

INFOWATCH

InfoWatch Traffic Monitor 6.10

Руководство по установке

29/07/2019

© 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 6
3 Установка Системы 13
3.1 Установка сервера Traffic Monitor и Базы данных 14
3.1.1 Установка ТМ в режиме "Все-в-одном" 15
3.1.2 Распределенная установка ТМ 22
3.1.2.1 Установка Базы данных 23
3.1.2.2 Установка Сервера Traffic Monitor 31
3.2 Установка подсистемы Краулер 36
3.3 Установка InfoWatch Device Monitor 43
3.3.1 Установка серверной части InfoWatch Device Monitor 44
3.3.1.1 Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server 44
3.3.1.2 Рекомендации по развертыванию базы данных под управлением СУБД Oracle 45
3.3.1.3 Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL 46
3.3.1.4 Рекомендации по установке Сервера InfoWatch Device Monitor 46
3.3.1.5 Порядок установки серверной части InfoWatch Device Monitor 48
3.3.2 Установка Агента InfoWatch Device Monitor 59
3.3.2.1 Локальная установка Агента 60
3.3.2.2 Установка Агента с помощью средств распространения программного обеспечения 62
3.3.3 Схема развертывания InfoWatch Device Monitor 65
3.4 Предустановленные серверные параметры 68
4 Обновление Системы 71
4.1 Обновление ТМ Все-в-одном (All-in-one) 75
4.2 Обновление ТМ при распределенной установке 87
4.3 Обновление подсистемы Краулер 107
4.4 Обновление InfoWatch Device Monitor 108
4.4.1 Обновление серверной части InfoWatch Device Monitor 109
4.4.2 Обновление Агента InfoWatch Device Monitor 110

4.5 Объединение конфигурационных файлов 111
4.5.1 Объединение конфигурационных файлов в Midnight Commander 111
4.5.2 Объединение конфигурационных файлов с помощью vimdiff 113
4.6 Обновление СУБД PostgreSQL 114
4.6.1 Подготовка к обновлению 114
4.6.2 Обновление 116
4.6.3 Удаление бэкапа старой БД 117
4.6.4 Откат обновления 118
4.6.5 Действия при ошибках 118
5 Удаление Системы 120
5.1 Удаление схемы базы данных 120
5.2 Удаление подсистемы Краулер 122
5.3 Удаление InfoWatch Device Monitor 122
5.3.1 Удаление Агента, установленного с помощью средств распространения программного обеспечения 124
6 Приложение А. Рекомендации по составлению имен и паролей ... 125
7 Приложение В. Лицензии на стороннее программное обеспечение ... 127

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.

В максимально развернутой конфигурации Система может выглядеть следующим образом:

- **Сервер Traffic Monitor**. Обеспечивает работу 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 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.
- **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.

Существуют следующие типы установки:

- *Все-в-одном* – все компоненты Системы 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 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 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, работающий на Windows-системах. *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.

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 с Device Monitor может потребоваться использовать отдельный сервер для процесса **iw_xapi_xapi**, а для трафика с Краулера - отдельный сервер для процесса **iw_expressd**.

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 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	ОС Astra Linux Special Edition "Смоленск" 1.5; ОС Astra Linux Special Edition "Смоленск" 1.6 (начиная с версии Monitor 6.10.10).	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	ОС Astra Linux Special Edition "Смоленск" 1.5; ОС Astra Linux Special Edition "Смоленск" 1.6 (начиная с версии Traffic Monitor 6.10.10).	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	ОС Astra Linux Special Edition "Смоленск" 1.5; ОС Astra Linux Special Edition "Смоленск" 1.6 (начиная с версии Traffic Monitor 6.10.10).	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков.
Сервер БД 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	ОС Astra Linux Special Edition "Смоленск" 1.5; ОС Astra Linux Special Edition "Смоленск" 1.6 (начиная с версии Traffic Monitor 6.10.10).	
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 2; • Microsoft Windows Vista 8 Service Pack 2; • Microsoft Windows Server 2008 R2 Service Pack 1; • Microsoft Windows Server 2012 Service Pack 2; • Microsoft Windows 7 Service Pack 1. Платформа: • Microsoft .Net Framework 4.5.1.	• На сервере TM должен быть включен автозапуск процесса **iw_expressd** • 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 1 GB свободного пространства для установки	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; • Microsoft Windows Server 2016. 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; • Microsoft SQL Server 2005, 2008, 2012, 2014, 2016 (Standard, Enterprise); • PostgreSQL версии 9.	• На сервере ТМ должен быть включен автозапуск процесса **iw_xapi_xapi** • Наличие локального DNS для перевода доменных имен в адреса
Агент Device Monitor для рабочих станций				

Не менее 320 GB свободного пространства для временного хранения файлов, предназначенных для передачи на анализ	От 2-х ядер	От 2.5 GB	ОС: • ОС Astra Linux Special Edition "Смоленск" 1.5 • ОС Astra Linux Special Edition "Смоленск" 1.6 (начиная с версии Traffic Monitor 6.10.10). • 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 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2.	Наличие локального DNS для перевода доменных имен в адреса Необходимо отключение проверки цифровой подписи. Поддерживается работы только с обычным ядром Linux (PaX-ядро не поддерживается).
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:
				  • LG Nexus 5X (Nexus 5X), версия Android 6.0.1 (версия прошивки MTC20K)
				  • Samsung Galaxy A3 2017 (SM-A320F), версия Android 6.0.1 (версия прошивки MMB29K.A320FXXU1AQA1)
				  • Samsung Galaxy A5 (SM-A510F), версия Android 6.0.1 (версия прошивки MMB29K.A510FXXU2BPH6)
				  • Samsung Galaxy J1 (SM-J120F), версия Android 5.1.1 (версия прошивки LMY47X.J120FXXU1APH1)
				  • Samsung Galaxy S6 (SM-G920F), версия Android 6.0.1 (версия прошивки MMB29K.G920FXXU4DPJN)
				  • Samsung Galaxy J5 (SM-J510FN), версия Android 6.0.1 (версия прошивки MMB29M.J510FNXXU2AQG3)
				  • Samsung Galaxy Tab A (SM-T355), версия Android 6.0.1 (версии прошивки MMB29M.T355XXU1BQA2)
				  • Samsung Galaxy Tab Active (SM-T365), версия Android 5.1.1 (версии прошивки LMY47X.T365XXU1BPK2)

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, Citrix 6.0, 7.6, 7.13, 7.14 и 7.15 LTSR или других систем виртуализации.

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 устанавливаются на один компьютер	**All-in-one**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка и настройка СУБД PostgreSQL • Установка схемы базы данных IW Traffic Monitor • Установка DEB пакетов сервера IWTM • Установка подсистемы мониторинга • Установка консоли управления
Установка сервера СУБД со схемой БД Traffic Monitor на отдельный компьютер	**DB node**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка и настройка СУБД PostgreSQL • Установка схемы базы данных IW Traffic Monitor

Установка сервера Traffic Monitor на отдельный компьютер	**TM node**	• Установка ОС Linux • Настройка сетевого интерфейса • Установка DEB пакетов сервера IWTM • Установка подсистемы мониторинга • Установка консоли управления

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

- Установка сервера Traffic Monitor и Базы данных
- Установка TM Enterprise в режиме "Все-в-одном" (Astra Linux)
- Распределенная установка TM
  - Установка Базы данных
  - Установка Сервера Traffic Monitor
- Установка InfoWatch Device Monitor (опционально)
- Установка подсистемы Crawler (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 Astra Linux приведены в следующих разделах:

- Установка TM в режиме "Все-в-одном" (Astra Linux)
- Распределенная установка TM (Astra Linux)

Важно!

Для установки потребуется 2 диска:

- Astra-Linux-Smolensk
- Astra-Linux-Smolensk-Devel

В Системе, работающей на ОС Astra Linux, перехват осуществляется только на агентах подсистемы Device Monitor.

На сервере Traffic Monitor не будут задействованы перехватчики, работающие на шлюзе: ICAP, SMTPD (до версии Traffic Monitor 6.10.10), SNIFFER, поэтому следующие процессы окажутся выключенными:

- iw_icap
- iw_proxy_http
- iw_proxy_icq
- iw_proxy_smtp
- iw_smtpd (до версии Traffic Monitor 6.10.10)
- iw_sniffer
- iw_capstack
- iw_qmover_client
- iw_qmover_server

3.1.1 Установка TM в режиме "Все-в-одном"

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

Важно!

Для установки потребуется 2 диска:

- Astra-Linux-Smolensk
- Astra-Linux-Smolensk-Devel

Установка Traffic Monitor версий 6.10.0 и 6.10.1 на Astra Linux 1.5

Чтобы установить Traffic Monitor (Astra Linux) в режиме «Все-в-одном», выполните следующие действия:

1. Запустите установку ОС Astra Linux:
   a. Подключите диск с дистрибутивом (Astra-Linux-Smolensk).
   b. Перезагрузите сервер и выполните в BIOS настройку загрузки системы с CD-ROM.
   c. После сохранения изменений сервер перезагрузится, и запустится программа-инсталлятор.
2. В окне приветствия выберите русский язык, затем - **Графическая установка**.
   Будет запущен стандартный графический мастер установки.
3. Пройдите стандартные шаги установки. Большинство настроек по умолчанию следует оставить без изменения. Обратите внимание, что:
   - требуется запомнить вводимые имя компьютера, имя учетной записи и пароль;
   - при выборе способа разметки дисков рекомендуется указать **Авто - использовать весь диск**;
   - при выборе схемы разметки дисков рекомендуется указать **Все файлы в одном разделе**;
   - чтобы подтвердить выбранные способ и разметку дисков, нужно указать **Закончить разметку и записать изменения на диск**, а в следующем окне - выбрать **Да** для подтверждения;
   - для установки SSH требуется установить флажок в поле **Сетевые сервисы** в окне **Выбор программного обеспечения** (SSH потребуется, например, для копирования на компьютер дистрибутива Traffic Monitor);
   - требуется запомнить вводимый пароль системного загрузчика GRUB.

Важно!

Права пользователя, созданного на этапе установки, ограничены в операционной системе, поэтому:

- при выполнении части команд в командной строке потребуется использовать программу **sudo**. Например, для создания директории `disk1` в корневой директории необходимо ввести команду:
  `sudo mkdir /disk1`
- копировать данные по SSH можно только в домашний каталог пользователя и вложенные в него каталоги (например, это касается дистрибутива Traffic Monitor при копировании его на компьютер по SSH).

Чтобы работать с правами пользователя *root*, в командной строке введите `sudo su`. **Внимание!** К данному способу работы, ввиду возможности допустить серьезную ошибку, крайне не рекомендуется прибегать без помощи специалистов компании InfoWatch.

По завершении установки будет выполнен перезапуск сервера, а затем появится предложение войти в операционную систему.

Примечание:

Более детальное описание установки см. в документации к операционной системе Astra Linux.

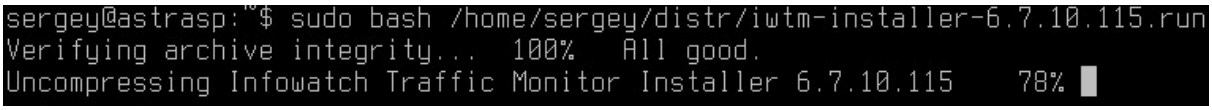
4. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя, созданного при установке).
5. Вставьте в CD-привод диск Astra-Linux-Smolensk.
6. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk1`.
7. Вставьте в CD-привод диск Astra-Linux-Smolensk-Devel.
8. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk2`.
9. Откройте на редактирование файл **sources.list**, расположенный в директории `/etc/apt`
10. Удалите все строки и введите следующее:
    ```
    deb file:///директория_1/ smolensk main non-free contrib
    deb file:///директория_2/ smolensk main non-free
    ```
    где:
    - `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
    - `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel

    В нашем примере текст файла будет следующим:
    ```
    deb file:///disk1/ smolensk main non-free contrib
    deb file:///disk2/ smolensk main non-free
    ```

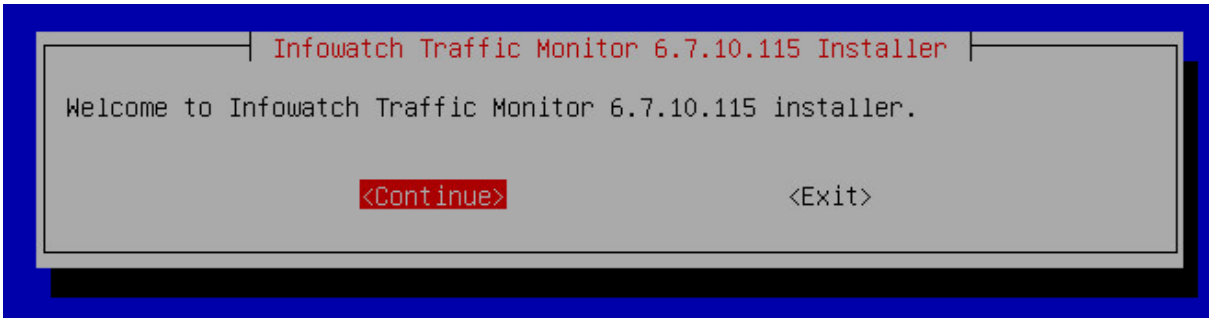
11. Сохраните файл **sources.list**.
12. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки) и архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**, поставляемые на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера . **Например**, в директорию `/distr`.
13. Введите команду для перехода в нужную директорию:
    `cd /<директория_с_архивом/`

    где `/<директория_с_архивом>/` - путь к директории, содержащей архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**.
    В нашем примере команда будет следующей:
    `cd /distr`
14. Введите команду для извлечения архива:
    `sudo tar -xzf astra-linux-smolensk-1.5-pg96_x86_64.tar.gz -C /opt`
15. Введите команду для перехода в нужную директорию:
    `cd /opt`
16. Выполните следующую команду:
    `sudo mv astra-linux-smolensk-1.5-pg96-local.list /etc/apt/sources.list.d`
17. Выполните следующую команду:
    `sudo apt-get update`
18. Выполните следующую команду:
    `sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk.run`
    где `<директория_с_файлом>` - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run**.

    В нашем примере команда будет следующей:
    `sudo bash /distr/iwtm-installer-6.10.0.267-astra-smolensk.run`
    Начнется распаковка файлов, необходимых для установки Traffic Monitor.

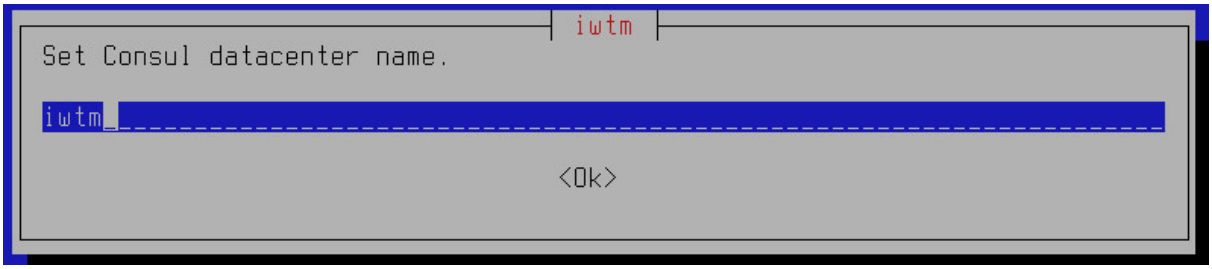


    По завершении на экране отобразится окно с приглашением установить Traffic Monitor (номер в окне соответствует номеру устанавливаемой версии Системы):



19. Для продолжения нажмите **Continue**.
20. В окне **IWTM Server Role** выберите **All-in-one**, нажмите **Ok**.

21. Введите название дата-центра Consul и нажмите **OK**.



22. Настройте адрес сервера для синхронизации времени (NTP-server) - убедитесь, что знак астериска (*) установлен в поле **DNS** и нажмите **OK**. Для перемещения астериска установите курсор в нужное поле и нажмите пробел.

> **Примечание:**
>
> Данную настройку возможно изменить позднее (подробнее о настройке NTP-сервера см. в документе "InfoWatch Traffic Monitor. Руководство администратора", статья "Настройка синхронизации времени").

23. 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**.
24. 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/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/pgdata1** для СУБД PostgreSQL).
h. Нажмите **Enter**.
i. Выберите **Number of days to store in fast tablespaces for fast/slow method** (данная настройка доступна, если выбран режим хранения *normal*) 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** (данная настройка доступна, если выбран режим хранения *normal*) 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**.

25. 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**.

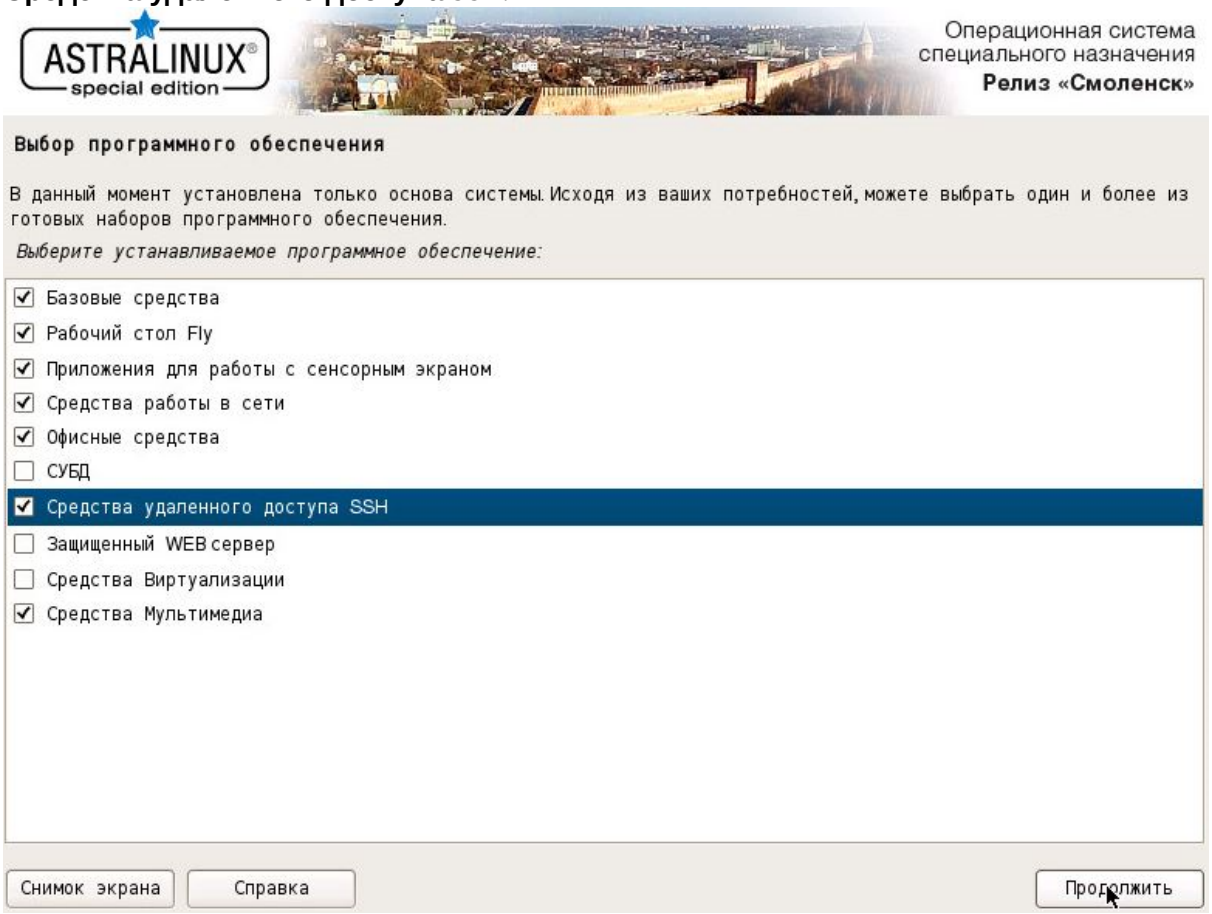
Начнется установка схемы БД и пакетов сервера Traffic Monitor. Прогресс выполнения будет отображаться на экране.
Процесс может занять некоторое время.

Установка Traffic Monitor версий 6.10.10 и 6.10.11 на Astra Linux 1.6

Чтобы установить Traffic Monitor (Astra Linux) в режиме «Все-в-одном», выполните следующие действия:

> **Важно!**
>
> Если Вы выполняете установку во время обновления Системы, на этапе разметки дисков обязательно убедитесь, что не будет отформатирован раздел, на котором хранится резервная копия индексов и Базы данных.

1. Выполните действия 1-8 инструкции по установке Traffic Monitor версии 6.10.0, но используйте дистрибутивы Astra Linux 1.6.
   Для установки SSH в окне **Выбора программного обеспечения** установите флажок **Средства удаленного доступа SSH**.



2. Для того, чтобы включить службу ssh и выставить уровень мандатного контроля целостности для пользователя root, выполните команды:
   ```
   sudo /etc/init.d/ssh start
   systemctl enable ssh.service
   sudo pdpl-user -i 63 root
   ```
3. Чтобы изменения вступили в силу, повторно войдите в вашу учетную запись:
   a. Введите команду для выхода:
      ```
      exit
      ```
   b. Снова введите логин и пароль.

> **Примечание:**
>
> Если используется подключение по SSH, выполните повторное подключение.

4. Откройте на редактирование файл **sources.list**, расположенный в директории `/etc/apt`
5. Удалите все строки и введите следующее:
   ```
   deb file:///директория_1/ smolensk main non-free contrib
   deb file:///директория_2/ smolensk main non-free contrib
   ```
   где:

- `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
- `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel

В нашем примере текст файла будет следующим:

```
deb file:///disk1/ smolensk main non-free contrib
deb file:///disk2/ smolensk main non-free contrib
```

6. Сохраните файл **sources.list**.
7. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки), поставляемый на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера.
   Например, в директорию `/distr`.
8. Выполните действия 17-25 инструкции по установке Traffic Monitor версии 6.10.0, но используйте файл установки Traffic Monitor версии 6.10.10 или 6.10.11.
9. Для перехвата smtp с учетом мандатных меток:
   a. Введите команду для вызова файлового менеджера:
      `sudo mc`
   b. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
   c. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.
   d. Для выхода из файлового менеджера введите команду:
      `exit`
   e. Чтобы вступили в силу изменения привилегий пользователя `iwtm`, которые необходимы для считывания мандатных меток, перезагрузите сервер командой:
      `sudo reboot`

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

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

Установка Веб-консоли управления происходит в автоматическом режиме с помощью программы-инсталлятора. 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».

3.1.2 Распределенная установка TM

Traffic Monitor позволяет развернуть Систему так, чтобы сервер Traffic Monitor и СУБД (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;
2. Установка Сервера Traffic Monitor.

Важно!

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

Каждый сервер должен иметь уникальный корректный FQDN.

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

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. 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».

Установка Базы данных

Важно!

Каждый сервер должен иметь уникальный корректный FQDN.

