

INFOWATCH

InfoWatch Traffic Monitor 7.0

Руководство по установке

15/09/2021

© 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

2.3 Требования к настройкам ОС и сети сервера 12

3 Установка Системы 14

3.1 Установка сервера Traffic Monitor и Базы данных 15

3.1.1 Установка ТМ в режиме "Все-в-одном" 16

3.1.2 Распределенная установка ТМ 23

3.1.2.1 Установка Базы данных 24

3.1.2.2 Установка Сервера Traffic Monitor 30

3.2 Установка подсистемы Краулер 35

3.3 Установка InfoWatch Device Monitor 41

3.3.1 Установка серверной части InfoWatch Device Monitor 42

3.3.1.1 Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server 42

3.3.1.2 Рекомендации по развертыванию базы данных под управлением СУБД Oracle 43

3.3.1.3 Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL 44

3.3.1.4 Рекомендации по установке Сервера InfoWatch Device Monitor 45

3.3.1.5 Порядок установки серверной части InfoWatch Device Monitor 46

3.3.2 Установка Агента InfoWatch Device Monitor 56

3.3.2.1 Локальная установка Агента 58

3.3.2.2 Установка Агента с помощью средств распространения программного обеспечения 60

3.3.3 Схема развертывания InfoWatch Device Monitor 64

3.4 Предустановленные серверные параметры 67

4 Обновление Traffic Monitor на ОС Astra Linux 69

4.1 Обновление ТМ Все-в-одном (All-in-one) 72

4.2 Обновление ТМ при распределенной установке 79

5 Удаление Системы 88

5.1 Удаление схемы базы данных 88

5.2 Удаление подсистемы Краулер 89
5.3 Удаление InfoWatch Device Monitor 90
5.3.1 Удаление Агента, установленного с помощью средств распространения программного обеспечения 91
5.4 Удаление Traffic Monitor 92
6 Приложение А. Рекомендации по составлению имен и паролей 95
7 Приложение В. Лицензии на стороннее программное обеспечение ... 97

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/services/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
- требованиях к настройкам ОС и сети сервера.

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 рабочие станции 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 отдельно стоящего сервера TM Enterprise.*
- **Сервер Traffic Monitor** – отдельно стоящий 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 или Mozilla Firefox 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 или Краулера может потребоваться использовать отдельные сервера для процессов **iw_xapi_xapi**.

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

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Сервер TM 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" 1.6 с установленным обновлением безопасности Update 5 (20200327SE16) Требуется 2 диска: • Astra-Linux-Smolensk • Astra-Linux-Smolensk-Devel	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков. Проверка цифровой подписи должна быть отключена.
Сервер TM Enterprise, от 10 до 50 GB трафика в день				
RAID-массив с fault tolerance	2SRVx2 CPU 10xC	32-48 GB на каждый из серверов	ОС Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 5 (20200327SE16) Требуется 2 диска: • Astra-Linux-Smolensk • Astra-Linux-Smolensk-Devel	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков. Проверка цифровой подписи должна быть отключена.
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" 1.6 с установленным обновлением безопасности Update 5 (20200327SE16) Требуется 2 диска: • Astra-Linux-Smolensk • Astra-Linux-Smolensk-Devel	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков. Проверка цифровой подписи должна быть отключена.
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 Для хранения логов действий (xlog) необходимо выделить директории u01 дополнительное пространство, равное объему оперативной памяти сервера БД. Если оперативной памяти меньше 20 GB, выделите под логи 20 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" 1.6 с установленным обновлением безопасности Update 5 (20200327SE16) Требуется 2 диска: • Astra-Linux-Smolensk • Astra-Linux-Smolensk-Devel	
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 7 Service Pack 1; • Microsoft Windows 8; • Microsoft Windows Server 2008 R2 Service Pack 1; • Microsoft Windows Server 2012 R2 ; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019. Платформа: • Microsoft .Net Framework 4.5.1.	• На сервере TM должен быть включен автозапуск процесса **iw_xapi_xapi** • И сервер, и сканер Crawler должны быть установлены на компьютеры, находящиеся в одном домене: в том, к которому принадлежат компьютеры, которые предполагается сканировать. • Рекомендуется выбирать расположение компьютера, на котором будет работать сканер Crawler, так, чтобы он находился в сегменте сети, максимально близком к тем сегментам, которые будут подлежать сканированию. Удаленность может существенно увеличить нагрузку на сеть. • Если сегменты сети, где развернута система InfoWatch Traffic Monitor с Crawler, разделены между собой межсетевыми экранами, для корректной работы Crawler должны быть открыты порты 1337 (подключение Traffic Monitor к серверу Crawler) и 6556 (подключение сканера Crawler к серверу Crawler).
Сервер Device Monitor				

Не менее 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; • Microsoft Windows Server 2019. Платформа: • Microsoft .Net Framework 4.5.1. СУБД: • Oracle Database 12; • Microsoft SQL Server 2005, 2008, 2012, 2014, 2016 (Standard, Enterprise); • PostgreSQL версии 9. Ограничение: Microsoft Windows Server 2019 не поддерживает установку PostgreSQL версии 9.	• На сервере TM должен быть включен автозапуск процесса **iw_xapi_xapi** • Наличие локального DNS для перевода доменных имен в адреса • Должен поддерживаться протокол TLS 1.2
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: • Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 5 (20200327SE16) • [1]Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 и 8.1; • Microsoft Windows 10; • [1]Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019.	• Наличие локального DNS для перевода доменных имен в адреса • Должен поддерживаться протокол TLS 1.2 На Astra Linux Special Edition "Смоленск": • поддерживается работа только с отключенной проверкой цифровой подписи; • .поддерживается работа только с обычным ядром Linux (PaX-ядро не поддерживается)
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 Server 2016; • Microsoft Windows Server 2019; • Microsoft Windows 7 Service Pack 1 • Microsoft Windows 8 и 8.1; • Microsoft Windows 10.	

Примечание:

[1] - для указанных ОС требуется установка следующих исправлений от компании Microsoft: KB4474419, KB4490628. Проверка на наличие данных исправлений на компьютере проводится Системой перед установкой и/или обновлением продукта.

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.

2.3 Требования к настройкам ОС и сети сервера

Для успешной установки Системы сервер должен отвечать следующим требованиям:

- На сервере должна быть установлена ОС Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 5 (20200327SE16);
- Должны быть настроены репозитории ОС с возможностью установить пакеты `lsb-release` и `lshw`.
- Минимальный объем Swap-пространства - 500MB (рекомендации приведены в статье "Рекомендации по разбиению дискового пространства серверов при установке в разных режимах").
  Просмотреть информацию о Swap-пространстве можно с помощью команды:

`swapon -s`

- Опции точки монтирования не должны содержать `nosuid` и `noxattr` (можно проверить, открыв содержимое файла `/etc/fstab`);
- На сервере должны быть выполнены корректные сетевые настройки (в случае проблем с сетевыми параметрами обратитесь к системному администратору):
    - Внешний DNS-сервер должен преобразовывать ваше имя хоста (hostname) в тот же IP-адрес, который задан на одном из сетевых интерфейсов сервера;
    - IP-адрес должен принадлежать диапазонам частных IP-адресов:
      10.0.0.0 — 10.255.255.255 (RFC1918);
      172.16.0.0 — 172.31.255.255 (RFC1918);
      192.168.0.0 — 192.168.255.255 (RFC1918).
    - Должна выполняться команда:
      `ping -c 1 <hostname>`
      где `<hostname>` - ваше имя хоста.
      В результате выполнения команды должен быть успешно принят пакет.
    - Длина имени хоста (hostname) не должна превышать 15 символов;
- У пользователя должен быть необходимый для установки мандатный уровень доступа (63). Проверить мандатный уровень доступа пользователя можно командой `pdp-id -i`

3 Установка Системы

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 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 и настройка СУБД PostgreSQL • Установка схемы базы данных IW Traffic Monitor
Установка сервера Traffic Monitor на отдельный компьютер	**TM node**	• 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)

> **Примечание:**
>
> В процессе установки IW Traffic Monitor будут выполнены действия, требующие прав sysdba:
>
> - Создание оберточных функций для чтения файлов, остановки и обрывания сессий, создания табличных пространств и выдача iwtm прав на них;
> - Удаление всех представлений (view) и функций из схемы iwtm для создания в новой версии нужных с помощью обновления;
> - Выдача пользователю iwtm:
>   - Прав на создание объектов в БД;
>   - Прав для установки, обновления и удаления схемы БД;
>   - Прав для создания, удаления, архивации и восстановления табличных пространств;
>   - Прав на функции обнуления статистики сервера postgres, которые используются в скрипте диагностики pgstat;
>   - Прав на статистические представления (view) и таблицы, для сбора статистики работы БД;
>   - Прав, используемых в коде продукта InfoWatch Traffic Monitor;
>   - Прав для просмотра статистики БД;
>   - Прав на схему pgagent для создания и управления заданиями (job).

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

Перед установкой ознакомьтесь с рекомендациями в статье "Рекомендации по разбиению дискового пространства серверов при установке в разных режимах").

Важно!

Для установки InfoWatch Traffic Monitor 7.0 на сервере должно быть установлено обновление безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16).

Для установки потребуются 4 диска:

- Astra-Linux-Smolensk;
- Astra-Linux-Smolensk-Devel;
- обновление установочного диска;
- обновление диска со средствами разработки.

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_icap_buf
- 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!

Перед началом установки убедитесь, что сервер соответствует требованиям к настройкам ОС и сети сервера.Для установки InfoWatch Traffic Monitor 7.0 на сервере должно быть установлено обновление безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16).

Чтобы узнать версию установленного обновления, выполнить команду:

```
cat /etc/astra_update_version
```

Для установки потребуются 4 диска:

- Astra-Linux-Smolensk;
- Astra-Linux-Smolensk-Devel;
- обновление установочного диска;
- обновление диска со средствами разработки.

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 в окне **Выбора программного обеспечения** установите флажок **Средства удаленного доступа SSH**.
   - 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. 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
   ```
6. 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.

7. Вставьте в CD-привод диск Astra-Linux-Smolensk.
8. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk1`.
9. Вставьте в CD-привод диск Astra-Linux-Smolensk-Devel.
10. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk2`.
11. Откройте на редактирование файл **sources.list**, расположенный в директории `/etc/apt`
12. 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
    ```
13. Сохраните файл **sources.list**.
14. Установите обновления безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16) (см. официальную инструкцию).

> **Важно!**
>
> При установке обновления безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16) **обязательно** используйте и диск с обновлениями и диск со средствами разработки.
> Ссылки для скачивания доступны на странице с официальной инструкцией.
> Не удаляйте репозитории, подключенные в процессе установки Astra Linux Special Edition 1.6 Update 5.
> В итоге должны быть доступны репозитории с **4-х** дисков.

15. Выполните перезагрузку сервера командой:
    `sudo reboot`
16. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.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`.

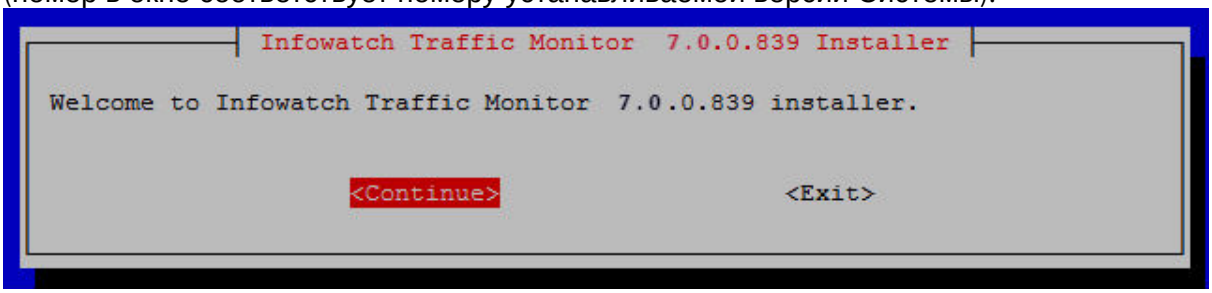
    > **Важно!**
    >
    > Перед началом установки убедитесь, что сервер соответствует требованиям к настройкам ОС и сети сервера.

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-1.6.run`
    где `<директория_с_файлом>` - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run**.

    В нашем примере команда будет следующей:
    `sudo bash /distr/iwtm-installer-7.0.0.839-astra-smolensk-1.6.run`
    Начнется распаковка файлов, необходимых для установки Traffic Monitor.

    ```
    Verifying archive integrity...  100%   All good.
    Uncompressing Infowatch Traffic Monitor Installer  7.0.0.839  100%
    ```

    Перед запуском установщик выполнит проверку Системы и, если будет обнаружено несоответствие требованиям, прервет установку, выведя сообщение об ошибке.
    В этом случае необходимо исправить указанное установщиком несоответствие и повторно запустить установку.
    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/oradata** для СУБД Oracle и **/u02/pgdata** для СУБД PostgreSQL).
d. Нажмите **Enter**.
e. Выберите **Daily tablespace path count** и укажите количество путей для файлов ежедневных табличных пространств (число от 1 до 10, по умолчанию указано 1).
f. Нажмите **Enter**.
g. Выберите **Daily tablespace paths** и укажите путь к диску хранения данных ежедневного табличного пространства (по умолчанию указан путь **/u02/oradata** для СУБД Oracle и **/u02/pgdata** 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.

26. 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".

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 ТМ

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.
>
> Для установки потребуются 4 диска:
>
> - Astra-Linux-Smolensk;
> - Astra-Linux-Smolensk-Devel;
> - обновление установочного диска;
> - обновление диска со средствами разработки.

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".

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!

Перед началом установки убедитесь, что сервер соответствует требованиям к настройкам ОС и сети сервера.Для установки InfoWatch Traffic Monitor 7.0 на сервере должно быть установлено обновление безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16).

Чтобы узнать версию установленного обновления, выполнить команду:

```
cat /etc/astra_update_version
```

Для установки потребуются 4 диска:

- Astra-Linux-Smolensk;
- Astra-Linux-Smolensk-Devel;
- обновление установочного диска;
- обновление диска со средствами разработки.

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 в окне **Выбора программного обеспечения** установите флажок **Средства удаленного доступа SSH**.
   - 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. 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
```
6. 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.

