

INFOWATCH

InfoWatch Traffic Monitor 7.15

Руководство по установке

03/04/2026

© 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 16

2.2.1 Поддерживаемые СУБД 21

2.3 Требования к настройкам ОС и сети сервера 22

2.3.1 Рекомендации по разбиению дискового пространства 25

2.4 Настройка удаленной базы данных 27

2.4.1 Настройка СУБД PostgreSQL 12 28

2.4.2 Настройка СУБД PostgreSQL 15 32

2.4.3 Настройка СУБД Postgres Pro Enterprise 36

2.4.4 Настройка СУБД Jatoba 42

2.4.5 Настройка СУБД Pangolin 47

2.4.6 Настройка СУБД Tantor 52

3 Установка Системы 59

3.1 Установка Data Storage 61

3.1.1 Подготовка сервера 62

3.1.2 Установка Платформы 67

Чтобы установить Платформу в режиме central: 67

Чтобы установить Платформу в режиме office: 69

Установка Платформы с указанием параметров в командной строке 71

3.2 Установка InfoWatch Traffic Monitor 74

3.2.1 Установка TM Enterprise и TM Standard в режиме "Все-в-одном" 74

3.2.2 Распределенная установка TM Enterprise 103

3.2.3 Установка в тихом режиме с файлом параметров 148

Файл параметров (option file) 154

Тихий режим установки 155

Полный состав файла параметров 157

3.3 Предустановленные серверные параметры 168

4 Обновление Системы 172

4.1 Перед обновлением ... 173
4.2 Обновление Системы ... 175
4.3 Удаление дубликатов графических объектов ... 175
4.4 Обновление ТМ Все-в-одном (All-in-one) Enterprise и Standard ... 176
4.4.1 Файл параметров (option file) ... 197
4.4.2 Тихий режим обновления ... 197
4.4.3 Полный состав файла параметров ... 199
4.5 Обновление ТМ при распределенной установке ... 207
4.5.1 Файл параметров (option file) ... 228
4.5.2 Тихий режим обновления ... 229
4.5.3 Полный состав файла параметров ... 231
4.6 Объединение конфигурационных файлов ... 244
4.6.1 Объединение конфигурационных файлов в Midnight Commander ... 245
4.6.2 Объединение конфигурационных файлов с помощью vimdiff ... 247
4.7 Обновление Data Storage ... 247
4.7.1 Прямое обновление Платформы ... 248
4.7.2 Обновление Платформы с помощью сброса установки (reset) ... 250
5 Удаление Системы ... 253
5.1 Удаление Data Storage ... 253
5.2 Удаление схемы базы данных ... 253
5.3 Удаление Traffic Monitor ... 255
6 Приложение A. Рекомендации по составлению имен и паролей ... 258
7 Приложение B. Лицензии на стороннее программное обеспечение 260

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.

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;
- настройке удаленной базы данных.

2.1 Схемы развертывания Системы и выбор типа установки

Система InfoWatch Traffic Monitor (далее – TM) поставляется в нескольких вариантах. При этом имеет значение режим установки Системы, распределение компонентов, используемая СУБД (система управления базами данных) и редакция системы.

Редакции Traffic Monitor

Можно выделить следующие типичные варианты решений:

- **InfoWatch Traffic Monitor Standard** – решение для компаний, использующих до 500 рабочих станций. Имеет ряд ограничений по сравнению с Enterprise-версией (подробнее см. статью *Различия Enterprise и Standard редакций InfoWatch Traffic Monitor*). Разворачивается на едином сервере.
- **InfoWatch Traffic Monitor Enterprise** – полное масштабируемое решение с гибким конфигурированием компонентов.
  Максимально развернутая конфигурация:
  - **Отдельные серверы Traffic Monitor с функциональными ролями:**
    - **База данных**
    - **Индексер**
    - **Веб-консоль**
    - **Перехватчики**

      > **Примечание:**
      >
      > На серверах 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 управления и Агентов, распространяемых на рабочие станции компании.
  - **Адаптеры**. Набор модулей перехвата для интеграции со сторонними системами.
  - **Vision**. Модуль для визуального представления расследования инцидентов. Использует данные, полученных от InfoWatch Traffic Monitor.
  - **Activity Monitor**. Модуль для контроля за деятельностью сотрудников.
  - **Prediction**. Модуль предиктивной и поведенческой аналитики.
  - **Data Discovery**. Модуль для поиска конфиденциальной информации на общих сетевых ресурсах, рабочих станциях, серверах и в хранилищах документов.
  - **Data Analysis Service**. Сервис для анализа данных, полученных от InfoWatch Traffic Monitor или других продуктов InfoWatch.
  - **Data Storage**. Внешнее хранилище бинарных данных.

Также в любой редакции Traffic Monitor без приобретения дополнительной лицензии доступны:

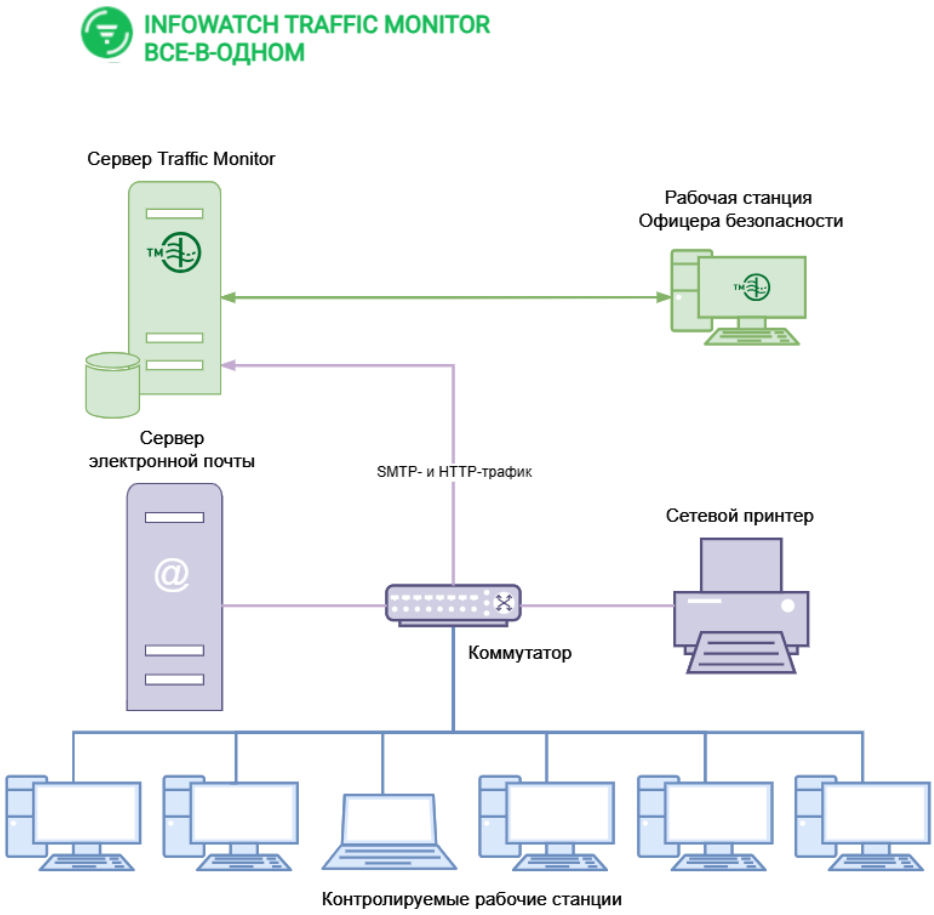
- Технология анализа текстовых данных **Автолингвист**. Подробнее см. *InfoWatch Traffic Monitor. Руководство пользователя. Автолингвист*.
- **Data Explorer**. Программный продукт, который автоматизирует формирование политик DLP-системы, выделяя тематические кластеры документов в информационных потоках компании.
- Экспорт данных из Traffic Monitor в Центр расследований InfoWatch.

> **Примечание:**
>
> Токен для интеграции Центра расследований с Traffic Monitor доступен сразу после установки Traffic Monitor. Вы можете найти его в разделе **Управление** -> **Плагины** Консоли управления Traffic Monitor, на вкладке **Токены** предустановленного плагина **InfoWatch Investigation Centre**.

Типы установки Traffic Monitor

Traffic Monitor можно установить в одном из режимов:

- **Все-в-одном** (All-in-one) – все компоненты Системы и СУБД 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. Пример развертывания:

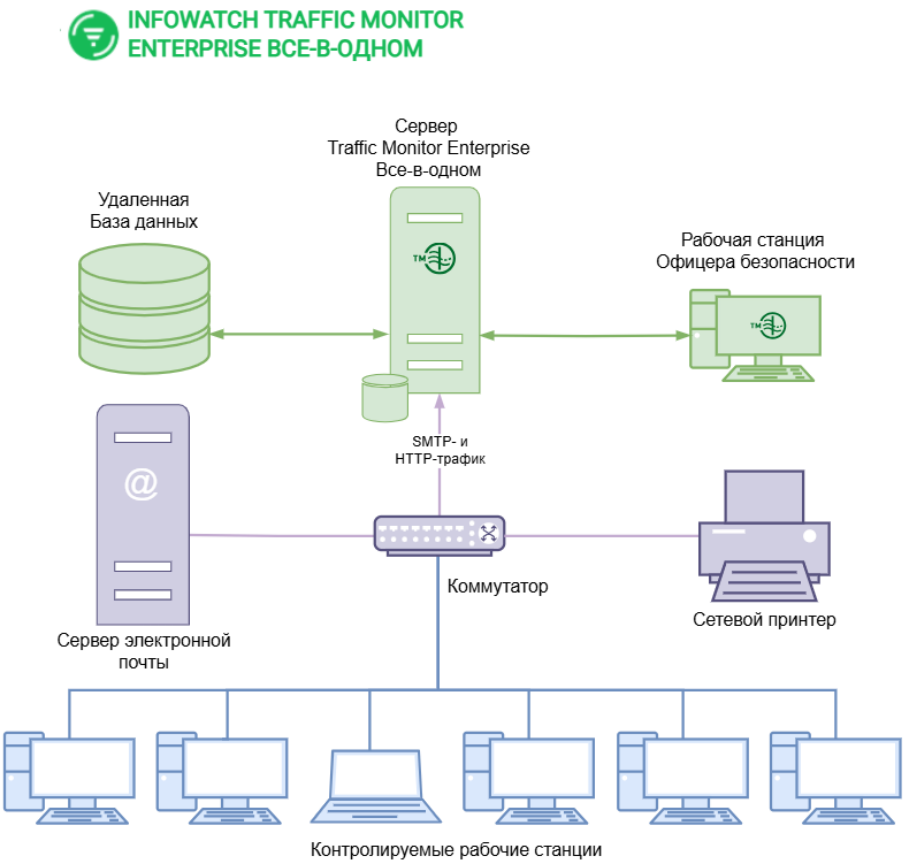


Установка "Все-в-одном" доступна для обеих редакций Traffic Monitor:

- при развертывании Traffic Monitor редакции **Standard** в режиме **Все-в-одном** устанавливается СУБД, поставляемая в дистрибутиве;
- при развертывании Traffic Monitor редакции **Enterprise** в режиме **Все-в-одном** вы можете:
  - выбрать СУБД, поставляемые в дистрибутиве;
  - подключиться к уже установленной СУБД. При этом СУБД может быть развернута:
    - на одном сервере с ТМ;
    - на отдельном сервере. В обоих случаях СУБД будет считаться удаленной (`remote`).