Для установки потребуется 2 диска:

- Astra-Linux-Smolensk
- Astra-Linux-Smolensk-Devel

Установка Traffic Monitor версий 6.10.0 и 6.10.1 на Astra Linux 1.5

Чтобы установить Traffic Monitor (Astra Linux) в режиме DB node, выполните следующие действия:

1. Запустите установку ОС Astra Linux:
   a. Подключите диск с дистрибутивом (Astra-Linux-Smolensk).
   b. Перезагрузите сервер и выполните в BIOS настройку загрузки системы с CD-ROM.
   c. После сохранения изменений сервер перезагрузится, и запустится программа-инсталлятор.
2. В окне приветствия выберите русский язык, затем - **Графическая установка**.
   Будет запущен стандартный графический мастер установки.
3. Пройдите стандартные шаги установки. Большинство настроек по умолчанию следует оставить без изменения. Обратите внимание, что:
   - требуется запомнить вводимые имя компьютера, имя учетной записи и пароль;
   - при выборе способа разметки дисков рекомендуется указать **Авто - использовать весь диск**;
   - при выборе схемы разметки дисков рекомендуется указать **Все файлы в одном разделе**;

- чтобы подтвердить выбранные способ и разметку дисков, нужно указать **Закончить разметку и записать изменения на диск**, а в следующем окне - выбрать **Да** для подтверждения;
- для установки SSH требуется установить флажок в поле **Сетевые сервисы** в окне **Выбор программного обеспечения** (SSH потребуется, например, для копирования на компьютер дистрибутива Traffic Monitor);
- требуется запомнить вводимый пароль системного загрузчика GRUB.

> **Важно!**
>
> Права пользователя, созданного на этапе установки, ограничены в операционной системе, поэтому:
> - при выполнении части команд в командной строке потребуется использовать программу **sudo**. Например, для создания директории `disk1` в корневой директории необходимо ввести команду:
> `sudo mkdir /disk1`
> - копировать данные по SSH можно только в домашний каталог пользователя и вложенные в него каталоги (например, это касается дистрибутива Traffic Monitor при копировании его на компьютер по SSH).
>
> Чтобы работать с правами пользователя *root*, в командной строке введите `sudo su`. **Внимание!** К данному способу работы, ввиду возможности допустить серьезную ошибку, крайне не рекомендуется прибегать без помощи специалистов компании InfoWatch.

По завершении установки будет выполнен перезапуск сервера, а затем появится предложение войти в операционную систему.

> **Примечание:**
>
> Более детальное описание установки см. в документации к операционной системе Astra Linux.

4. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя, созданного при установке).
5. Вставьте в CD-привод диск Astra-Linux-Smolensk.
6. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию /disk1.
7. Вставьте в CD-привод диск Astra-Linux-Smolensk-Devel.
8. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию /disk2.
9. Откройте на редактирование файл **sources.list**, расположенный в директории `/etc/apt`
10. Удалите все строки и введите следующее:
```
deb file:///директория_1/ smolensk main non-free contrib
deb file:///директория_2/ smolensk main non-free
```
где:

- `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
- `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel

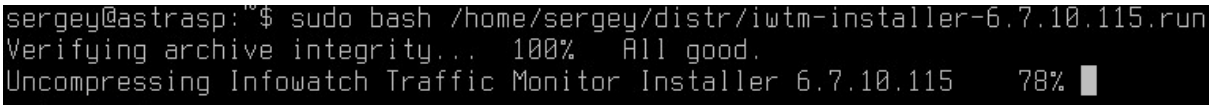
В нашем примере текст файла будет следующим:

```
deb file:///disk1/ smolensk main non-free contrib
deb file:///disk2/ smolensk main non-free
```

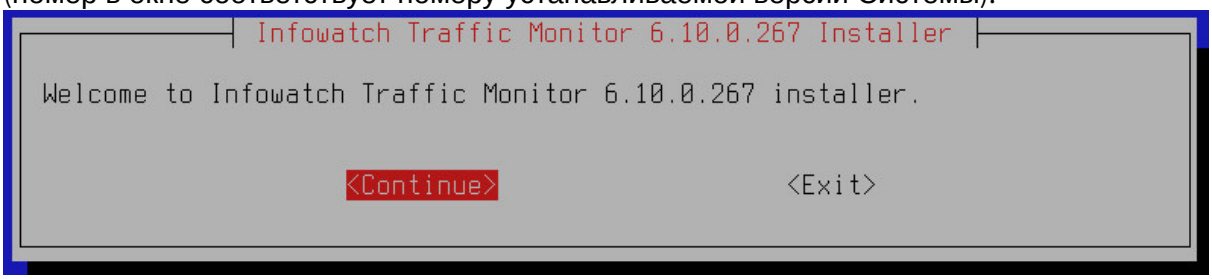
11. Сохраните файл **sources.list**.
12. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки) и архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**, поставляемые на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера . **Например**, в директорию `/distr`.
13. Введите команду для перехода в нужную директорию:
    `cd /<директория_с_архивом/`

    где `/<директория_с_архивом>/` - путь к директории, содержащей архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**.
    В нашем примере команда будет следующей:
    `cd /distr`
14. Введите команду для извлечения архива:
    `sudo tar -xzf astra-linux-smolensk-1.5-pg96_x86_64.tar.gz -C /opt`
15. Введите команду для перехода в нужную директорию:
    `cd /opt`
16. Выполните следующую команду:
    `sudo mv astra-linux-smolensk-1.5-pg96-local.list /etc/apt/sources.list.d`
17. Выполните следующую команду:
    `sudo apt-get update`
18. Выполните следующую команду:
    `sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk.run`
    где `<директория_с_файлом>` - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run**.

    В нашем примере команда будет следующей:
    `sudo bash /distr/iwtm-installer-6.10.0.267-astra-smolensk.run`
    Начнется распаковка файлов, необходимых для установки Traffic Monitor.



По завершении на экране отобразится окно с приглашением установить Traffic Monitor (номер в окне соответствует номеру устанавливаемой версии Системы):



19. Для продолжения нажмите **Continue**.

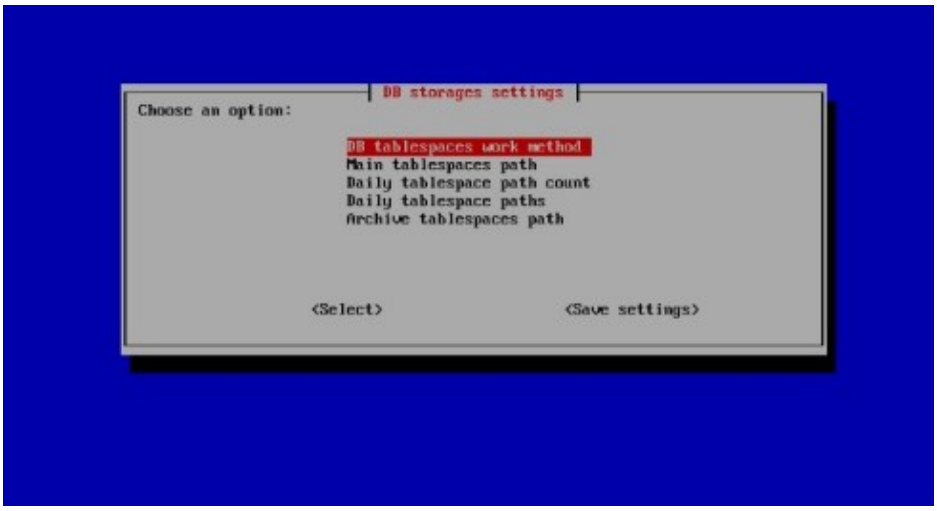
20. В окне **IWTM Server Role** выберите **DB node**, нажмите **Ok**.
21. Введите название дата-центра Consul и нажмите **OK**.



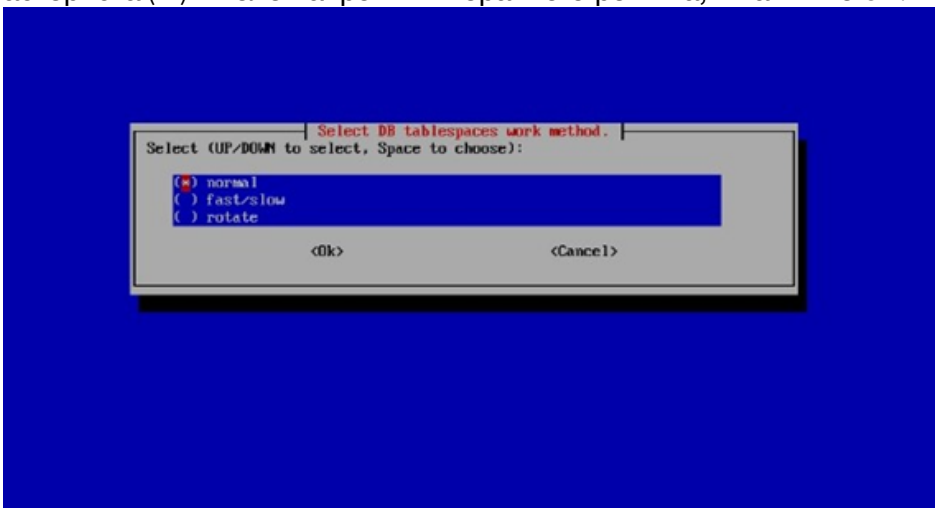
22. Настройте адрес сервера для синхронизации времени (NTP-server) - убедитесь, что знак астериска (*) установлен в поле **DNS** и нажмите **OK**. Для перемещения астериска установите курсор в нужное поле и нажмите пробел.

> **Примечание:**
>
> Данную настройку возможно изменить позднее (подробнее о настройке NTP-сервера см. в документе "InfoWatch Traffic Monitor. Руководство администратора", статья "Настройка синхронизации времени").

23. 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**.
24. 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/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/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**.

25. Настройте параметры автоматического удаления событий из БД (по умолчанию автоматическое удаление отключено):
    a. Выберите **Events cleaning** и нажмите **Enter**:
        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 **Enter**:
   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 **Enter**:
   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 **Enter**:
   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**.

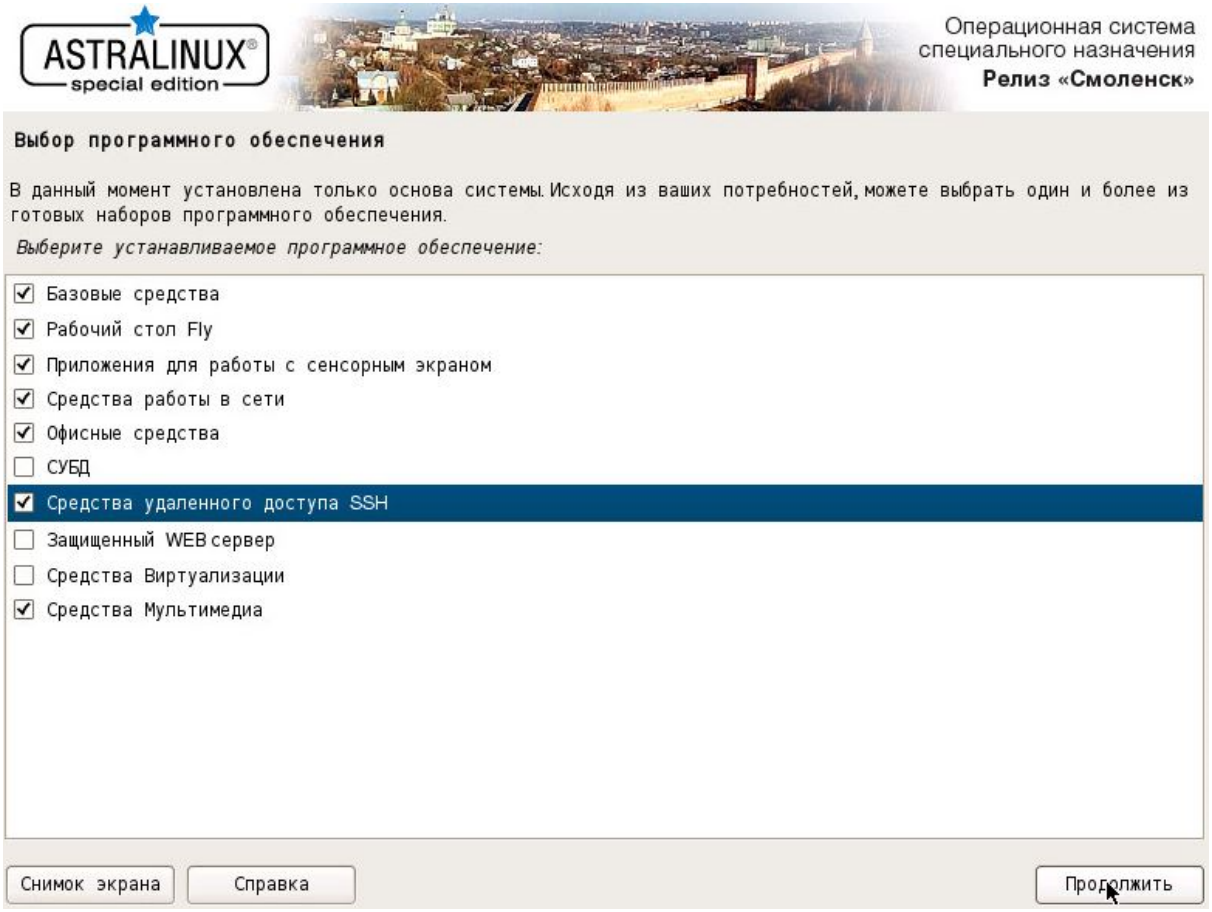
Начнется установка СУБД и схемы БД. Прогресс выполнения будет отображаться на экране. Процесс может занять некоторое время.

Установка Traffic Monitor версий 6.10.10 и 6.10.11 на Astra Linux 1.6

Чтобы установить Traffic Monitor (Astra Linux) в режиме DB node, выполните следующие действия:

> **Важно!**
>
> Если Вы выполняете установку во время обновления Системы, на этапе разметки дисков обязательно убедитесь, что не будет отформатирован раздел, на котором хранится резервная копия индексов и Базы данных.

1. Выполните действия 1-8 инструкции по установке Traffic Monitor версии 6.10.0, но используйте дистрибутивы Astra Linux 1.6.
   Для установки SSH в окне **Выбора программного обеспечения** установите флажок **Средства удаленного доступа SSH**.



2. Для того, чтобы включить службу ssh и выставить уровень мандатного контроля целостности для пользователя root, выполните команды:
```
sudo /etc/init.d/ssh start
systemctl enable ssh.service
sudo pdpl-user -i 63 root
```
3. Чтобы изменения вступили в силу, заново войдите в вашу учетную запись:
   a. Введите команду для выхода:
   ```
   exit
   ```
   b. Заново введите логин и пароль.

> **Примечание:**
>
> Если используется подключение по SSH, выполните повторное подключение.

4. Откройте на редактирование файл **sources.list**, расположенный в директории `/etc/apt`
5. Удалите все строки и введите следующее:
```
deb file:///директория_1/ smolensk main non-free contrib
deb file:///директория_2/ smolensk main non-free contrib
```
где:
   - `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk

- `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel

В нашем примере текст файла будет следующим:

```
deb file:///disk1/ smolensk main non-free contrib
deb file:///disk2/ smolensk main non-free contrib
```

6. Сохраните файл **sources.list**.
7. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки), поставляемый на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера.
   Например, в директорию `/distr`.
8. Выполните действия 17-24 инструкции по установке Traffic Monitor версии 6.10.0, но используйте файл установки Traffic Monitor версии 6.10.10 или 6.10.11.

По завершении выполните следующий шаг распределенной установки - Установка Сервера Traffic Monitor.

Установка Сервера Traffic Monitor

Важно!

Каждый сервер должен иметь уникальный корректный FQDN.

Для установки потребуется 2 диска:

- Astra-Linux-Smolensk
- Astra-Linux-Smolensk-Devel

Установка Traffic Monitor версий 6.10.0 и 6.10.1 на Astra Linux 1.5

Чтобы установить Traffic Monitor (Astra Linux) в режиме TM node, выполните следующие действия:

1. Запустите установку ОС Astra Linux:
   a. Подключите диск с дистрибутивом (Astra-Linux-Smolensk).
   b. Перезагрузите сервер и выполните в BIOS настройку загрузки системы с CD-ROM.
   c. После сохранения изменений сервер перезагрузится, и запустится программа-инсталлятор.
2. В окне приветствия выберите русский язык, затем - **Графическая установка**.
   Будет запущен стандартный графический мастер установки.
3. Пройдите стандартные шаги установки. Большинство настроек по умолчанию следует оставить без изменения. Обратите внимание, что:
   - требуется запомнить вводимые имя компьютера, имя учетной записи и пароль;
   - при выборе способа разметки дисков рекомендуется указать **Авто - использовать весь диск**;
   - при выборе схемы разметки дисков рекомендуется указать **Все файлы в одном разделе**;
   - чтобы подтвердить выбранные способ и разметку дисков, нужно указать **Закончить разметку и записать изменения на диск**, а в следующем окне - выбрать **Да** для подтверждения;
   - для установки SSH требуется установить флажок в поле **Сетевые сервисы** в окне **Выбор программного обеспечения** (SSH потребуется, например, для копирования на компьютер дистрибутива Traffic Monitor);

- требуется запомнить вводимый пароль системного загрузчика GRUB.

> **Важно!**
>
> Права пользователя, созданного на этапе установки, ограничены в операционной системе, поэтому:
> - при выполнении части команд в командной строке потребуется использовать программу **sudo**. Например, для создания директории `disk1` в корневой директории необходимо ввести команду:
> `sudo mkdir /disk1`
> - копировать данные по SSH можно только в домашний каталог пользователя и вложенные в него каталоги (например, это касается дистрибутива Traffic Monitor при копировании его на компьютер по SSH).
>
> Чтобы работать с правами пользователя *root*, в командной строке введите `sudo su`. **Внимание!** К данному способу работы, ввиду возможности допустить серьезную ошибку, крайне не рекомендуется прибегать без помощи специалистов компании InfoWatch.

По завершении установки будет выполнен перезапуск сервера, а затем появится предложение войти в операционную систему.

> **Примечание:**
>
> Более детальное описание установки см. в документации к операционной системе Astra Linux.

4. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя, созданного при установке).
5. Вставьте в CD-привод диск Astra-Linux-Smolensk.
6. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk1`.
7. Вставьте в CD-привод диск Astra-Linux-Smolensk-Devel.
8. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk2`.
9. Откройте на редактирование файл **sources.list**, расположенный в директории `/etc/apt`
10. Удалите все строки и введите следующее:
```
deb file:///директория_1/ smolensk main non-free contrib
deb file:///директория_2/ smolensk main non-free
```
где:
    - `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
    - `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel

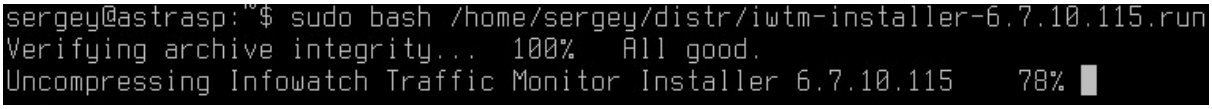
В нашем примере текст файла будет следующим:
```
deb file:///disk1/ smolensk main non-free contrib
```

```
deb file:///disk2/ smolensk main non-free
```

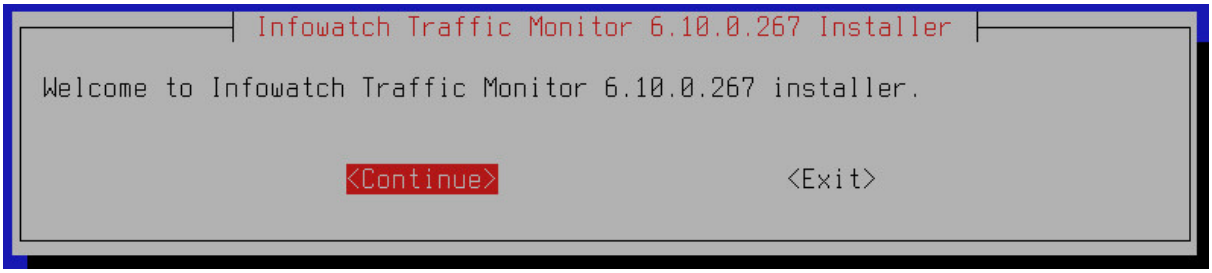
11. Сохраните файл **sources.list**.
12. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки) и архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**, поставляемые на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера . **Например**, в директорию `/distr`.
13. Введите команду для перехода в нужную директорию:
    `cd /<директория_с_архивом/`

    где `/<директория_с_архивом>/` - путь к директории, содержащей архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**.
    В нашем примере команда будет следующей:
    `cd /distr`
14. Введите команду для извлечения архива:
    `sudo tar -xzf astra-linux-smolensk-1.5-pg96_x86_64.tar.gz -C /opt`
15. Введите команду для перехода в нужную директорию:
    `cd /opt`
16. Выполните следующую команду:
    `sudo mv astra-linux-smolensk-1.5-pg96-local.list /etc/apt/sources.list.d`
17. Выполните следующую команду:
    `sudo apt-get update`
18. Выполните следующую команду:
    `sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk.run`
    где `<директория_с_файлом>` - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run**.

    В нашем примере команда будет следующей:
    `sudo bash /distr/iwtm-installer-6.10.0.267-astra-smolensk-astra-smolensk.run`
    Начнется распаковка файлов, необходимых для установки Traffic Monitor.



По завершении на экране отобразится окно с приглашением установить Traffic Monitor (номер в окне соответствует номеру устанавливаемой версии Системы):



19. Для продолжения нажмите **Continue**.
20. В окне **IWTM Server Role** выберите **TM node**, нажмите **Ok**.

21. Введите название дата-центра Consul и нажмите **OK**.



22. Настройте адрес сервера для синхронизации времени (NTP-server) - убедитесь, что знак астериска (*) установлен в поле **DNS** и нажмите **OK**. Для перемещения астериска установите курсор в нужное поле и нажмите пробел.

> **Примечание:**
>
> Данную настройку возможно изменить позднее (подробнее о настройке NTP-сервера см. в документе "InfoWatch Traffic Monitor. Руководство администратора", статья "Настройка синхронизации времени").

23. Введите IP-адрес сервера СУБД (**DB node**) в поле **Enter DB and Indexer ip address** и нажмите **Enter**:
```
Enter DB and Indexer ip address: _
```
На экран будет выведен запрос на подтверждение IP-адреса:
```
Is DB and Indexer ip address correct (y/n)? _
```
24. Проверьте введенный IP-адрес, введите "**Y**" и нажмите **Enter**.

