходимо создать. Для этого введите команду:
> `touch iwks_mode`

6. Установите курсор на файл **iwks_mode** и нажмите клавишу **F3**.
   На экране отобразится содержимое файла **iwks_mode**: слово "iwdb" (оно указывает на тип установки - **TME DB server**).

> **Примечание:**
>
> Если файл имеет другое содержимое:
> 1. повторно нажмите **F3**.
> 2. нажмите **F4**.
> 3. в открывшемся окне удалите все символы и, в зависимости от редакции Системы, введите `iwdb`
> 4. нажмите **F2**.
> 5. в открывшемся окне подтвердите сохранение файла, нажав **Save**.
> 6. нажмите **F10**.
> 7. нажмите **F3** и убедитесь в корректности содержимого файла.

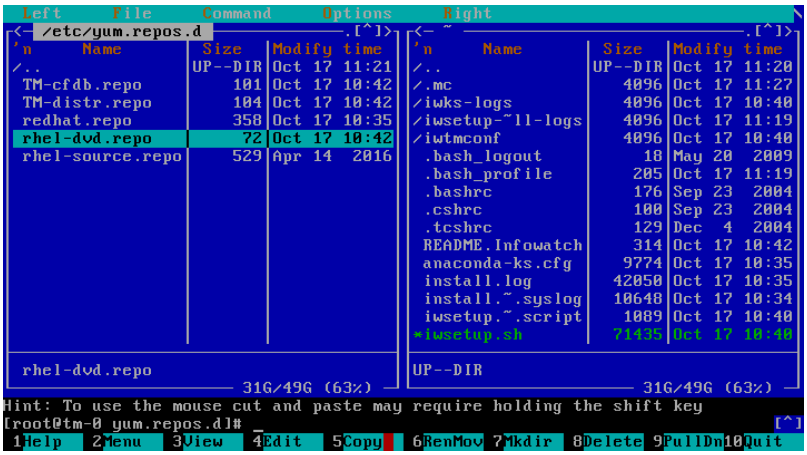
7. Нажмите **F3**.
8. Введите команду:
   `mkdir -p /mnt/rhel-dvd`
   Будет создана директория `/mnt/rhel-dvd`
9. Убедитесь, что диск с дистрибутивом InfoWatch Traffic Monitor подключен к серверу (см. статью "Обновление Системы", действие 2).
10. Введите команду:
    `mount /dev/cdrom /mnt/rhel-dvd`

> **Примечание:**
>
> Между частями команды "/dev/cdrom" и "/mnt/rhel-dvd" есть пробел.

Дистрибутивный диск, находящийся в разделе `/dev/cdrom`, будет подключен в качестве репозитория в директории `/mnt/rhel-dvd`.

11. Перейдите в директорию `/mnt/rhel-dvd` и убедитесь в наличии там файлов и папок. Если директория пуста, повторите действия 9 и 10.
12. Перейдите в директорию `/etc/yum.repos.d` и убедитесь в наличии там файла **rhel-dvd.repo** (этот файл потребуется для указания пути к файлам обновления).

> **Примечание:**
>
> Ввиду того, что в файловом менеджере алфавитная сортировка, папки стоят раньше файлов (поскольку имеют в начале префикс - дробную черту (**/** , *слеш*)). Поэтому директория **/yum.repos.d** стоит одной из последних в списке папок, начинающихся с символа дробной черты (**/**), но до первого файла.



> **Примечание:**
>
> Если файл **rhel-dvd.repo** отсутствует в директории, то его необходимо создать. Для этого введите команду:
> `touch rhel-dvd.repo`

13. Установите курсор на файл **rhel-dvd.repo** и нажмите **F4**.
14. Убедитесь, что файл имеет следующее содержимое:

```
[rhel-dvd]
name=Red Hat Enterprise Linux $releasever - $basearch - DVD
baseurl=file:///mnt/rhel-dvd/
enabled=0
gpgcheck=0
```

```
[rhel-dvd-iwtm]
name=DVD_IWTM
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/Linux/
enabled=0
gpgcheck=0
[rhel-dvd-iwtm-cfdb]
name=DVD_IW-CFDB
baseurl=file:///mnt/rhel-dvd/infowatch/traffic-monitor/cfdb/
enabled=0
gpgcheck=0
```

> **Важно!**
>
> Если текст файла отличается, замените его на указанный.

15. В параметрах `enabled` блоков `[rhel-dvd]` и `[rhel-dvd-iwtm]` замените значения с `0` на `1`.
16. Если вы хотите обновить стандартную БКФ, в параметре `enabled` блока `[rhel-dvd-iwtm-cfdb]` замените значение с `0` на `1`. Произведенные во время работы изменения БКФ будут сохранены.
17. Нажмите **F2**.
18. В открывшемся окне подтвердите сохранение файла, нажав **Save**.
19. Нажмите **F10**.
20. Нажмите **F3** и убедитесь в корректности содержимого файла, затем снова нажмите **F3** для закрытия файла.
21. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    `exit`
22. Введите команду для очищения кеша менеджера пакетов:
    `yum clean all`
23. Введите команду для остановки сервисов сервера Traffic Monitor:
    `service iwtm stop`

> **Примечание:**
>
> При наличии в Системе подсистемы Краулер потребуется приостановить службы указанной подсистемы (на сервере Краулер). Данная процедура выполняется на сервере, где установлена подсистема, стандартными средствами ОС Windows: **Пуск** - **Панель управления** - **Администрирование** - **Службы** , затем потребуется выделить службу в списке служб и нажать **Приостановка службы** .

24. Если в Системе используется СУБД Oracle, выполните следующие действия:
    a. Введите команду для остановки СУБД Oracle:
       service oracle stop
    b. Введите команду для переключения на нужного пользователя:
       `su - oracle`

c. Введите команду для получения списка установленных в Системе патчей:
`/u01/app/oracle/product/db_1/OPatch/opatch lsinventory | grep "Patch" | grep "applied"`

```
[oracle@                    ]$ /u01/app/oracle/product/db_1/OPatch/opatch lsinventory | grep "Patch" | grep "applied"
Patch  21538567     : applied on Tue Nov 22 12:37:41 MSK 2016
Patch  21538558     : applied on Tue Nov 22 12:37:39 MSK 2016
Patch  21538485     : applied on Tue Nov 22 12:37:32 MSK 2016
Patch  21352646     : applied on Tue Nov 22 12:37:31 MSK 2016
Patch  21179898     : applied on Tue Nov 22 12:37:29 MSK 2016
Patch  21051862     : applied on Tue Nov 22 12:37:19 MSK 2016
Patch  21051858     : applied on Tue Nov 22 12:36:56 MSK 2016
Patch  21051852     : applied on Tue Nov 22 12:36:43 MSK 2016
Patch  21051840     : applied on Tue Nov 22 12:36:42 MSK 2016
Patch  21051833     : applied on Tue Nov 22 12:36:41 MSK 2016
Patch  20631274     : applied on Tue Nov 22 12:36:39 MSK 2016
Patch  20506715     : applied on Tue Nov 22 12:36:31 MSK 2016
Patch  20506699     : applied on Tue Nov 22 12:36:24 MSK 2016
Patch  20142975     : applied on Tue Nov 22 12:36:19 MSK 2016
Patch  19972569     : applied on Tue Nov 22 12:36:17 MSK 2016
Patch  19972568     : applied on Tue Nov 22 12:36:14 MSK 2016
Patch  19972566     : applied on Tue Nov 22 12:36:13 MSK 2016
Patch  19972564     : applied on Tue Nov 22 12:36:07 MSK 2016
Patch  19584068     : applied on Tue Nov 22 12:36:00 MSK 2016
Patch  19544839     : applied on Tue Nov 22 12:35:57 MSK 2016
Patch  19463893     : applied on Tue Nov 22 12:35:43 MSK 2016
Patch  18203838     : applied on Tue Nov 22 12:35:37 MSK 2016
Patch  18203837     : applied on Tue Nov 22 12:35:35 MSK 2016
Patch  18203835     : applied on Tue Nov 22 12:35:28 MSK 2016
Patch  17811447     : applied on Tue Nov 22 12:35:27 MSK 2016
Patch  17811438     : applied on Tue Nov 22 12:35:25 MSK 2016
Patch  17811429     : applied on Tue Nov 22 12:35:19 MSK 2016
Patch  19396455     : applied on Tue Nov 22 12:34:40 MSK 2016
```