7. Вставьте в CD-привод диск Astra-Linux-Smolensk.
8. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk1`.
9. Вставьте в CD-привод диск Astra-Linux-Smolensk-Devel.
10. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk2`.
11. Откройте на редактирование файл **sources.list**, расположенный в директории `/etc/apt`
12. 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
```

13. Сохраните файл **sources.list**.
14. Установите обновления безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16) (см. официальную инструкцию).

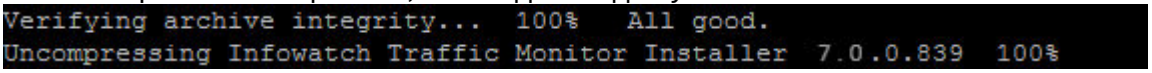
> **Важно!**
>
> При установке обновления безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16) **обязательно** используйте и диск с обновлениями и диск со средствами разработки.
> Ссылки для скачивания доступны на странице с официальной инструкцией.
> Не удаляйте репозитории, подключенные в процессе установки Astra Linux Special Edition 1.6 Update 5.
> В итоге должны быть доступны репозитории с **4-х** дисков.

15. Выполните перезагрузку сервера командой:
    ```
    sudo reboot
    ```
16. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.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`.

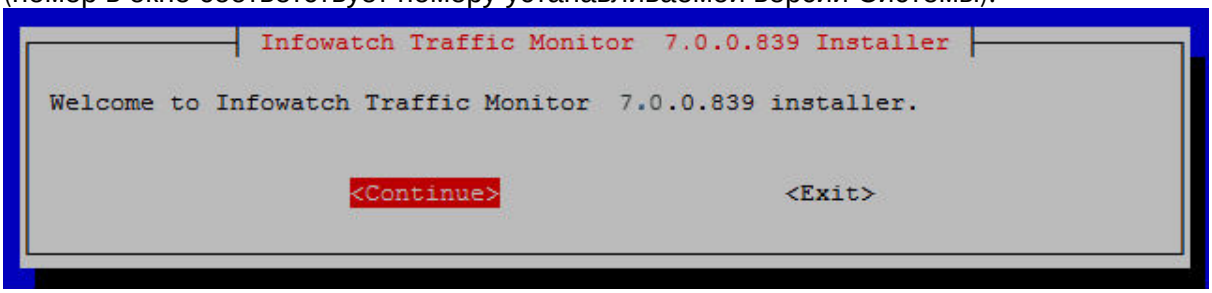
> **Важно!**
>
> Перед началом установки убедитесь, что сервер соответствует требованиям к настройкам ОС и сети сервера.

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-1.6.run
    ```
    где <директория_с_файлом> - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run**.

    В нашем примере команда будет следующей:
    ```
    sudo bash /distr/iwtm-installer-7.0.0.839-astra-smolensk-1.6.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:

    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.

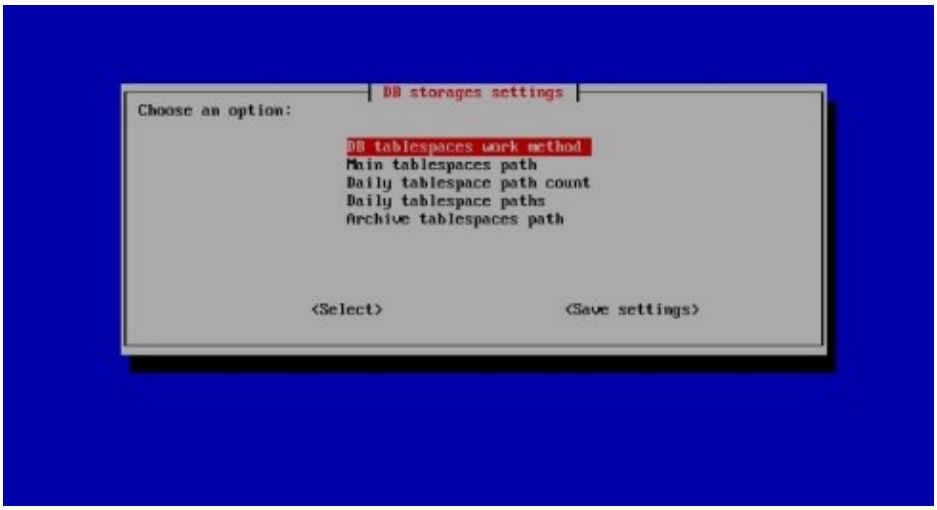
    Укажите язык интерфейса:
    i. Выберите **Interface**, нажмите **Enter**.
    ii. Выберите требуемый язык.
    На выбранном языке будет установлена консоль управления.
    iii. Нажмите **OK**.

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

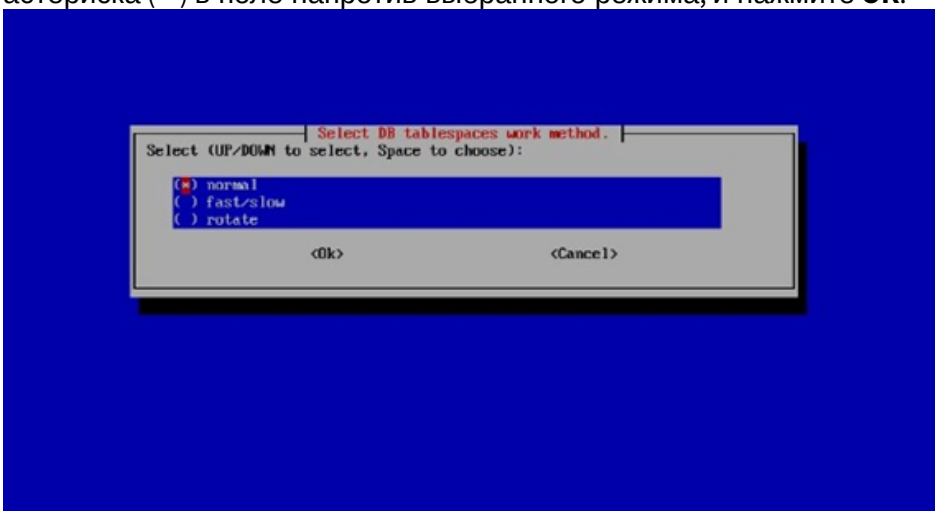
iii. Нажмите **OK**.

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/oradata** для СУБД Oracle и **/u02/pgdata** для СУБД PostgreSQL).
d. Нажмите **Enter**.
e. Выберите **Daily tablespace path count** и укажите количество путей для файлов ежедневных табличных пространств (число от 1 до 10, по умолчанию указано 1).
f. Нажмите **Enter**.
g. Выберите **Daily tablespace paths** и укажите путь к диску хранения данных ежедневного табличного пространства (по умолчанию указан путь **/u02/oradata** для СУБД Oracle и **/u02/pgdata** 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):

Выберите **Events cleaning** и нажмите **Enter**:

Установите курсор в нужное поле и нажмите пробел до появления в поле значка астериска (*):

1. **Violation** – включить автоматическое удаление событий, которые являются нарушением (подробнее о нарушениях см. «*InfoWatch Traffic Monitor. Руководство пользователя*»);
2. **Non-violation** – включить автоматическое удаление событий, которые не являются нарушением;

3. **Screenshots** – включить автоматическое удаление снимков экрана, полученных от Агентов Device Monitor.
   При необходимости вы можете выбрать несколько пунктов.

ii. Нажмите **Ok**.

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**.

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**.

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.

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

Установка Сервера Traffic Monitor

Важно!

Каждый сервер должен иметь уникальный корректный FQDN.
Перед началом установки убедитесь, что сервер соответствует требованиям к настройкам ОС и сети сервера.

Для установки InfoWatch Traffic Monitor 7.0 на сервере должно быть установлено обновление безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16).

Чтобы узнать версию установленного обновления, выполнить команду:

```
cat /etc/astra_update_version
```

Для установки потребуются 4 диска:

- Astra-Linux-Smolensk;

- Astra-Linux-Smolensk-Devel;
- обновление установочного диска;
- обновление диска со средствами разработки.

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 в окне **Выбора программного обеспечения** установите флажок **Средства удаленного доступа SSH**.
   - 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. 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
   ```
6. 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.

7. Вставьте в CD-привод диск Astra-Linux-Smolensk.
8. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk1`.
9. Вставьте в CD-привод диск Astra-Linux-Smolensk-Devel.
10. Скопируйте все содержимое диска в произвольную директорию на жестком диске . **Например**, в директорию `/disk2`.
11. Откройте на редактирование файл **sources.list**, расположенный в директории `/etc/apt`
12. 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
    ```
13. Сохраните файл **sources.list**.
14. Установите обновления безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16) (см. официальную инструкцию).

Важно!

При установке обновления безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16) **обязательно** используйте и диск с обновлениями и диск со средствами разработки.
Ссылки для скачивания доступны на странице с официальной инструкцией.
Не удаляйте репозитории, подключенные в процессе установки Astra Linux Special Edition 1.6 Update 5.
В итоге должны быть доступны репозитории с **4-х** дисков.

15. Выполните перезагрузку сервера командой:
    `sudo reboot`
16. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run** (где x.x.x.xxx - номер сборки), поставляемый на дистрибутивном диске InfoWatch Traffic Monitor, в любую директорию на жестком диске сервера.
17. **Например**, в директорию `/distr`.

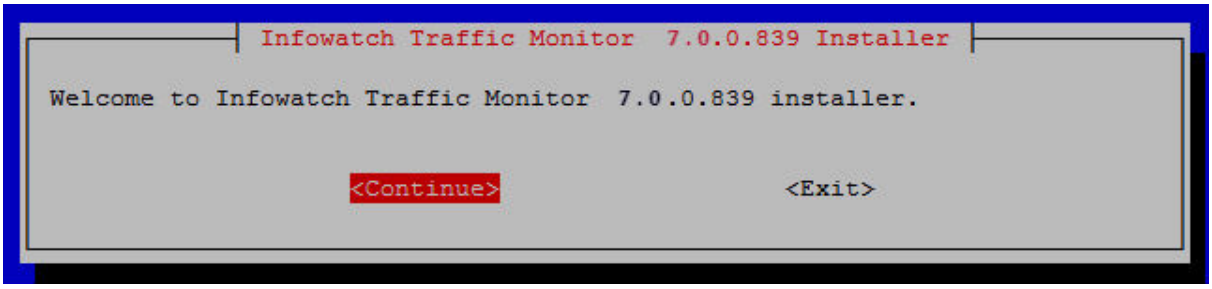
Важно!

Перед началом установки убедитесь, что сервер соответствует требованиям к настройкам ОС и сети сервера.

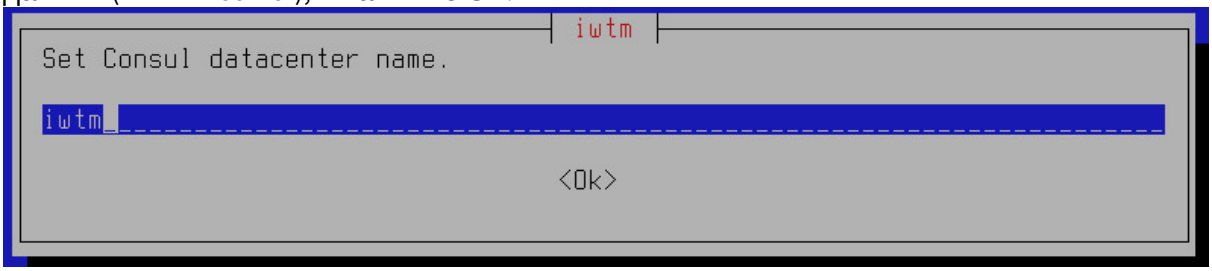
18. Выполните следующую команду:
    `sudo apt-get update`
19. Выполните следующую команду:
    `sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run`
    где `<директория_с_файлом>` - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run**.
    В нашем примере команда будет следующей:
    `sudo bash /distr/iwtm-installer-7.0.0.839-astra-smolensk-1.6.run`
    Начнется распаковка файлов, необходимых для установки Traffic Monitor.

```
Verifying archive integrity...  100%   All good.
Uncompressing Infowatch Traffic Monitor Installer  7.0.0.839  100%
```

Перед запуском установщик выполнит проверку Системы и, если будет обнаружено несоответствие требованиям, прервет установку, выведя сообщение об ошибке.
В этом случае необходимо исправить указанное установщиком несоответствие и повторно запустить установку.
По завершении на экране отобразится окно с приглашением установить Traffic Monitor (номер в окне соответствует номеру устанавливаемой версии Системы):



20. Для продолжения нажмите **Continue**.
21. В окне **IWTM Server Role** выберите **TM node**, нажмите **Ok**.
22. Введите название дата-центра Consul, который был указан при установке сервера Базы данных (TME DB server), и нажмите **OK**.