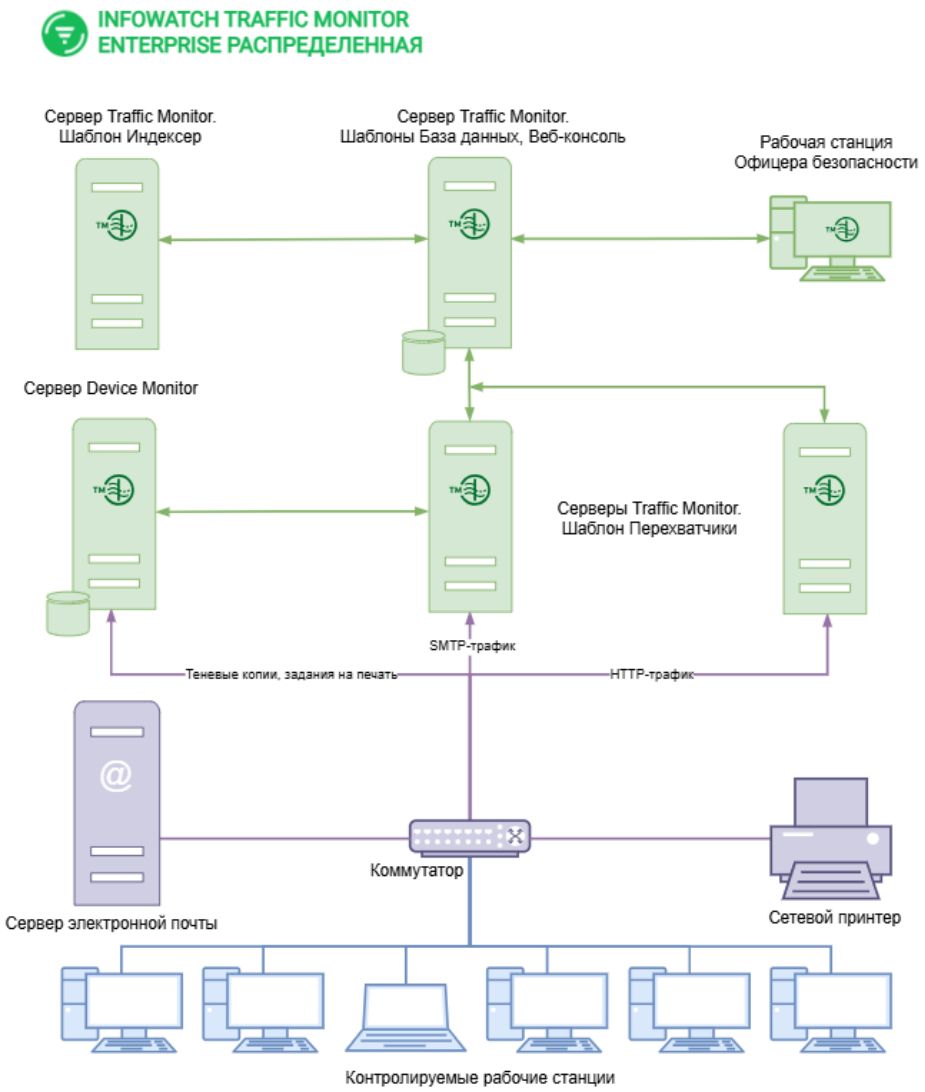
> **Примечание:**
>
> Подробнее о совместимых СУБД см. раздел *Поддерживаемые СУБД* статьи *Аппаратные и программные требования*.

Пример развертывания ТМ Enterprise "Все-в-одном" с подключением к удаленной базе данных:



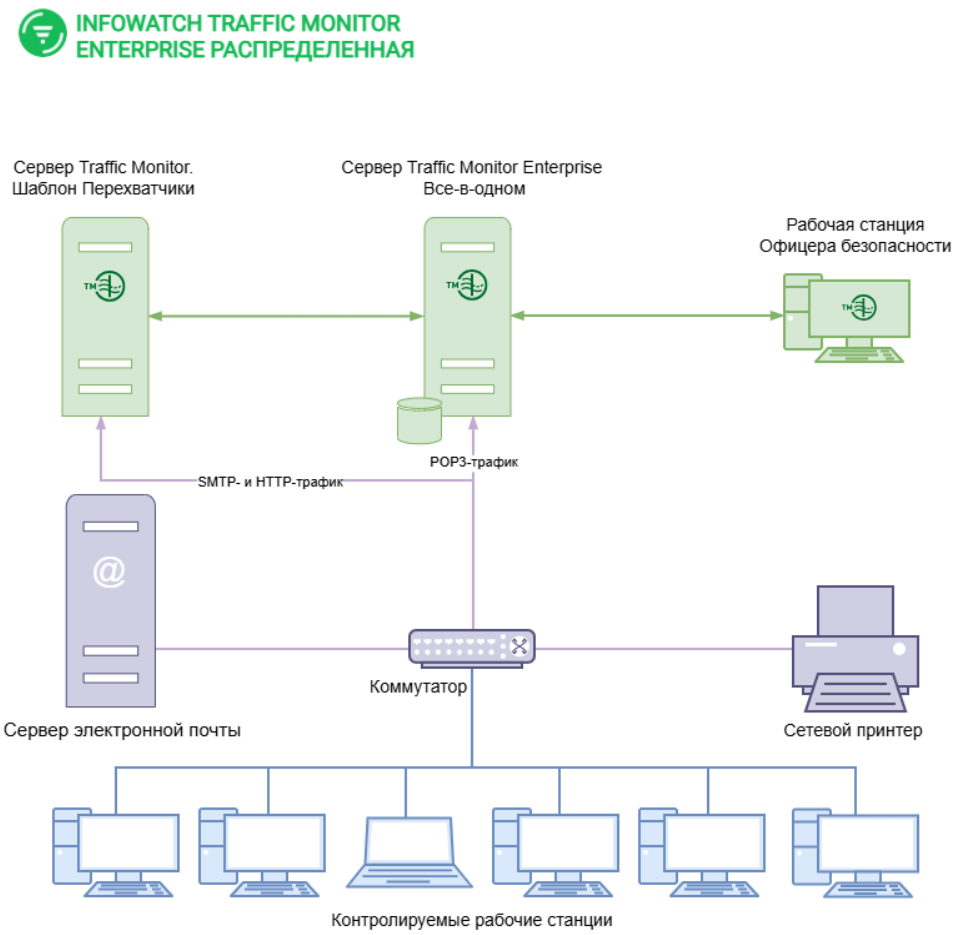
- **Распределенная установка** (Distributed) – компоненты Traffic Monitor и СУБД устанавливаются на разные компьютеры согласно их функциональным ролям. Распределенная установка доступна только для редакции **Enterprise**. Она позволяет увеличить производительность сервисов Traffic Monitor и СУБД за счет их распределения по нескольким компьютерам с учетом предполагаемой нагрузки. Функциональные роли серверов определяются при помощи *шаблонов*. Пример

развертывания Системы на нескольких серверах:



Сервер Traffic Monitor редакции Enterprise, установленный в режиме "Все-в-одном", можно использовать при распределенной установке как один из компонентов Системы. Например, на

схеме ниже сервер "Все-в-одном" дополнен сервером перехвата:

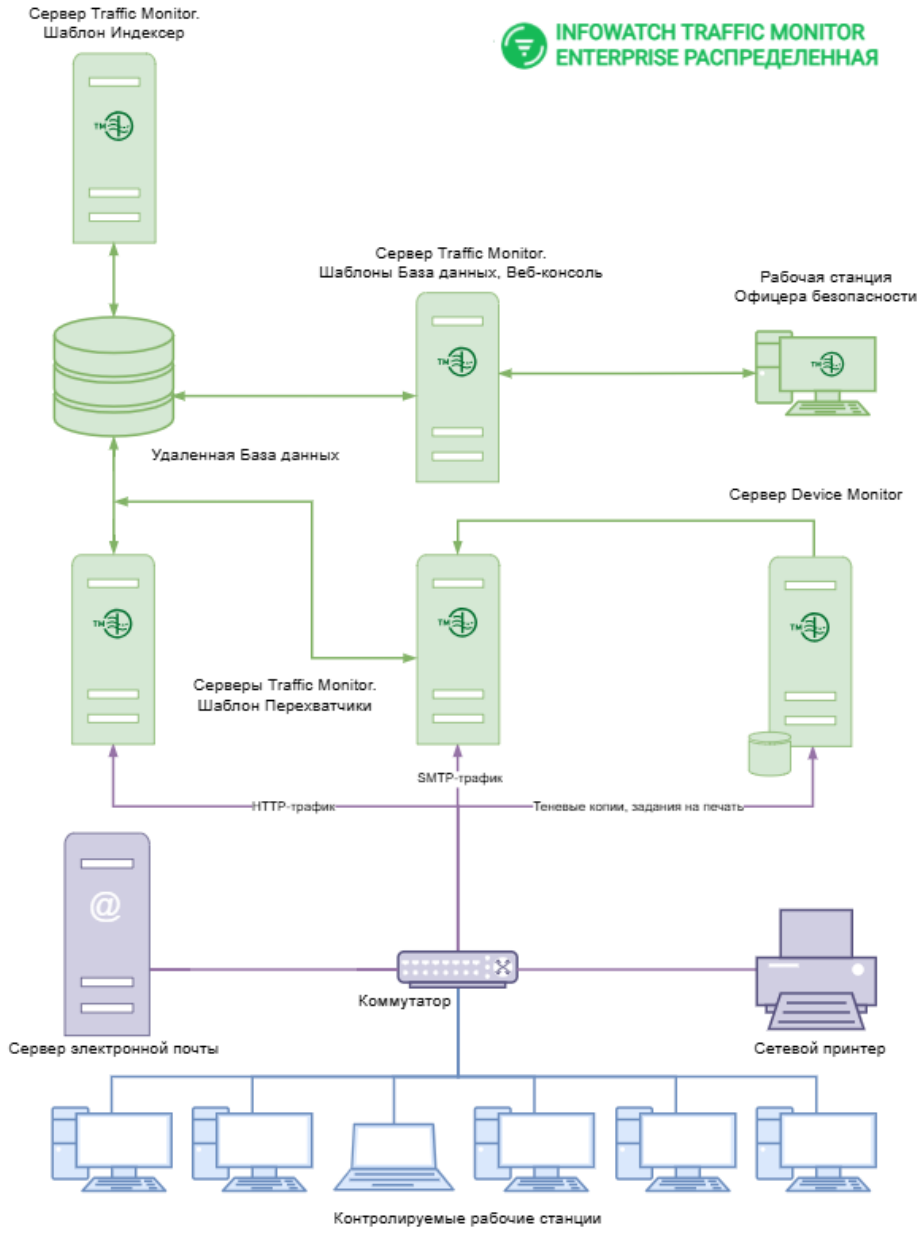


При распределенной установке Traffic Monitor вы можете:

- выбрать СУБД, поставляемые в дистрибутиве;
- подключиться к уже установленной СУБД. При этом СУБД может быть развернута:
  - на одном сервере с TM;
  - на отдельном сервере. В обоих случаях СУБД будет считаться удаленной (`remote`).

> **Примечание:**
>
> Подробнее о совместимых СУБД см. раздел *Поддерживаемые СУБД* статьи *Аппаратные и программные требования*.

Пример распределенного развертывания TM Enterprise с подключением к удаленной базе данных:



Data Storage

Вне зависимости от типа установки, в дополнение к базе данных рекомендуется *установить внешнее хранилище бинарных данных Data Storage*. В нем будут храниться контенты из событий перехвата, например вложения, снимки экрана, звуковые файлы и т.д. Таким образом Data Storage позволит:

- оптимизировать хранение данных;
- увеличить производительность СУБД;
- ускорить процесс обновления Traffic Monitor;
- существенно снизить нагрузку на БД при работе с большими объемами данных.

Data Storage можно установить как на один сервер с Traffic Monitor, так и на разные. Если количество рабочих станций в компании более 2000, рекомендуем устанавливать хранилище на отдельный сервер.

Шаблоны установки

В инсталляторе Traffic Monitor используется система шаблонов установки. Каждый шаблон – это набор компонентов Traffic Monitor, которые будут активированы после развертывания Системы. Наборы компонентов соответствуют функциональным ролям серверов. Роли серверов, выделенные еще на этапе установки, заметно упрощают планирование развертывания Системы, сокращают время ее установки и последующей подготовки к эксплуатации. Использование шаблонов также упрощает масштабирование Системы в ходе эксплуатации.

Шаблон определяет только набор активных компонентов, поэтому на сервер будут установлены все компоненты Traffic Monitor, независимо от выбранного шаблона. После установки вы можете изменить набор активных компонентов на сервере.

На один сервер можно одновременно установить несколько шаблонов. Установка в режиме "Все-в-одном" – это аналог установки всех шаблонов на один сервер.

Совокупность серверов, выделенных для развертывания Системы, образует кластер.

Доступны четыре шаблона установки:

- **База данных** (`Database`)
- **Индексер** (`Indexer service`)
- **Веб-консоль** (`Web console`)
- **Перехватчики** (`Traffic interceptors`)

> **Важно!**
>
> Шаблоны **База данных**, **Индексер** и **Веб-консоль** в одном кластере должны быть в единственном экземпляре.

Во всех шаблонах после установки будут включены компоненты:

- `iwtm-consul` – обеспечение межсервисного взаимодействия;
- `iwtm-nagios` – набор датчиков для контроля состояния Системы.