на экране отобразится список патчей, установленных в Системе. Запишите все номера, указанные после слов "Patch" (в другой записи номер патча - это первые восемь цифр после буквы **p**. Например, номер патча **p19972569_112040_Linux-x86-64.zip** - это 19972569). Данные номера понадобятся для того, чтобы сверить установленные и необходимые для обновления патчи.

d. Снова введите команду для вызова файлового менеджера:
`mc`

e. Перейдите в директорию `/mnt/rhel-dvd/infowatch/extras/OraclePatches` и убедитесь, что номера патчей, расположенных в директории, входят в список номеров патчей, установленных в Системе (которые вы записали).



> **Примечание:**
>
> Если какого-либо патча из директории `/mnt/rhel-dvd/infowatch/extras/OraclePatches` нет в списке установленных, потребуется установить данный патч.

Перед установкой патча может потребоваться обновить утилиту OPatch. Для это выполните следующие действия:

i. Если файловый менеджер *Midnight Commander* работает, для выхода (требуется для лучшего контроля выполнения команд) введите команду:
```
exit
```
ii. Введите команду для перехода в нужную директорию
```
cd /mnt/rhel-dvd/infowatch/extras/OraclePatches
```
iii. Для создания резервной копии введите команду:
```
mv /u01/app/oracle/product/db_1/OPatch /u01/app/oracle/
product/db_1/OPatch_backup
```
iv. Введите команду для извлечения архива с новой версией:
```
unzip p6880880_112000_Linux-x86-64.zip -d /tmp/
```
v. Для предоставления пользователю oracle прав на работу с директорией и файлами введите команду:
```
chown oracle:oinstall -R /tmp/OPatch
```
vi. Для переноса новой версии введите команду:
```
mv /tmp/OPatch /u01/app/oracle/product/db_1
```

Для установки патча выполните следующие действия (пример приведен для патча с номером 12345678 - p12345678_112040_Linux-x86-64.zip):

i. Если файловый менеджер *Midnight Commander* работает, для выхода (требуется для лучшего контроля выполнения команд) введите команду:
```
exit
```
ii. Введите команду для извлечения патча:
```
unzip /mnt/rhel-dvd/infowatch/extras/OraclePatches/
p12345678_112040_Linux-x86-64.zip -d /tmp/
```
iii. Введите команду для перехода в нужную директорию:
```
cd /tmp/12345678/
```
iv. В зависимости от типа патча введите команду для установки:
- `/u01/app/oracle/product/db_1/OPatch/opatch napply . -silent -ocmrf /mnt/rhel-dvd/infowatch/extras/OraclePatches/ocm0.rsp` (в случае копозитного (составного) патча);
- `/u01/app/oracle/product/db_1/OPatch/opatch apply -silent -ocmrf /mnt/rhel-dvd/infowatch/extras/OraclePatches/ocm0.rsp` (в случае одиночного патча).

Когда патч установится, на экран будет выведено сообщение:
```
OPatch completed with warnings.
Press any key to continue..._
```
v. Нажмите любую клавишу для продолжения.
vi. Введите команды для удаления более ненужных файлов:
```
cd /tmp/ && rm -rf /tmp/12345678/ && rm -f /tmp/
PatchSearch.xml
```

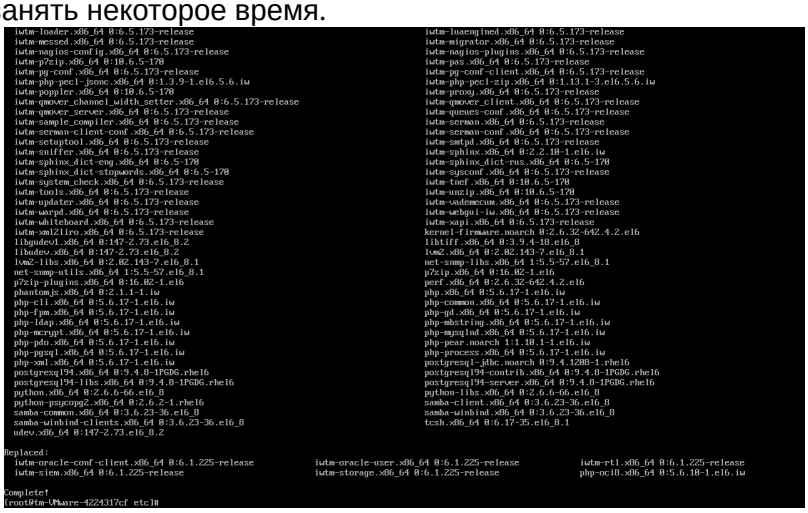
f. Если файловый менеджер *Midnight Commander* работает, для выхода (требуется для лучшего контроля выполнения команд) введите команду:
```
exit
```

g. Введите команду для переключения обратно на пользователя *root*:
`logout`
h. Введите команду для запуска СУБД Oracle:
`service oracle start`

25. **В зависимости от используемой СУБД и необходимости обновить БКФ** введите команду для запуска процесса обновления пакетов:
    a. Если в параметре `enabled` блока `[rhel-dvd-iwtm-cfdb]` установлено значение `0`:
        - `yum upgrade --exclude=iwtm-rtl-pg,iwtm-siem-pg,iwtm-policy*` (если используется **СУБД Oracle**)
        - `yum upgrade --exclude=iwtm-rtl-oracle,iwtm-siem-oracle,iwtm-policy*` (если используется **СУБД PostgreSQL**)

    b. Если в параметре `enabled` блока `[rhel-dvd-iwtm-cfdb]` установлено значение `1`
        - `yum upgrade --exclude=iwtm-rtl-pg,iwtm-siem-pg` (если используется **СУБД Oracle**)
        - `yum upgrade --exclude=iwtm-rtl-oracle,iwtm-siem-oracle` (если используется **СУБД PostgreSQL**)

26. Перед загрузкой нужных для установки пакетов будет выведен запрос вида
```
Total download size: 4.4 M
Is this ok [y/N]:
```
. Для продолжения наберите **Y** на клавиатуре и нажмите **Enter**.
Начнется скачивание пакетов из репозитория, а затем - установка пакетов. Это может занять некоторое время.