23. 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").

24. 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)? _
```
25. 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.
26. 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".

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.

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.

> **Важно!**
>
> Перед началом процесса установки подсистемы необходимо убедиться, что связь между серверами Traffic Monitor и Краулер установлена. Для этого на сервере Traffic Monitor проверьте доступность сервера Краулер по короткому

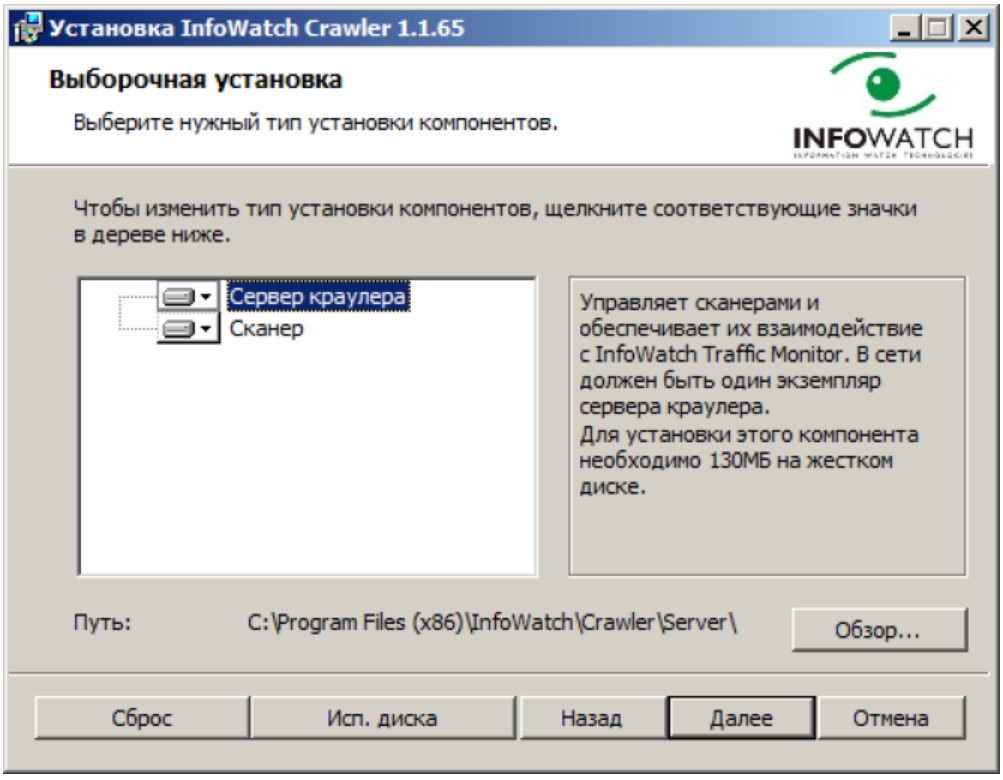
имени, выполнив команду: ping <короткое имя сервера Краулер>. Иначе, Краулер может быть установлен, но не появится в Консоли управления Traffic Monitor.

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**).

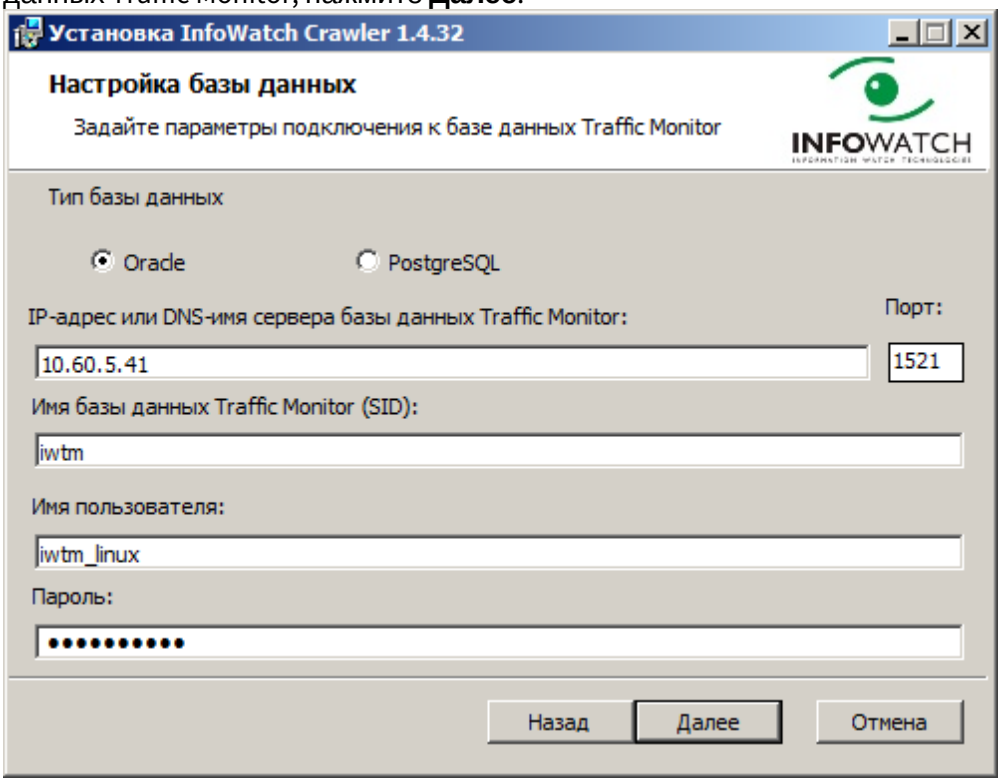
2. В окне приветствия мастера установки InfoWatch Crawler нажмите **Далее**.
3. В окне выбора области установки нажмите **Далее**.
4. На шаге **Выборочная установка** определите, какие компоненты Crawler нужно установить и укажите директорию, в которую будет установлен компонент:
   - **Сервер краулера**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

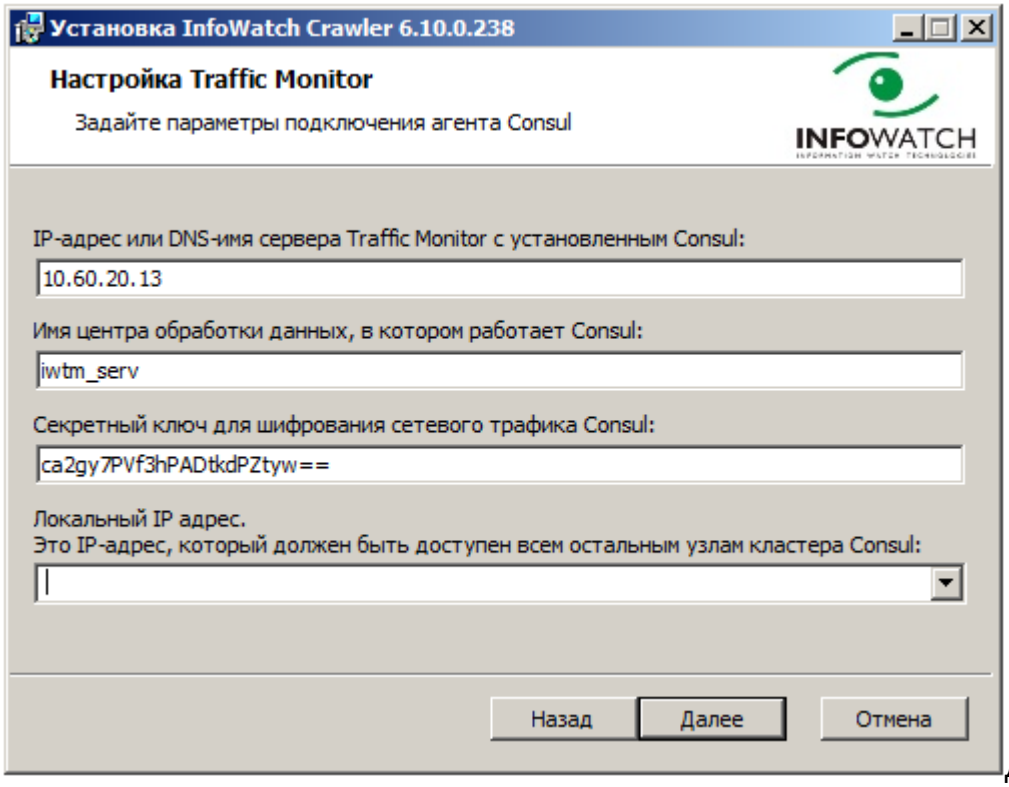
5. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сервер краулера**:
   a. Укажите параметры соединения службы `InfoWatch.Crawler.Server` с базой данных Traffic Monitor, нажмите **Далее**.



Параметры подключения для СУБД PostgreSQL:

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

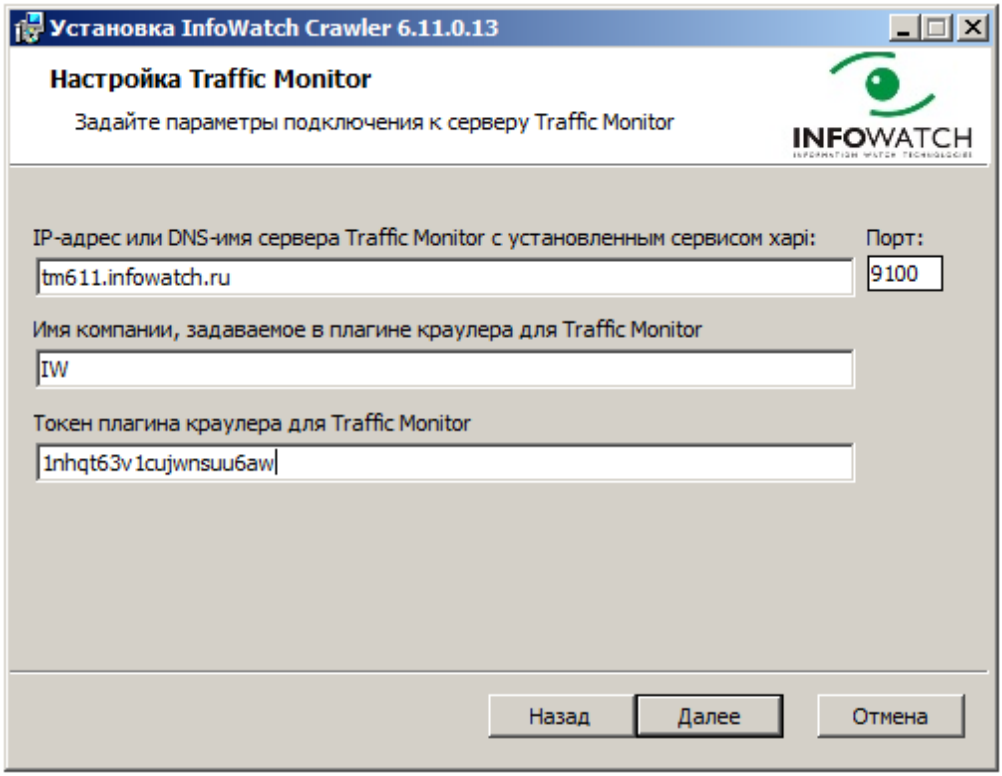
   b. Укажите параметры подключения агента Consul к серверу Traffic Monitor, нажмите **Далее**.



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**.



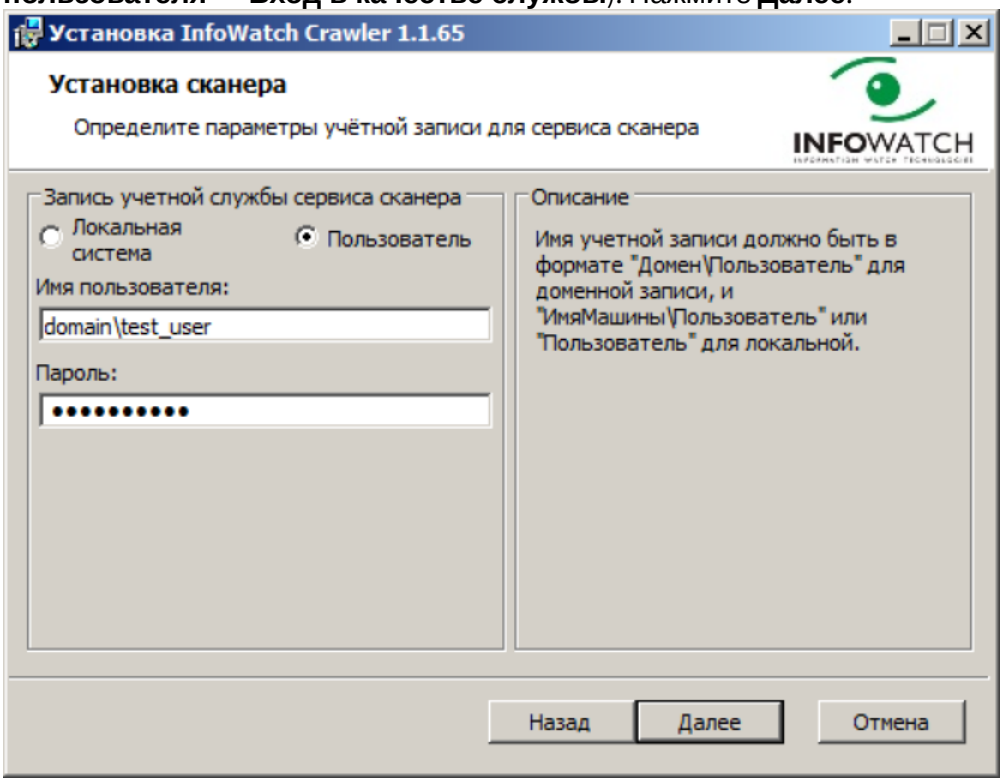
В случае распределенной установки в поле **IP-адрес или DNS-имя сервера Traffic Monitor с установленным сервисом xapi** укажите IP-адрес или DNS-имя сервера TM (TME Node Server).

d. Заполните поля следующим образом:

- **Имя компании, задаваемое в плагине краулера для Traffic Monitor** - всегда "IW",
- **Токен плагина краулера для Traffic Monitor** - используйте данные из Консоли управления Traffic Monitor (раздел **Плагины**).

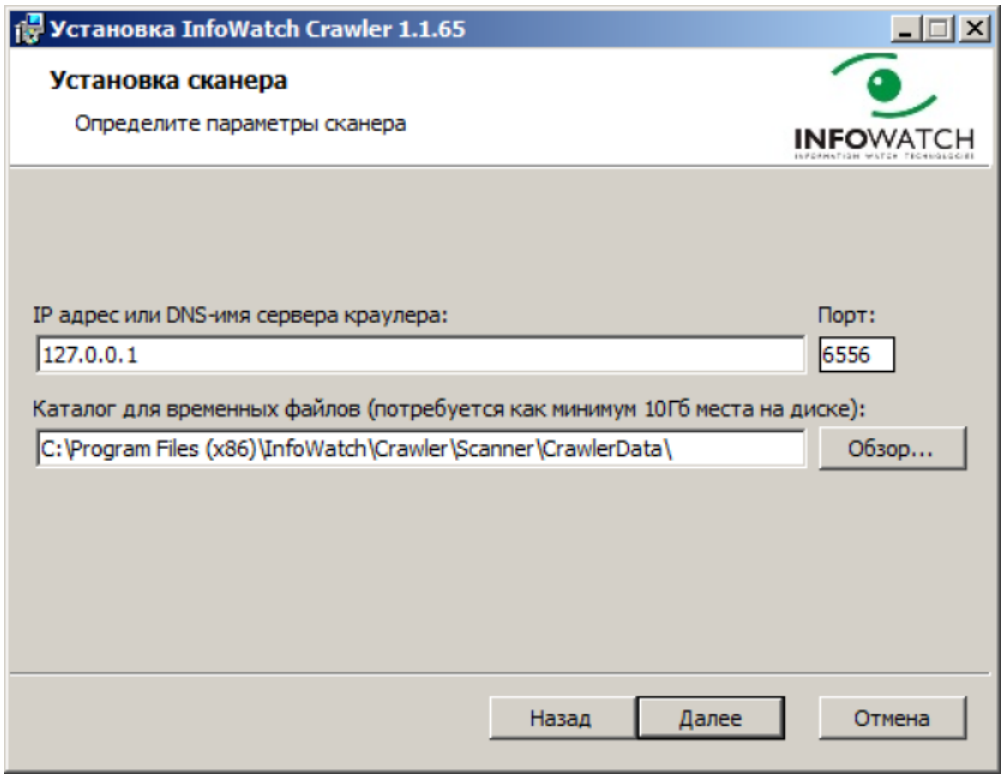
6. Если на шаге **Выборочная установка** вы выбрали установку компонента **Сканер**:
   a. укажите, от имени какой учетной записи будет запускаться служба InfoWatch.Crawler.Scaner. Вы можете выбрать стандартную учетную запись Local System (рекомендуется) или ввести параметры учетной записи, имеющей право 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: `iwtm restart kicker`.

> **Важно!**
>
> По окончании процесса установки необходимо убедиться, что связь между Консолью управления Traffic Monitor и сервером Краулер установлена. Для этого зайдите в Консоль управления, откройте раздел **Краулер** и убедитесь, что в нем отображаются настройки Краулера.

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").

> **Важно!**
>
> Для корректной работы версии Traffic Monitor и Device Monitor должны совпадать. Подробнее о совместимости Device Monitor см. в статье Базы знаний InfoWatch "Особенности совместимости разных версий TM, DM и Агентов".

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 7).

Рекомендации по развертыванию базы данных под управлением СУБД Oracle

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

- пакет Microsoft .NET Framework 4.5
- клиент СУБД Oracle (только после установки пакета 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 указать параметры подключения. Выберите один из двух вариантов, представленных ниже.

Вариант 1. Настроить файл tnsnames.ora ([ORACLE_HOME]\network\admin)

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.

Вариант 2. Указать в качестве сервера БД строковое представление TNS из файла tnsnames.ora.

Пример строкового представления

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=iwdm.infowatch.ru)(PORT=1521))
(CONNECT_DATA=(SERVER=dedicated)(SERVICE_NAME=iwtm)))
```