Шаблон "База данных"

Шаблон включает в себя СУБД и модули контроля состояния сервера.
СУБД хранит результаты анализа данных, информацию о перехваченных объектах и о применении политик. Если предполагается подключение к уже развернутой базе данных, на сервере с шаблоном "База данных" будет установлен клиент СУБД, с помощью которого компоненты других шаблонов будут отправлять данные в удаленную базу.

К шаблону "База данных" относятся следующие процессы:

Имя процесса	Краткое описание назначения
`iw_agent`	Нужен для управления конфигурацией Системы
`iw_system_check`	Контролирует состояние Системы
`iw_space_manager`	Управляет табличными пространствами

> **Важно!**

Процесс `iw_space_manager` должен быть в единственном экземпляре на кластер. В противном случае возникнет несогласованность данных в Системе.

Шаблон "Индексер"

Шаблон включает в себя компоненты для индексации текста объектов, перехваченных Системой и сохраненных в базе данных. Также компоненты шаблона используются для индексации метаданных о событиях перехвата и аудита. Модули шаблона позволяют выполнять поиск по событиям с помощью запросов. Для полнотекстового поиска используется механизм Sphinx.

К шаблону "Индексер" относятся следующие процессы:

Имя процесса	Краткое описание назначения
`iw_agent`	Нужен для управления конфигурацией Системы
`iw_indexer`	Индексирует текст событий
`iw_is`	Индексирует метаданные
`iw_metainfo_fetcher`	Выбирает данные для индексации из базы
`iw_system_check`	Контролирует состояние Системы

Важно!

Следующие процессы в одном кластере должны быть в единственном экземпляре:

- `iw_indexer`
- `iw_is`

В противном случае возникнет несогласованность данных в Системе.

Шаблон "Веб-консоль"

Шаблон включает в себя компоненты Консоли управления Traffic Monitor – графического пользовательского интерфейса. Также к этому шаблону относятся классификаторы текстовых и графических объектов, компоненты лицензирования.
С помощью Консоли управления вы можете проводить мониторинг сводной информации, создавать политики и объекты защиты, добавлять контакты, просматривать события, выгружать данные и формировать отчеты.

К шаблону "Веб-консоль" относятся следующие процессы:

Имя процесса	Краткое описание назначения
`iw_adlibitum`	Обеспечивает интеграцию с LDAP-каталогами
`iw_agent`	Нужен для управления конфигурацией Системы

Имя процесса	Краткое описание назначения
`iw_blackboard`	Отвечает за: • добавление/удаление статуса персонам/рабочим станциям из политик; • добавление новых контактов; • добавление новых приложений в автоподсказки поиска; • добавление в очередь уведомлений из политик.
`iw_bookworm`	Выполняет роль справочника в Системе
`iw_configerator`	Формирует конфигурацию для Агентов Device Monitor в части политик защиты данных на агентах
`iw_deliver`	Досылает письма из карантина по решению Офицера безопасности при работе "в разрыв"
`iw_image_autoling`	Автоматически классифицирует графические объекты
`iw_kicker`	Взаимодействует с другими сервисами, необходим для множества функций, в том числе для: • импорта/экспорта конфигурации; • добавления эталонных документов; • работы процессов `iw_image_autoling` и `iw_text_autoling`; • уведомлений; • работы запросов и отчетов.
`iw_licensed`	Управляет лицензиями
`iw_sample_compiler`	Создает цифровые отпечатки из загруженных эталонных файлов
`iw_system_check`	Контролирует состояние Системы
`iw_tech_tools`	Вспомогательные утилиты для модуля контентного анализа
`iw_text_autoling`	Выполняет автоматическую классификацию текстовых объектов
`iw_updater`	Загружает конфигурацию из базы данных
`iw_warpd`	Управляет извлечением данных из объектов, загружаемых посредством веб-интерфейса

Важно!

Следующие процессы в одном кластере должны быть в единственном экземпляре:

- `iw_adlibitum`
- `iw_bookworm`
- `iw_configerator`
- `iw_deliver`
- `iw_image_autoling`
- `iw_kicker`
- `iw_licensed`
- `iw_text_autoling`

В противном случае возникнет несогласованность данных в Системе.

Шаблон "Перехватчики"

К шаблону относятся модули, отвечающие за сбор и анализ данных, а также применение политик. Компоненты шаблона обеспечивают перехват трафика в потоке/на шлюзе, передаваемого по протоколам:

- SMTP
- POP3
- HTTP
- HTTPS
- OSCAR
- NRPC
- IMAP
- ICAP

Получение шаблоном данных от некоторых сторонних систем реализовано при помощи специальных адаптеров. Подробнее см. документ *InfoWatch Traffic Monitor. Руководство администратора. Обработка трафика, полученного от сторонних источников*.

Рекомендуем горизонтально масштабировать серверы с ролью "Перехватчики", если показатель средней загрузки (load average) становится равным количеству ядер.

К шаблону "Перехватчики" относятся следующие процессы:

Имя процесса	Краткое описание назначения
`iw_agent`	Нужен для управления конфигурацией Системы
`iw_analysis`	Используется для контентного анализа: • объектов от сторонних систем; • HTTP- и ICQ-трафика от модуля Sniffer; • объектов в событиях Device Monitor, которые не относятся к почтовым протоколам.
`iw_blackboard`	Отвечает за: • добавление/удаление статуса персонам/рабочим станциям из политик; • добавление новых контактов; • добавление новых приложений в автоподсказки поиска; • добавление в очередь уведомлений из политик.
`iw_capstack`	Обрабатывает трафик, передаваемый по протоколам POP3, IMAP, NRPC. По умолчанию выключен
`iw_cas`	Выполняет контентный анализ перехваченных данных
`iw_icap`	Обрабатывает HTTP-трафик, полученный от ICAP-клиента
`iw_messed`	Используется для обработки SMTP-писем и объектов в событиях Device Monitor, которые относятся к почтовым протоколам
`iw_pas`	Сервис обработки данных после анализа
`iw_proxy_icq`	Принимает копию ICQ-трафика от модуля Sniffer. По умолчанию выключен
`iw_proxy_http`	Принимает копию HTTP-трафика от модуля Sniffer. По умолчанию выключен
`iw_proxy_smtp`	Принимает копию SMTP-трафика от модуля Sniffer. По умолчанию выключен
`iw_qmover_client`	Клиентская часть модуля для передачи объектов в удаленную базу данных. По умолчанию выключена

Имя процесса	Краткое описание назначения
`iw_sniffer`	Принимает копию трафика со SPAN-порта коммутатора. По умолчанию выключен
`iw_smtpd`	Принимает SMTP-письма
`iw_system_check`	Контролирует состояние Системы
`iw_updater`	Загружает конфигурацию из базы данных
`iw_warpd`	Управляет извлечением данных из перехваченных объектов
`iw_xapi_xapi`	Получает объекты от InfoWatch Device Monitor и Data Discovery
`iw_xapi_puppy`	Получает объекты от сторонних систем
`iw_x2db`	Загружает объекты в базу данных
`iw_x2x`	Преобразовывает объекты от перехватчиков в стандартизированный формат. Пересылает модифицированные данные процессу `iw_x2db`

Примечание:

Описание процессов смотрите в документе *InfoWatch Traffic Monitor. Руководство администратора. Список процессов серверной части Traffic Monitor*.