27. Снова введите команду для вызова файлового менеджера:
`mc`
28. Если во время использования Системы в конфигурационные файлы с расширением **.conf** вносились изменения, перейдите в директории `/opt/iw/tm5/etc` и `/etc/nginx` и проверьте наличие файлов с расширением **conf.rpmnew**. Если такие файлы есть, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew").

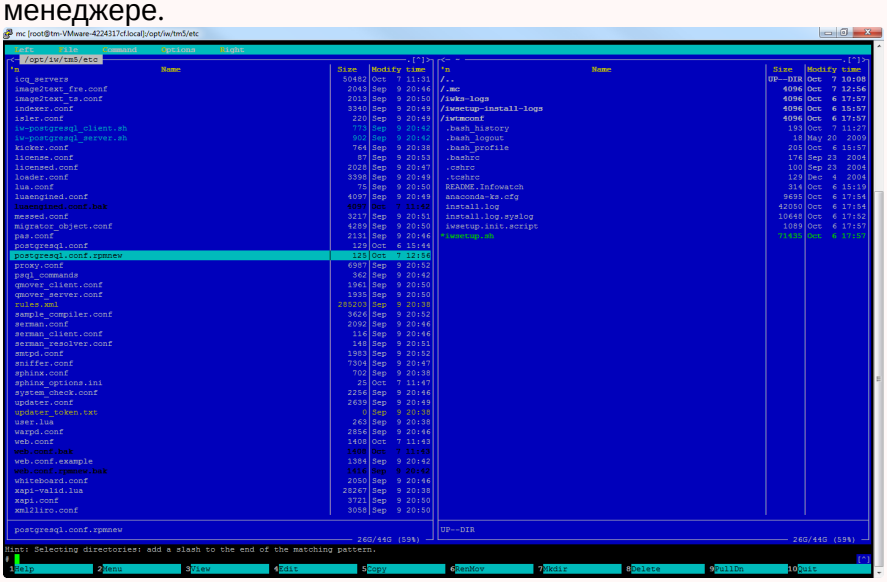
Важно!

На данном этапе необходимо убедиться, что в конфигурационном файле **serman.conf** , в секции *DefaultInterface* , указан IP-адрес сервера с СУБД.

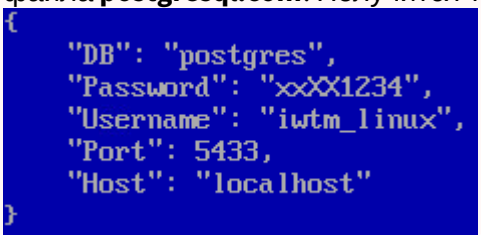
Важно!

При обновлении Traffic Monitor с версии 6.0 или 6.1 до 6.5 и более новых обязательно выполните следующие действия:

a. Перейдите в директорию `/opt/iw/tm5/etc`
b. Установите курсор на файл **postgresql.conf.rpmnew** в файловом менеджере.



c. Нажмите **F4**.
d. Замените значения секций файла значениями соответствующих секций файла **postgresql.conf**. Получится так:



> **Примечание:**
>
> При распределенном типе установки значением поля "Host" будет IP-адрес сервера, на котором установлена СУБД. Например:
> `"Host": "10.60.23.6",`

e. Нажмите **F2**.
f. В открывшемся окне подтвердите сохранение файла, нажав **Save**.
g. Нажмите **F10**.
h. Установите курсор на файл **postgresql.conf** в файловом менеджере.
i. Нажмите **F8** для удаления файла **postgresql.conf**.
j. В открывшемся окне подтвердите удаление файла, нажав **Yes**.
k. Выделите файл **postgresql.conf.rpmnew** в файловом менеджере.
l. Нажмите **F6**.
m. В поле **to** введите `/opt/iw/tm5/etc/postgresql.conf` и нажмите **Enter**. Теперь в Системе есть только один конфигурационный файл PostgreSQL - **postgresql.conf**. Он имеет структуру файла новой версии и нужное наполнение:

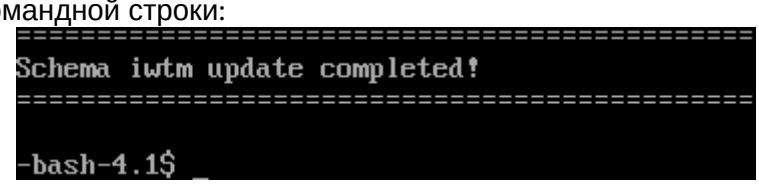
```
{
    "DB": "postgres",
    "Password": "xxXX1234",
    "Username": "iwtm_linux",
    "Port": 5433,
    "Host": "localhost"
}
```

29. Если во время использования Системы в конфигурационные файлы с расширением **.cfg** (служба Nagios) вносились изменения, перейдите в директории `/etc/nagios/iwmon` и `/etc/nagios` и проверьте наличие файлов с расширением **cfg.rpmnew**. Если такие файлы есть, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew").
30. Если во время использования Системы в файлы сценариев LUA (файлы с расширением **.lua**) вносились изменения, перейдите в директорию `/opt/iw/tm5/etc/scripts/` и проверьте наличие файлов с расширением **.lua.rpmnew**. Если такие файлы есть, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew").
31. **В зависимости от используемой СУБД** перейдите в директорию:
    - `/opt/iw/tm5/csw/oracle` (если используется **СУБД Oracle**);
    - `/opt/iw/tm5/csw/postgres` (если используется **СУБД PostgreSQL**).

32. Выделите файл **database.conf**.



33. Нажмите **F3**.
34. Убедитесь, что для параметра `\set schema_version` указана версия, до которой происходит обновление. Если указана старая версия, повторите действия 25 - 33.
35. Нажмите **F3**.
36. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    `exit`
37. Введите команду для остановки служб:
    `service iwtm stop`
38. Убедитесь, что нет активных пользователей, подключенных к серверу через консоль управления (во всех веб-консолях произведен выход).
39. **В зависимости от используемой СУБД** введите команду для переключения на нужного пользователя:
    - `su - oracle` - для переключения на пользователя *oracle* (если в Системе используется **СУБД Oracle**)
    - `su - postgres` - для переключения на пользователя *postgres* (если в Системе используется **СУБД PostgreSQL**)
40. **В зависимости от используемой СУБД** введите команду для перехода в нужную директорию:
    - `cd /opt/iw/tm5/csw/oracle` - (если в Системе используется **СУБД Oracle**)
    - `cd /opt/iw/tm5/csw/postgres` - (если в Системе используется **СУБД PostgreSQL**)
41. Введите команду для запуска скрипта (сценария) обновления БД:
    `./update.sh`
    Начнется процесс обновления схемы данных. Это может занять некоторое время. По окончании обновления на экране отобразятся информационное сообщение и приглашение командной строки:



42. Если пакет `web-gui` установлен на сервере СУБД (TME DB Server), введите команду для очистки кеша:
    `redis-cli flushall`
43. Введите команду для переключения обратно на пользователя *root* (суперпользователя):

```
logout
```

44. Введите команду для запуска службы *iw_serman*:
```
service iwtm start serman
```
45. Проверьте работоспособность внутренних сервисов Системы - описание смотрите ниже.