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".

После установки PostgreSQL откройте конфигурационный файл `postgresql.conf` и присвойте параметру `"max_connections"` значение 250.

> **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.

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

   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**. В этом случае все существующие настройки и элементы конфигурации будут заменены на импортированные.

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

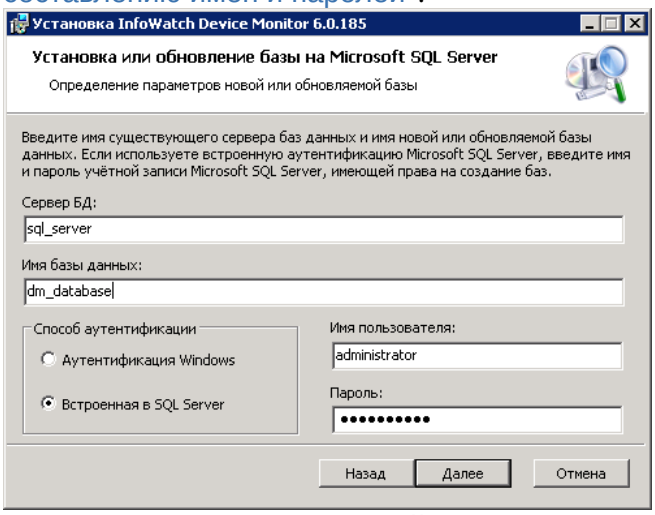
   Если на Шаге 4 вы решили использовать уже существующую базу данных (опция **Установить новую базу данных** не была выбрана), то вам будет необходимо дополнительно указать параметры соединения с существующей базой данных Device Monitor.
   Нажмите **Далее**.
7. **Настройка базы данных**
   Этот шаг будет пропущен, если на Шаге 4 вы решили использовать уже существующую базу данных.
   Принцип настройки базы данных зависит от типа используемой СУБД.
   При использовании СУБД Microsoft SQL Server укажите следующие параметры:
   - **Сервер БД**. NetBIOS имя сервера СУБД Microsoft SQL Server, на котором будет создана база данных.

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

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

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

ознакомьтесь с рекомендациями в статье "Приложение А. Рекомендации по составлению имен и паролей".



Настройка базы данных Microsoft SQL Server

При использовании СУБД Oracle настройте следующие параметры:

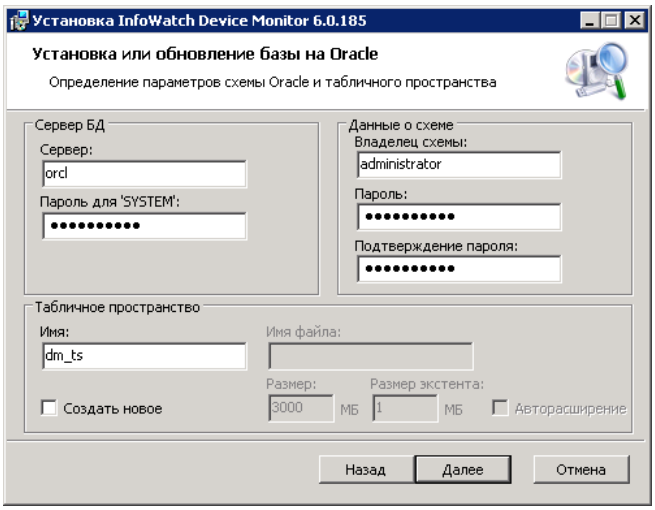
a. В области **Сервер БД** задайте параметры соединения с сервером базы данных:
   - **Сервер**. Имя сервера базы данных. В качестве значения данного параметра укажите псевдоним сервера `tns_name` из файла **tnsnames.ora** или строковое представление TNS.
   - **Пароль для 'SYSTEM'**. Пароль учетной 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.

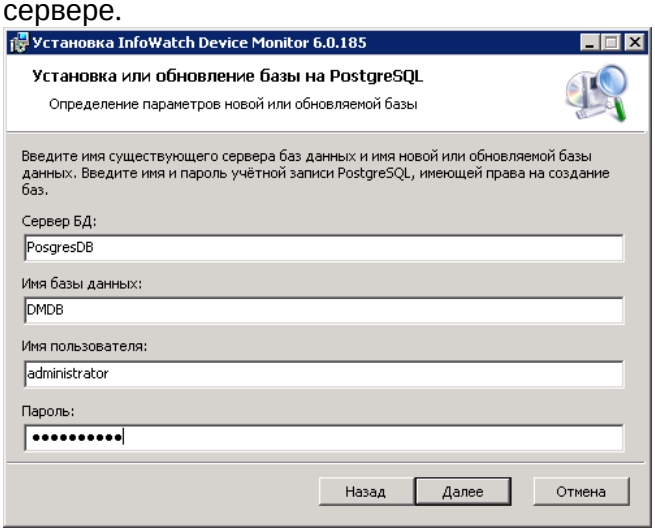
   - **Владелец схемы**. Имя учетной записи владельца схемы базы данных.
   - **Пароль, Подтверждение пароля**. Пароль учетной записи владельца схемы базы данных.

   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**.

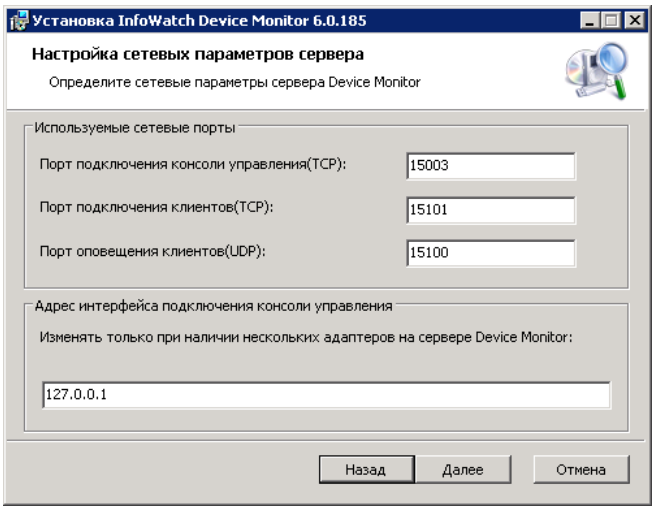
8. **Настройка сетевых параметров сервера**

   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. 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**

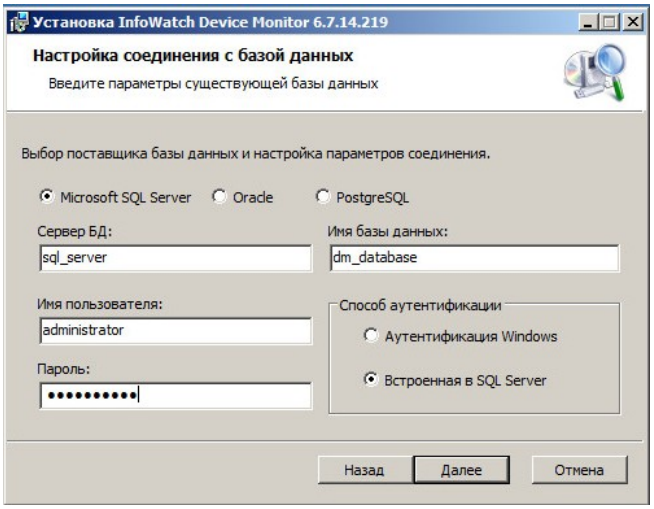
Работа вспомогательного сервера связана с основным, и настройки основного распространяются на вспомогательный сервер, что гарантирует принцип соединения серверов Device Monitor.