Важно!

После установки администратор настраивает Систему в зависимости от целей внедрения (см. документ *Infowatch Traffic Monitor. Руководство администратора. 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" (All-in-one)** – используется для редакции:

    - TM Standard – установка Standard-решения. См. *требования для сервера TM Standard.*
    - TM Enterprise – установка Enterprise-решения в режиме"Все-в-одном". См. *требования для отдельного сервера TM Enterprise.*
- **Сервер Traffic Monitor** – отдельный сервер или кластер серверов TM Enterprise. *Требования* см. ниже.
- **Сервер базы данных** – сервер СУБД. На этом компьютере не рекомендуется устанавливать и запускать приложения (особенно серверные) или использовать его в качестве файл-сервера. *Требования* см. ниже.

> **Примечание:**
>
> Список СУБД, с которыми может взаимодействовать Traffic Monitor, зависит от ОС сервера, на который он установлен. Подробнее см. в разделе *Поддерживаемые СУБД*.

- **Адаптеры** – требования к этим компонентам описаны в документации, поставляемой вместе с программным обеспечением адаптеров.
- **Сервер Device Monitor с Агентами Device Monitor** – модуль, имеющий агенты на Windows, macOS и Linux-системах. Требования см. в *InfoWatch Device Monitor (Windows). Руководство по установке, конфигурированию и администрированию* или *InfoWatch Device Monitor (Linux). Руководство по установке.*
- **Консоль управления** – автоматически устанавливается вместе с сервером Traffic Monitor, без дополнительных программно-аппаратных требований к серверу. Для доступа к Консоли следует использовать браузер Google Chrome или Mozilla Firefox актуальной версии.
- **Внешнее хранилище бинарных данных Data Storage** – может быть установлено на одном сервере с Traffic Monitor или на разных. *Требования* см. ниже.

Аппаратно-программные требования к серверу Traffic Monitor сильно варьируются. Так, минимальная конфигурация подразумевает следующие ограничения:

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

Также на количество и назначение серверов Traffic Monitor может влиять существенная разница в нагрузке на те или иные каналы перехвата. Например, для эффективной обработки трафика с Device Monitor может потребоваться использовать отдельные серверы для процессов **iw_xapi_xapi**.

В следующей таблице приведены программные и примерные минимальные аппаратные требования. Требования к объему дисковой подсистемы и оперативной памяти в зависимости от количества пользователей, срока хранения данных, а также с учетом сбора данных Device Monitor см. в статье *Рекомендации по разбиению дискового пространства*. Для подробного расчета конфигурации рекомендуем обращаться к специалистам InfoWatch или компании-партнера, у которой вы приобретаете продукт.

Аппаратные требования	Операционная система	Дополнительные требования
Сервер TM Standard		
Дисковая подсистема: RAID-массив с fault tolerance, 300 ГБ	• Red Hat Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9 с	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом.

Аппаратные требования	Операционная система	Дополнительные требования
Процессор: 2CPU 6xC, частота 2,6 ГГц Оперативная память: 24 ГБ	нужной для обновления подпиской; • Red Hat Enterprise Linux 8.10; • РЕД ОС 7.3.3, 7.3.4, 7.3.5 и 7.3.6; • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10; • Альт Сервер 10.2.	Нужно выполнить требования перехватчиков* См. Поддерживаемые СУБД.
Сервер TM Enterprise, менее 10 ГБ трафика в день		
Дисковая подсистема: RAID-массив с fault tolerance, 600 ГБ Процессор: 2CPU 8xC + Hyper-threading (Intel® Xeon® Processor E5-2640 v3 – частота 2,6 Гц) Оперативная память: 24 ГБ	• Red Hat Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9 с нужной для обновления подпиской; • Red Hat Enterprise Linux 8.10; • РЕД ОС 7.3.3, 7.3.4, 7.3.5 и 7.3.6; • РЕД ОС 7.3 Сертифицированная редакция (далее РЕД ОС 7.3 С); • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10; • Альт Сервер 10.2.	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков нужно выполнить требования перехватчиков* См. Поддерживаемые СУБД.
Сервер TM Enterprise, от 10 до 50 ГБ трафика в день		
Дисковая подсистема: RAID-массив с fault tolerance Процессор: 2SRVx2CPU 10xC Оперативная память: 32–48 ГБ на каждый из серверов	• Red Hat Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9 с нужной для обновления подпиской; • Red Hat Enterprise Linux 8.10; • РЕД ОС 7.3.3, 7.3.4, 7.3.5 и 7.3.6; • РЕД ОС 7.3 С; • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10;	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков нужно выполнить требования перехватчиков* См. Поддерживаемые СУБД.