ШАГ 3. ПРОВЕРКА РАБОТОСПОСОБНОСТИ ВНУТРЕННИХ СЕРВИСОВ СИСТЕМЫ

Запустите службы `iw_bookworm`, `iw_licensed`, `iw_updater` и `iw_kicker` на тех серверах, на которых они установлены и добавлены в автозапуск, и проверьте их состояние.

Для корректной работы службы **`iw_licensed`** и **`iw_kicker`** должны быть запущены в единственном экземпляре.

> **Важно!**
>
> Если служба не запустилась успешно, проверьте соответствующий лог-файл на наличие ошибок в процессе обновления и обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.
> Вы также можете посетить раздел технической поддержки на нашем сайте:
>
> http://www.infowatch.ru/support.
>
> Лог-файлы служб для проверки:
>
> - `/opt/iw/tm5/log/bookworm.log` - для службы `iw_bookworm`
> - `/opt/iw/tm5/log/updater.log` - для службы `iw_updater`
> - `/opt/iw/tm5/log/licserv.log` - для службы `iw_licensed`
> - `/opt/iw/tm5/log/web-console-error.log` - для службы `iw_kicker`
>
> Лог-файлы служб рекомендуется проверить и в случае успешного запуска служб, чтобы исключить возникновение ошибок.
> Рекомендованный уровень логирования для проверки - не ниже INFO. Лог-файл может отсутствовать, если не было записей об ошибках.

Для проверки выполните следующие действия:

1. Для установки необходимых утилит на всех Серверах TM (TME Node Server) введите команду:
```
yum install iwtm-qatools
```
Перед загрузкой пакетов будет выведен запрос вида
==========
==========
Package Arch Version Repository Size
==========
==========
Installing:
iwtm-qatools x86_64 6.7.21.419-release TM-distr 3.9 M
Installing for dependencies:
iwtm-adlibitum-tool x86_64 6.7.21.419-release TM-distr 121 k
iwtm-liro2json x86_64 6.7.21.419-release TM-distr 405 k

Transaction Summary
==========

```
==========================================
Install 3 Package(s)

Total download size: 4.4 M
Installed size: 22 M
Is this ok [y/N]:
```

Для продолжения наберите **Y** на клавиатуре и нажмите **Enter**.

2. Выполните команду для запуска службы `iw_bookworm`**:**
   ```
   service iwtm start bookworm
   ```
3. Службе может потребоваться время на включение. Для проверки состояния службы введите команду:
   ```
   /opt/iw/tm5/bin/serman_prober --action GetServices -p /opt/iw/tm5/etc -l info --host localhost --port 9998 --username serman_client --password <пароль_для_подключения> 2>&1 | grep bookworm
   ```
   где <пароль_для_подключения> - пароль, необходимый для подключения к службе `serman`. Он указан в файле `/opt/iw/tm5/etc/`**`serman.conf`** в блоке "`serman_client`".
   В нашем примере команда будет следующей:
   ```
   /opt/iw/tm5/bin/serman_prober --action GetServices -p /opt/iw/tm5/etc -l info --host localhost --port 9998 --username serman_client --password xx1234 2>&1 | grep bookworm
   ```

   В результате выполнения команды будет выведена информация об указанной службе:
   ```
   6 2019-04-08 16:57:33.293297 (10778:0x00007f267ca27720) [INFO   ] : <Root> {service_name: bookworm, host: 10.60.21.159, port: 9090, status: {load: 0}}
   ```
4. Проверьте значения блоков "`host`" и "`port`":
   a. В блоке "host" должен быть указан IP-адрес ноды, на которой установлена проверяемая служба;
   b. В блоке "port" должен быть указан порт, который задан в конфигурационном файле проверяемой службы.
5. Выполните команду для запуска службы `iw_licensed`**:**
   ```
   servicve iwtm start licensed
   ```
6. Службе может потребоваться время на включение. Для проверки состояния службы введите команду:
   ```
   /opt/iw/tm5/bin/serman_prober --action GetServices -p /opt/iw/tm5/etc -l info --host localhost --port 9998 --username serman_client --password <пароль_для_подключения> 2>&1 | grep licserv
   ```

   где <пароль_для_подключения> - пароль, необходимый для подключения к службе `serman`. Он указан в файле `/opt/iw/tm5/etc/`**`serman.conf`** в блоке "`serman_client`".
   В нашем примере команда будет следующей:
   ```
   /opt/iw/tm5/bin/serman_prober --action GetServices -p /opt/iw/tm5/etc -l info --host localhost --port 9998 --username serman_client --password xx1234 2>&1 | grep licserv
   ```

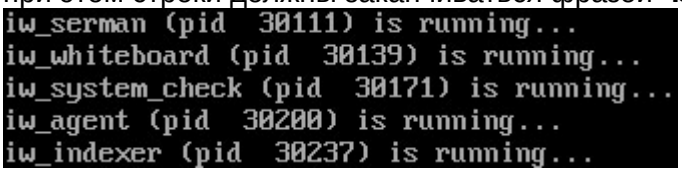
   Выполните действие 4 текущего шага.
7. Выполните команду для запуска службы `iw_updater`**:**
   ```
   service iwtm start updater
   ```
8. Службе может потребоваться время на включение. Для проверки состояния службы `iw_updater` необходимо проверить файл `/opt/iw/tm5/log/updater.log` на наличие ошибок в процессе обновления.
   Введите команду, предварительно убедившись, что адрес в команде указан верно:

`grep -r 'error' /opt/iw/tm5/log/updater.log || echo "All good"`
В случае отсутствия ошибок будет выведено сообщение `All good`.

9. Выполните команду для запуска службы `iw_kicker`:
   `service iwtm start kicker`
10. Службе может потребоваться время на включение. Для проверки состояния службы `iw_kicker` необходимо проверить файл `/opt/iw/tm5/log/web-console-error.log` на наличие ошибок в процессе обновления.
    Введите команду, предварительно убедившись, что адрес в команде указан верно:
    `grep -r 'error' /opt/iw/tm5/log/web-console-error.log || echo "All good"`
    В случае отсутствия ошибок будет выведено сообщение `All good`.
11. Выполните команду для остановки служб:
    `service iwtm stop`
12. Завершите обновление сервера БД - описание смотрите ниже.