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

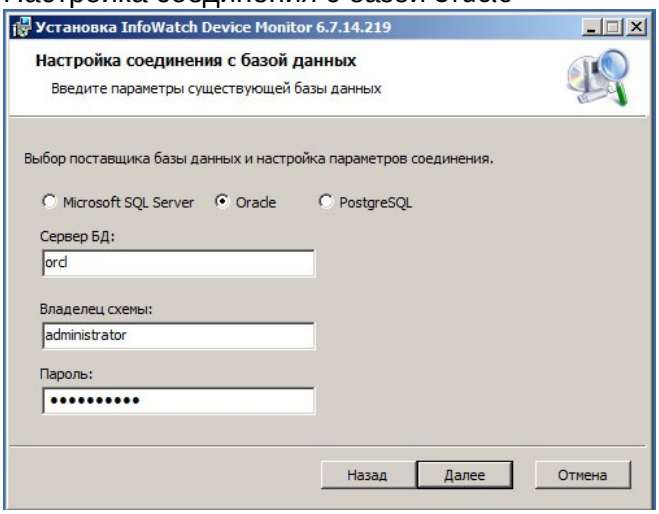
   Если необходимо, измените состав устанавливаемых компонентов. Так, например, если вы рассчитываете использовать Консоль управления на другой рабочей станции, то вам не нужно устанавливать этот компонент: нажмите **Консоль управления** и в раскрывшемся списке выберите пункт **Этот компонент будет полностью 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.

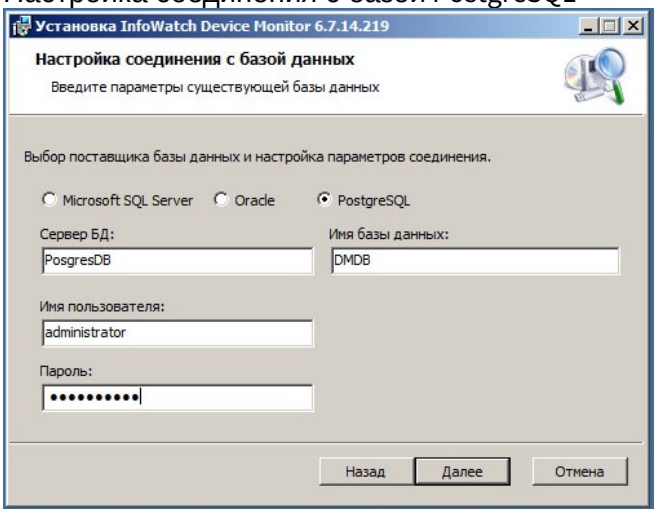
e. Настройка соединения с базой данных
   Укажите СУБД, под управлением которой находится база данных Device Monitor и введите оставшиеся параметры соединения такими же, которые были использованы при установке основного сервера:
   Настройка соединения с базой Microsoft SQL Server
   Если учетной записи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

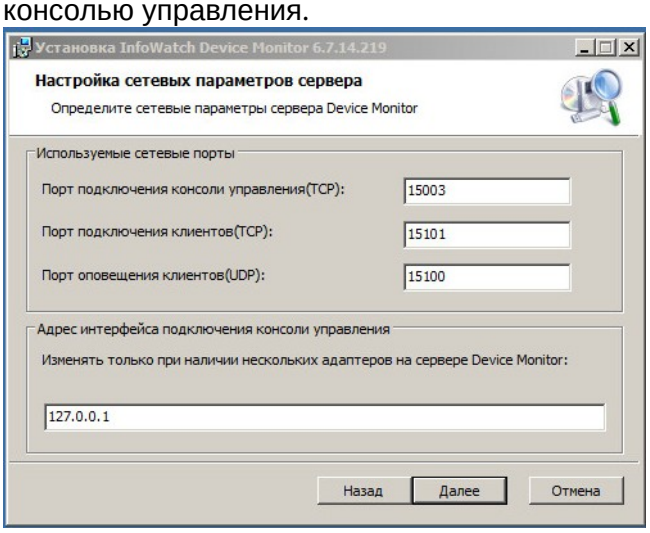
f. Настройка сетевых параметров сервера

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. 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.

Если на компьютере установлен Агент InfoWatch Device Monitor версии ниже 7.0, для установки Агента новой версии **обязательно** выполните следующие действия:

1. Удалите Агент InfoWatch Device Monitor;

2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 5 (20200327SE16) (см. официальную инструкцию);
3. Установите Агент InfoWatch Device Monitor 7.0.

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").

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. Если на рабочих станциях используется VMWare Horizon VDI 8.0.0-16530, то необходимо отключить компонент ftapihook654.dll версии 3.2.4.1. (подробнее см. "Проблема совместимости с VmWare Horizon VDI")
6. 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");
7. Для установления соединения убедитесь, что доменные имена сервера InfoWatch Device Monitor и машины, на которую устанавливается Агент InfoWatch Device Monitor, корректно преобразовываются (резолвятся) DNS-сервером в IP-адреса;

> **Примечание:**
>
> Для проверки выполните команду в консоли:
> `nslookup <имя_хоста>`
> Пример:
> `nslookup dmserv`
> В случае проблем с сетевыми параметрами обратитесь к системному администратору.

8. Если не требуется использовать компонент контроля сетевых соединений, отключите его при создании дистрибутива Агента InfoWatch Device Monitor;
9. Установите Агенты InfoWatch Device Monitor сначала на тестовые машины или 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:

Перед установкой Агента на рабочей станции с ОС Windows 7 Service Pack 1 или Windows Server 2008 R2 следует установить пакеты исправлений Windows для указанных ОС (подробнее см. в статье Аппаратные и программные требования).

Примечание:

При установке Агента на ОС Windows 7 и Windows 2008 R2 Server следует учесть, что:

Если Агент устанавливается впервые, компонент Контроль сетевых соединений не будет установлен. При необходимости, данный компонент возможно установить вручную, используя командную строку.

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.

Если на компьютере установлен Агент InfoWatch Device Monitor версии ниже 7.0, для установки Агента новой версии **обязательно** выполните следующие действия:

1. Удалите Агент InfoWatch Device Monitor;
2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 5 (20200327SE16) (см. официальную инструкцию);
3. Установите Агент InfoWatch Device Monitor 7.0.

Создайте актуальный пакет для установки Агента (см. документ "Traffic Monitor. Руководство пользователя. Создания пакета установки") и запишите его на внешний носитель. Установку Агента может выполнять пользователь, имеющий права локального администратора на том компьютере, на который выполняется установка.

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

1. **Запуск мастера установки**
   Вставьте внешний носитель с дистрибутивом Агента в компьютер. 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.

> **Важно!**
>
> Если на компьютере установлен Агент InfoWatch Device Monitor версии ниже 7.0, для установки Агента новой версии **обязательно** выполните следующие действия:
>
> 1. Удалите Агент InfoWatch Device Monitor;
> 2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 5 (20200327SE16) (см. официальную инструкцию);

3. Установите Агент InfoWatch Device Monitor 7.0.

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Astra Linux:

1. **Подготовка к установке:**
   a. Если ранее было установлено обновление на Astra Linux (например, Update 5), то выполните шаги b-e.
   b. Узнайте текущую версию ядра Astra Linux (например, **4.15.3-2-generic**):
   `uname -r`
   c. Проверьте, что директория */boot* не содержит старых пакетов ядра с более ранней версией, чем в предыдущем шаге (например, **initrd.img-4.15.3-1-generic** или **initrd.img-4.15.3-1-hardened.**
   d. Удалите такие пакеты при наличии:
   `apt-get purge linux-image-4.15.3-1`
   e. Удалите неиспользуемые Системой пакеты:
   `apt-get autoremove`
   `apt-get autoclean`
   f. 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.
   g. 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.

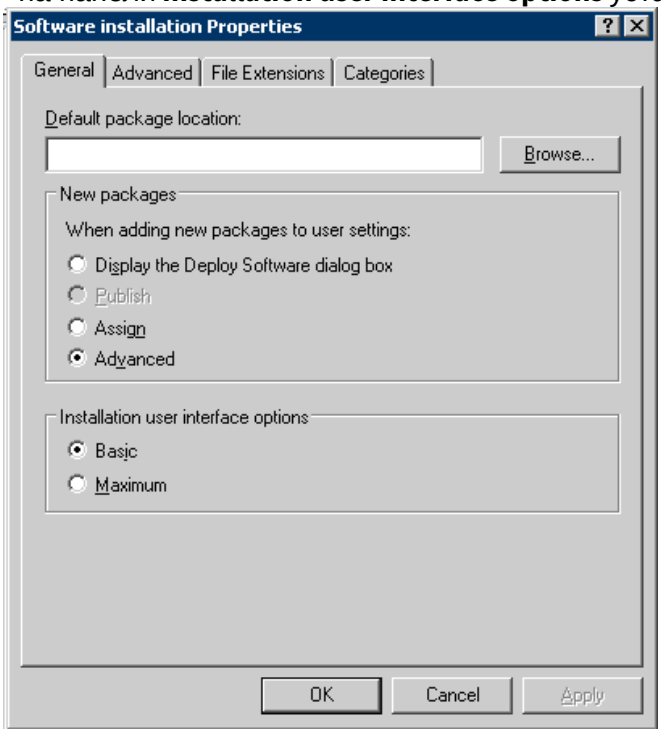
1. **Создание инсталляционного комплекта**

   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. **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**.

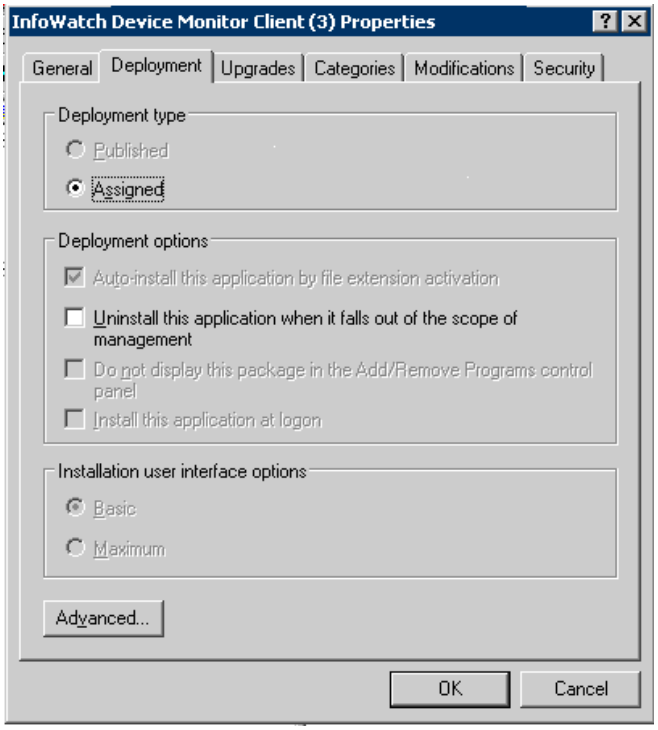
3. **Подготовка задания на установку Агента**

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**.

4. **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

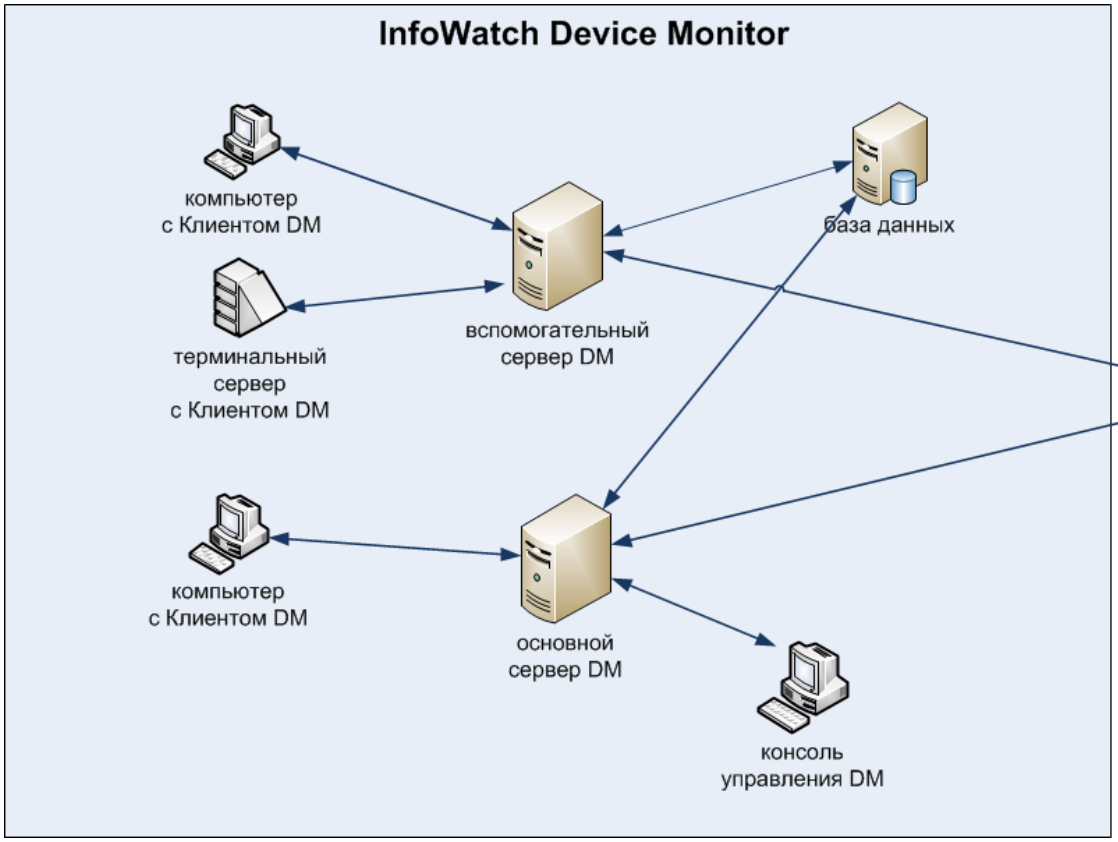
навигации. Чтобы получить актуальные сведения об установленных Агентах, воспользуйтесь кнопкой **Обновить**, расположенной на панели инструментов.