Аппаратные требования	Операционная система	Дополнительные требования
	• Альт Сервер 10.2.	
Сервер TM Enterprise, более 50 ГБ трафика в день		
Дисковая подсистема: RAID-массив с fault tolerance Процессор: рассчитывается по запросу Оперативная память: от 32 ГБ на каждый из серверов	• Red Hat Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9 с нужной для обновления подпиской; • Red Hat Enterprise Linux 8.10; • РЕД ОС 7.3.3, 7.3.4, 7.3.5 и 7.3.6; • РЕД ОС 7.3 С; • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10; • Альт Сервер 10.2.	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков нужно выполнить требования перехватчиков* См. Поддерживаемые СУБД.
Сервер БД (Обеспечивает хранение трафика для 1–2 тыс. пользователей сроком до 3 месяцев; в случае использования OCR и Device Monitor требования рассчитываются по запросу)		
Дисковая подсистема: RAID-массив с fault tolerance: 500 ГБ Процессор: 2CPU от 6xC, частота 2,6 ГГц Оперативная память: 16 ГБ и более, в зависимости от объема данных, интенсивности вставки и обработки Для хранения логов действий (`redo log` – для Oracle, `xlog` – для PostgreSQL и Postgres Pro) нужно выделить директории `u01` дополнительное пространство, равное объему оперативной памяти сервера БД. Если оперативной памяти меньше 20 ГБ, выделите под логи 20 ГБ.	• Red Hat Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9 с нужной для обновления подпиской; • Red Hat Enterprise Linux 8.10; • РЕД ОС 7.3.3, 7.3.4 и 7.3.5 и 7.3.6; • РЕД ОС 7.3 С; • Oracle Linux 7.7, 7.8, 7.9; • Oracle Linux 8.10; • AlmaLinux 8.10; • Rocky Linux 8.10; • Альт Сервер 10.2.	См. Поддерживаемые СУБД.

Аппаратные требования	Операционная система	Дополнительные требования
Внешнее хранилище бинарных данных Data Storage		
При использовании Data Storage требования к дисковой подсистеме Traffic Monitor, приведенные выше, распределяются на базу данных Traffic Monitor и Data Storage в соотношении примерно 15% к 85%. При установке Traffic Monitor и Data Storage на один сервер дополнительное место для хранения данных не требуется. **Пример:** Traffic Monitor и Data Storage устанавливаются на разные серверы. Для дисковой подсистемы Traffic Monitor нужно 400 ГБ. Тогда на сервере Traffic Monitor потребуется 60 ГБ для базы данных, а на сервере Data Storage – 340 ГБ для хранения бинарных данных. Процессор: CPU от 4xC, частота 2,1 ГГц Оперативная память: от 16 ГБ	• Red Hat Enterprise Linux, версии: • 7.9; • 8.9; • 8.10 (поддерживается для версий Платформы начиная с 2.4.X). • Oracle Linux, версии: • 7.9; • 8.4; • 8.10; • РЕД ОС, версии: • 7.3.3; • 8 (поддерживается для версий Платформы начиная с 2.4.X). • ОС Альт: • Сервер 10.2; • СП 10. • МОС ОС Арбат 15.5.	Для работы Data Storage должна быть установлена Платформа версии 2.0.0 и выше.

Примечание:

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

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

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

Важно!

Перехват трафика с помощью **iw_sniffer** не поддерживается при установке Traffic Monitor на Red Hat Enterprise Linux 8.10, Oracle Linux 8.10, AlmaLinux 8.10, Rocky Linux 8.10 и Альт Сервер.

2.2.1 Поддерживаемые СУБД

При установке **Traffic Monitor Standard** вместе с продуктом устанавливается СУБД PostgreSQL 15, поставляемая в дистрибутиве.

При установке **Traffic Monitor Enterprise** вы можете:

- использовать СУБД, поставляемую в дистрибутиве. В таком случае СУБД устанавливается вместе с продуктом и считается локальной (`local`);
- подключиться к уже установленной СУБД. В таком случае СУБД считается удаленной (`remote`). При этом она может быть развернута:
  - на одном сервере с TM;
  - на отдельном сервере.

Важно!

Если вы планируете использовать СУБД в качестве удаленной, ее нужно настроить перед установкой Traffic Monitor. См. статью *Настройка удаленной базы данных*.

В таблице представлены СУБД, с которыми может взаимодействовать Traffic Monitor Enterprise в зависимости от ОС сервера, на котором он установлен:

ОС сервера Traffic Monitor	СУБД	
	В режиме `local` , поставляемая в дистрибутиве	В режиме `remote`
Red Hat Enterprise Linux 7.x	• Oracle 19c • PostgreSQL 15	• Oracle Enterprise 19c

ОС сервера Traffic Monitor	СУБД	
	В режиме `local`, поставляемая в дистрибутиве	В режиме `remote`
		• PostgreSQL 15 • Postgres Pro Enterprise 15 • Jatoba 5 • Tantor 15
Red Hat Enterprise Linux 8.10	PostgreSQL 15	• PostgreSQL 15 • Postgres Pro Enterprise 15 • Jatoba 5 • Tantor 15
РЕД ОС 7.3.3, 7.3.4 и 7.3.5	PostgreSQL 15	• PostgreSQL 15 • Postgres Pro Enterprise 15 • Jatoba 5 • Tantor 15 • Pangolin 6.x, начиная с 6.4.2
РЕД ОС 7.3 С	–	PostgreSQL 12, поставляемая в ОС
Oracle Linux 7.x	• Oracle 19c • PostgreSQL 15	• Oracle Enterprise 19c • PostgreSQL 15 • Jatoba 5 • Tantor 15
Oracle Linux 8.10	PostgreSQL 15	• PostgreSQL 15 • Postgres Pro Enterprise 15 • Jatoba 5 • Tantor 15
AlmaLinux 8.10		
Rocky Linux 8.10		
Альт Сервер 10.2		

2.3 Требования к настройкам ОС и сети сервера

Для успешной установки Системы сервер должен отвечать следующим требованиям:

- На сервере должна быть установлена ОС Red Hat Enterprise Linux 7.x (последняя версия)

  Примечание:

Вы также можете установить Систему на одну из других поддерживаемых ОС:

- РЕД ОС;
- Oracle Linux;
- Red Hat Enterprise Linux 8;
- AlmaLinux;
- Rocky Linux;
- Альт Сервер.

Версии поддерживаемых ОС указаны в статье *Аппаратные и программные требования*. Все последующие инструкции по установке и эксплуатации Системы актуальны для работы с этими операционными системами.

Важно!

Во время загрузки ОС Oracle Linux нужно вручную выбрать ядро Red Hat Compatible Kernel (RHCK), например Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`.