ШАГ 4. ЗАВЕРШЕНИЕ ОБНОВЛЕНИЯ НА СЕРВЕРЕ СУБД (TME DB Server)

Чтобы завершить обновление на Сервере СУБД (TME DB Server) , выполните следующие действия:

1. Введите команду для перезагрузки сервера:
   `reboot`
2. Дождитесь загрузки сервера и выполните вход от имени пользователя *root* (ШАГ 1, действия **2** и **3** данной инструкции).
3. Введите команду для проверки запуска процессов:
   `service iwtm status`
   На экране отобразится список процессов и их статус. Сервисы должны быть запущены, при этом строки должны заканчиваться фразой "**is running...**":
   

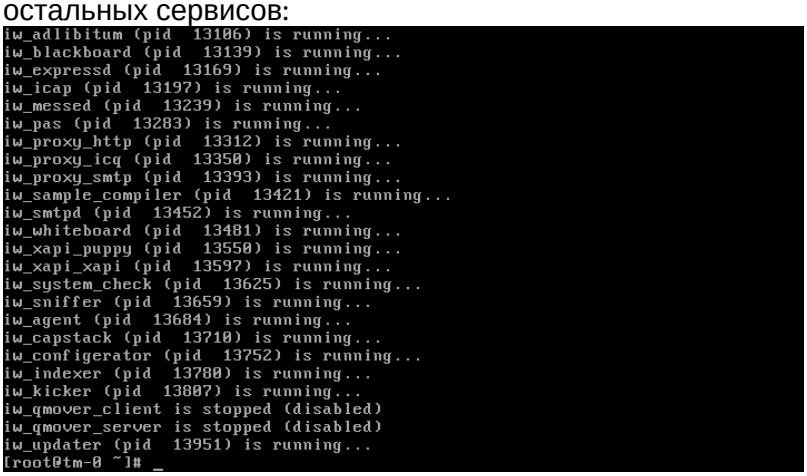
4. Запустите все Серверы TM (TME Node Server) - описание смотрите ниже.

ШАГ 5. ПЕРЕЗАПУСК СЕРВЕРОВ TM (TME Node Server)

Чтобы перезапустить Серверы TM (TME Node Server), на каждом из них выполните следующие действия:

1. Если пакет `web-gui` установлен на сервере TM (TME Node Server), введите команду для очистки кеша:
   `redis-cli flushall`
2. Введите команду для перезагрузки сервера:
   `reboot`
3. Дождитесь загрузки сервера и выполните вход от имени пользователя *root* (ШАГ 1, действия **2** и **3** данной инструкции).
4. Введите команду для проверки запуска процессов:
   `service iwtm status`
   На экране отобразится список процессов и их статус. Обычно сервисы `iw_qmover_client` и `iw_qmover_server` бывают остановлены, а все остальные сервисы - запущены, при этом строки должны заканчиваться фразой "**is stopped (disabled)...**" для сервисов `iw_qmover_client` и `iw_qmover_server` и фразой "**is running...**" для всех

остальных сервисов:



Примечание:

При наличии в Системе подсистемы Краулер потребуется запустить службы указанной подсистемы (на сервере Краулер). Данная процедура выполняется на сервере, где установлена подсистема, стандартными средствами ОС Windows: **Пуск** - **Панель управления** - **Администрирование** - **Службы**, затем потребуется выделить службу в списке служб и нажать **Запуск службы**.

Обновление серверов Traffic Monitor распределенного типа установки завершено. Номер версии Системы в окне **О системе** Консоли управления Traffic Monitor должен измениться на новый. Если в Системе есть другие серверы или подсистемы, подлежащие обновлению, воспользуйтесь инструкциями данного раздела.

Примечание:

Для корректного отображения консоли управления до начала работ удалите кеш в вашем браузере. Данное действие выполняется стандартными средствами браузера.

4.3 Обновление подсистемы Краулер

Чтобы обновить подсистему Краулер:

1. Удалите текущую версию Краулера, как описано в статье "Удаление подсистемы Краулер".
2. Установите новую версию Краулера, как описано в статье "Установка подсистемы Краулер".

4.4 Обновление InfoWatch Device Monitor

Если у вас установлен InfoWatch Device Monitor, то вы можете обновить его до более поздней версии.

Обновление Device Monitor выполняется в том же порядке, что и установка:

1. Обновление серверной части InfoWatch Device Monitor (база данных, сервер, и консоль управления).

   Важно!

   Если требуется обновить Device Monitor до версии 6.9, данное обновление необходимо проводить последовательно - сначала обновляя до промежуточных версий. Например, обновить DM 6.5 следует сначала до 6.7, а уже затем до 6.9.
   Если требуется обновить Device Monitor версии 3.4, удалите старую версию сервера (не удаляя базу данных) и установите сервер заново, указав при этом параметры соединения с существующей базой данных. Начиная с версии 4.0 обновление выполняется без удаления предыдущей версии.
   При обновлении Device Monitor версии 6.0 путем удаления и повторной установки Сервера, для того, чтобы Агенты Device Monitor смогли подключиться и привязаться к новому серверу, необходимо:
   1. При удалении - сохранить ключ шифрования, хранящийся в папке установки сервера DM, файл `SSLServerKey.pfx`.
   2. При установке - указать путь к сохраненному ключу шифрования, который использовался на старом сервере.

2. Обновление Агента InfoWatch Device Monitor.
   InfoWatch Device Monitor поддерживает совместимость с прежними версиями Агента, начиная с 3.4.875. Поэтому обновление Агента выполняется по мере необходимости.

   Важно!

   Обновление Агентов Device Monitor следует проводить после обновления Сервера Device Monitor и Сервера Traffic Monitor.

4.4.1 Обновление серверной части InfoWatch Device Monitor

Важно!

Если требуется обновить Device Monitor версии **3.4** - **4.0**, удалите старую версию сервера (не удаляя базу данных) и установите сервер заново, указав при этом параметры соединения с существующей базой данных.
Начиная с версии **4.0**, обновление выполняется без удаления предыдущей версии.
При обновлении Device Monitor версии **6.0** путем удаления и повторной установки Сервера, для того чтобы Агенты Device Monitor смогли подключиться и привязаться к новому серверу, необходимо:

1. При удалении - сохранить ключ шифрования, хранящийся в папке установки сервера DM, файл `SSLServerKey.pfx`.
2. При установке - указать путь к сохраненному ключу шифрования, который использовался на старом сервере.

Шаг 1. Начало обновления

> **Важно!**
>
> При использовании нескольких серверов начните установку обновления с главного сервера. При этом обязательно выключите все используемые второстепенные серверы. Обновление серверов происходит по очереди, начиная с главного сервера.

Откройте папку с дистрибутивом Device Monitor. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы.

В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите кнопку **Далее**, чтобы перейти к следующему окну мастера установки.

Шаг 2. Принятие лицензионного соглашения

Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите **Далее**.

Шаг 3. Настройка базы данных

При обновлении база данных сохраняется, и в окне **Установка или обновление базы** по умолчанию указываются параметры ранее использовавшейся базы данных. Однако вам потребуется указать некоторые параметры, в зависимости от используемой СУБД.

Обновление встроенной базы данных

Если вы используете встроенную БД, то этот шаг пропускается.

Обновление базы данных под управлением СУБД Microsoft SQL Server

На панели **Способ аутентификации** выберите способ аутентификации, назначенный пользователю, от имени которого обновляется база данных. В качестве значения данного параметра укажите способ аутентификации, выбранный при подготовке учетной записи (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server").

Если учетной записи назначена аутентификация Windows, то выберите значение **Аутентификация Windows**.