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
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. 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** 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. С контролируемых рабочих станций 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.

Директории установки Системы (могут располагаться на разных серверах):

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

После установки Системы смените пароли:

- пользователя **postgres**;
- учетной записи Linux (подробнее см. документ "Traffic Monitor. Руководство администратора", ст. "Изменение предустановленного пароля")

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

Параметры базы данных Traffic Monitor:

oinstall - группа владельца инсталляции клиента СУБД, в состав которой включены пользователи:

- **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 PostgreSQL	**postgres**	xxXX1234

Учетные записи баз данных:Учетные записи доступны после запуска **psql** для PostgreSQL.

Назначение		**Имя учетной записи PostgreSQL**	**Пароль**
Учетные записи для администрирования базы данных		**postgres**	xxXX1234
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 Traffic Monitor на ОС Astra Linux

Важно!

В версии 7.0 поддерживается обновление только внутри версии: с версии 7.0.x на версию 7.0.y.

Примечание:

Обновление 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.

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.

Примечание:

В процессе обновления IW Traffic Monitor будут выполнены действия, требующие прав sysdba при использовании СУБД PostgreSQL:

- Создание оберточных функций для чтения файлов, остановки и обрывания сессий, создания табличных пространств и выдача iwtm прав на них;
- Удаление всех представлений (view) и функций из схемы iwtm для создания в новой версии нужных с помощью обновления;
- Выдача пользователю iwtm:
  - Прав на создание объектов в БД;
  - Прав для установки, обновления и удаления схемы БД;
  - Прав для создания, удаления, архивации и восстановления табличных пространств;
  - Прав на функции обнуления статистики сервера postgres, которые используются в скрипте диагностики pgstat;
  - Прав на статистические представления (view) и таблицы, для сбора статистики работы БД;
  - Прав, используемых в коде продукта InfoWatch Traffic Monitor;
  - Прав для просмотра статистики БД;
  - Прав на схему pgagent для создания и управления заданиями (job).

Перед обновлением убедитесь в наличии:

- дистрибутивных дисков ОС Astra Linux Smolensk;
- дистрибутива 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:

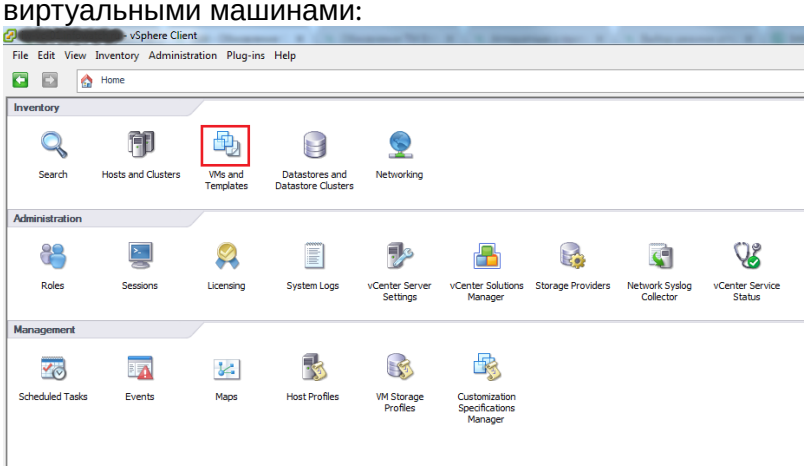
- какой тип установки в Системе (могут быть типы *Все-в-одном (All-in-one)* и *Распределенная установка (Node Server + Database Server)*) - данная информация понадобится для выбора инструкции по обновлению;
- на каком сервере установлен пакет `web-gui` - данная информация понадобится для очистки кеша сервера после обновления схемы БД. **Подсказка:** пакет установлен на том сервере, к которому подключается консоль управления Traffic Monitor.

До начала обновления выполните следующие действия:

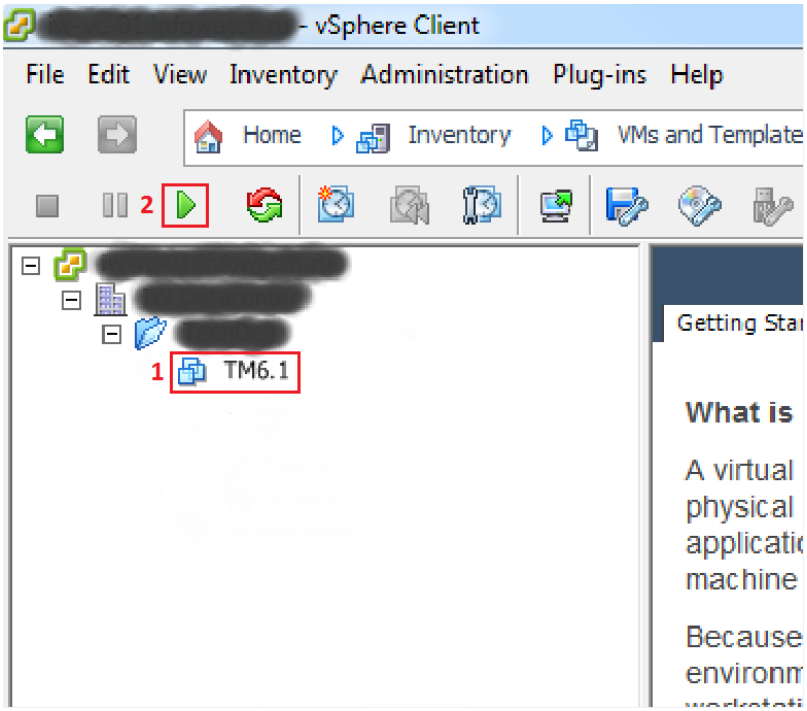
1. Включите (если он был выключен) каждый сервер, предназначенный для обновления:
   - в случае физического сервера - нажмите кнопку включения, расположенную на корпусе сервера (подробнее см. в инструкции к серверу);
   - в случае виртуального сервера - выполните команду **Power On** (см. пример ниже).

   > **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.

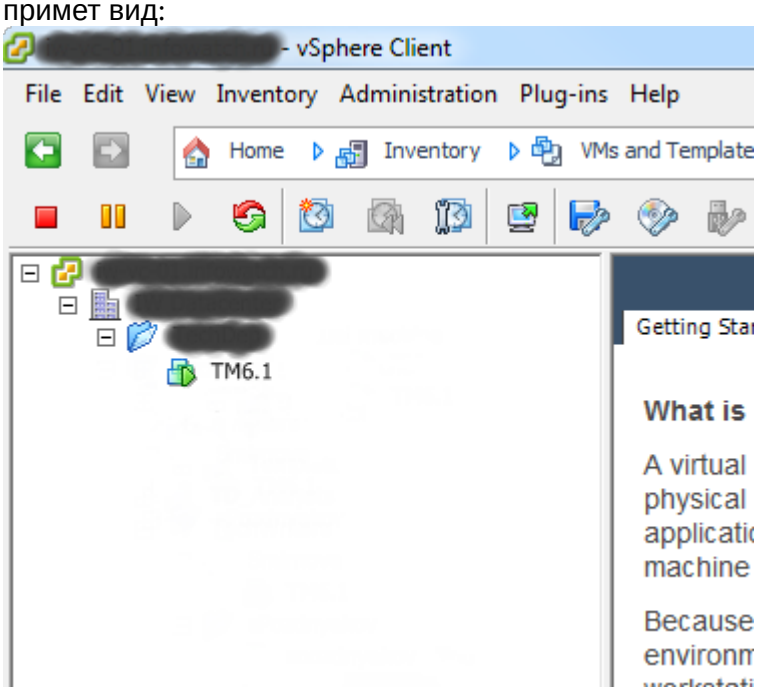
   Запустите клиентское приложение VMware vSphere Client от имени администратора (щелкните правой кнопкой мыши на иконке приложения и выберите **Запуск от имени администратора**). Войдите в приложение, используя логин и пароль, выданные администратором вашей информационной сети. Перейдите в раздел с виртуальными 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 дистрибутив InfoWatch Traffic Monitor к серверам, предназначенным для обновления, используя средства вашей ОС или системы виртуализации.

Обновите серверы согласно следующим инструкциям:

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

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)

Важно!

В версии 7.0 поддерживается обновление только внутри версии: с версии 7.0.x на версию 7.0.y.

Рекомендуется выполнить резервное копирование базы данных.

Для обновления потребуются 4 диска:

- Astra-Linux-Smolensk;
- Astra-Linux-Smolensk-Devel;
- обновление установочного диска;
- обновление диска со средствами разработки.

Перед обновлением Системы, 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*).

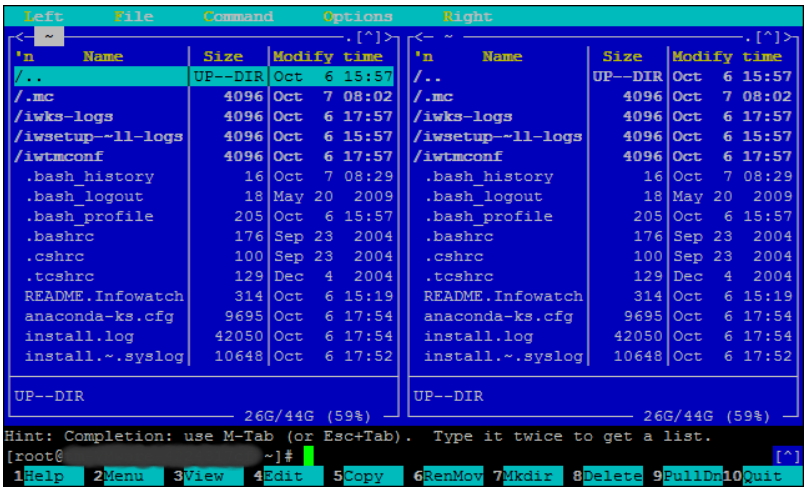
   Важно!

   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.