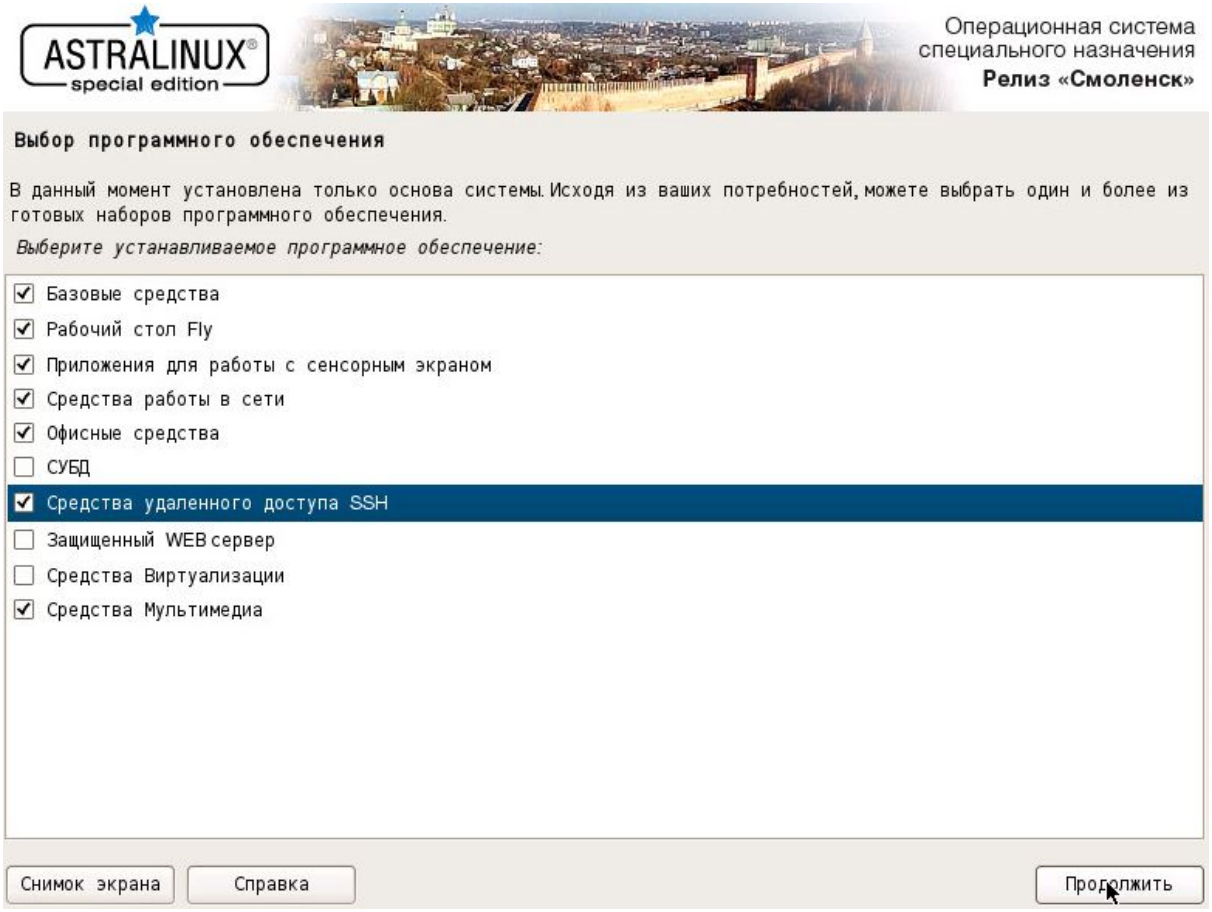
Начнется установка пакетов сервера Traffic Monitor. Прогресс выполнения будет отображаться на экране.
Процесс может занять некоторое время.

Установка Traffic Monitor версий 6.10.10 и 6.10.11 на Astra Linux 1.6

Чтобы установить Traffic Monitor (Astra Linux) в режиме TM node, выполните следующие действия:

> **Важно!**
>
> Если Вы выполняете установку во время обновления Системы, на этапе разметки дисков обязательно убедитесь, что не будет отформатирован раздел, на котором хранится резервная копия индексов и Базы данных.

1. Выполните действия 1-8 инструкции по установке Traffic Monitor версии 6.10.0, но используйте дистрибутивы Astra Linux 1.6.
   Для установки SSH в окне **Выбора программного обеспечения** установите флажок **Средства удаленного доступа SSH**.



2. Для того, чтобы включить службу ssh и выставить уровень мандатного контроля целостности для пользователя root, выполните команды:
```
sudo /etc/init.d/ssh start
systemctl enable ssh.service
sudo pdpl-user -i 63 root
```
3. Чтобы изменения вступили в силу, повторно войдите в вашу учетную запись:
   a. Введите команду для выхода:
   ```
   exit
   ```
   b. Снова введите логин и пароль.

> **Примечание:**
>
> Если используется подключение по SSH, выполните повторное подключение.

4. Откройте на редактирование файл **sources.list**, расположенный в директории `/etc/apt`
5. Удалите все строки и введите следующее:
```
deb file:///директория_1/ smolensk main non-free contrib
deb file:///директория_2/ smolensk main non-free contrib
```
где:
   - `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk

- `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel

В нашем примере текст файла будет следующим:
```
deb file:///disk1/ smolensk main non-free contrib
deb file:///disk2/ smolensk main non-free contrib
```

6. Сохраните файл **sources.list**.
7. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки), поставляемый на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера.
   Например, в директорию `/distr`.
8. Выполните действия 17-24 инструкции по установке Traffic Monitor версии 6.10.0, но используйте файл установки Traffic Monitor версии 6.10.10 или 6.10.11.
9. Для перехвата smtp с учетом мандатных меток:
   a. Введите команду для вызова файлового менеджера:
      `sudo mc`
   b. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
   c. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.
   d. Для выхода из файлового менеджера введите команду:
      `exit`
   e. Чтобы вступили в силу изменения привилегий пользователя `iwtm`, которые необходимы для считывания мандатных меток, перезагрузите сервер командой:
      `sudo reboot`

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

При необходимости установите еще серверы Traffic Monitor, выполнив те же шаги.

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

3.2 Установка подсистемы Краулер

Перехватчик Краулер реализован в виде трех служб:

- `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;
- `Consul Agent` - регистрирует сервисы, осуществляет обнаружение и мониторинг компонентов 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.

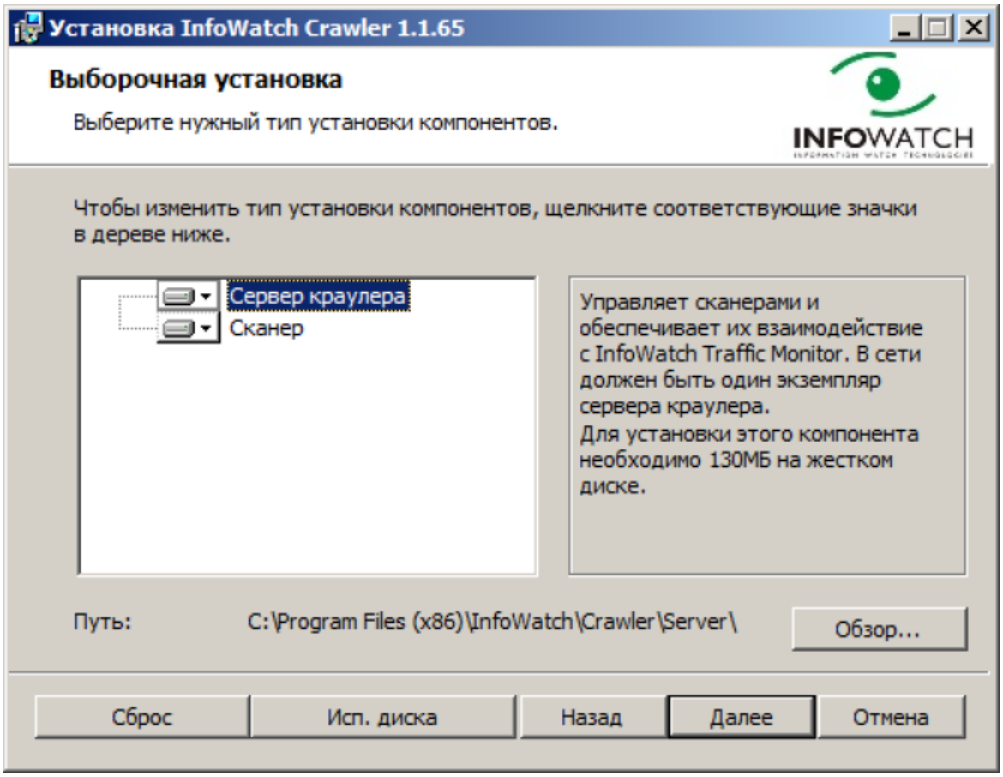
Чтобы установить Краулер:

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**).

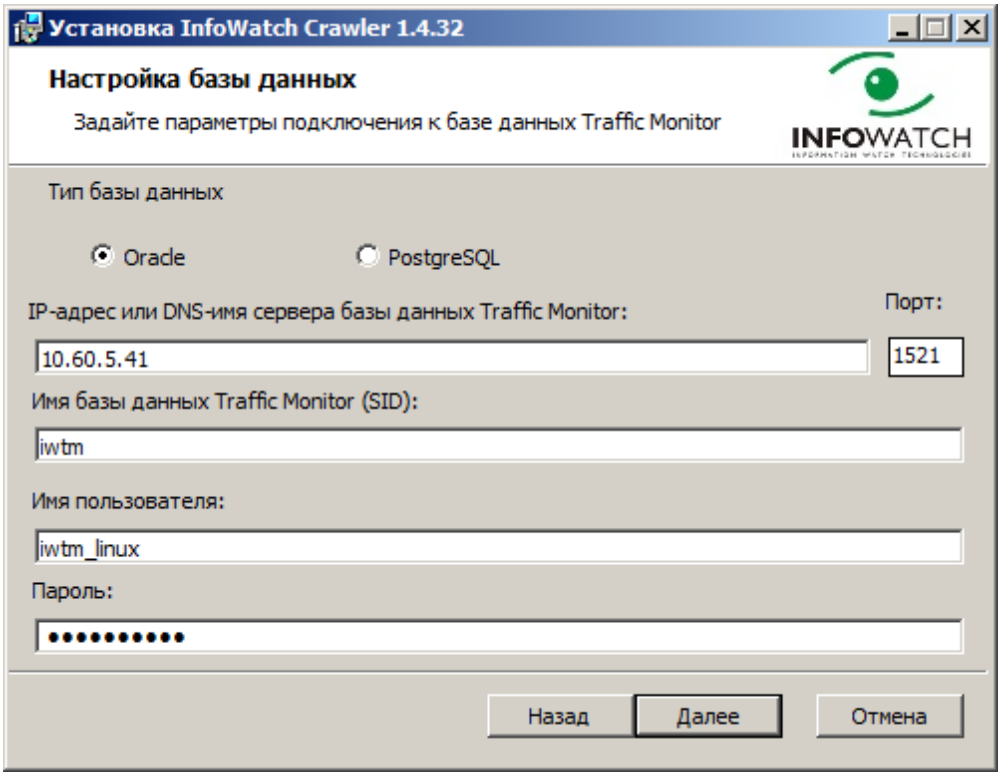
2. В окне приветствия мастера установки InfoWatch Crawler нажмите **Далее**.
3. В окне выбора области установки нажмите **Далее**.
4. На шаге **Выборочная установка** определите, какие компоненты Crawler нужно установить и укажите директорию, в которую будет установлен компонент:
   - **Сервер краулера** – 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**.

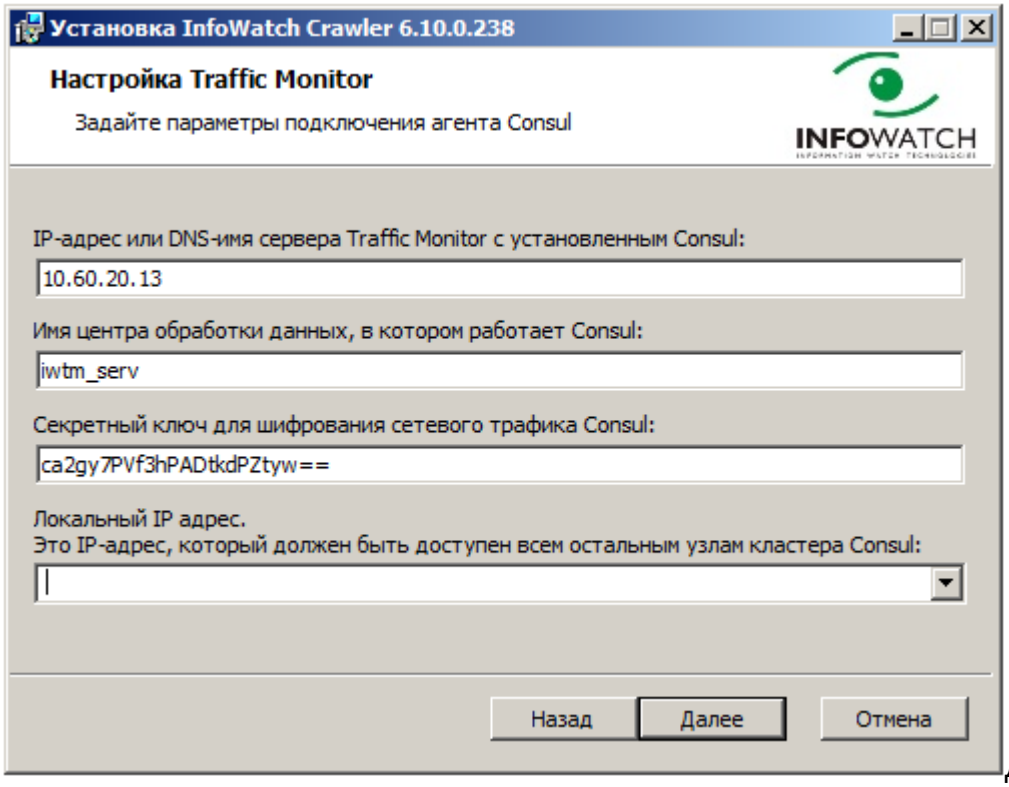
5. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сервер краулера**:
   a. Укажите параметры соединения службы `InfoWatch.Crawler.Server` с базой данных Traffic Monitor, нажмите **Далее**.



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.

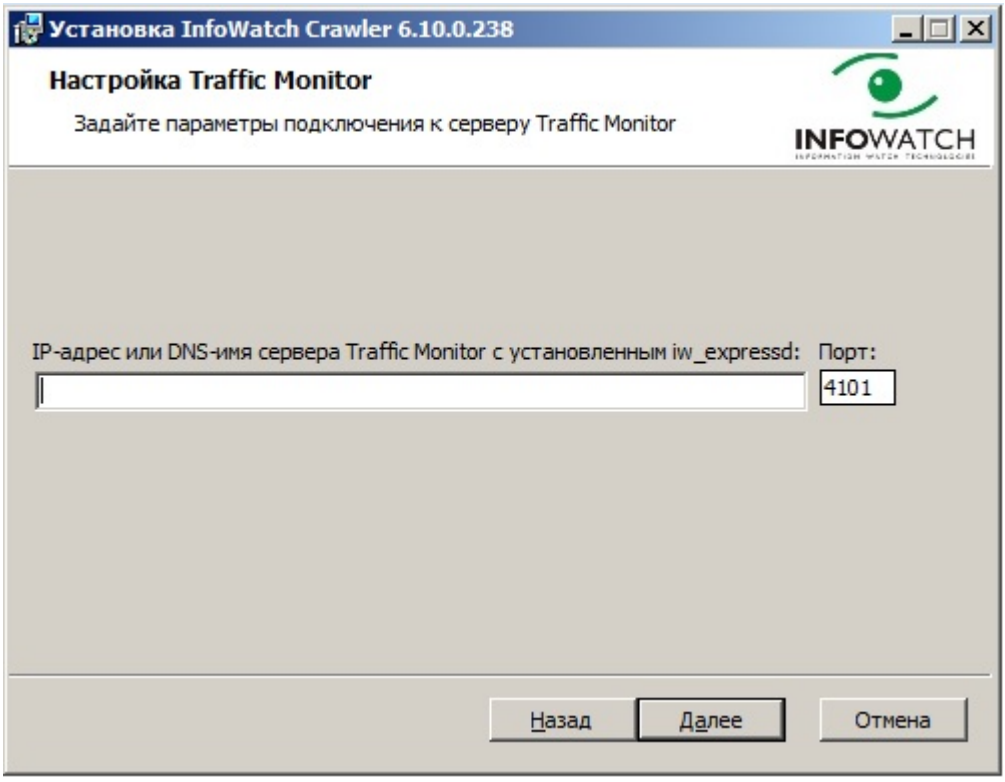
b. Укажите параметры подключения агента Consul к серверу Traffic Monitor, нажмите **Далее**.



Для заполнения полей **Имя центра обработки данных, в котором работает Consul** и **Секретный ключ для шифрования сетевого трафика Consul** выполните следующие действия:

i. подключитесь к серверу Traffic Monitor, на котором установлен Consul.
ii. Перейдите в директорию `/opt/iw/tm5/etc/consul`.
iii. Откройте файл `consul.json`.
iv. Необходимые для установки данные находятся в блоках:
   - `datacenter` - **Имя центра обработки данных, в котором работает Consul**;
   - `encrypt` - **Секретный ключ для шифрования сетевого трафика Consul**.
v. Закройте файл, не изменяя его содержимое.

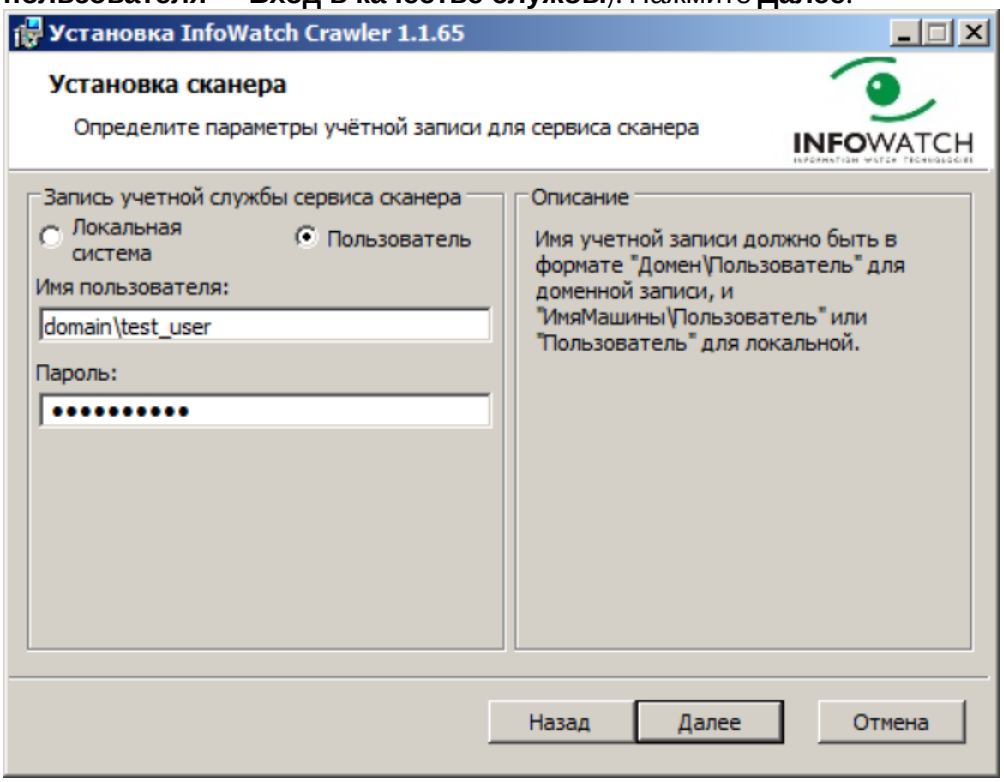
c. Укажите параметры соединения службы `InfoWatch.Crawler.Server` с сервером Traffic Monitor, нажмите **Далее**.



В случае распределенной установки 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).

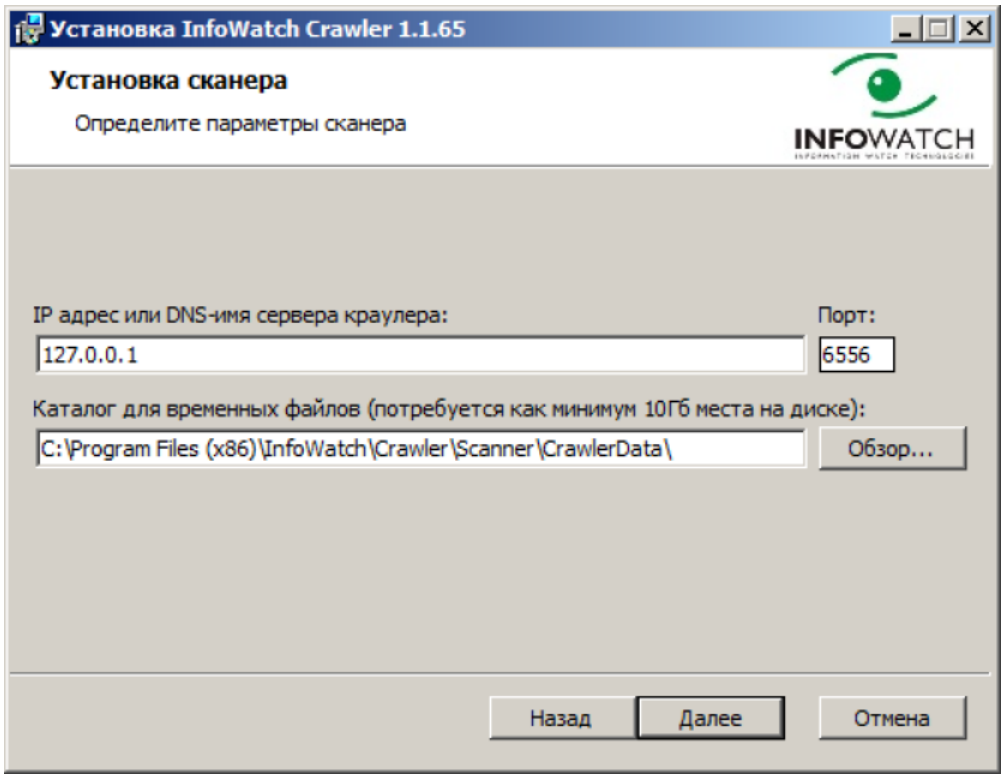
6. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сканер**:
   a. укажите, от имени какой учетной записи будет запускаться служба InfoWatch.Crawler.Scaner. Вы можете выбрать стандартную учетную запись Local System (рекомендуется) или ввести параметры учетной записи, имеющей право 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`. Если вы работаете в Traffic Monitor 6.10.10, установленном на ОС Astra Linux 1.6, то: `/etc/init.d/iwtm restart kicker`

Важно!