Если учетной записи назначена встроенная аутентификация SQL Server, выберите значение **Встроенная в SQL Server**. Затем укажите имя и пароль подготовленной учетной записи в полях **Имя пользователя** и **Пароль** соответственно.

> **Примечание:**
>
> В процессе обновления вы можете указать прежние параметры аутентификации или задать новые. Рекомендации по выбору способа аутентификации и подготовке необходимой учетной записи приведены в статье "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server".

Обновление базы данных под управлением СУБД Oracle

На панели **Сервер БД** укажите параметр **Пароль для 'SYSTEM'** - пароль учетной записи пользователя SYSTEM, используемый для работы с обновляемой базой данных.

На панели **Данные о схеме** укажите параметры **Пароль**, **Подтверждение пароля** - пароль учетной записи владельца схемы базы данных, используемый для работы с обновляемой базой данных.

Обновление базы данных под управлением PostgreSQL

В поле **Пароль** укажите пароль учетной записи, используемой для работы с обновляемой базой данных.

После того как необходимые параметры будут настроены, нажмите кнопку **Далее**.

Шаг 4. Завершение обновления

После перехода к следующему окну, нажмите на кнопку **Установить**, чтобы запустить процесс обновления серверной части Device Monitor.

Следуйте дальнейшим указаниям мастера установки, чтобы завершить обновление серверной части.

> **Примечание:**
>
> При обновлении сервера Device Monitor конвертация фильтров предыдущей версии не предусмотрена.

4.4.2 Обновление Агента InfoWatch Device Monitor

Device Monitor поддерживает совместимость с версиями Агента, начиная от 3.4.875 включительно. Таким образом, обновленные компоненты Device Monitor могут работать со старыми версиями Агента. Однако вы можете обновить Агента до более поздней версии.

Обновление Агента выполняется аналогично установке:

- локальное обновление с использованием мастера установки;
- удаленное обновление с помощью средств распространения программного обеспечения;
- централизованное обновление через Консоль управления (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", раздел "Удаленная установка, обновление и удаление Клиентов").

Чтобы успешно установить или обновить Агент InfoWatch Device Monitor, следуйте рекомендациям, указанным на странице Установка Агента InfoWatch Device Monitor.

При обновлении Агента Device Monitor до новой версии следует действовать следующим образом:

1. Произвести обновление на группе не более 10 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
2. Произвести обновление на группе не более 50 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
3. Произвести обновление на группе не более 500 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
4. Произвести обновление на группе не более 1000 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
5. Произвести обновление на оставшихся компьютерах до полного завершения процесса обновления.

4.5 Объединение конфигурационных файлов .conf, .cfg и .lua с файлами .conf.rpmnew, .cfg.rpmnew и .lua.rpmnew

Во время обновления сервера Traffic Monitor файлы с расширениями **.conf**, **.cfg** и **.lua**, которые были изменены во время использования предыдущей версии, не перезаписываются новыми. В тех же директориях создаются новые файлы с теми же названиями, но с расширением **.conf.rpmnew**, **.cfg.rpmnew** и **.lua.rpmnew** , соответственно. Это сделано для того, чтобы поддержать возможность изменения структуры файлов новых версий. Для корректной работы Системы потребуется объединить файлы старой и новой версий.

Используйте любой из приведенных ниже способов объединения файлов.

4.5.1 Объединение конфигурационных файлов в Midnight Commander

Рассмотрим объединение на примере файлов **postgresql.conf** и **postgresql.conf.rpmnew**.

> **Подсказка:**
>
> Чтобы просмотреть файл, нажмите **F3**, чтобы отредактировать - **F4**.

Файл **postgresql.conf** имеет вид:

```
{
    "DB": "postgres",
    "Host": "localhost",
    "Password": "xxXX1234",
    "Port": 5433,
    "Username": "iwtm_linux"
}
```

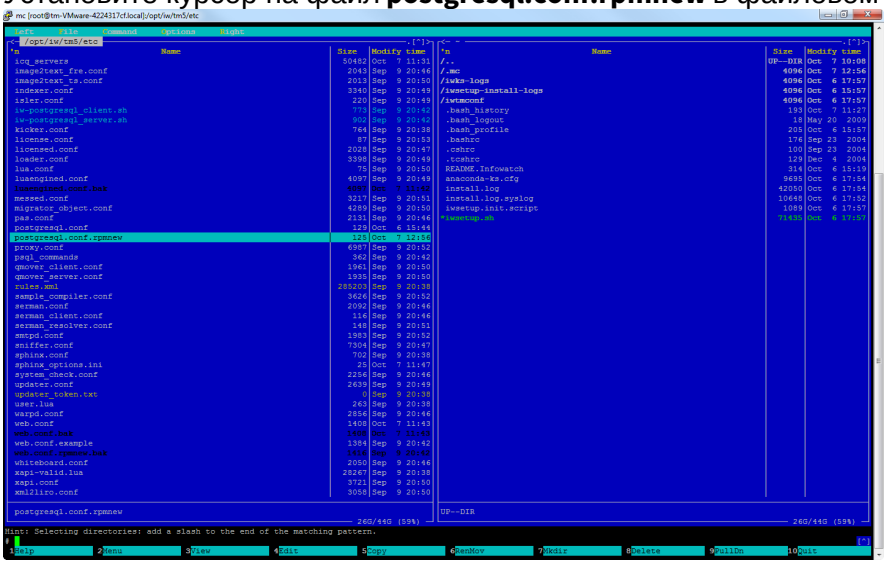
Файл **postgresql.conf.rpmnew** имеет вид:

```
{
    "DB": "put postgresql database name here",
    "Password": "put postgresql password here",
    "Username": "put postgresql username here",
    "Port": 5432,
    "Host": "put postgresql host address here"
}
```

Для объединения требуется перенести данные из секций файла **postgresql.conf** в соответствующие секции файла **postgresql.conf.rpmnew**. Для этого:

1. Перейдите в директорию `/opt/iw/tm5/etc`

2. Установите курсор на файл **postgresql.conf.rpmnew** в файловом менеджере.



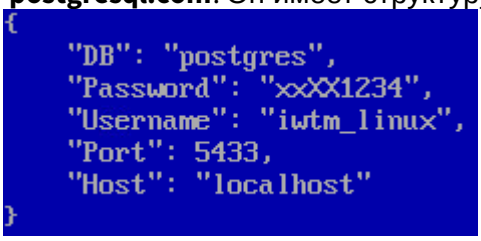
3. Нажмите **F4**.
4. Замените значения секций файла значениями соответствующих секций файла **postgresql.conf**. Получится так:

```
{
    "DB": "postgres",
    "Password": "xxXX1234",
    "Username": "iwtm_linux",
    "Port": 5433,
    "Host": "localhost"
}
```

> **Примечание:**
>
> При распределенном типе установки значением поля "Host" будет IP-адрес сервера, на котором установлена СУБД. Например: `"Host": "10.60.23.6",`