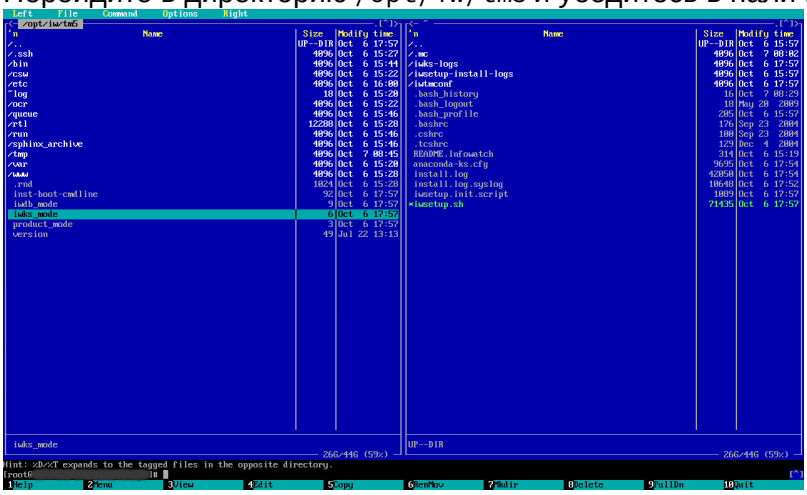
5. Введите команду для вызова файлового менеджера:

```
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. Чтобы проверить версию установленной Системы, откройте файл **version**.

Чтобы обновить Систему, выполните следующие действия:

1. Введите команды для остановки перехватчиков:
   ```
   sudo systemctl stop iw_smtpd
   sudo systemctl stop iw_xapi_xapi
   sudo systemctl stop iw_xapi_puppy
   ```
2. Дождитесь, пока обработаются все события, стоящие в очереди на обработку.
   События, находящиеся в очереди, хранятся в следующих директориях:
   ```
   /opt/iw/tm5/queue/analysis/.db/
   /opt/iw/tm5/queue/analysis/.in/
   /opt/iw/tm5/queue/analysis/.out/
   /opt/iw/tm5/queue/db/.db/
   /opt/iw/tm5/queue/db/.in/
   /opt/iw/tm5/queue/db/.out/
   /opt/iw/tm5/queue/smtp/.db/
   /opt/iw/tm5/queue/smtp/.in/
   /opt/iw/tm5/queue/smtp/.out/
   ```
   По завершении обработки событий данные директории должны стать пустыми.

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

3. Последовательно выполните команды для остановки служб:
   ```
   iwtm stop
   sudo service postgresql stop
   sudo service pgagent stop
   ```
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

Важно!

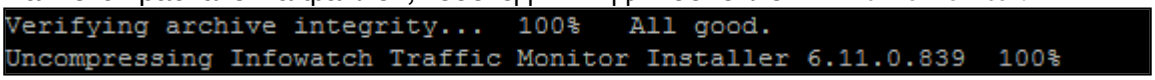
Ранее при установке обновления безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16) были использованы диск с обновлениями и диск со средствами разработки.
Ссылки для скачивания доступны на странице с официальной инструкцией.
Не удаляйте репозитории, подключенные в процессе установки Astra Linux Special Edition 1.6 Update 5.
В итоге должны быть доступны репозитории с **4-х** дисков.

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 TM в режиме "Все-в-одном", действия 7-13).

Примечание:

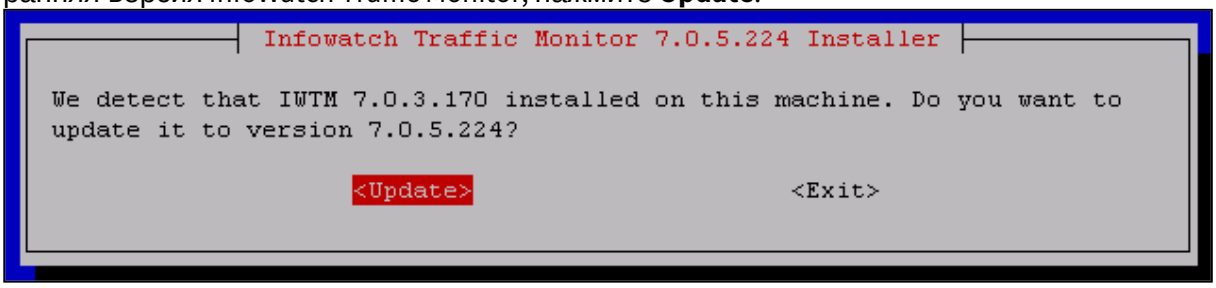
Содержание файла **sources.list** должно соответствовать действию 4.

8. Последовательно выполните команды для остановки служб:
9. `sudo service iwtm-php-fpm stop`
   `sudo service nagios3 stop`
10. Выполните следующую команду:
    `sudo apt-get update`
11. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.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. Для запуска обновления Traffic Monitor введите команду:
    `sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run`
    где `<директория_с_файлом>` - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run**.
    В нашем примере команда будет следующей:
    `sudo bash /distr/iwtm-installer-7.0.5.224-astra-smolensk-1.6.run`
    Начнется распаковка файлов, необходимых для обновления Traffic Monitor.



    Перед запуском установщик выполнит проверку Системы и, если будет обнаружено несоответствие требованиям, прервет обновление, выведя сообщение об ошибке. В этом случае необходимо исправить указанное установщиком несоответствие и повторно запустить обновление.

По завершении на экране отобразится окно, оповещающее о том, что найдена более ранняя версия InfoWatch Traffic Monitor, нажмите **Update**:



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



14. 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").
15. Введите команду для вызова файлового менеджера:
    `sudo mc`
16. 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.dpkg-dist`** (см. статью "Объединение конфигурационных файлов").
17. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    `exit`
18. Введите команду для очистки кеша:
    `redis-cli flushall`
19. Введите команду для перезагрузки сервера:
    `sudo reboot`
20. Дождитесь загрузки сервера и войдите в консоль.

> **Важно!**
>
> После запуска Traffic Monitor подключается к базе данных и загружает оттуда файл конфигурации `cas_config.xml`. В зависимости от объема конфигурации загрузка файла может занять некоторое время.
> В это время Система может записывать сообщения об ошибках в лог-файлы:

- /opt/iw/tm5/log/cas_config_compiler.log

  Запись об ошибке вида

  ```
  1 2019-10-07 17:00:57.351489 (3936:0x00007f4008de8880) [ERROR  ] : <Root>
  Exception:.
  Diagnostic information..
  /sandbox/src/cas3/config/details/cas_factory.cpp(233): Throw in function bool
  cas::CasConfigFactory::LoadXmlConfig(cas::ConfigCreator::Ptr&, const
  boost::filesystem::path&) const
  Dynamic exception type:
  boost::exception_detail::clone_impl<cas::ExceptionCasConfig>
  ```

- /opt/iw/tm5/log/cas.log

  Запись об ошибке вида

  ```
  1 2019-10-03 17:39:13.348146 (14262:0x00007fe83892ba80) [WARNING] : <Root>
  Prometheus server is off, therefore the statistics is unavailable. That's
  what you wanted, isn't it?
  2 2019-10-03 17:39:14.364655 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
  Error when loading config of tech: Cannot open xml file with cas
  configuration: etc/config/cas/cas_config.xml
  3 2019-10-03 17:39:14.364856 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
  failed to initialize thrift server
  Diagnostic information.
  /sandbox/src/cas3/handler.cpp(682): Throw in function
   cas::Handler::LoadedConfigData cas::Handler::GetLoadedConfigData(const
  prop::Property&, const Ptr&)
  Dynamic exception type:
  boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
  std::exception::what: Cannot open xml file with cas configuration: etc/
  config/cas/cas_config.xml
  ```

После успешной загрузки файла конфигурации cas_config.xml Система прекратит запись сообщений об ошибках и заработает в штатном режиме.
Если в течение длительного времени Система продолжает запись об ошибках, проверьте соединение с базой данных.

21. Введите команду для проверки запуска процессов:
    `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_cap stack`, `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  32463) is running...
iw_x2db (pid  32498) is running...
iw_x2x (pid  32531) is running...
iw_deliver (pid  32570) is running...
iw_warpd (pid  32602) is running...
iw_licensed (pid  32631) is running...
iw_luaengined (pid  32660) is running...
iw_cas (pid  32689) is running...
iw_analysis (pid  32739) is running...
iw_tech_tools (pid  320) is running...
iw_pas (pid  371) is running...
iw_adlibitum (pid  406) is running...
iw_blackboard (pid  464) is running...
iw_expressd (pid  504) is running...
iw_icap is stopped (disabled)
iw_image2text_fre_batch is stopped (disabled)
iw_messed (pid  606) is running...
iw_proxy_http is stopped (disabled)
iw_proxy_icq is stopped (disabled)
iw_proxy_smtp is stopped (disabled)
iw_sample_compiler (pid  736) is running...
iw_smtpd (pid  784) is running...
iw_xapi_puppy (pid  829) is running...
iw_xapi_xapi (pid  871) is running...
iw_system_check (pid  912) is running...
iw_sniffer is stopped (disabled)
iw_agent (pid  966) is running...
iw_capstack is stopped (disabled)
iw_configerator (pid  1031) is running...
iw_indexer (pid  1074) is running...
iw_kicker (pid  1109) is running...
iw_qmover_client is stopped (disabled)
iw_qmover_server is stopped (disabled)
iw_updater (pid  1244) 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.

Важно!

Если в Системе настроены автоматические синхронизации с LDAP-серверами, для гарантированной загрузки сущностей после обновления выполните синхронизации вручную (см. "Infowatch Traffic Monitor. Руководство пользователя", статья "Запуск синхронизации с сервером вручную").

Примечание:

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

4.2 Обновление ТМ при распределенной установке

Важно!

В версии 7.0 поддерживается обновление только внутри версии: с версии 7.0.x на версию 7.0.y.

Рекомендуется выполнить резервное копирование базы данных.

Для обновления потребуются 4 диска:

- Astra-Linux-Smolensk;
- Astra-Linux-Smolensk-Devel;
- обновление установочного диска;
- обновление диска со средствами разработки.

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

Важно!

Каждый сервер должен иметь уникальный корректный FQDN.

Перед обновлением Системы, выполните следующие действия:

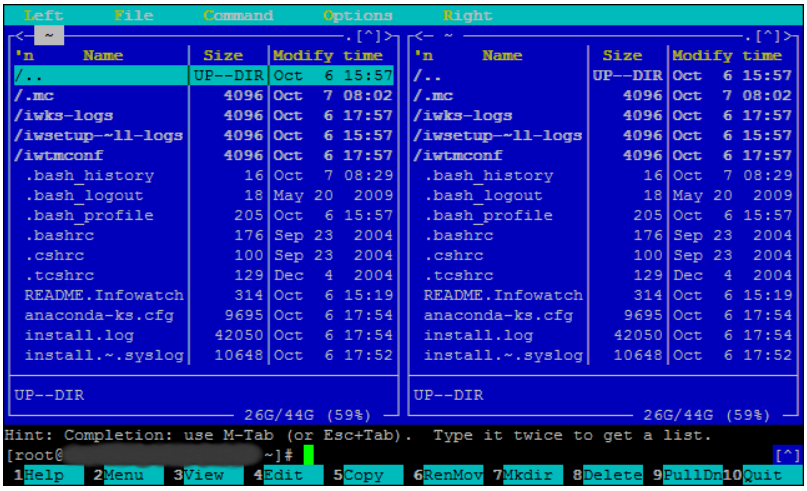
1. Откройте консоль обновляемого сервера.
2. Введите имя пользователя, от имени которого планируется обновление, и нажмите **Enter**.
3. Введите пароль и нажмите **Enter**.
4. Вызовите командную строку (например, терминал *Fly*).

   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. Проверьте содержимое файла **iwks_mode**, отличающееся в зависимости от типа сервера:
   - слово "`iwtm`" (оно указывает на тип установки - **TM Node**);
   - слово "`iwdb`" (оно указывает на тип установки - **DB Node**).

Примечание:

Если файл имеет другое содержимое, удалите все символы и введите:
`iwtm` - для сервера Traffic Monitor (**TM Node**);
`iwdb` - для сервера СУБД (**DB Node**).

8. Чтобы проверить версию установленной Системы, откройте файл **version**.
9. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
   `exit`

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. Введите команды для остановки перехватчиков:
   ```
   sudo systemctl stop iw_smtpd
   sudo systemctl stop iw_xapi_xapi
   sudo systemctl stop iw_xapi_puppy
   ```
2. Дождитесь, пока обработаются все события, стоящие в очереди на обработку. События, находящиеся в очереди, хранятся в следующих директориях:
   ```
   /opt/iw/tm5/queue/analysis/.db/
   /opt/iw/tm5/queue/analysis/.in/
   /opt/iw/tm5/queue/analysis/.out/
   /opt/iw/tm5/queue/db/.db/
   /opt/iw/tm5/queue/db/.in/
   /opt/iw/tm5/queue/db/.out/
   /opt/iw/tm5/queue/smtp/.db/
   ```

```
/opt/iw/tm5/queue/smtp/.in/
/opt/iw/tm5/queue/smtp/.out/
```
По завершении обработки событий данные директории должны стать пустыми.

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

3. Для остановки сервисов Traffic Monitor выполните команду:
```
iwtm 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.

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

Важно!

Ранее при установке обновления безопасности Astra Linux Special Edition 1.6 Update 5 (20200327SE16) были использованы диск с обновлениями и диск со средствами разработки.
Ссылки для скачивания доступны на странице с официальной инструкцией.
Не удаляйте репозитории, подключенные в процессе установки Astra Linux Special Edition 1.6 Update 5.
В итоге должны быть доступны репозитории с **4-х** дисков.

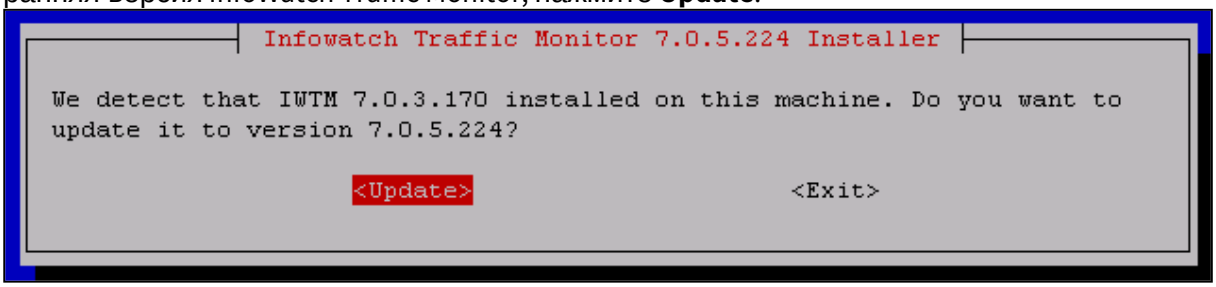
5. Закройте файл **sources.list**.
   Перейдите в указанные в файле директории, и убедитесь в наличии в них папок и файлов репозиториев.
6. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
   `exit`
7. Если в указанных директориях не созданы репозитории, создайте их (см. статью "Установка TM в режиме "Все-в-одном", действия 7-13).

Примечание:

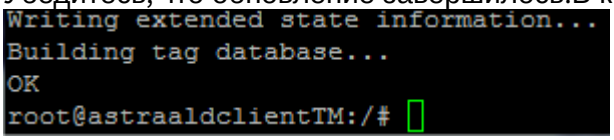
Содержание файла **sources.list** должно соответствовать действию 4.