По окончании процесса установки необходимо убедиться что связь между Консолью управления Traffic Monitor и сервером Краулер установлена, для этого на сервере Traffic Monitor выполните команду: ping <имя сервера Краулер>

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 9.6 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

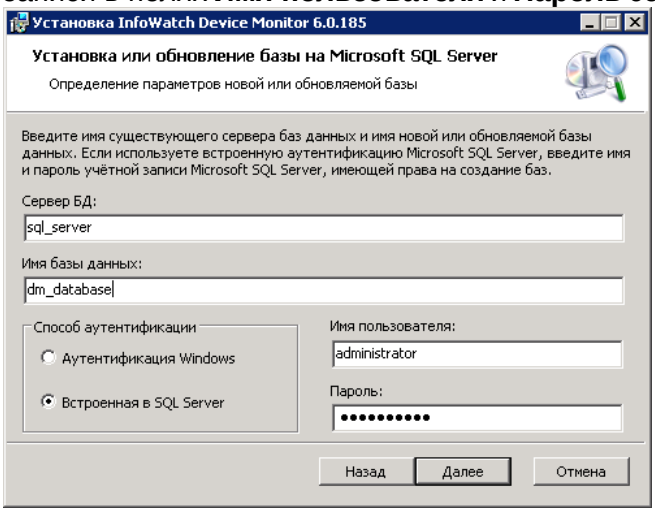
   Если на Шаге 4 вы решили использовать уже существующую базу данных (опция **Установить новую базу данных** не была выбрана), то вам будет необходимо дополнительно указать параметры соединения с существующей базой данных Device Monitor.
   Нажмите **Далее**.
7. **Настройка базы данных**
   Этот шаг будет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



Настройка базы данных Microsoft SQL Server

При использовании СУБД Oracle настройте следующие параметры:

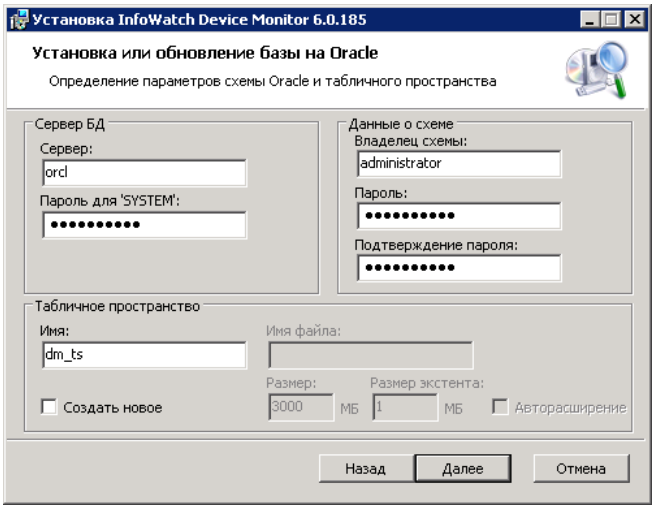
a. В области **Сервер БД** задайте параметры соединения с сервером базы данных:
   - **Сервер**. Имя сервера базы данных. В качестве значения данного параметра указывают псевдоним сервера из файла tnsnames.ora.
   - **Пароль для 'SYSTEM'**. Пароль учетной записи пользователя SYSTEM.
b. В области **Данные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

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

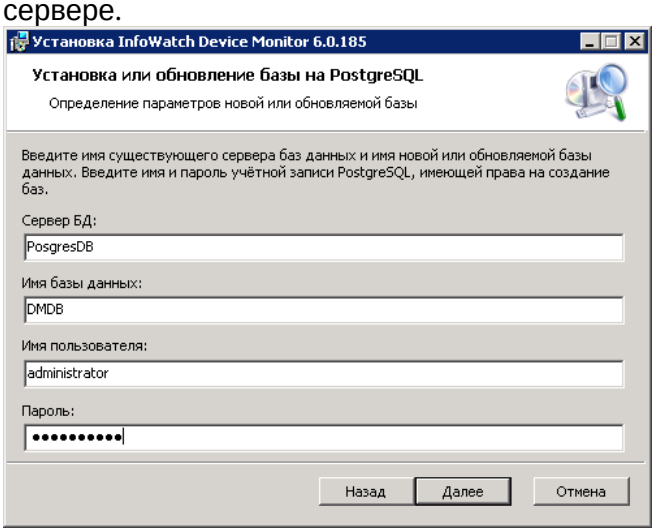
   - **Владелец схемы**. Имя учетной записи владельца схемы базы данных.
   - **Пароль, Подтверждение пароля**. Пароль учетной записи владельца схемы базы данных.

   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**.

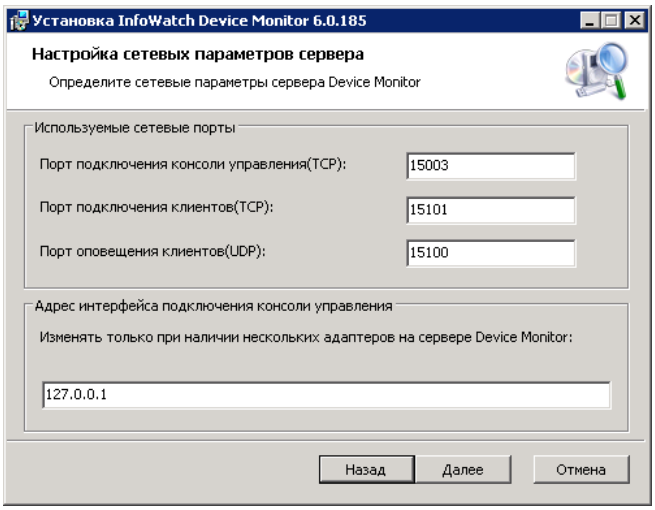
8. **Настройка сетевых параметров сервера**

   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.

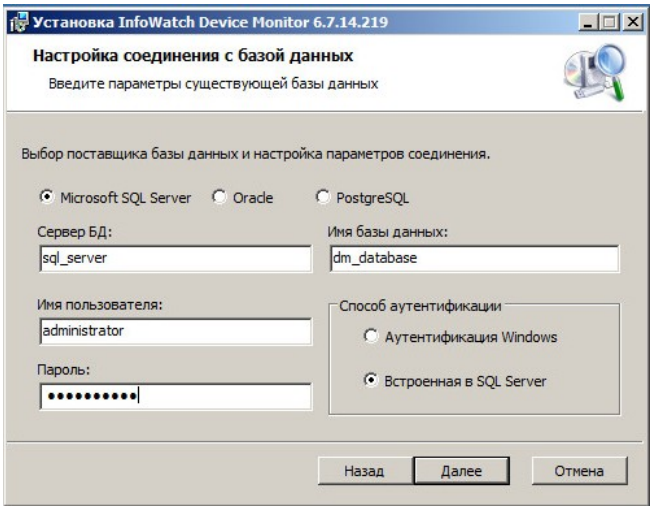
a. Запуск мастера установки
Вставьте диск с дистрибутивом Device Monitor в дисковод. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы. В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите **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**.

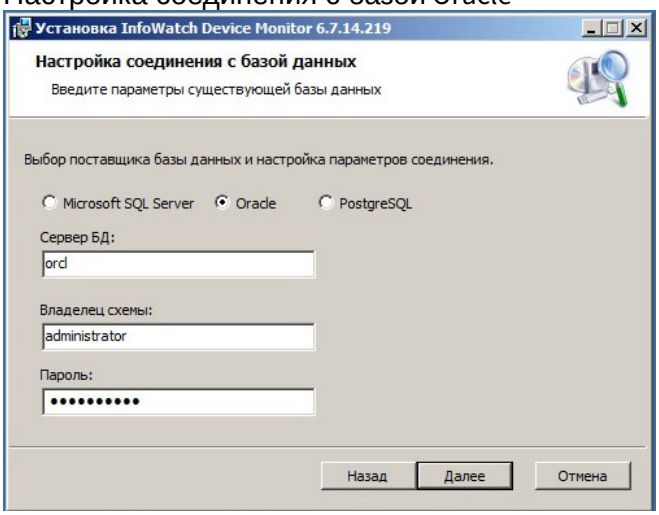
Важно!

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

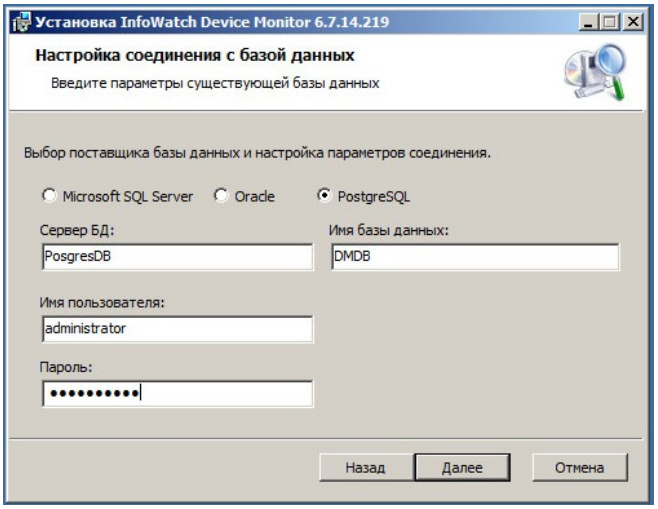
e. Настройка соединения с базой данных
Укажите СУБД, под управлением которой находится база данных Device Monitor и введите оставшиеся параметры соединения такими же, которые были использованы при установке основного сервера:
Настройка соединения с базой Microsoft SQL Server
Если учетной записи назначена 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

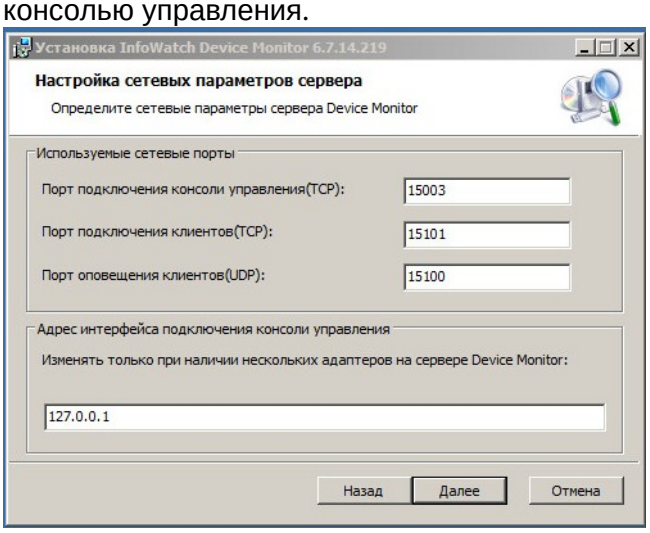


Настройка соединения с базой PostgreSQL



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.

Примечание:

Запуск Агента InfoWatch Device Monitor осуществляется автоматически сразу после установки. До перезагрузки компьютера функционал Агента ограничен только:
- перехватом трафика, проходящего через proxy-сервер,
- сетевым перехватом (при установке Агента на ОС Windows 8 и более поздние),
- перехватом копирования на внешние носители.

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.

Установка Агента InfoWatch Device Monitor на компьютер по управлением ОС Microsoft Windows:

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 InfoWatch Device Monitor на компьютер под управлением ОС Astra Linux:

1. **Подготовка к установке:**
   a. На компьютере, на котором установлен Сервер Infowatch Device Monitor перейдите в директорию `InfoWatch\Device Monitor\Server\`**`SetupPackages`**.
   Дистрибутив Агента InfoWatch Device Monitor представляет собой архив **`Setup.AstraLinux.Client.x64.tar.gz`**.
   Скопируйте архив на целевой компьютер.
   b. На целевом компьютере перейдите в директорию, в которую скопирован архив, и для распаковки введите команду:
   `sudo tar –xvzf Setup.AstraLinux.Client.x64.tar.gz`
   В результате будут созданы файлы
   `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<версия_агента>.deb`.
2. **Установка и удаление Агента InfoWatch Device Monitor:**
   a. Перейдите в директорию, в которую распаковано содержимое архива **`Setup.AstraLinux.Client.x64.tar.gz`**.
   b. Для установки Агента запустите скрипт, выполнив команду:
   `sudo ./install.sh <сервер>:<порт>`
   где `<сервер>` - ip-адрес или доменное имя Сервера Infowatch Device Monitor, `<порт>` - порт подключения к Серверу Infowatch Device Monitor.
   В нашем примере команда будет следующей:

```
sudo ./install.sh <dm-server>:<15101>
```
Продукт будет установлен в директорию `/opt/iw/dmagent`.
Проверить статус сервисов можно командой:
```
sudo systemctl status iwdm*
```
c. Для удаления Агента запустите скрипт, выполнив команду:
```
sudo ./remove.sh
```

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**.

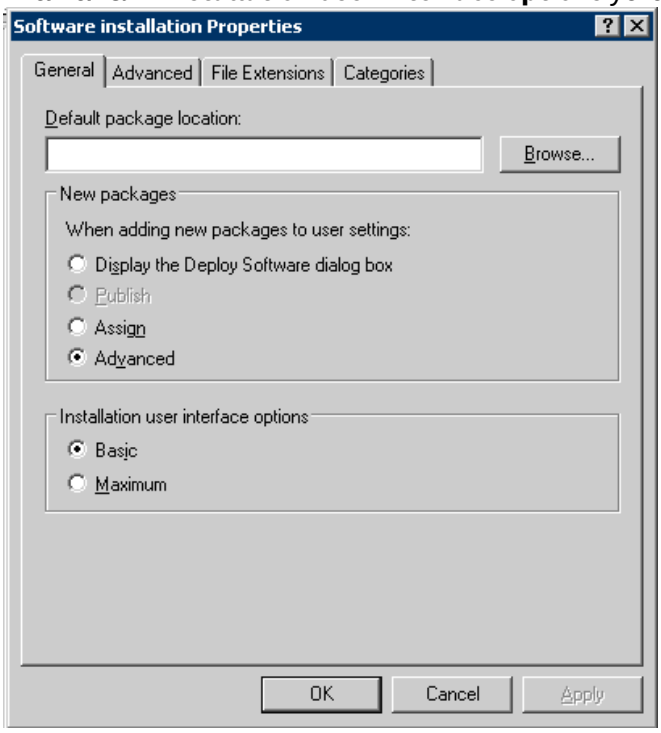
> **Примечание:**
>
> Если данная функция не отключена, то для установки Агента потребуется еще одна дополнительная перезагрузка, связанная с механизмом распространения групповой политики Windows.

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**.

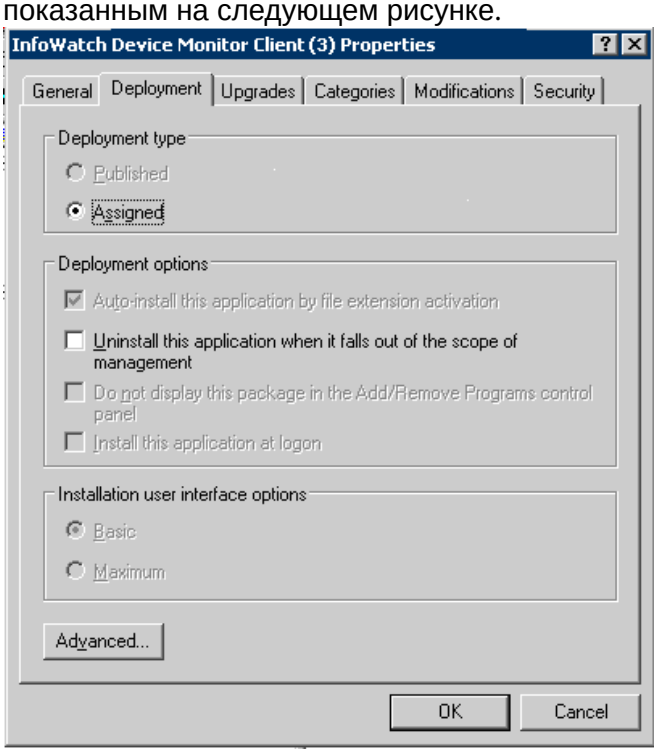
4. **Подготовка задания на установку Агента**

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.

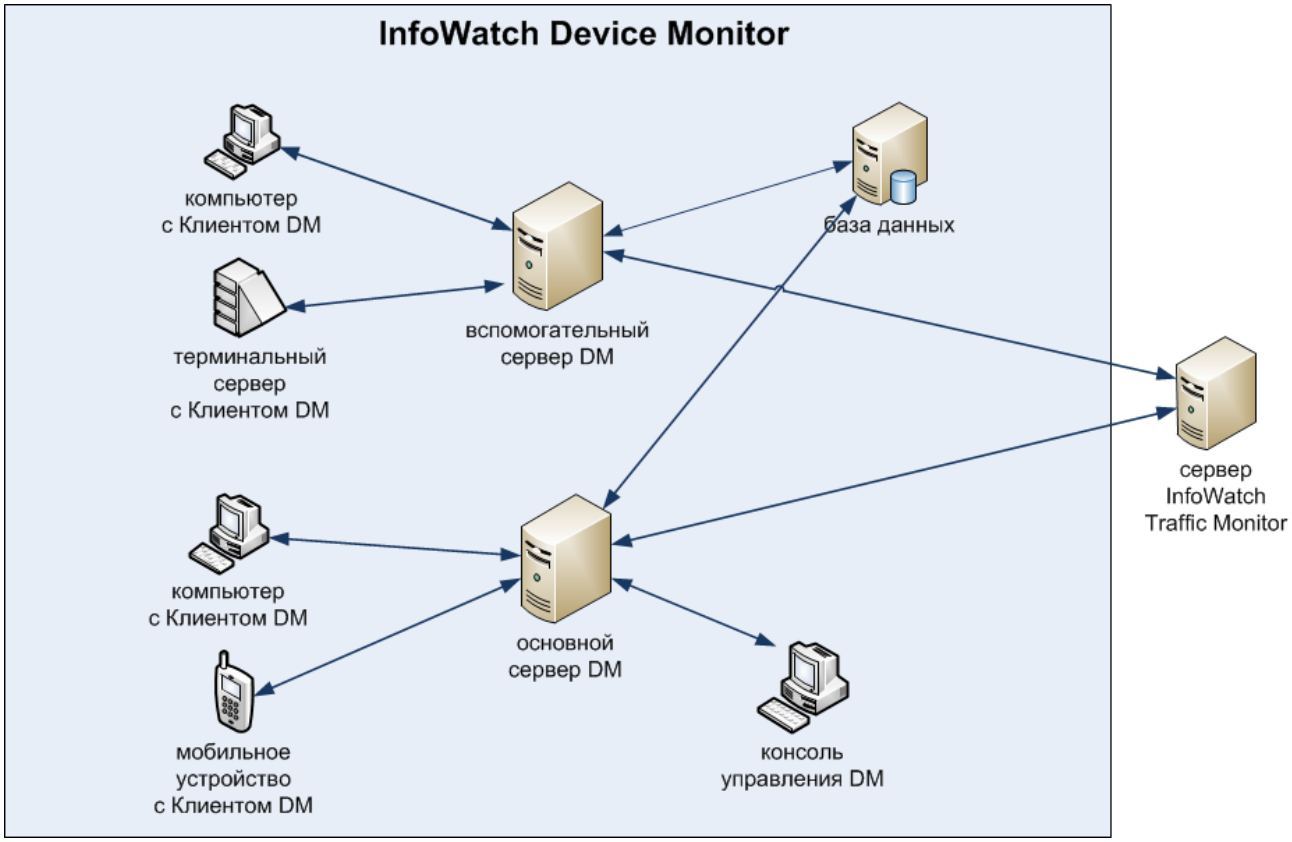
3.3.3 Схема развертывания InfoWatch Device Monitor

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

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:

- дистрибутивных дисков ОС Astra Linux Smolensk;
- дистрибутивного диска InfoWatch Traffic Monitor той версии, до которой планируется обновление;
- доступа к физическому или виртуальному серверу (серверам), которые необходимо обновить;

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;
- 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.

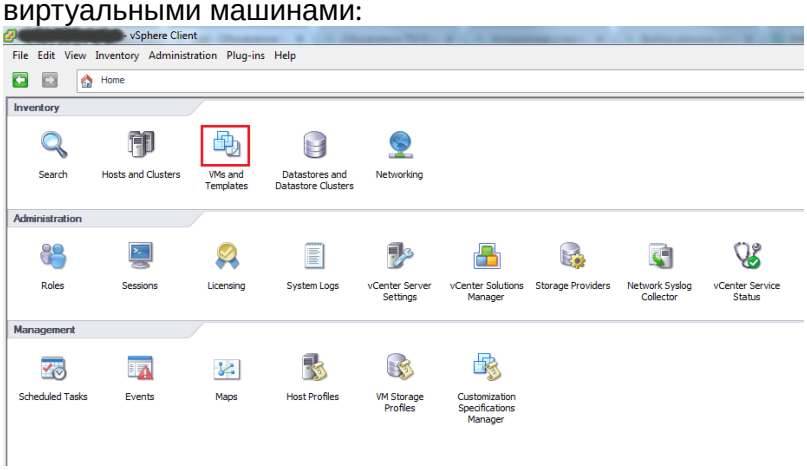
До начала обновления выполните следующие действия:

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).

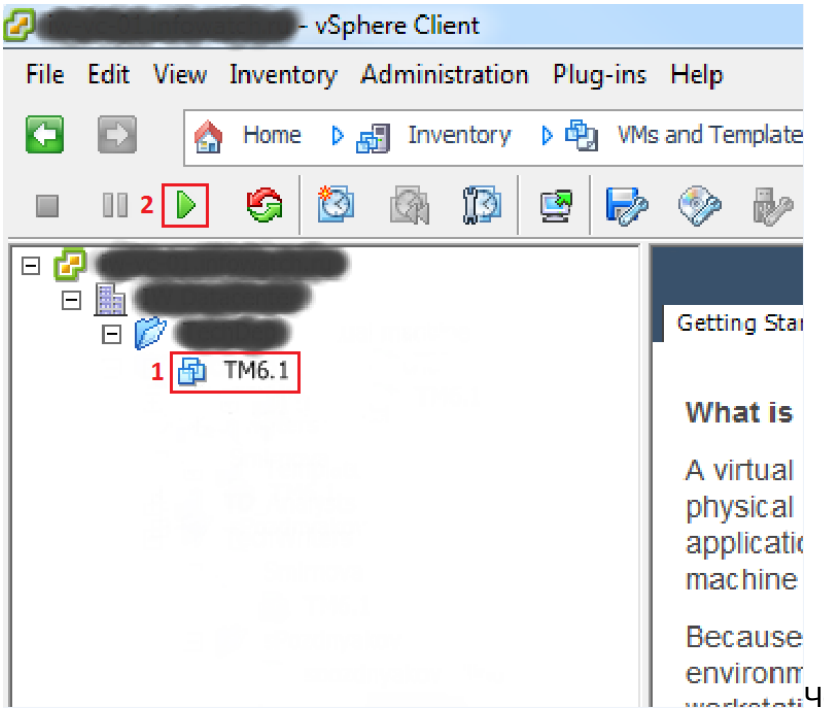
Примечание:

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.