5. Нажмите **F2**.
6. В открывшемся окне подтвердите сохранение файла, нажав **Save**.
7. Нажмите **F10**.
8. Установите курсор на файл **postgresql.conf** в файловом менеджере.
9. Нажмите **F8** для удаления файла **postgresql.conf**.
10. В открывшемся окне подтвердите удаление файла, нажав **Yes**.
11. Выделите файл **postgresql.conf.rpmnew** в файловом менеджере.
12. Нажмите **F6**.
13. В поле **to** введите `/opt/iw/tm5/etc/postgresql.conf` и нажмите **Enter**.
    Теперь в Системе есть только один конфигурационный файл PostgreSQL -

postgresql.conf. Он имеет структуру файла новой версии и нужное наполнение:



4.5.2 Объединение конфигурационных файлов с помощью vimdiff

Рассмотрим объединение на примере файлов **iwssid.lua** и **iwssid.lua.rpmnew**. После обновления (при условии, если в штатный файл **iwssid.lua** вносились изменения) появится файл **iwssid.lua.rpmnew**. Необходимо корректно перенести все установленные ранее значения параметров и настроек из **iwssid.lua.rpmnew** в **iwssid.lua**. Для этого:

1. Перейдите в директорию `/opt/iw/tm5/etc/scripts`
2. Введите в командной строке:
   `vimdiff iwssid.lua.rpmnew iwssid.lua`
3. Перейдите в режим редактирования (клавиша **Insert**).
4. Вручную перенесите различающиеся значения параметров из **iwssid.lua.rpmnew** в **iwssid.lua.**
5. Выйдите из режима редактирования (клавиша **Esc**).
6. Сохраните изменения в файле **iwssid.lua** и выйдите из редактора (введите **:wq**).
7. Закройти уже не актуальный файл **iwssid.lua.rpmnew** (введите **:q**).
8. Удалите файл **iwssid.lua.rpmnew.**

Важно!

Чтобы избежать потери данных и ошибок в работе Системы (конфигурационные файлы серверной части Traffic Monitor) необходимо внимательно следовать инструкциям.

Важно!

Во избежание некорректной работы Системы не стоит объединять следующие файлы с файлами из старых версий:

1. /etc/pear.conf.rpmnew
2. /etc/php-fpm.d/www.conf.rpmnew
3. /etc/rc.d/init.d/postgresql-9.4.rpmnew
4. /etc/sgml/docbook/xmlcatalog.rpmnew

5 Удаление Системы

Удаление Системы подразумевает удаление всех пакетов Системы, а также удаление используемой схемы базы данных. Для полного удаления операционной системы и СУБД вы можете, например, выполнить форматирование используемых разделов стандартными средствами.

- О порядке удаления схемы БД (как Oracle, так и PostrgreSQL) см. "Удаление схемы базы данных".
- О порядке удаления Device Monitor (серверная и клиентская часть) см. "Удаление InfoWatch Device Monitor"
- Подсистема Crawler (как сервер, так и сканер) удаляется стандартными средствами ОС Windows: **Пуск -> Панель управления -> Программы и компоненты**, команда **Удалить**.
- Чтобы удалить отдельный пакет, выполните команду:
  ```
  rpm –e имя_пакета
  ```
- Все серверные компоненты Traffic Monitor (в том числе компоненты веб-консоли, модули Sniffer, IW ICAP, модуль взаимодействия с удаленной базой данных и другие) удаляются при помощи следующей команды:
  ```
  yum remove `rpm –qa | grep iwtm`
  ```

По окончании удаления Сервера Traffic Monitor верните внешнюю инфраструктуру, настроенную на Traffic Monitor, в исходное состояние:

- если выполнялась интеграция с почтовым relay-сервером - убедитесь, что параметры Postfix возвращены в исходное состояние;
- если Система выполняла перехват и фильтрацию SMTP-трафика - настройте доставку SMTP-писем через корпоративный почтовый сервер, минуя InfoWatch Traffic Monitor.

После удаления на компьютере остаются только:

- операционная система;
- конфигурационные файлы, в которые были внесены изменения (измененным файлам присваивается суффикс **.rpmsave** - например, **detector.conf.rpmsave**; файлы, которые не изменялись, будут удалены);
- очередь объектов (о порядке удаления файлов из директории временных файлов операционной системы и данных из директорий файловых очередей Traffic Monitor см. «*InfoWatch Traffic Monitor. Руководство администратора*», статья "Удаление временных файлов");
- категории и термины;
- файл лицензии;
- учетная запись пользователя – владельца InfoWatch Traffic Monitor, и группа, в состав которой входил этот пользователь.

5.1 Удаление схемы базы данных

Данная инструкция актуальна для СУБД Oracle и PostrgreSQL.

Важно

Не удаляйте схему базы данных, от которой для архивирования были отключены ежедневные табличные пространства. Иначе Вы не сможете восстановить данные из этих табличных пространств.

1. **Проверка сервера СУБД Oracle**
   Убедитесь, что:
   - версия установленной схемы базы данных соответствует версии программного пакета, используемого для ее удаления;
   - запущен сервер СУБД;
   - в конфигурационном файле **database.conf** корректно указаны имя и пароль учетной записи, обладающей правами SYSDBA (значения параметров `sysdba` и `sysdba_password`).
2. **Остановка TrafficMonitor**
   a. Остановить все процессы Traffic Monitor:
   `service iwtm stop`
   b. Закрыть все экземпляры консоли управления;
   c. Остановить веб-сервис:
   `service php-fpm stop`
   d. Прекратить все соединения с удаляемой схемой базы данных, осуществляемые из других программ.
3. **Запуск удаления схемы**
   a. Перейдите в директорию
   `/opt/iw/tm5/csw/oracle` или `/opt/iw/tm5/csw/postgres`
   b. Выполните скрипт:
   ./uninstall.sh

Важно

При удалении схемы БД из Системы будут также удалены следующие компоненты:

- политики, в том числе предустановленные (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Предустановленные политики");
- плагины и токены (см. "*Infowatch Traffic Monitor. Руководство администратора*", статья "Плагины").

Для восстановления плагина Device Monitor и повторного распространения предустановленных политик выполните следующие действия:

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

Далее нужно вручную добавить остальные плагины (см. "*Infowatch Traffic Monitor. Руководство администратора*", статья "Добавление плагина") и создать необходимые политики (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статьи "Создание политики защиты данных" и "Создание политики контроля персон").

5.2 Удаление подсистемы Краулер

Подсистема Crawler (как сервер, так и сканер) удаляется стандартными средствами ОС Windows: **Пуск -> Панель управления -> Программы и компоненты**, команда **Удалить**.

5.3 Удаление InfoWatch Device Monitor

> **Важно!**
>
> Если вы планируете вновь устанавливать сервер Device Monitor, то для обеспечения Агентам Device Monitor возможности подключаться и привязываться к новому серверу, начиная с версии 6.0, рекомендуется сохранить ключ шифрования старого сервера.
>
> Ключ шифрования хранится в папке установки сервера InfoWatch Device Monitor, файл `SSLServerKey.pfx`.