8. Последовательно выполните команды для остановки служб:
   ```
   sudo service iwtm-php-fpm stop
   sudo service nagios3 stop
   ```
9. Выполните следующую команду:
   ```
   sudo apt-get update
   ```
10. Скопируйте файл **iwtm-installer-x.x.x.xxx-astra-smolensk.-1.6.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`.
11. Для запуска обновления Traffic Monitor введите команду:
    ```
    sudo bash /<директория_с_файлом>/iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run
    ```
    где <директория_с_файлом> - путь к директории, содержащей файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run**.
    В нашем примере команда будет следующей:
    ```
    sudo bash /distr/iwtm-installer-7.0.5.224-astra-smolensk-1.6.run
    ```
    Начнется распаковка файлов, необходимых для обновления Traffic Monitor.
    ```
    Verifying archive integrity...  100%   All good.
    Uncompressing Infowatch Traffic Monitor Installer 6.11.0.839  100%
    ```
    Перед запуском установщик выполнит проверку Системы и, если будет обнаружено несоответствие требованиям, прервет обновление, выведя сообщение об ошибке. В этом случае необходимо исправить указанное установщиком несоответствие и повторно запустить обновление.

По завершении на экране отобразится окно, оповещающее о том, что найдена более ранняя версия InfoWatch Traffic Monitor, нажмите **Update**:



12. Убедитесь, что обновление завершилось.В консоли отобразится сообщение вида:

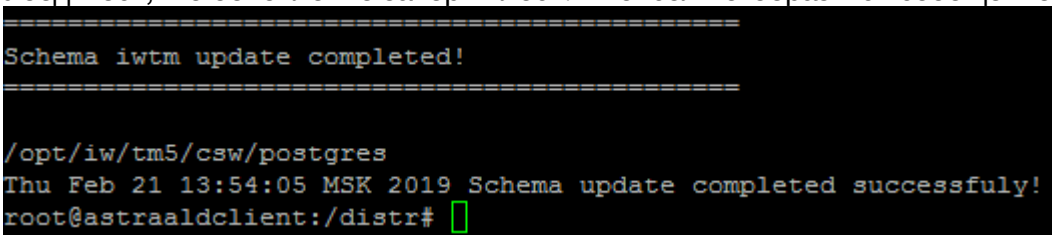


13. Введите команду для поиска и вывода на экран консоли списка файлов с расширением **.dpkg-dist**.
    `sudo find / -name "*dpkg-dist*" -print`
    Если такие файлы найдены, их нужно корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов").
14. Введите команду для вызова файлового менеджера:
    `sudo mc`
15. 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.dpkg-dist** (см. статью "Объединение конфигурационных файлов").
16. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
    `exit`
17. 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. Последовательно выполните команды для остановки служб:
   `iwtm stop`
   `sudo service postgresql stop`
   `sudo service pgagent stop`
2. Выполните действия 4-11 Шага 1 данной инструкции по обновлению.
   Убедитесь, что обновление завершилось. В консоли отобразится сообщение вида:



3. 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").

> **Важно!**
>
> В процессе обновления не вносите изменения в файлы **database.conf**, **consul.json**. Также рекомендуется не менять файл /etc/nagios/**nagios.cfg**.

4. Введите команду для вызова файлового менеджера:
   `sudo mc`
5. 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.dpkg-dist** (см. статью "Объединение конфигурационных файлов").
6. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
   `exit`
7. Введите команду для перезагрузки сервера:
   `sudo reboot`
8. Дождитесь загрузки сервера и повторно войдите в консоль.
9. Введите команду для проверки запуска процессов:
   `iwtm status`
   На экране отобразится список процессов и их статус. Сервисы должны быть запущены, при этом строки должны заканчиваться фразой "**is running...**":
   ```
   Service iw_system_check.service is active (running); enabled state: loaded (enabled)
   Service iw_agent.service is active (running); enabled state: loaded (enabled)
   Service iw_indexer.service is active (running); enabled state: loaded (enabled)
   Service iw_is.service is active (running); enabled state: loaded (enabled)
   ```
10. 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.

> **Важно!**
>
> После запуска Traffic Monitor подключается к базе данных и загружает оттуда файл конфигурации cas_config.xml. В зависимости от объема конфигурации

загрузка файла может занять некоторое время.
В это время Система может записывать сообщения об ошибках в лог-файлы:

- /opt/iw/tm5/log/cas_config_compiler.log

Запись об ошибке вида

```
1 2019-10-07 17:00:57.351489 (3936:0x00007f4008de8880) [ERROR  ] : <Root>
Exception:.
Diagnostic information..
/sandbox/src/cas3/config/details/cas_factory.cpp(233): Throw in function bool
cas::CasConfigFactory::LoadXmlConfig(cas::ConfigCreator::Ptr&, const
boost::filesystem::path&) const
Dynamic exception type:
boost::exception_detail::clone_impl<cas::ExceptionCasConfig>
```

- /opt/iw/tm5/log/cas.log

Запись об ошибке вида

```
1 2019-10-03 17:39:13.348146 (14262:0x00007fe83892ba80) [WARNING] : <Root>
Prometheus server is off, therefore the statistics is unavailable. That's
what you wanted, isn't it?
2 2019-10-03 17:39:14.364655 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
Error when loading config of tech: Cannot open xml file with cas
configuration: etc/config/cas/cas_config.xml
3 2019-10-03 17:39:14.364856 (14262:0x00007fe83892ba80) [ERROR  ] : <Root>
failed to initialize thrift server
Diagnostic information.
/sandbox/src/cas3/handler.cpp(682): Throw in function
 cas::Handler::LoadedConfigData cas::Handler::GetLoadedConfigData(const
prop::Property&, const Ptr&)
Dynamic exception type:
boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
std::exception::what: Cannot open xml file with cas configuration: etc/
config/cas/cas_config.xml
```

После успешной загрузки файла конфигурации cas_config.xml Система прекратит запись сообщений об ошибках и заработает в штатном режиме.
Если в течение длительного времени Система продолжает запись об ошибках, проверьте соединение с базой данных.

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_cap stack`, `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...**":

```
Service iw_bookworm.service is active (running); enabled state: loaded (enabled)
Service iw_x2db.service is active (running); enabled state: loaded (enabled)
Service iw_x2x.service is active (running); enabled state: loaded (enabled)
Service iw_deliver.service is active (running); enabled state: loaded (enabled)
Service iw_warpd.service is active (running); enabled state: loaded (enabled)
Service iw_licensed.service is active (running); enabled state: loaded (enabled)
Service iw_luaengined.service is active (running); enabled state: loaded (enabled)
Service iw_cas.service is active (running); enabled state: loaded (enabled)
Service iw_analysis.service is active (running); enabled state: loaded (enabled)
Service iw_tech_tools.service is active (running); enabled state: loaded (enabled)
Service iw_pas.service is active (running); enabled state: loaded (enabled)
Service iw_adlibitum.service is active (running); enabled state: loaded (enabled)
Service iw_blackboard.service is active (running); enabled state: loaded (enabled)
Service iw_icap.service is inactive (dead); enabled state: masked (bad)
Service iw_image2text_fre_batch.service is inactive (dead); enabled state: masked (bad)
Service iw_messed.service is active (running); enabled state: loaded (enabled)
Service iw_proxy_http.service is inactive (dead); enabled state: masked (bad)
Service iw_proxy_icq.service is inactive (dead); enabled state: masked (bad)
Service iw_proxy_smtp.service is inactive (dead); enabled state: masked (bad)
Service iw_sample_compiler.service is active (running); enabled state: loaded (enabled)
Service iw_smtpd.service is inactive (dead); enabled state: loaded (enabled)
Service iw_xapi_puppy.service is active (running); enabled state: loaded (enabled)
Service iw_xapi_xapi.service is active (running); enabled state: loaded (enabled)
Service iw_system_check.service is active (running); enabled state: loaded (enabled)
Service iw_sniffer.service is inactive (dead); enabled state: masked (bad)
Service iw_agent.service is active (running); enabled state: loaded (enabled)
Service iw_capstack.service is inactive (dead); enabled state: masked (bad)
Service iw_configerator.service is active (running); enabled state: loaded (enabled)
Service iw_kicker.service is active (running); enabled state: loaded (enabled)
Service iw_qmover_client.service is inactive (dead); enabled state: masked (bad)
Service iw_qmover_server.service is inactive (dead); enabled state: masked (bad)
Service iw_updater.service is active (running); enabled state: loaded (enabled)
```

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.

Важно!

Если в Системе настроены автоматические синхронизации с LDAP-серверами, для гарантированной загрузки сущностей после обновления выполните синхронизации вручную (см. "Infowatch Traffic Monitor. Руководство пользователя", статья "Запуск синхронизации с сервером вручную").

Примечание:

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

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".

  > **Примечание:**
  >
  > В случае удаления всей Системы удаление схемы БД можно не выполнять отдельно, так как этот процесс будет выполнен в рамках "Удаления Traffic Monitor".

- 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**.
- О порядке удаления Traffic Monitor (все установленные на сервере компоненты: веб-консоль, модули перехвата, СУБД с содержимым базы данных и другие) см. "Удаление Traffic Monitor".

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.

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:
      `iwtm stop`
   b. Закрыть все экземпляры консоли управления;
   c. Остановить сервис:
      `service iwtm-php-fpm stop`
   d. Прекратить все соединения с удаляемой схемой базы данных, осуществляемые из других программ.
3. **Запуск удаления схемы**
   a. Перейдите в директорию
      `/opt/iw/tm5/csw/oracle` или `/opt/iw/tm5/csw/postgres`
   b. Выполните скрипт:
      ./uninstall.sh
4. **Удаление старых версий конфигурации**
   a. Перейдите в директорию
      `/opt/iw/tm5/etc/configerator`
   b. Удалите все содержимое директории.

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**:
   `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 Агента InfoWatch Device Monitor на ОС Astra Linux:

1. Перейдите в директорию, в которую при установке было распаковано содержимое архива **`Setup.AstraLinux.Client.x64.tar.gz`**.
2. Для удаления Агента запустите скрипт, выполнив команду:
   `sudo ./remove.sh`

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.

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.

5.4 Удаление Traffic Monitor

Важно!

В процессе удаления Traffic Monitor **будут удалены все компоненты**, которые установлены на сервере, включая веб-консоль, модули перехвата, конфигурационные файлы, настройки, элементы технологий, объекты защиты, пользователи, роли, политики, файлы лицензии.

Если база данных находится на сервере, на котором будет запущен процесс удаления, будут удалены и СУБД, и все данные, включая события, индексы и настройки.
Удаление затронет **только** тот сервер, на котором будет выполнена команда удаления. Если используется база данных на удаленном сервере, процесс удаления ее не коснется.

Для возможности восстановления событий в случае переустановки Traffic Monitor рекомендуем перед удалением создать резервную копию базы данных (см. "*InfoWatch Traffic Monitor. Руководство администратора*", раздел Администрирование базы данных > PostgreSQL > Резервное копирование базы данных, статья "Создание резервной копии базы данных").
Также рекомендуется создать резервные копии конфигурации и настроек.

Процесс удаления Traffic Monitor запускается в консоли сервера. Удаление осуществляется с помощью инсталлятора InfoWatch Traffic Monitor.

Чтобы удалить Traffic Monitor выполните следующие действия:

1. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя, созданного при установке).

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).

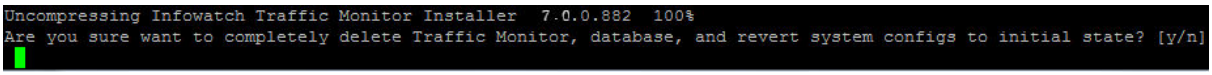
Чтобы работать с правами пользователя *root*, в командной строке введите `sudo su`. **Внимание!** К данному способу работы, ввиду возможности допустить серьезную ошибку, крайне не рекомендуется прибегать без помощи специалистов компании InfoWatch.

2. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. **Например**, для создания директории с именем `distr` в корне файловой системы выполните следующую команду:
   `sudo mkdir /distr`
3. Скопируйте в созданную директорию файл **iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run** (где x.x.x.xxx - номер сборки), поставляемый в дистрибутиве InfoWatch Traffic Monitor.
   В нашем примере:
   `iwtm-installer-7.0.0.882-astra-smolensk-1.6.run`
4. Введите команду для перехода в директорию с инсталлятором InfoWatch Traffic Monitor.
   В нашем примере:
   `cd /distr`
5. Для запуска процесса удаления выполните следующую команду:
   `sudo bash ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.6.run -- --uninstall`
   В нашем примере:
   `sudo bash ./iwtm-installer-7.0.0.882-astra-smolensk-1.6.run -- --uninstall`

Важно!

Выполнение команды возвращает сервер в состояние перед установкой InfoWatch Traffic Monitor.

   Начнется подготовка к удалению.
6. После подготовки будет выведено предупреждение о готовящемся удалении Traffic Monitor и базы данных, а также о возврате системных настроек к изначальному состоянию.



   Для продолжения введите "**Y**" и нажмите **Enter**.
   Начнется остановка сервисов Traffic Monitor, затем будет выполнено удаление пакетов Traffic Monitor и базы данных. Прогресс выполнения будет отображаться на экране.
   Дождитесь завершения процесса удаления.
7. Если удаление проводилось для переустановки Traffic Monitor, перезагрузите сервер, выполнив команду:
   `sudo reboot`

Примечание:

В случае распределенной установки для удаления Traffic Monitor выполните действия данной инструкции на каждом сервере Traffic Monitor (TM Node) и сервере базы данных (DB Node).

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.

Требование к паролям пользователей БД

- Пароль не должен содержать символы «"» и «'».

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