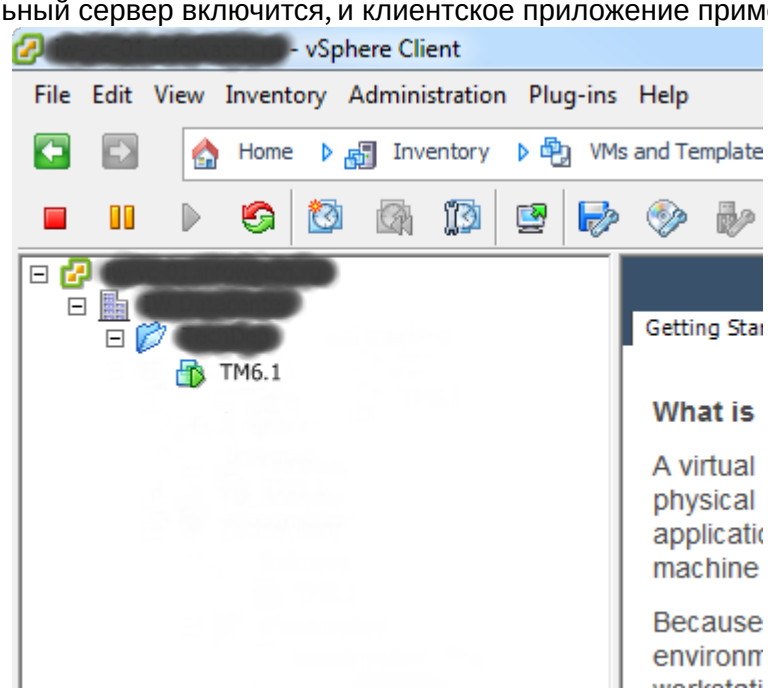
Запустите клиентское приложение VMware vSphere Client от имени администратора (щелкните правой кнопкой мыши на иконке приложения и выберите **Запуск от имени администратора**). Войдите в приложение, используя логин и пароль, выданные администратором вашей информационной сети. Перейдите в раздел с виртуальными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



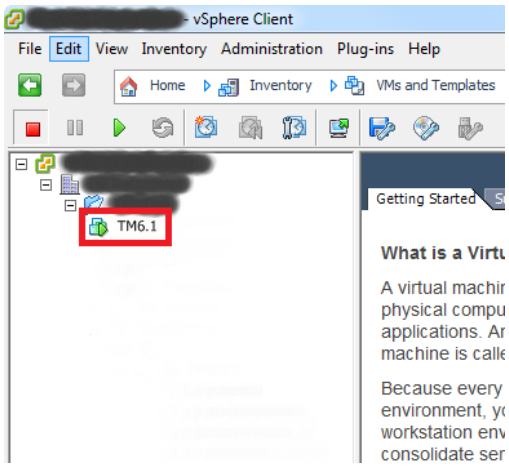
2. Подключите дистрибутивный диск InfoWatch Traffic Monitor к серверам, предназначенным для обновления:
   - в случае физического сервера:
     - если дистрибутив поставлен на оптическом диске - вставьте диск в cd- или dvd-привод сервера и дождитесь, пока сервер прочитает диск;
     - если диск поставлен 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).

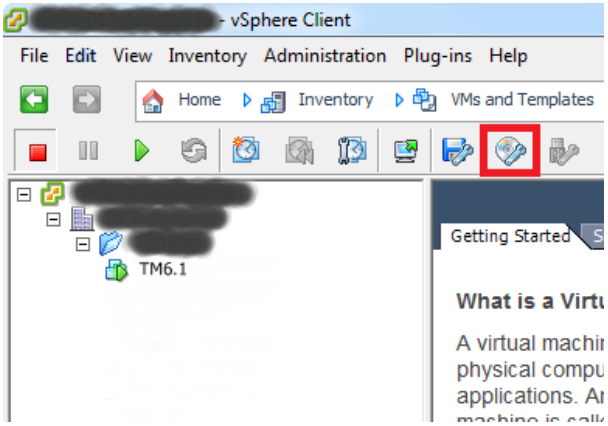
Примечание:

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).

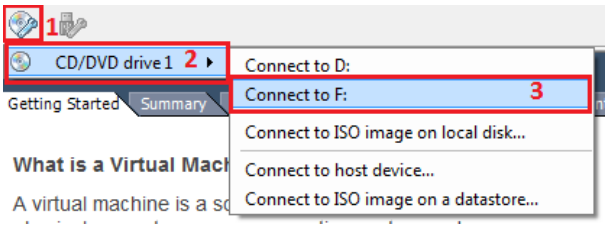
1)



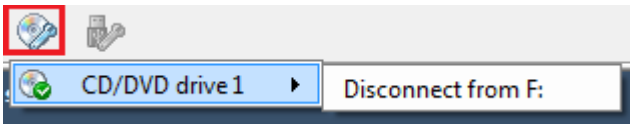
2)



3)



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



Обновите серверы согласно следующим инструкциям:

- Обновление ТМ Все-в-одном (All-in-one) - 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".

Примечание:

После обновления Системы предустановленные привилегии на полное управление запросами и отчетами для пользователей с ролями *Офицер безопасности* и *Администратор* в Системе отсутствуют.

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

Обновление Traffic Monitor на Astra Linux 1.5 до версий 6.10.0 и 6.10.1

Чтобы обновить Систему, выполните следующие действия:

1. Откройте консоль обновляемого сервера.
2. Введите имя пользователя, от имени которого планируется обновление, и нажмите **Enter**.
3. Введите пароль и нажмите **Enter**.
4. Вызовите командную строку (например, терминал *Fly*).

Важно!

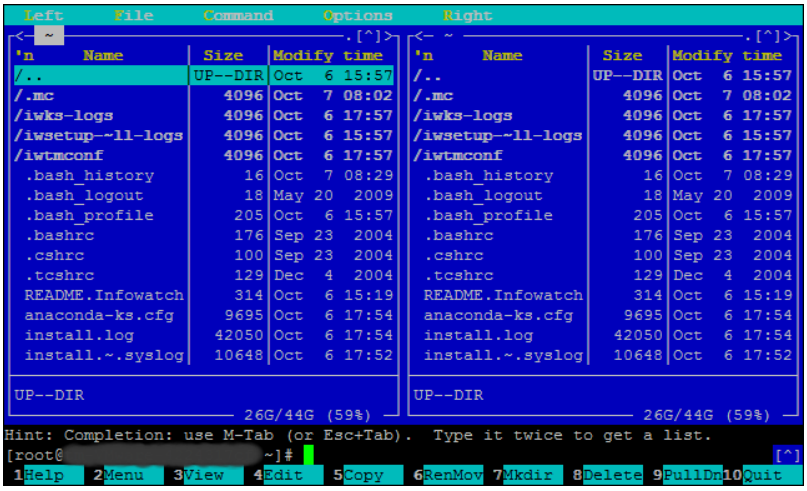
Права пользователя, созданного на этапе установки, ограничены в операционной системе, поэтому:

- при выполнении части команд в командной строке потребуется использовать программу **sudo**. Например, для создания директории `disk1` в корневой директории необходимо ввести команду:
  `sudo mkdir /disk1`

- копировать данные по SSH можно только в домашний каталог пользователя и вложенные в него каталоги (например, это касается дистрибутива Traffic Monitor при копировании его на компьютер по SSH).

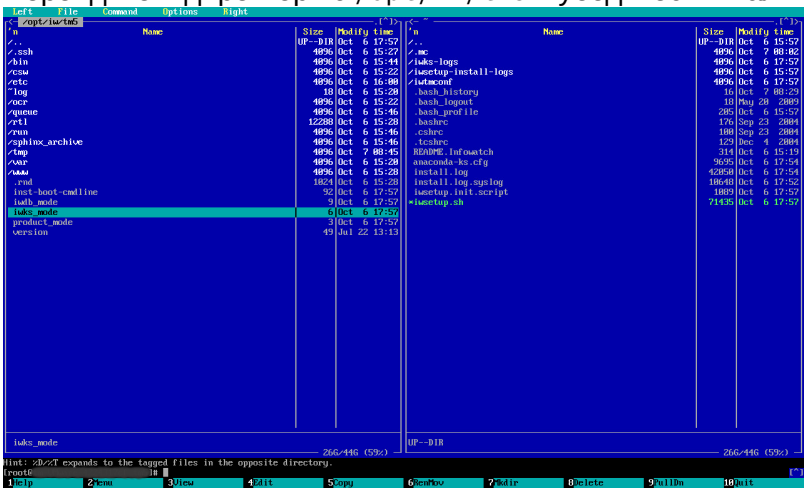
Чтобы работать с правами пользователя *root*, в командной строке введите `sudo su`. **Внимание!** К данному способу работы, ввиду возможности допустить серьезную ошибку, крайне не рекомендуется прибегать без помощи специалистов компании InfoWatch.

5. Введите команду для вызова файлового менеджера:
   `sudo mc`



На экране отобразится окно файлового менеджера *Midnight Commander*, в котором удобно просматривать файлы.

6. 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`

7. Убедитесь, что содержимое файла - слово "iwall".

   > **Примечание:**
   >
   > Если файл имеет другое содержимое, удалите все символы и введите `iwall`

8. Откройте файл **sources.list**, расположенный в директории `/etc/apt`, и проверьте соответствие его содержимого следующему виду:
   ```
   deb file:///директория_1/ smolensk main non-free contrib
   deb file:///директория_2/ smolensk main non-free
   ```
   где:
   - `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
   - `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel
9. Закройте файл **sources.list**.
   Перейдите в указанные в файле директории, и убедитесь в наличии в них папок и файлов репозиториев.
10. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    ```
    exit
    ```
11. Если в указанных директориях не созданы репозитории, создайте их (см. статью "Установка TM в режиме "Все-в-одном", действия 5-11).
12. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки) и архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**, поставляемые на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера . **Например**, в директорию `/distr`.
13. Введите команду для перехода в нужную директорию:
    ```
    cd /<директория_с_архивом/
    ```

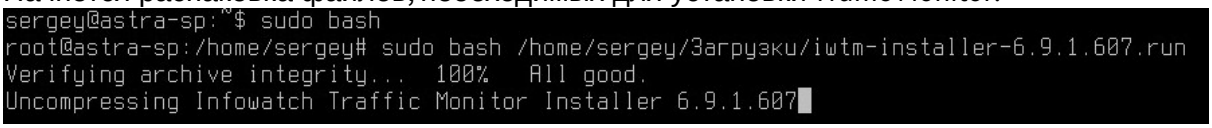
    где `/<директория_с_архивом>/` - путь к директории, содержащей архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**.
    В нашем примере команда будет следующей:
    ```
    cd /distr
    ```
14. Введите команду для извлечения архива:
    ```
    sudo tar -xzf astra-linux-smolensk-1.5-pg96_x86_64.tar.gz -C /opt
    ```
15. Введите команду для перехода в нужную директорию:
    ```
    cd /opt
    ```
16. Выполните следующую команду:
    ```
    sudo mv astra-linux-smolensk-1.5-pg96-local.list /etc/apt/sources.list.d
    ```
17. Выполните следующую команду:
    ```
    sudo apt-get update
    ```
18. Введите команды для остановки перехватчиков:
    ```
    sudo service iwtm stop expressd
    sudo service iwtm stop xapi_xapi
    sudo service iwtm stop xapi_puppy
    ```

19. 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/
    ```
    По завершении обработки событий данные директории должны стать пустыми.

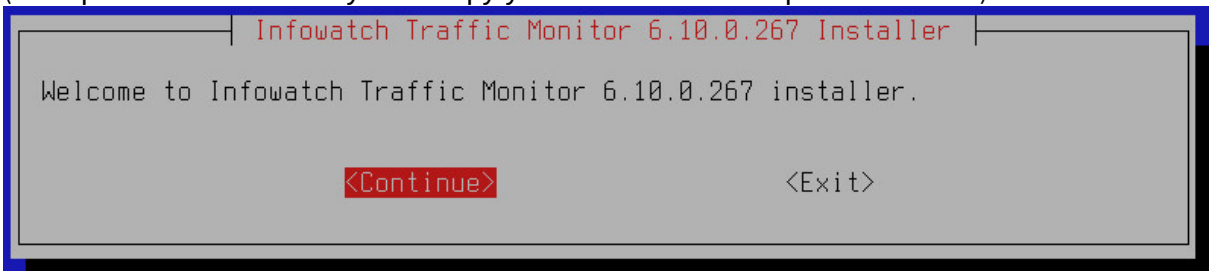
    > **Важно!**
    >
    > До продолжения обновления настоятельно рекомендуется убедиться в том, что все указанные выше директории пусты. В противном случае нельзя гарантировать успешное обновление и дальнейшую работоспособность Системы.
    > Если по какой-либо причине дождаться завершения обработки невозможно, 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**.

20. Последовательно введите команды для остановки служб:
    ```
    sudo service iwtm stop
    sudo service php5-fpm stop
    sudo service nagios3 stop
    ```
21. Выполните следующую команду:
    ```
    sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk.run
    ```
    где <директория_с_файлом> - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run**.

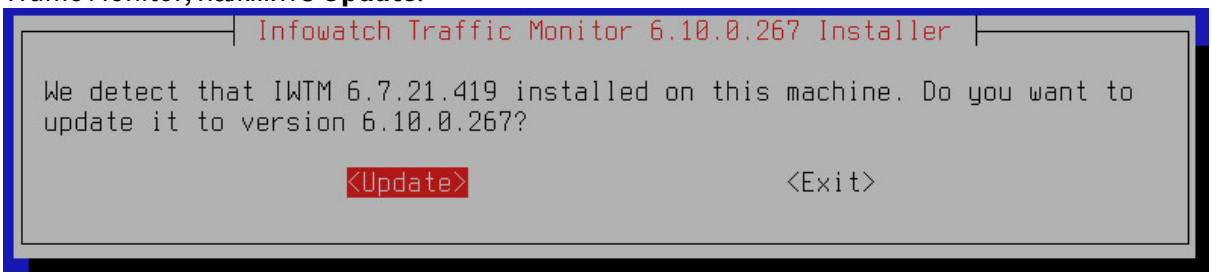
    В нашем примере команда будет следующей:
    ```
    sudo bash /distr/iwtm-installer-6.10.0.267-astra-smolensk.run
    ```
    Начнется распаковка файлов, необходимых для установки Traffic Monitor.



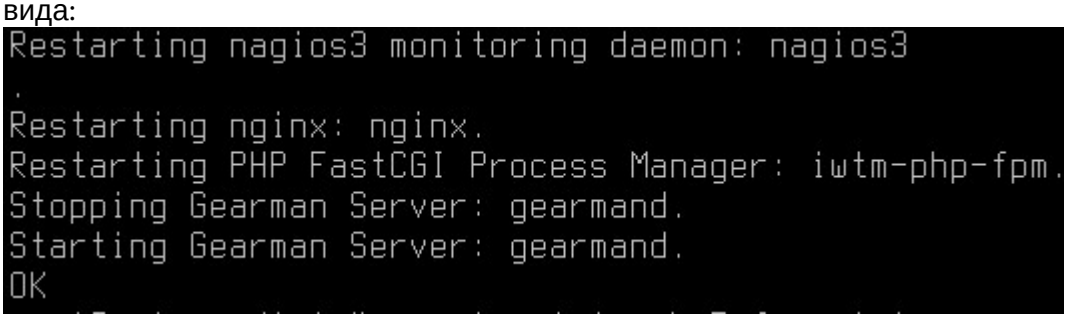
    По завершении на экране отобразится окно с приглашением установить Traffic Monitor (номер в окне соответствует номеру устанавливаемой версии Системы):



22. Для продолжения нажмите **Continue**.
23. В открывшемся окне, оповещающем о том, что найдена более ранняя версия InfoWatch Traffic Monitor, нажмите **Update**:



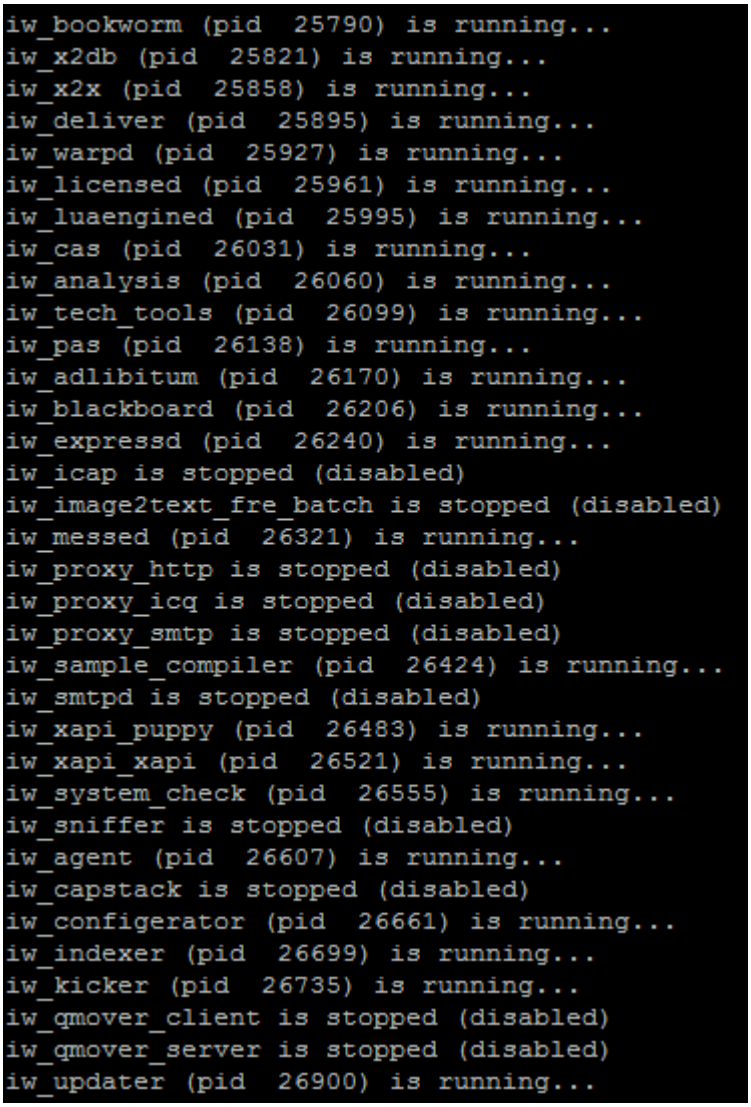
24. Убедитесь в том, что обновление завершилось - в консоли отобразится сообщение вида:



25. Введите команду для поиска и вывода на экран консоли списка файлов с расширением **.dpkg-dist**.
    ```
    sudo find / -name "*dpkg-dist*" -print
    ```
    Если такие файлы найдены, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов").
26. Введите команду для вызова файлового менеджера:
    ```
    sudo mc
    ```
27. Перейдите в директорию `/opt/iw/tm5/etc/scripts/` и убедитесь в наличии файла **`iwssid.lua.upgrade`**.
    Файл **`iwssid.lua.upgrade`** не используется Системой, он служит источником информации для восстановления работоспособности Системы в случае ее глубокой кастомизации.
28. Также в директории `/opt/iw/tm5/etc/scripts/` должен быть файл **`iwssid.lua`**, его рекомендуется оставить без изменений, если выполнено по крайней мере одно из условий:
    - обновление Системы ведется с версии 6.9;
    - до обновления файл **`iwssid.lua`** не редактировался.

    В противном случае его необходимо корректно объединить с конфигурационным файлом **`iwssid.lua.rpmnew`** (см. статью "Объединение конфигурационных файлов").
29. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    ```
    exit
    ```
30. Выполните Обновление СУБД PostgreSQL.
31. Для переключения на пользователя *postgres* введите команду:
    ```
    sudo su - postgres
    ```
32. Введите команду для запуска скрипта (сценария) обновления БД:
    ```
    sudo bash /opt/iw/tm5/csw/postgres/update.sh
    ```
33. Введите команду:
    ```
    exit
    ```

34. Введите команду для очистки кеша:
    `redis-cli flushall`
35. Введите команду для перезагрузки сервера:
    `sudo reboot`
36. Дождитесь загрузки сервера и повторите шаги **1**, **2** и **3** данной инструкции для входа в консоль.
37. Чтобы подключиться к серверу БД из консоли введите команды:
    `sudo su - iwtm`
    `psql postgres iwtm -p 5433`
38. Для вывода списка пользователей выполните команду:
    `select* from pg_user;`
    Просмотрите список и проверьте, был ли создан пользователь `siem`.
    Нажмите **q**.
39. Для выхода введите команду:
    `\q`
40. Введите команду:
    `exit`
41. Если пользователь `siem` был создан, то:
    a. Удалите пользователя siem (см. документ "InfoWatch Traffic Monitor. Руководство администратора", статья "Удаление пользователя siem").
    b. Создайте нового пользователя siem (см. документ "InfoWatch Traffic Monitor. Руководство администратора", статья "Создание пользователя siem").
42. Введите команду для проверки запуска процессов:
    `sudo service iwtm status`
    На экране отобразится список процессов и их статус. Обычно сервисы `iw_icap`, `iw_proxy_http`, `iw_proxy_icq`, `iw_proxy_smtp`, `iw_smtpd`, `iw_sniffer`, `iw_capstack`, `iw_qmover_client`, `iw_qmover_server` и `iw_image2test_fre_batch` бывают остановлены, для этих сервисов строки должны заканчиваться фразой "**is stopped (disabled)**". А все остальные сервисы - запущены, для них строки заканчиваются фразой "**is running...**":



Обновление Traffic Monitor до версий 6.10.10 и 6.10.11 на Astra Linux 1.6

> **Важно!**
>
> После перехода Системы на ОС Astra Linux 1.6 конфигурацию Traffic Monitor необходимо будет настроить вновь.

Чтобы обновить Систему, выполните следующие действия:

1. Выполните действия 1-7 инструкции по обновлению Traffic Monitor до версии 6.10.0.
2. Чтобы проверить версию установленной Системы, откройте файл **version**.
3. Если установленная версия Traffic Monitor ниже 6.10.0, обновите Систему по инструкции до версии 6.10.0 или 6.10.1, используя дистрибутивы Astra Linux 1.5.
4. Выполните команды:
   ```
   sudo service iwtm stop
   sudo service iwtm-php-fpm stop
   ```
5. Подключитесь к Базе данных и проверьте количество содержащихся в ней событий:

1. Чтобы подключиться к серверу БД, из консоли введите команды:
   ```
   su - iwtm
   psql postgres iwtm -p 5433
   ```
2. Далее введите команду:
   ```
   select count(1) from object;
   ```
3. Для выхода введите команду:
   ```
   \q
   ```
4. Введите команду:
   ```
   exit
   ```

- Выполните команду:
  ```
  sudo service postgresql stop
  ```
- Создайте резервные копии:

> **Важно!**
>
> Для успешного восстановления файлы должны быть скопированы с сохранением их **прав, пользователей и групп**.
> Для этого копируйте файлы только на **файловую систему Linux** (например, Ext4 или XFS).
> После установки резервные копии будет необходимо скопировать по адресам исходных файлов.