Чтобы удалить серверную часть InfoWatch Device Monitor вместе с Консолью управления:

1. Выполните одно из следующих действий:
   - На диске с дистрибутивом системы откройте каталог `Setup\Unified`. В данном каталоге найдите и запустите файл установки для требуемой платформы.
   - В оснастке **Добавить или удалить программы** (**Add or remove programs**), входящей в состав операционной системы Windows, выберите **InfoWatch Device Monitor Server** и нажмите на кнопку **Изменить** (**Change**).
2. В окне **Изменение, восстановление или удаление…** выберите команду **Удалить**.
3. Если вы хотите удалить систему вместе с базой данных, в окне **Удаление базы данных…** отметьте поле **Удалить базу**. В этом случае вам потребуется задать параметры удаления; параметры зависят от вида используемой СУБД:
   - **Microsoft SQL Server** – укажите используемый способ аутентификации, выбрав нужный вариант на панели **Способ аутентификации** (см. также "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server"). Если аутентификация выполнялась средствами SQL-сервера (**Встроенная в SQL Server**), то на панели **Администратор базы данных**, в полях **Имя пользователя** и **Пароль** укажите параметры той учетной записи, при помощи которой осуществлялось подключение к базе данных.
   - **Oracle** – в поле **Пароль учетной записи SYSTEM** укажите необходимый пароль. В результате будет удалена учетная запись владельца схемы базы данных, а также все объекты, за исключением табличного пространства.
   - **PostgreSQL** – в полях **Имя пользователя** и **Пароль** укажите имя и пароль учетной записи, от имени которой была создана эта БД при установке сервера (см. "Порядок установки серверной части InfoWatch Device Monitor").

> **Важно!**
>
> Если БД не функционирует или ограниченно функционирует, то для удаления InfoWatch Device Monitor рекомендуется снять отметку с поля **Удалить базу**, иначе удаление может произойти не полностью.

4. После того как необходимые параметры будут заданы, нажмите **Далее**, а затем – **Удалить**, чтобы запустить процесс удаления.

Чтобы удалить серверную часть InfoWatch Device Monitor или Консоль управления отдельно:

1. В оснастке **Добавить или удалить программы** (**Add or remove programs**) воспользуйтесь кнопкой **Изменить** (**Change**).
2. В окне **Выборочная установка** нажмите  слева от компонента, который вы намерены удалить, и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**. Нажмите **Далее**.
3. Если на предыдущем шаге вы выбрали для удаления сервер, то в окне **Удаление базы данных…** определите необходимость удаления базы данных и при необходимости задайте параметры учетной записи, имеющей на это права (подробнее см. выше).
4. Нажмите **Изменить**, чтобы запустить процесс удаления.

Чтобы удалить Агент InfoWatch Device Monitor:

на компьютере, где он установлен, в оснастке **Добавить или удалить программы** (**Add or remove programs**) выберите **InfoWatch Device Monitor Client** и воспользуйтесь кнопкой **Удалить** (**Remove**).

Удаление Агентов можно также выполнять централизованно:

- с помощью средств Active Directory (если Агенты были установлены при помощи средств распространения программного обеспечения), как описано в статье "Удаление Агента, установленного с помощью средств распространения программного обеспечения".
- с помощью задач распространения в Консоли управления (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", раздел "Удаленная установка, обновление и удаление Агентов").

> **Важно!**
>
> Выключение питания компьютера в процессе установки/удаления Агента может привести к ошибкам, ведущим к нестабильной работе операционной системы.

О порядке удаления Клиентов с мобильных устройств см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Удаление мобильного устройства".

5.3.1 Удаление Агента, установленного с помощью средств распространения программного обеспечения

Агенты, установленные с помощью средств распространения программного обеспечения, могут быть удалены тем же способом.

Например, если установка Агентов была выполнена через Microsoft Active Directory, то администратор корпоративной сети может удалить назначенное задание на установку из соответствующей групповой

политики. Порядок редактирования групповой политики описывается в статье "Установка Агента с помощью средств распространения программного обеспечения", шаг 3.

Чтобы удалить Агента со всех контролируемых компьютеров:

1. Выделите задание на установку, которое нужно удалить. Затем щелкните правой кнопкой мыши по выделенной строке и в раскрывшемся контекстном меню выберите пункт **All tasks** > **Remove**.
2. В открывшемся диалоговом окне **Remove software** выберите **Immediately uninstall thesoftware from users and computers**.

   > **Примечание.**
   >
   > Если будет выбрано другое действие, то задание на установку будет удалено, но все ранее установленные Агенты останутся. Удаление этих Агентов средствами Microsoft Active Directory в дальнейшем будет невозможно.

3. Нажмите **OK**.

Агент будет удален со всех компьютеров, на которые распространяется выбранная групповая политика.

6 Приложение А. Рекомендации по составлению имен и паролей

Требования к именам пользователей

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

Требования к паролям пользователей

- Длина пароля может составлять от 1 до 30 символов.
- Пароль пользователя может состоять из букв латинского алфавита, цифр и символов:

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

- Пароль чувствителен к регистру символов.

Рекомендации по составлению надежных паролей

- Рекомендуемая длина пароля: от 10 до 30 символов.
- Пароль должен представлять собой смешанный набор букв верхнего и нижнего регистров, цифр и символов.
- Не рекомендуется:
    - включать в состав пароля слова и словосочетания;
    - включать в состав пароля несколько идущих подряд одинаковых символов;
    - начинать и заканчивать пароль одним и тем же символом;
    - создавать новый пароль путем добавления символов к текущему паролю.

Общие рекомендации
Не рекомендуется начинать имена и пароли пользователей с последовательностей: SYS_ и ORA_.
В составе имени и пароля пользователя не рекомендуется использовать зарезервированные слова СУБД Oracle:

ACCESS	EXCLUSIVE	MODE	SELECT
ADD	EXISTS	MODIFY	SESSION
ALL	FILE	NOAUDIT	SET
ALTER	FLOAT	NOCOMPRESS	SHARE
AND	FOR	NOT	SIZE
ANY	FROM	NOWAIT	SMALLINT
AS	GRANT	NULL	START
ASC	GROUP	NUMBER	SUCCESSFUL
AUDITBETWEEN	HAVING	OF	SYNONYM

BY	IDENTIFIED	OFFLINE	SYSDATE
CHAR	IMMEDIATE	ON	TABLE
CHECK	IN	ONLINE	THEN
CLUSTER	INCREMENT	OPTION	TO
COLUMN	INDEX	OR	TRIGGER
COMMENT	INITIAL	ORDER	UID
COMPRESS	INSERT	PCTFREE	UNION
CONNECT	INTEGER	PRIOR	UNIQUE
CREATE	INTERSECT	PRIVILEGES	UPDATE
CURRENT	INTO	PUBLIC	USER
DATE	IS	RAW	VALIDATE
DECIMAL	LEVEL	RENAME	VALUES
DEFAULT	LIKE	RESOURCE	VARCHAR
DELETE	LOCK	REVOKE	VARCHAR2
DESC	LONG	ROW	VIEW
DISTINCT	MAXEXTENTS	ROWID	WHENEVER
DROP	MINUS	ROWNUM	WHERE
ELSE	MLSLABEL	ROWS	WITH

7 Приложение В. Лицензии на стороннее программное обеспечение

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

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

Также использовалось программное обеспечение:

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