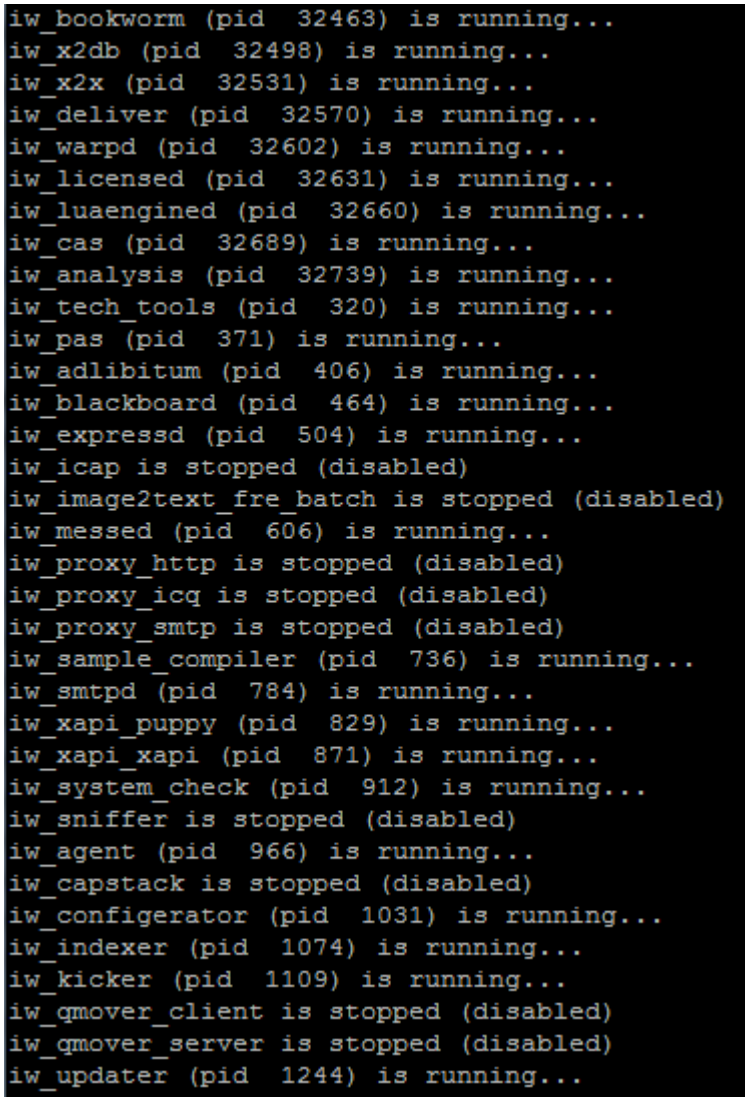
1. Создайте резервную копию Базы данных. По умолчанию База данных расположена в директориях **/u01, /u02** и т.д.
   Скопируйте Базу данных либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство;
2. Создайте резервную копию индексов. Для этого:
   a. Введите команду для вызова файлового менеджера:
      ```
      sudo mc
      ```
   b. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на просмотр файл **`indexer.conf`**.
   c. В параметре `"SphinxBaseDir"` указан путь к директории с индексами. В параметре "ArchiveDir" указан относительный путь к архивам индексов. Путь к архивам указывается относительно содержимого параметра `"NookDir"`.
      Скопируйте директории с индексами и архивами индексов либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство.
3. Создайте резервную копию конфигурации службы `iw_adlibitum`. Для этого:

1. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на просмотр файл **`adlibitum.conf`**.
2. В параметре "ConfigDir" указан относительный путь к директории с конфигурации службы `iw_adlibitum`. Путь к директории указывается относительно содержимого параметра `"NookDir"`.
   Скопируйте директорию с конфигурацией либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство.
3. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
   ```
   exit
   ```

- Перезагрузите сервер, выполнив команду:
  ```
  sudo reboot
  ```
  Не дожидаясь завершения перезагрузки сервера, укажите для загрузки операционной системы диск с

дистрибутивом (Astra-Linux-Smolensk) и установите Traffic Monitor версии 6.10.10 или 6.10.11 на Astra Linux 1.6.

- Введите команды для остановки служб:
  ```
  sudo /etc/init.d/iwtm stop
  sudo /etc/init.d/iwtm-php-fpm stop
  sudo /etc/init.d/postgresql stop
  sudo /etc/init.d/pgagent stop
  ```
- Удалите содержимое директорий **/u01, /u02** и т.д
- Скопируйте созданную в действии 7a резервную копию Базы данных таким образом, чтобы расположение соответствовало исходной.
- Введите команды для запуска Базы данных:
  ```
  sudo /etc/init.d/postgresql start
  sudo /etc/init.d/pgagent start
  ```
- Для переключения на пользователя *postgres* введите команду:
  ```
  sudo su - postgres
  ```
- Введите команду для запуска скрипта (сценария) обновления БД:
  ```
  sudo bash /opt/iw/tm5/csw/postgres/update.sh
  ```
  Обновление должно завершиться без ошибок.
- Введите команду:
  ```
  exit
  ```
- Выполните действие 5 данной инструкции, чтобы сравнить количество событий в Базе данных до и после обновления.
- Скопируйте созданные в действиях 7b и 7c резервные копии таким образом, чтобы расположение соответствовало исходным директориям и файлам.
  Если исходное расположение не являлось расположением по умолчанию, его необходимо будет указать в соответствующих разделах конфигурационных файлов (см. действия 7b и 7c).
- Для перехвата smtp с учетом мандатных меток:
  1. Введите команду для вызова файлового менеджера:
     ```
     sudo mc
     ```
  2. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
  3. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.
  4. Для выхода из файлового менеджера введите команду:
     ```
     exit
     ```
  5. Чтобы вступили в силу изменения привилегий пользователя `iwtm`, которые необходимы для считывания мандатных меток, перезагрузите сервер командой:
     ```
     sudo reboot
     ```
- Введите команду для проверки запуска процессов:
  ```
  sudo /etc/init.d/iwtm status
  ```
  На экране отобразится список процессов и их статус. Обычно сервисы `iw_icap`, `iw_proxy_http`, `iw_proxy_icq`, `iw_proxy_smtp`, `iw_sniffer`, `iw_capstack`, `iw_qmover_client`, `iw_qmover_server` и `iw_image2test_fre_batch` бывают остановлены, для этих сервисов строки должны заканчиваться фразой "**is stopped (disabled)**". А все остальные сервисы - запущены, для них строки заканчиваются фразой "**is running...**":



Обновление Traffic Monitor 6.10.10 до версии 6.10.11 на Astra Linux 1.6

> **Важно!**
>
> После перехода Системы на ОС Astra Linux 1.6 конфигурацию Traffic Monitor необходимо будет настроить вновь.

Чтобы обновить Систему, выполните следующие действия:

1. Выполните действия 1-7 инструкции по обновлению Traffic Monitor до версии 6.10.0.
2. Чтобы проверить версию установленной Системы, откройте файл **`version`**.
3. Если установлена версия Traffic Monitor:
   - **ниже 6.10.10** - обновите Систему по инструкции до версии 6.10.11.
   - **6.10.10** - продолжайте следовать инструкции по обновлению Системы.
4. Откройте файл **`sources.list`**, расположенный в директории `/etc/apt`, и проверьте соответствие его содержимого следующему виду:
   ```
   deb file:///директория_1/ smolensk main non-free contrib
   deb file:///директория_2/ smolensk main non-free contrib
   ```
   где:

a. `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
b. `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel

5. Закройте файл **`sources.list`**.
Перейдите в указанные в файле директории, и убедитесь в наличии в них папок и файлов репозиториев.
6. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
`exit`
7. Если в указанных директориях не созданы репозитории, создайте их (см. статью "Установка ТМ в режиме "Все-в-одном", действия 5-11).

> **Примечание:**
>
> Содержание файла **`sources.list`** должно соответствовать действию 4.

8. Выполните следующую команду:
`sudo apt-get update`
9. Введите команды для остановки перехватчиков:
```
sudo /etc/init.d/iwtm stop expressd
sudo /etc/init.d/iwtm stop xapi_xapi
sudo /etc/init.d/iwtm stop xapi_puppy
```
10. 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/
```
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**.

11. Последовательно введите команды для остановки служб:

12. `sudo /etc/init.d/iwtm stop`
    `sudo /etc/init.d/iwtm-php-fpm stop`
    `sudo /etc/init.d/nagios3 stop`
13. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки), поставляемый на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера.
    Например, в директорию `/distr`.
14. Выполните действия 21-29, 34-36 инструкции по обновлению Traffic Monitor до версии 6.10.0.
15. Введите команду для проверки запуска процессов:
    `sudo /etc/init.d/iwtm status`
    На экране отобразится список процессов и их статус. Обычно сервисы `iw_icap`, `iw_proxy_http`, `iw_proxy_icq`, `iw_proxy_smtp`, `iw_sniffer`, `iw_capstack`, `iw_qmover_client`, `iw_qmover_server` и `iw_image2test_fre_batch` бывают остановлены, для этих сервисов строки должны заканчиваться фразой "**is stopped (disabled)**". А все остальные сервисы - запущены, для них строки заканчиваются фразой "**is running...**":



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

Обновлению подлежат все серверы TM (тип установки TM Node) и сервер СУБД (тип установки DB Node).

> **Важно!**
>
> Каждый сервер должен иметь уникальный корректный FQDN.

Обновление Traffic Monitor на Astra Linux 1.5 до версий 6.10.0 и 6.10.1

Порядок обновления следующий:

Шаг 1. Обновление всех серверов TM (TM Node).

Шаг 2. Обновление и перезапуск сервера СУБД (DB Node).

Шаг 3. Перезапуск всех серверов TM (TM Node).

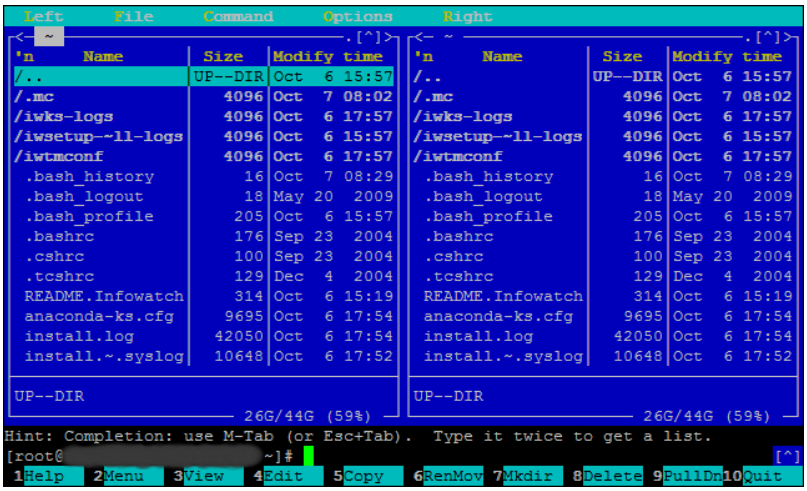
> **Важно!**
>
> Права пользователя, созданного на этапе установки, ограничены в операционной системе, поэтому:
>
> - при выполнении части команд в командной строке потребуется использовать программу **sudo**. Например, для создания директории `disk1` в корневой директории необходимо ввести команду:
>
>   ```
>   sudo mkdir /disk1
>   ```
> - копировать данные по SSH можно только в домашний каталог пользователя и вложенные в него каталоги (например, это касается дистрибутива Traffic Monitor при копировании его на компьютер по SSH).
>
> Чтобы работать с правами пользователя *root*, в командной строке введите `sudo su`. **Внимание!** К данному способу работы, ввиду возможности допустить серьезную ошибку, крайне не рекомендуется прибегать без помощи специалистов компании InfoWatch.

ШАГ 1. ОБНОВЛЕНИЕ ВСЕХ СЕРВЕРОВ TM (TM Node)

Чтобы обновить серверы TM (TM Node), на каждом из них выполните следующие действия:

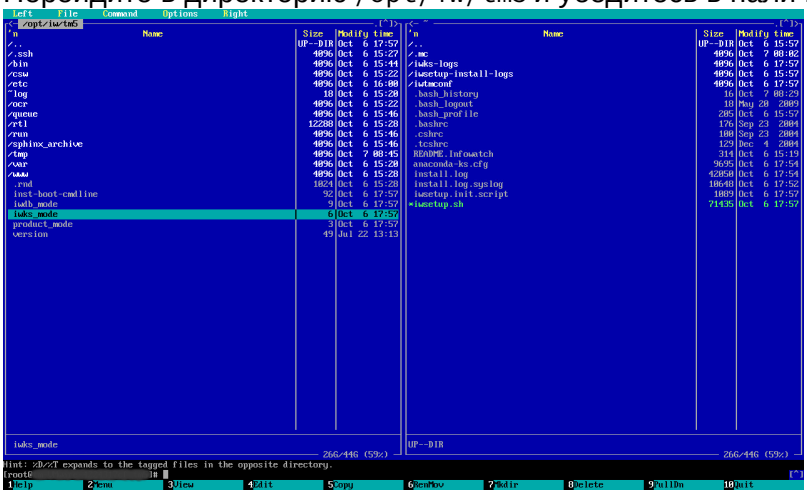
1. Откройте консоль обновляемого сервера.
2. Введите имя пользователя, от имени которого планируется обновление, и нажмите **Enter**.
3. Введите пароль и нажмите **Enter**.
4. Вызовите командную строку (например, терминал *Fly*).
5. Введите команду для вызова файлового менеджера:

```
sudo mc
```



На экране отобразится окно файлового менеджера *Midnight Commander*, в котором удобно просматривать файлы.

6. 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`

7. Убедитесь, что содержимое файла - слово "iwtm".

> **Примечание:**
>
> Если файл имеет другое содержимое, удалите все символы и введите: `iwtm`

8. Для подготовки Системы к обновлению, выполните действия:
   a. На **Сервере СУБД (TME DB Server)**:

i. Выполните действия 1-7 Шага 2 (см. ниже).
ii. Перейдите в директорию `/opt/iw/tm5/etc`, установите курсор на файл **serman.conf** и нажмите **F3**.
iii. В блоке `DefaultInterface` найдите IP-адрес.

b. На **всех Серверах TM (TME Node Server)**:
i. Перейдите в директорию `/opt/iw/tm5/etc`, установите курсор на файл **serman_client.conf** и нажмите **F4**.
ii. Найдите блок `SermanHost`.
Сравните его значение с IP-адресом, который указан в файле **serman.conf** на **Сервере СУБД (TME DB Server)**.
iii. Если они не совпадают, замените значение в блоке SermanHost на **СерверахTM (TME Node Server)** на IP-адрес, который указан в блоке `DefaultInterface` файла **serman.conf** на **Сервере СУБД (TME DB Server)**.
iv. Нажмите **F2**.
v. В открывшемся окне подтвердите сохранение файла, нажав **Save**.
vi. Нажмите **F10**.

c. На **Сервере СУБД (TME DB Server)** нажмите **F3**.

9. Откройте файл **sources.list**, расположенный в директории `/etc/apt`, и проверьте соответствие его содержимого следующему виду:
```
deb file:///директория_1/ smolensk main non-free contrib
deb file:///директория_2/ smolensk main non-free
```
где:
a. `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
b. `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel
10. Закройте файл **sources.list**.
Перейдите в указанные в файле директории, и убедитесь в наличии в них папок и файлов репозиториев.
11. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
```
exit
```
12. Если в указанных директориях не созданы репозитории, создайте их (см. статью "Установка TM в режиме "Все-в-одном", действия 5-11).
13. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки) и архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**, поставляемые на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера . **Например**, в директорию `/distr`.
14. Введите команду для перехода в нужную директорию:
```
cd /<директория_с_архивом>
```
где `/<директория_с_архивом>` - путь к директории, содержащей архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**.
В нашем примере команда будет следующей:
```
cd /distr
```
15. Введите команду для извлечения архива:
```
sudo tar -xzf astra-linux-smolensk-1.5-pg96_x86_64.tar.gz -C /opt
```
16. Введите команду для перехода в нужную директорию:

```
cd /opt
```

17. Выполните следующую команду:
```
sudo mv astra-linux-smolensk-1.5-pg96-local.list /etc/apt/sources.list.d
```
18. Выполните следующую команду:
```
sudo apt-get update
```
19. Выполните команды для остановки перехватчиков:
```
sudo service iwtm stop expressd
sudo service iwtm stop xapi_xapi
sudo 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.

20. 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/
```
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**.

21. Необходимо получить файл (имя файла - **sd_nodes.out**), содержащий IP-адреса нод для обновления. Для этого запустите установщик .run с параметром:

Если 2 ноды (сервер TM и сервер СУБД), то:	`sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk.run -- --before-upgrade`

Если нод больше, чем 2:	`sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk.run -- --before-upgrade --tm_nodes_count=<количество нод>`

где `/<директория_с_файлом>` - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run**;
`<количество_нод>` - количество всех серверов, включая сервер СУБД.
В нашем примере команда будет следующей:

```
sudo bash /distr/iwtm-installer-6.10.0.279-astra-smolensk.run -- --before-upgrade
```

Примерный вывод в консоль будет таким:

```
See log files for more details:
    /var/log/infowatch/generate_serman_services_nodes_for_consul.out
    /var/log/infowatch/generate_serman_services_nodes_for_consul.err

Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name            Version      Architecture Description
+++-===============-============-=============
==================================
ii  iwtm-serman-cli 6.7.12.200-r amd64        InfoWatch Traffic Monitor Service M
WARNING: missing binary '/opt/iw/tm5/bin/serman_prober', trying to install 'iwtm-qatools' package...
Reading package lists...
Building dependency tree...
Reading state information...
...
ldconfig deferred processing now taking place
==> /opt/iw/tm5/tmp/sd_nodes.out <==
10.20.30.40
10.20.30.41

OK: Please copy the file to all nodes before upgrading TM on them, e.g.:
    scp /opt/iw/tm5/tmp/sd_nodes.out <username>@10.20.30.40:/home/<username>/sd_nodes.out
```

22. Скопируйте файл **sd_nodes.out** на все указанные ноды, исключая ту, на которой он был создан. Выполните команды:

```
sudo scp /opt/iw/tm5/tmp/sd_nodes.out <имя_пользователя>@10.20.30.40:/home/<имя_пользователя>/sd_nodes.out
```

где `<имя_пользователя>` - пользователь, который имеет права на работу в указанной директории на целевой ноде.
Команды для копирования файла **sd_nodes.out** на все необходимые IP-адреса указаны последними строками в выводе в консоль на предыдущем шаге.
В нашем примере команда будет следующей:

```
sudo scp /opt/iw/tm5/tmp/sd_nodes.out astra@10.20.30.40:/home/astra/
sd_nodes.out
```

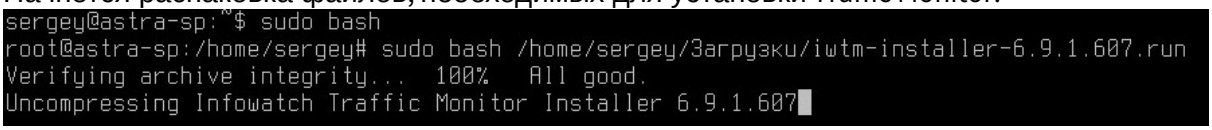
После ввода команды копирования будет выведен запрос вида:

```
Are you sure you want to continue connecting (yes/no)?
```

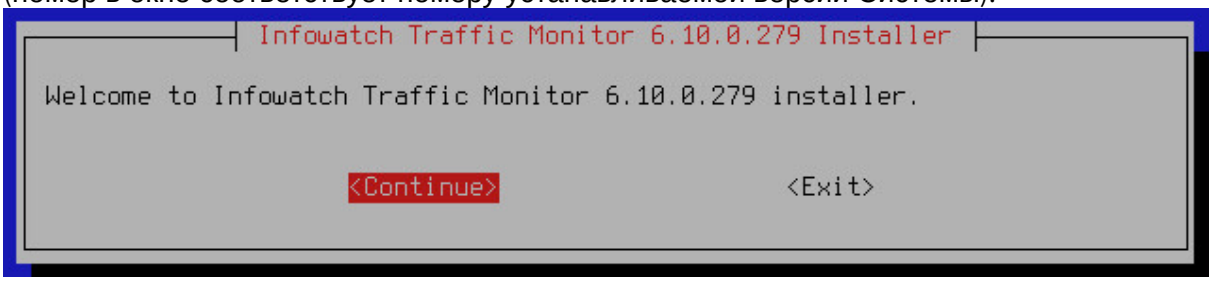
Для продолжения наберите **yes** на клавиатуре и нажмите **Enter**.
Затем введите пароль от целевой ноды и нажмите **Enter**.

> **Примечание:**
>
> Выполните действия 21 и 22 только на одной ноде. Допускается выбрать любую ноду.

23. Если серверов TM (TM Node) больше одного, на каждом сервере кроме того, на котором был создан файл **sd_nodes.out**, выполните следующую команду:
    `sudo mv /home/<имя_пользователя>/sd_nodes.out /opt/iw/tm5/tmp`
    где `<имя_пользователя>` - пользователь, который имеет права на работу в указанной директории.
24. Введите команды для остановки сервисов сервера Traffic Monitor:
    ```
    sudo service iwtm stop
    sudo service php5-fpm stop
    sudo service nagios3 stop
    ```
25. Выполните следующую команду:
    `sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk.run`
    В нашем примере команда будет следующей:
    `sudo bash /distr/iwtm-installer-6.10.0.279-astra-smolensk.run`
    Начнется распаковка файлов, необходимых для установки Traffic Monitor.

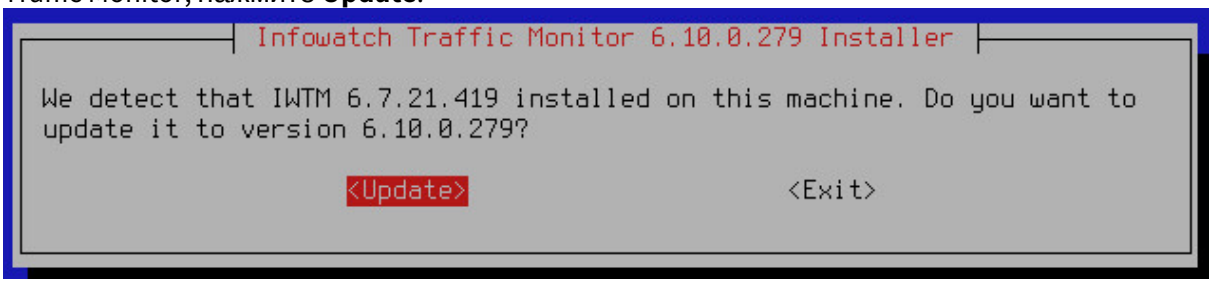


По завершении на экране отобразится окно с приглашением установить Traffic Monitor (номер в окне соответствует номеру устанавливаемой версии Системы):



26. Для продолжения нажмите **Continue**.

27. В открывшемся окне, оповещающем о том, что найдена более ранняя версия InfoWatch Traffic Monitor, нажмите **Update**:



28. Убедитесь в том, что обновление завершилось - в консоли отобразится сообщение вида:



29. Введите команду для поиска и вывода на экран консоли списка файлов с расширением **.dpkg-dist**.
    `sudo find / -name "*dpkg-dist*" -print`
    Если такие файлы найдены, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов").
30. Введите команду для вызова файлового менеджера:
    `sudo mc`
31. Перейдите в директорию `/opt/iw/tm5/etc/scripts/` и убедитесь в наличии файла **`iwssid.lua.upgrade`**.
    Файл **`iwssid.lua.upgrade`** не используется Системой, он служит источником информации для восстановления работоспособности Системы в случае ее глубокой кастомизации.
32. Также в директории `/opt/iw/tm5/etc/scripts/` должен быть файл **`iwssid.lua`**, его рекомендуется оставить без изменений, если до обновления файл **`iwssid.lua`** не редактировался.
    В противном случае его необходимо корректно объединить с конфигурационным файлом **`iwssid.lua.rpmnew`** (см. статью "Объединение конфигурационных файлов").
33. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    `exit`
34. Обновите сервер СУБД (DB Node) - описание смотрите ниже.

ШАГ 2. ОБНОВЛЕНИЕ СЕРВЕРА СУБД (DB Node)

Чтобы обновить сервер СУБД (DB Node), выполните следующие действия:

1. Откройте консоль обновляемого сервера.
2. Введите имя пользователя, от имени которого планируется обновление, и нажмите **Enter**.
3. Введите пароль и нажмите **Enter**.
4. Вызовите командную строку (например, терминал *Fly*).

5. Введите команду для вызова файлового менеджера:
   `sudo mc`
6. 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`

7. Убедитесь, что содержимое файла - слово "iwdb".

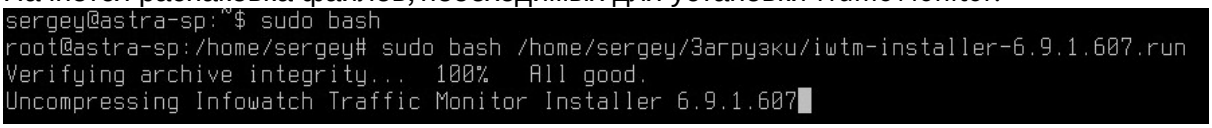
> **Примечание:**
>
> Если файл имеет другое содержимое, удалите все символы и введите `iwdb`

8. Откройте файл **sources.list**, расположенный в директории `/etc/apt`, и проверьте соответствие его содержимого следующему виду:
   ```
   deb file:///директория_1/ smolensk main non-free contrib
   deb file:///директория_2/ smolensk main non-free
   ```
   где:
   a. `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
   b. `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel
9. Закройте файл **sources.list**.
   Перейдите в указанные в файле директории, и убедитесь в наличии в них папок и файлов репозиториев.
10. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    `exit`
11. Если в указанных директориях не созданы репозитории, создайте их (см. статью "Установка ТМ в режиме "Все-в-одном", действия 5-11).

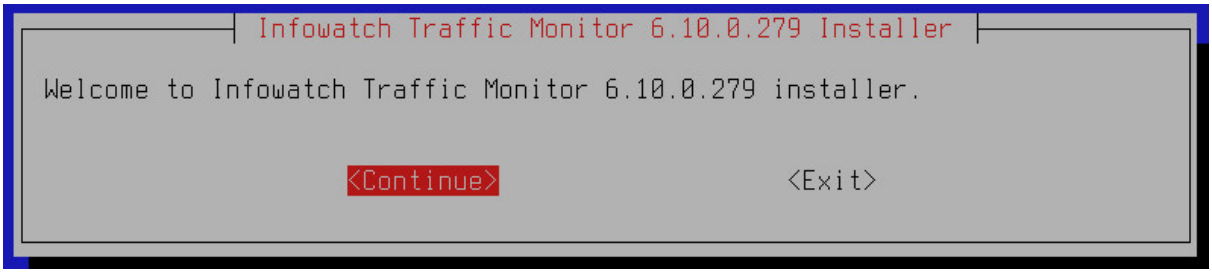
12. Выполните следующую команду:
    `sudo mv /home/<имя_пользователя>/sd_nodes.out /opt/iw/tm5/tmp`
    где <имя_пользователя> - пользователь, который имеет права на работу в указанной директории.
    В нашем примере команда будет следующей:
    `sudo mv /home/astra/sd_nodes.out /opt/iw/tm5/tmp`
13. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки) и архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**, поставляемые на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера . **Например**, в директорию `/distr`.
14. Введите команду для перехода в нужную директорию:
    `cd /<директория_с_архивом/`

    где `/<директория_с_архивом>/` - путь к директории, содержащей архив **astra-linux-smolensk-1.5-pg96_x86_64.tar.gz**.
    В нашем примере команда будет следующей:
    `cd /distr`
15. Введите команду для извлечения архива:
    `sudo tar -xzf astra-linux-smolensk-1.5-pg96_x86_64.tar.gz -C /opt`
16. Введите команду для перехода в нужную директорию:
    `cd /opt`
17. Выполните следующую команду:
    `sudo mv astra-linux-smolensk-1.5-pg96-local.list /etc/apt/sources.list.d`
18. Выполните следующую команду:
    `sudo apt-get update`
19. Введите команду для остановки служб:
    `sudo service iwtm stop`
20. Убедитесь, что нет активных пользователей, подключенных к серверу через консоль управления (во всех веб-консолях произведен выход).
21. Выполните следующую команду:
    `sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk.run`
    где <директория_с_файлом> - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run**.

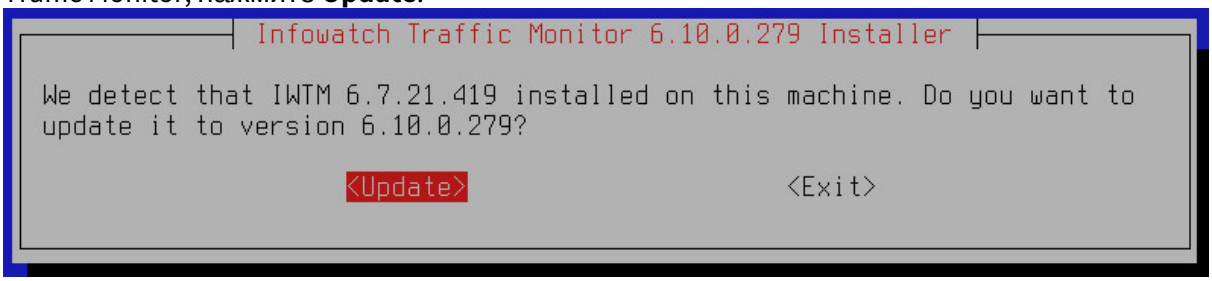
    В нашем примере команда будет следующей:
    `sudo bash /distr/iwtm-installer-6.10.0.279-astra-smolensk.run`
    Начнется распаковка файлов, необходимых для установки Traffic Monitor.



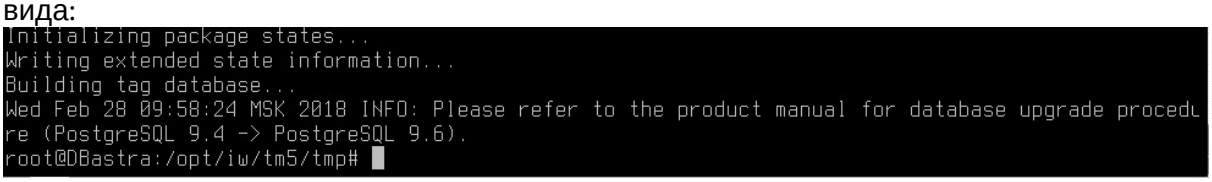
    По завершении на экране отобразится окно с приглашением установить Traffic Monitor (номер в окне соответствует номеру устанавливаемой версии Системы):



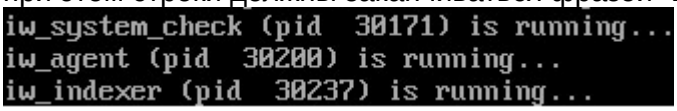
22. Для продолжения нажмите **Continue**.
23. В открывшемся окне, оповещающем о том, что найдена более ранняя версия InfoWatch Traffic Monitor, нажмите **Update**:



24. Убедитесь в том, что обновление завершилось - в консоли отобразится сообщение вида:



25. Введите команду для поиска и вывода на экран консоли списка файлов с расширением **.dpkg-dist**.
    `sudo find / -name "*dpkg-dist*" -print`
    Если такие файлы найдены, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов").
26. Введите команду для вызова файлового менеджера:
    `sudo mc`
27. Перейдите в директорию `/opt/iw/tm5/etc/scripts/` и убедитесь в наличии файла **`iwssid.lua.upgrade`**.
    Файл **`iwssid.lua.upgrade`** не используется Системой, он служит источником информации для восстановления работоспособности Системы в случае ее глубокой кастомизации.
28. Также в директории `/opt/iw/tm5/etc/scripts/` должен быть файл **`iwssid.lua`**, его рекомендуется оставить без изменений, если до обновления файл **`iwssid.lua`** не редактировался.
    В противном случае его необходимо корректно объединить с конфигурационным файлом **`iwssid.lua.rpmnew`** (см. статью "Объединение конфигурационных файлов").
29. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    `exit`
30. Выполните обновление СУБД PostgreSQL.
31. Для переключения на пользователя *postgres* введите команду:
    `sudo su - postgres`
32. Введите команду для запуска скрипта (сценария) обновления БД:
    `bash /opt/iw/tm5/csw/postgres/update.sh`

33. Введите команду:
    `exit`
34. Введите команду для перезагрузки сервера:
    `sudo reboot`
35. Дождитесь загрузки сервера и повторите действия **1**, **2** и **3** ШАГА 1 данной инструкции.
36. Чтобы подключиться к серверу БД из консоли введите команды:
    `sudo su - iwtm`
    `psql postgres iwtm -p 5433`
37. Для вывода списка пользователей выполните команду:
    `select* from pg_user;`
    Просмотрите список и проверьте, был ли создан пользователь `siem`.
    Нажмите **q**.
38. Для выхода введите команду:
    `\q`
39. Введите команду:
    `exit`
40. Если пользователь `siem` был создан, то:
    a. Удалите пользователя siem (см. документ "InfoWatch Traffic Monitor. Руководство администратора", статья "Удаление пользователя siem").
    b. Создайте нового пользователя siem (см. документ "InfoWatch Traffic Monitor. Руководство администратора", статья "Создание пользователя siem").
41. Введите команду для проверки запуска процессов:
    `sudo service iwtm status`
    На экране отобразится список процессов и их статус. Сервисы должны быть запущены, при этом строки должны заканчиваться фразой "**is running...**":
    
    ```
    iw_system_check (pid  30171) is running...
    iw_agent (pid  30200) is running...
    iw_indexer (pid  30237) is running...
    ```
42. Запустите все Серверы TM (TM Node) - описание смотрите ниже.

ШАГ 3. ПЕРЕЗАПУСК СЕРВЕРОВ TM (TM Node)

Чтобы перезапустить серверы TM (TM Node), на каждом из них выполните следующие действия:

1. На сервере TM (TME Node Server), на котором функционирует пакет `web-gui`, введите команду для очистки кеша:
   `redis-cli flushall`
2. Введите команду для перезагрузки сервера:
   `sudo reboot`
3. Дождитесь загрузки сервера и повторите действия **1**, **2** и **3** ШАГА 1 данной инструкции.
4. Введите команду для проверки запуска процессов:
   `sudo service iwtm status`
   На экране отобразится список процессов и их статус. Обычно сервисы `iw_icap`, `iw_proxy_http`, `iw_proxy_icq`, `iw_proxy_smtp`, `iw_smtpd`, `iw_sniffer`, `iw_capstack`, `iw_qmover_client`, `iw_qmover_server` и `iw_image2test_fre_batch` бывают остановлены, для этих сервисов строки должны заканчиваться фразой "**is stopped (disabled)**". А все остальные сервисы - запущены, для

них строки заканчиваются фразой "**is running...**"::

```
iw_bookworm (pid  25790) is running...
iw_x2db (pid  25821) is running...
iw_x2x (pid  25858) is running...
iw_deliver (pid  25895) is running...
iw_warpd (pid  25927) is running...
iw_licensed (pid  25961) is running...
iw_luaengined (pid  25995) is running...
iw_cas (pid  26031) is running...
iw_analysis (pid  26060) is running...
iw_tech_tools (pid  26099) is running...
iw_pas (pid  26138) is running...
iw_adlibitum (pid  26170) is running...
iw_blackboard (pid  26206) is running...
iw_expressd (pid  26240) is running...
iw_icap is stopped (disabled)
iw_image2text_fre_batch is stopped (disabled)
iw_messed (pid  26321) is running...
iw_proxy_http is stopped (disabled)
iw_proxy_icq is stopped (disabled)
iw_proxy_smtp is stopped (disabled)
iw_sample_compiler (pid  26424) is running...
iw_smtpd is stopped (disabled)
iw_xapi_puppy (pid  26483) is running...
iw_xapi_xapi (pid  26521) is running...
iw_system_check (pid  26555) is running...
iw_sniffer is stopped (disabled)
iw_agent (pid  26607) is running...
iw_capstack is stopped (disabled)
iw_configerator (pid  26661) is running...
iw_indexer (pid  26699) is running...
iw_kicker (pid  26735) is running...
iw_qmover_client is stopped (disabled)
iw_qmover_server is stopped (disabled)
iw_updater (pid  26900) is running...
```

Обновление Traffic Monitor до версий 6.10.10 и 6.10.11 на Astra Linux 1.6

> **Важно!**
>
> После перехода Системы на ОС Astra Linux 1.6 конфигурацию Traffic Monitor необходимо будет настроить вновь.

Порядок обновления следующий:

Шаг 1. Подготовка Системы к обновлению.

Шаг 2. Обновление сервера СУБД (DB Node).

Шаг 3. Обновление всех серверов ТМ (TM Node).

Важно!

Права пользователя, созданного на этапе установки, ограничены в операционной системе, поэтому:

- при выполнении части команд в командной строке потребуется использовать программу **sudo**. Например, для создания директории `disk1` в корневой директории необходимо ввести команду:
  `sudo mkdir /disk1`
- копировать данные по SSH можно только в домашний каталог пользователя и вложенные в него каталоги (например, это касается дистрибутива Traffic Monitor при копировании его на компьютер по SSH).

Чтобы работать с правами пользователя *root*, в командной строке введите `sudo su`. **Внимание!** К данному способу работы, ввиду возможности допустить серьезную ошибку, крайне не рекомендуется прибегать без помощи специалистов компании InfoWatch.

ШАГ 1. ПОДГОТОВКА СИСТЕМЫ К ОБНОВЛЕНИЮ

Чтобы подготовить Систему к обновлению выполните следующие действия:

1. На всех обновляемых серверах выполните действия 1-5 Шага 1 инструкции по обновлению Traffic Monitor до версии 6.10.0.
2. Чтобы проверить версию установленной Системы, перейдите в директорию `/opt/iw/tm5` и откройте файл **version**.
3. Если установленная версия Traffic Monitor ниже 6.10.0, обновите Систему по инструкции до версии 6.10.0 или 6.10.1, используя дистрибутивы Astra Linux 1.5.
4. На **всех серверах TM (TM Node)**:
   a. Выполните команды для остановки служб:
   ```
   sudo service iwtm stop
   sudo service iwtm-php-fpm stop
   sudo service nagios3 stop
   sudo service iwtm-consul stop
   ```
   b. Создайте резервную копию конфигурации службы `iw_adlibitum`. Для этого:

   Важно!

   Для успешного восстановления файлы должны быть скопированы с сохранением их **прав, пользователей и групп**.
   Для этого копируйте файлы только на **файловую систему Linux** (например, Ext4 или XFS).
   После установки резервные копии будет необходимо скопировать по адресам исходных файлов.

   a. Введите команду для вызова файлового менеджера:
   `sudo mc`
   b. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на просмотр файл **`adlibitum.conf`**;
   c. В параметре "ConfigDir" указан относительный путь к директории с конфигурации службы `iw_adlibitum`. Путь к директории указывается относительно содержимого

параметра "NookDir".
Скопируйте директорию с конфигурацией либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство;

d. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
```
exit
```

- На **сервере СУБД (DB Node)**:

1. Выполните команды для остановки служб:
```
sudo service iwtm stop
sudo service nagios3 stop
sudo service iwtm-consul stop
```
2. Подключитесь к Базе данных и проверьте количество содержащихся в ней событий:

1. Чтобы подключиться к серверу БД, из консоли введите команды:
```
su - iwtm
psql postgres iwtm -p 5433
```
2. Далее введите команду:
```
select count(1) from object;
```
3. Для выхода введите команду:
```
\q
```
4. Введите команду:
```
exit
```

- Выполните команду:
```
sudo service postgresql stop
```

- Создайте резервную копию Базы данных, учитывая требования. По умолчанию База данных расположена в директориях **/u01, /u02** и т.д.
Скопируйте Базу данных либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство;

- Создайте резервную копию индексов, учитывая требования. Для этого:
1. Введите команду для вызова файлового менеджера:
```
sudo mc
```
2. Перейдите в директорию /opt/iw/tm5/etc и откройте на просмотр файл **indexer.conf**;
3. В параметре "SphinxBaseDir" указан путь к директории с индексами. В параметре "ArchiveDir" указан относительный путь к архивам индексов. Путь к архивам указывается относительно содержимого параметра "NookDir".
Скопируйте директории с индексами и архивами индексов либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство;
4. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
```
exit
```

- Обновите сервер СУБД (DB Node) - описание смотрите ниже
ШАГ 2. ОБНОВЛЕНИЕ СЕРВЕРА СУБД (DB NODE)

Чтобы обновить сервер СУБД (DB Node), выполните следующие действия:

1. Перезагрузите сервер СУБД, выполнив команду:
```
sudo reboot
```
Не дожидаясь завершения перезагрузки сервера, укажите для загрузки операционной системы диск с дистрибутивом (Astra-Linux-Smolensk) и установите Traffic Monitor версии 6.10.10 или 6.10.11 на Astra Linux 1.6 в режиме DB node.

2. Введите команды для остановки служб:
   `sudo /etc/init.d/iwtm stop`
   `sudo /etc/init.d/postgresql stop`
   `sudo /etc/init.d/pgagent stop`
3. Удалите содержимое директорий **`/u01`, `/u02`** и т.д
4. Скопируйте созданную в действии 5d Шага 1 резервную копию Базы данных таким образом, чтобы расположение соответствовало исходной.
5. Введите команды для запуска Базы данных:
   `sudo /etc/init.d/postgresql start`
   `sudo /etc/init.d/pgagent start`
6. Для переключения на пользователя *postgres* введите команду:
   `sudo su - postgres`
7. Введите команду для запуска скрипта (сценария) обновления БД:
   `sudo bash /opt/iw/tm5/csw/postgres/update.sh`
   Обновление должно завершиться без ошибок.
8. Введите команду:
   `exit`
9. Выполните действие 5b Шага 1 данной инструкции, чтобы сравнить количество событий в Базе данных до и после обновления.
10. Скопируйте созданную в действии 5e Шага 1 резервную копию индексов таким образом, чтобы расположение соответствовало исходным директориям и файлам.
    Если исходное расположение не являлось расположением по умолчанию, его необходимо будет указать в соответствующих разделах конфигурационных файлов (см. действия 5e Шага 1).
11. Введите команду для перезагрузки сервера:
    `sudo reboot`
12. Введите команду для проверки запуска процессов:
    `sudo /etc/init.d/iwtm status`
13. На экране отобразится список процессов и их статус. Сервисы должны быть запущены, при этом строки должны заканчиваться фразой "**`is running...`**":
    ```
    iw_system_check (pid  1168) is running...
    iw_agent (pid  1199) is running...
    iw_indexer (pid  1231) is running...
    ```
14. Обновите все серверы TM (TM Node) - описание смотрите ниже.

ШАГ 3. ОБНОВЛЕНИЕ ВСЕХ СЕРВЕРОВ TM (TM Node)

Чтобы обновить серверы TM (TM Node), на каждом из них выполните следующие действия:

1. Перезагрузите сервер TM, выполнив команду:
   `sudo reboot`
   Не дожидаясь завершения перезагрузки сервера, укажите для загрузки операционной системы диск с дистрибутивом (Astra-Linux-Smolensk) и установите Traffic Monitor версии 6.10.10 или 6.10.11 на Astra Linux 1.6 в режиме TM node .
2. Введите команды для остановки служб:
   `sudo /etc/init.d/iwtm stop`
   `sudo /etc/init.d/iwtm-php-fpm stop`
3. На сервере, на котором установлена и добавлена в автозапуск служба `iw_adlibitum`, скопируйте созданную в действии 4b Шага 1 резервную копию конфигурации таким образом, чтобы расположение соответствовало исходным директориям и файлам.
   Если исходное расположение не являлось расположением по умолчанию, его

необходимо будет указать в соответствующих разделах конфигурационных файлов (см. действия 4b Шага 1).

4. Для перехвата smtp с учетом мандатных меток:
    a. Введите команду для вызова файлового менеджера:
    `sudo mc`
    b. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
    c. Установите параметру "`EnablePrivSock`" значение `true`, сохраните изменения и закройте файл.
    d. Для выхода из файлового менеджера введите команду:
    `exit`
    e. Чтобы вступили в силу изменения привилегий пользователя `iwtm`, которые необходимы для считывания мандатных меток, перезагрузите сервер командой:
    `sudo reboot`

5. Введите команду для проверки запуска процессов:
`sudo /etc/init.d/iwtm status`
На экране отобразится список процессов и их статус. Обычно сервисы `iw_icap`, `iw_proxy_http`, `iw_proxy_icq`, `iw_proxy_smtp`, `iw_sniffer`, `iw_capstack`, `iw_qmover_client`, `iw_qmover_server` и `iw_image2test_fre_batch` бывают остановлены, для этих сервисов строки должны заканчиваться фразой "**is stopped (disabled)**". А все остальные сервисы - запущены, для них строки заканчиваются фразой "**is running...**":



Обновление Traffic Monitor 6.10.10 до версии 6.10.11 на Astra Linux 1.6

Порядок обновления следующий:

Шаг 1. Обновление всех серверов TM (TM Node).

Шаг 2. Обновление и перезапуск сервера СУБД (DB Node).

Шаг 3. Перезапуск всех серверов TM (TM Node).

Важно!

Права пользователя, созданного на этапе установки, ограничены в операционной системе, поэтому:

- при выполнении части команд в командной строке потребуется использовать программу **sudo**. Например, для создания директории `disk1` в корневой директории необходимо ввести команду:
  `sudo mkdir /disk1`

- копировать данные по SSH можно только в домашний каталог пользователя и вложенные в него каталоги (например, это касается дистрибутива Traffic Monitor при копировании его на компьютер по SSH).

Чтобы работать с правами пользователя *root*, в командной строке введите `sudo su`. **Внимание!** К данному способу работы, ввиду возможности допустить серьезную ошибку, крайне не рекомендуется прибегать без помощи специалистов компании InfoWatch.

ШАГ 1. ОБНОВЛЕНИЕ ВСЕХ СЕРВЕРОВ ТМ (ТМ Node)

Чтобы обновить серверы ТМ (ТМ Node), на каждом из них выполните следующие действия:

1. Выполните действия 1-7 Шага 1 инструкции по обновлению Traffic Monitor до версии 6.10.0.
2. Чтобы проверить версию установленной Системы, откройте файл **version**.
3. Если установлена версия Traffic Monitor:
   - **ниже 6.10.10** - обновите Систему по инструкции до версии 6.10.11.
   - **6.10.10** - продолжайте следовать инструкции по обновлению Системы.
4. Откройте файл **`sources.list`**, расположенный в директории `/etc/apt`, и проверьте соответствие его содержимого следующему виду:
   ```
   deb file:///директория_1/ smolensk main non-free contrib
   deb file:///директория_2/ smolensk main non-free contrib
   ```
   где:
   a. `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
   b. `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel
5. Закройте файл **`sources.list`**.
   Перейдите в указанные в файле директории, и убедитесь в наличии в них папок и файлов репозиториев.
6. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
   ```
   exit
   ```
7. Если в указанных директориях не созданы репозитории, создайте их (см. статью "Установка ТМ в режиме "Все-в-одном", действия 5-11).

   Примечание:

   Содержание файла **`sources.list`** должно соответствовать действию 4.

8. Выполните следующую команду:
   ```
   sudo apt-get update
   ```
9. Введите команды для остановки перехватчиков:
   ```
   sudo /etc/init.d/iwtm stop expressd
   sudo /etc/init.d/iwtm stop xapi_xapi
   sudo /etc/init.d/iwtm stop xapi_puppy
   ```

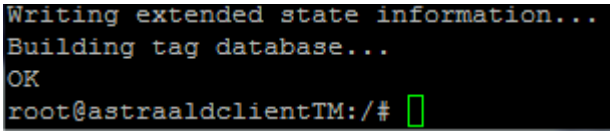
10. Дождитесь, пока обработаются все события, стоящие в очереди на обработку.
    События, находящиеся в очереди, хранятся в следующих директориях:
    `opt/iw/tm5/queue/analysis/.db/`
    `opt/iw/tm5/queue/analysis/.in/`
    `opt/iw/tm5/queue/analysis/.out/`
    `opt/iw/tm5/queue/db/.db/`
    `opt/iw/tm5/queue/db/.in/`
    `opt/iw/tm5/queue/db/.out/`
    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**.

11. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки), поставляемый на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера.
    Например, в директорию `/distr`.
12. Последовательно введите команды для остановки служб:
    ```
    sudo /etc/init.d/iwtm stop
    sudo /etc/init.d/iwtm-php-fpm stop
    sudo /etc/init.d/nagios3 stop
    ```

    > **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.

13. Выполните действия 25-27 Шага 1 инструкции по обновлению Traffic Monitor до версии 6.10.0.
    Убедитесь, что обновление завершилось.В консоли отобразится сообщение вида:

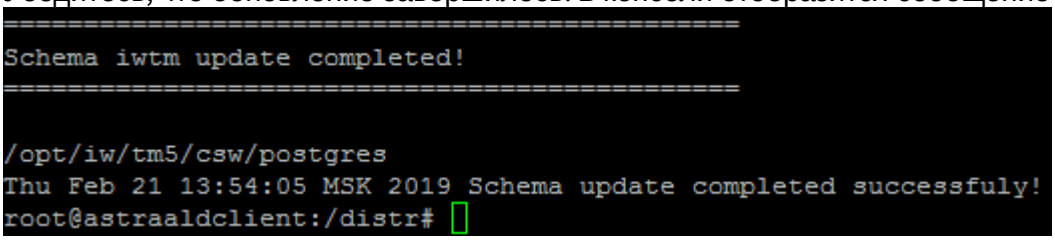
    

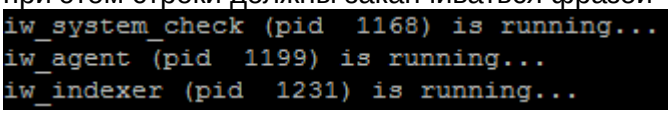
14. Выполните действия 29-33 Шага 1 инструкции по обновлению Traffic Monitor до версии 6.10.0.

15. Обновите сервер СУБД (DB Node) - описание смотрите ниже.

ШАГ 2. ОБНОВЛЕНИЕ СЕРВЕРА СУБД (DB Node)

Чтобы обновить сервер СУБД (DB Node), выполните следующие действия:

1. Выполните действия 1-7 Шага 2 инструкции по обновлению Traffic Monitor до версии 6.10.0.
2. Выполните действия 4-7 Шага 1 данной инструкции по обновлению.
3. Выполните следующую команду:
   `sudo apt-get update`
4. Введите команду для остановки служб:
   `sudo /etc/init.d/iwtm stop`
5. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.run** (где x.x.x.xxx - номер сборки), поставляемый на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера.
   Например, в директорию `/distr`.
6. Выполните действия 20-23 Шага 2 инструкции по обновлению Traffic Monitor до версии 6.10.0.
   Убедитесь, что обновление завершилось. В консоли отобразится сообщение вида:
   
   ```
   ================================================
   Schema iwtm update completed!
   ================================================

   /opt/iw/tm5/csw/postgres
   Thu Feb 21 13:54:05 MSK 2019 Schema update completed successfuly!
   root@astraaldclient:/distr#
   ```
7. Выполните действия 25-29 Шага 2 инструкции по обновлению Traffic Monitor до версии 6.10.0.
8. Введите команду для перезагрузки сервера:
   `sudo reboot`
9. Дождитесь загрузки сервера и повторно войдите в консоль.
10. Введите команду для проверки запуска процессов:
    `sudo /etc/init.d/iwtm status`
    На экране отобразится список процессов и их статус. Сервисы должны быть запущены, при этом строки должны заканчиваться фразой "**is running...**":
    
    ```
    iw_system_check (pid  1168) is running...
    iw_agent (pid  1199) is running...
    iw_indexer (pid  1231) is running...
    ```
11. Запустите все Серверы TM (TM Node) - описание смотрите ниже.

ШАГ 3. ПЕРЕЗАПУСК СЕРВЕРОВ TM (TM Node)

Чтобы перезапустить серверы TM (TM Node), на каждом из них выполните следующие действия:

1. На сервере TM (TM Node Server), на котором функционирует пакет `web-gui`, введите команду для очистки кеша:
   `redis-cli flushall`
2. Введите команду для перезагрузки сервера:
   `sudo reboot`
3. Дождитесь загрузки сервера и повторно войдите в консоль.
4. Введите команду для проверки запуска процессов:
   `sudo /etc/init.d/iwtm status`
   На экране отобразится список процессов и их статус. Обычно сервисы `iw_icap`, `iw_proxy_http`, `iw_proxy_icq`, `iw_proxy_smtp`, `iw_sniffer`,

`iw_capstack`, `iw_qmover_client`, `iw_qmover_server` и `iw_image2test_fre_batch` бывают остановлены, для этих сервисов строки должны заканчиваться фразой "**is stopped (disabled)**". А все остальные сервисы - запущены, для них строки заканчиваются фразой "**is running...**":

```
iw_bookworm (pid  5476) is running...
iw_x2db (pid  5510) is running...
iw_x2x (pid  5539) is running...
iw_deliver (pid  5573) is running...
iw_warpd (pid  5603) is running...
iw_licensed (pid  5634) is running...
iw_luaengined (pid  5666) is running...
iw_cas (pid  5700) is running...
iw_analysis (pid  5732) is running...
iw_tech_tools (pid  5768) is running...
iw_pas (pid  5798) is running...
iw_adlibitum (pid  5830) is running...
iw_blackboard (pid  5859) is running...
iw_expressd (pid  5892) is running...
iw_icap is stopped (disabled)
iw_image2text_fre_batch is stopped (disabled)
iw_messed (pid  5974) is running...
iw_proxy_http is stopped (disabled)
iw_proxy_icq is stopped (disabled)
iw_proxy_smtp is stopped (disabled)
iw_sample_compiler (pid  6079) is running...
iw_smtpd (pid  6113) is running...
iw_xapi_puppy (pid  6158) is running...
iw_xapi_xapi (pid  6194) is running...
iw_system_check (pid  6226) is running...
iw_sniffer is stopped (disabled)
iw_agent (pid  6281) is running...
iw_capstack is stopped (disabled)
iw_configerator (pid  6347) is running...
iw_kicker (pid  6384) is running...
iw_qmover_client is stopped (disabled)
iw_qmover_server is stopped (disabled)
iw_updater (pid  6528) is running...
```

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.

`iw_adlibitum`

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 6.10, данное обновление необходимо проводить последовательно - сначала обновляя до промежуточных версий. Например, обновить DM 6.7 следует сначала до 6.9, а уже затем до 6.10.
   > 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

Во время обновления сервера Traffic Monitor конфигурационные файлы (например, 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 **.rpmnew**. Это сделано для того, чтобы поддержать возможность изменения структуры файлов новых версий. Для корректной работы Системы потребуется объединить файлы старой и новой версий.

> **Важно!**
>
> На серверах Traffic Monitor, работающих под управлением **ОС Astra Linux**, будут создаваться файлы с расширением **.dpkg-dist**.

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:

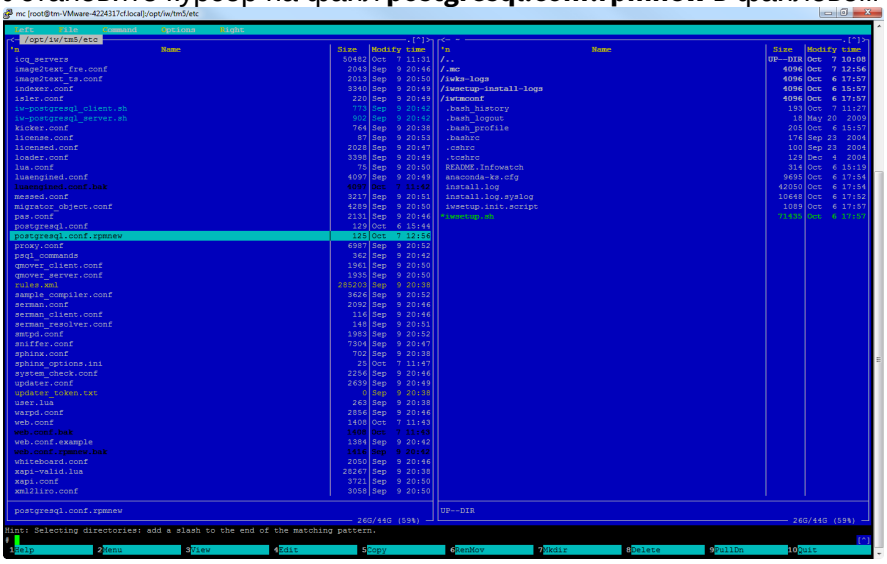
```
{
    "DB": "postgres",
    "Host": "localhost",
    "Password": "xxXX1234",
    "Port": 5433,
    "Username": "iwtm_linux"
}
```

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.



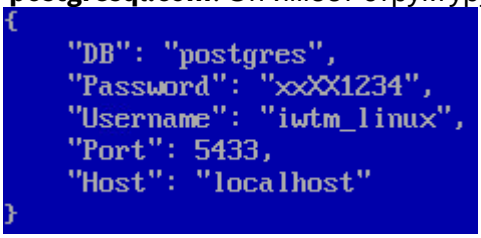
3. Нажмите **F4**.
4. Замените значения секций файла значениями соответствующих секций файла **postgresql.conf**. Получится так:

```
{
    "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

Для работы с vimdiff на сервере должен установлен текстовый редактор vim.

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

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

Важно!

Чтобы избежать потери данных и ошибок в работе Системы (конфигурационные файлы серверной части Traffic Monitor), необходимо внимательно следовать инструкциям.
В случае возникновения трудностей при объединении конфигурационных файлов рекомендуется обратиться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.
Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни РФ.
Вы также можете посетить раздел технической поддержки на нашем сайте: http://www.infowatch.ru/support.

Важно!

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

1. /etc/rc.d/init.d/postgresql-9.6.rpmnew
2. /etc/sgml/docbook/xmlcatalog.rpmnew

4.6 Обновление СУБД PostgreSQL

Обновление СУБД PostgreSQL с версии **9.4** до версии **9.6** будет вестись в консоли обновляемого сервера.
Процесс обновления может проходить в двух режимах:

- BACKUP - в этом режиме создается копия всей БД, включая все табличные пространства схемы БД iwtm.
  На диске, где размещаются табличные пространства схемы БД iwtm, должно быть столько же свободного пространства, сколько уже ими занято;
- LINK - в этом режиме файлы БД не копируются, а из новых папок создаются жесткие ссылки на файлы старой БД. После установки и запуска новой версии старая перестанет функционировать. Поэтому перед обновлением в режиме LINK необходимо сделать полный бэкап предыдущей базы со всеми табличными пространствами.
  В этом режиме на диске может потребоваться до 100 Мб свободного пространства.

Примечание:

Если вы используете удаленное подключение по протоколу SSH, рекомендуется использовать утилиту Screen. Это позволит избежать проблем в случае разрыва соединения с обновляемым сервером. При отключении от утилиты запущенные в ней процессы не прервутся, что позволит безопасно продолжить обновление Системы.
Важно! Использование Screen особенно рекомендуется при работе с БД и обновлении СУБД.

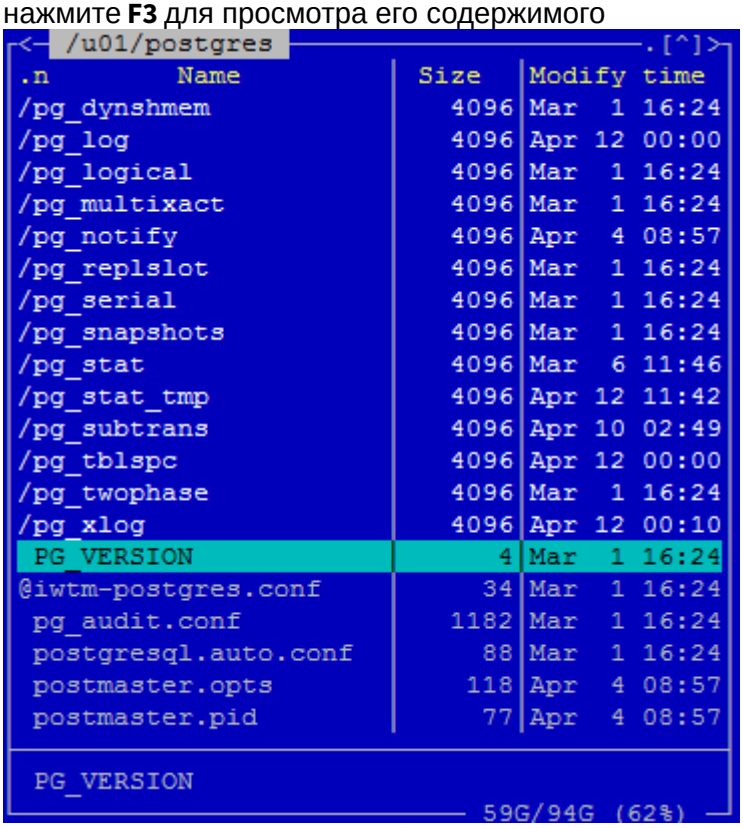
Основные команды:

- `screen` - запустить утилиту;
- `Ctrl+a d` - отключиться от screen (вводится в окне screen);
- `screen -ls` - вывести список запущенных screen;
- `screen -r` - повторно подключиться к screen;
- `screen -r name` - подключиться к определенному screen с именем «name»;
- `exit` - выйти из screen (вводится в окне screen).

4.6.1 Подготовка к обновлению

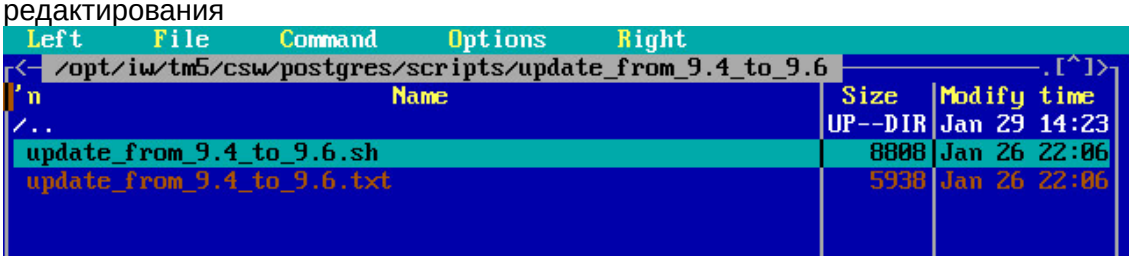
1. Перед обновлением СУБД обновите пакеты Traffic Monitor до актуальной версии, вместе с ними будут установлены пакеты с новой версией PostrgreSQL.
2. Для обновления СУБД PostgreSQL до версии **9.6** в Системе должна быть установлена версия **9.4**. Проверьте версию установленной СУБД. Для этого:
   a. Введите команду для открытия файлового менеджера:
      `mc`
   b. Перейдите в директорию `/u01/postgres`

c. Выделите файл **PG_VERSION**, в котором указана установленная версия СУБД, и нажмите **F3** для просмотра его содержимого



d. Нажмите **F3** для закрытия файла.
Если версия **9.6** уже установлена в Системе, **не запускайте** обновление СУБД и продолжайте следовать инструкции по обновлению Системы.

3. Выполните настройку скрипта обновления. Для этого:
   a. Перейдите в директорию `/opt/iw/tm5/csw/postgres/scripts/update_from_9.4_to_9.6`
   b. Выделите файл **update_from_9.4_to_9.6.sh** и нажмите **F4** для его редактирования



   c. В зависимости от выбранного режима обновления замените значение параметра `UPDATEMODE` на `BACKUP` или `LINK` (по умолчанию - `BACKUP`).
   d. Установите значение параметра `PARALLEL_DEGREE` равным количеству процессорных ядер сервера с БД (по умолчанию - `8`). Параметр влияет на скорость процесса обновления.
   e. Нажмите **F2**.
   f. В открывшемся окне подтвердите сохранение файла, нажав **Save**.
   g. Нажмите **F10**.
   h. Нажмите **F3** и убедитесь в корректности содержимого файла, затем снова нажмите **F3** для закрытия файла.

i. Введите команду для закрытия файлового менеджера:
```
exit
```

4. Перед обновлением СУБД должны быть остановлены все сервисы Traffic Monitor. Для этого введите команды:

> **Важно!**
>
> Права пользователя, созданного на этапе установки, ограничены в операционной системе, поэтому при выполнении части команд в командной строке потребуется использовать программу **sudo**. Например, для создания директории `disk1` в корневой директории необходимо ввести команду:
> `sudo mkdir /disk1`
> Чтобы работать с правами пользователя *root*, в командной строке введите `sudo su`.
> **Внимание!** К данному способу работы, ввиду возможности допустить серьезную ошибку, крайне не рекомендуется прибегать без помощи специалистов компании InfoWatch.
> На ОС Astra Linux служба nagios останавливается командой:
> `service nagios3 stop`

a. При установке Traffic Monitor Все-в-одном:
```
service iwtm stop
service iwtm-php-fpm stop
service nagios stop
```
b. При распределенной установке Traffic Monitor:
   i. На сервере Traffic Monitor:
   ```
   service iwtm stop
   service iwtm-php-fpm stop
   service nagios stop
   ```
   ii. На сервере БД:
   ```
   service iwtm stop
   ```

4.6.2 Обновление

1. Введите команду для перехода в нужную директорию:
```
cd /opt/iw/tm5/csw/postgres/scripts/update_from_9.4_to_9.6
```
2. Для запуска скрипта обновления выполните команду:
```
bash ./update_from_9.4_to_9.6.sh
```
Когда обновление установится, на экран будет выведено сообщение: `Update completed.`
3. После завершения процесса обновления подключитесь к базе данных и проверьте ее работоспособность:

1. Чтобы подключиться к серверу БД из консоли введите команды:
```
su - iwtm
psql postgres iwtm -p 5433
```

2. Далее введите команды:
   ```
   select version();
   select* from version;
   explain (analyze, buffers) select * from object_comment;
   ```
   Команды должны быть выполнены без ошибок.
3. Для выхода введите команду:
   ```
   \q
   ```
4. Введите команду:
   ```
   exit
   ```

> **Примечание:**
>
> Также эту проверку можно произвести с рабочих станций под управлением Windows. Для этого используйте программу pgAdmin.
> Проверка выполняется теми же командами (шаг b).

- Продолжайте следовать инструкции по обновлению Системы.

4.6.3 Удаление бэкапа старой БД

Если использовался режим обновления BACKUP, системой создан бэкап старой БД.

> **Примечание:**
>
> Перед удалением необходимо проверить работоспособность новой версии: убедиться в том, что события загружаются в БД, а также работает поиск по событиям.
> На это лучше выделить несколько дней.

Удаление будет вестись в консоли сервера БД. Чтобы удалить бэкап старой БД выполните команды:

1. Введите команду для перехода в нужную директорию:
   ```
   cd /var/log/infowatch/update/postgres96_update_дата
   ```
   где **дата** - дата обновления.

   В нашем примере:
   ```
   cd /var/log/infowatch/update/postgres96_update_2018-01-29_15:37:06
   ```
2. Для запуска скрипта удаления выполните команду:
   ```
   bash ./delete_old_cluster.sh
   ```
3. Процесс удаления не будет отображаться в консоли и будет успешно завершен, если не выведено сообщение об ошибке.

> **Важно!**
>
> После удаления бэкапа нельзя будет откатиться к старой версии.

4.6.4 Откат обновления

> **Примечание:**
>
> Откат СУБД используется только для повторного обновления, если в процессе возникла ошибка.

Откат обновления возможен, если:

- Обновление проводилось в режиме BACKUP.
- Перед обновлением в режиме LINK был создан бэкап вручную.

Откат обновления будет вестись в консоли сервера БД. Для отката обновления необходимо:

- Если обновление проводилось в режиме BACKUP:
  a. Введите команду для перехода в нужную директорию:
  `cd /opt/iw/tm5/csw/postgres/scripts/update_from_9.4_to_9.6`
  b. Для запуска скрипта отката обновления введите команду:
  `bash ./update_from_9.4_to_9.6.sh rollback`

- Если обновление проводилось в режиме LINK:
  a. Для остановки сервисов `postgresql` и `pgagent` старой и новой версий введите команды:
  ```
  service pgagent-9.4 stop
  service pgagent-9.6 stop
  service postgresql-9.4 stop
  service postgresql-9.6 stop
  ```
  b. Замените обновленные файлы и директории БД на созданные в результате резервного копирования.
  c. Для запуска сервисов `postgresql` и `pgagent` старой версии введите команды:
  ```
  service pgagent-9.4 start
  service postgresql-9.4 start
  ```

4.6.5 Действия при ошибках

Если возникает ошибка, соберите логи и отправьте их в службу технической поддержки.

Если ошибка возникла:

- В процессе обновления или при запуске сервисов после обновления:
  1. Логи из папки обновления.
  В нашем примере: `/var/log/infowatch/update/postgres96_update_2018-01-29_15:37:06`
  2. Все логи из папок `/u01/postgres*/pg_log`.

- В процессе отката обновления:
  1. Файл с именем rollback.log из папки логов обновления.
  В нашем примере: `/var/log/infowatch/update/postgres96_update_2018-01-29_15:37:06`

2. Все логи из папок `/u01/postgres*/pg_log`.

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) выполняются 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`
      Если вы работаете в Traffic Monitor 6.10.10, установленном на ОС Astra Linux 1.6, то: `systemctl stop iwtm`
   b. Закрыть все экземпляры консоли управления;
   c. Остановить сервис:
      `service iwtm-php-fpm stop`
      Если вы работаете в Traffic Monitor 6.10.10, установленном на ОС Astra Linux 1.6, то: `systemctl stop iwtm-php-fpm`
   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");
- запросы и отчеты (см. "*Infowatch Traffic Monitor. Руководство пользователя*", разделы "Запросы" и "Отчеты");
- плагины и токены (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Плагины").

Для восстановления плагина Device Monitor, предустановленных запросов и отчетов, а также для повторного распространения предустановленных политик после повторной установки БД 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`
   Если вы работаете в Traffic Monitor 6.10.10, установленном на ОС Astra Linux 1.6, то: `/etc/init.d/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 8 до 128 символов.
- Пароль пользователя может состоять из символов, соответствующих трем из следующих четырех категорий:

1. Прописные буквы латинского алфавита (A-Z)
2. Строчные буквы латинского алфавита (a-z)
3. Арабские цифры (0-9)
4. Символы: «#», «$», «!» или «%»

- Пароль не должен содержать имя пользователя или его часть.
- 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