После загрузки ОС Oracle Linux:

- удалите ядро UEK, выполнив команду:

```
yum remove kernel-uek-<версия_ядра>
```

Например, в ОС Oracle Linux 7.9 удалите ядро `uek-5.4.17`:

```
yum remove kernel-uek-5.4.17
```

- выключите репозиторий `uek-ol7.repo`:

```
sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/uek-ol7.repo
```

- Должны быть настроены репозитории ОС с возможностью установить пакеты:
  - `redhat-lsb-core`
  - `lshw`
  - `ntp`
  - `ntpdate`
  - `tuned`
  - `postfix`
  - `perl-Dist-CheckConflicts`
  - `perl-List-MoreUtils`
  - `urw-base35-fonts-legacy`
  - `python3-psycopg2`
  - `libzstd`
  - `redis`

С инструкцией по настройке локального репозитория можно ознакомиться на *официальном сайте Red Hat Enterprise Linux* (страница доступна на английском языке).

> **Примечание:**
>
> Если Traffic Monitor устанавливается на сервер без доступа в интернет, обеспечьте оффлайн-доступ к указанным репозиториям.
>
> Например, вы можете настроить локальные зеркала репозиториев. С инструкцией по настройке локального зеркала репозиториев можно ознакомиться на *официальном сайте Red Hat Enterprise Linux* (страница доступна на английском языке).

- Должны быть доступны следующие репозитории:
  - для ОС Red Hat Enterprise Linux 7:
    - `os`
    - `updates`
    - `optional`
  - для РЕД ОС:
    - `base`
    - `updates`
    - `kernels`

      > **Примечание:**
      >
      > На сервере под управлением РЕД ОС нужно добавить исключения для репозиториев `base` и `updates`. Для этого перейдите в директорию `/etc/yum.repos.d` и внесите эту строку в файлы репозиториев:
      >
      > ```
      > exclude=postgresql* pgagent*
      > ```

  - для ОС Oracle Linux 7:
    - `ol7_latest`
    - `ol7_optional_latest`
    - `ol7_developer_EPEL`
  - для ОС Альт Сервер:
    - `p10/branch/x86_64 classic`
    - `p10/branch/noarch classic`
    - `p10/branch/x86_64-i586 classic`
  - для ОС Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8:
    - `BaseOS`
    - `AppStream`
    - `EPEL`
- Разбиение дискового пространство должно быть выполнено в соответствии со статьей *Рекомендации по разбиению дискового пространства*.
- Если вы планируете установку Traffic Monitor на компьютер под управлением ОС Альт Сервер, убедитесь, что для директории `/tmp` не используется файловая система `tmpfs`. В противном случае переведите директорию `/tmp` на иную файловую систему (например, Ext4 или XFS).
- Опции точки монтирования не должны содержать `nosuid` и `noxattr` (можно проверить, открыв файл `/etc/fstab`).

- На сервере должны быть корректные сетевые настройки (в случае проблем с настройками 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.
- Антивирус на сервере должен быть настроен для совместной работы с Системой (см. статью *Настройка антивируса на сервере Traffic Monitor*).

2.3.1 Рекомендации по разбиению дискового пространства

Статья содержит рекомендации по разбиению дискового пространства при развертывании Traffic Monitor в режиме "Все-в-одном" (All-in-one) с учетом сбора данных Device Monitor. См. режимы развертывания в статье *Схемы развертывания Системы и выбор типа установки*.

Расчеты приведены в зависимости от предполагаемой нагрузки:

- 100 пользователей;
- 300 пользователей;
- 500 пользователей.

При предполагаемой нагрузке в 1000 и более пользователей рекомендуем использовать распределенную (Distributed) установку. Для подробного расчета конфигурации в случае распределенной установки рекомендуем обращаться к специалистам InfoWatch или компании-партнера, у которой вы приобретаете продукт.

> **Примечание:**
>
> Инструкции по *разбиению дискового пространства* и *настройке swap-пространства* доступны на официальном сайте Red Hat Enterprise Linux (на английском языке).

Рекомендации по разбиению дискового пространства для обработки трафика 100 пользователей:

	Срок хранения данных, мес.		
	3	6	12
Общий размер диска, ГБ	1228,8	1945,6	3584

		Срок хранения данных, мес.		
		3	6	12
Разделы диска, ГБ	`swap`	8	8	8
	`/boot`	1	1	1
	`/`	150	180	220
	`/opt`	150	150	150
	`/u01`	50	70	100
	`/u02`	868	1536	3174,4
ОЗУ, ГБ		22	28	40

Рекомендации по разбиению дискового пространства для обработки трафика 300 пользователей:

		Срок хранения данных, мес.			
		3	6	12	24
Общий размер диска, ГБ		2764,8	5017,6	9830,4	*Рекомендуется распределенная установка*
Разделы диска, ГБ	`swap`	16	16	32	
	`/boot`	1	1	1	
	`/`	180	200	200	
	`/opt`	220	220	220	
	`/u01`	100	150	200	
	`/u02`	2048	3993,6	8192	
	`/var/lib/sphinx`	200	400	800	
ОЗУ, ГБ		40	56	96	

Рекомендации по разбиению дискового пространства для обработки трафика 500 пользователей:

		Срок хранения данных, мес.		
		3	6	12
Общий размер диска, ГБ		4300,8	8192	*Рекомендуется распределенная установка*
Разделы диска, ГБ	`swap`	16	32	
	`/boot`	1	1	
	`/`	200	200	
	`/opt`	220	220	
	`/u01`	200	200	
	`/u02`	3379,2	6860,8	
	`/var/lib/sphinx`	300	600	
ОЗУ, ГБ		24	96	

2.4 Настройка удаленной базы данных

Если вы будете использовать уже развернутую базу данных, перед установкой Системы обязательно:

1. Убедитесь, что версия вашей СУБД поддерживается Traffic Monitor. Подробнее см. раздел *Поддерживаемые СУБД* в статье *Аппаратные и программные требования*.

   > **Примечание:**
   >
   > При необходимости обновите СУБД до поддерживаемой версии. Для этого воспользуйтесь официальной инструкцией.

2. Выполните предварительную настройку:

   - Настройка СУБД PostgreSQL 12
   - Настройка СУБД PostgreSQL 15
   - Настройка СУБД Postgres Pro Enterprise
   - Настройка СУБД Jatoba
   - Настройка СУБД Pangolin
   - Настройка СУБД Tantor

2.4.1 Настройка СУБД PostgreSQL 12

Чтобы подготовить удаленную базу данных к установке компонентов Traffic Monitor, выполните на сервере базы данных следующие действия:

1. Установите дополнительные пакеты, выполнив команды:

```
yum -y install pgagent_12* postgresql-contrib
```

2. Убедитесь, что SELinux отключен.
   С инструкцией по отключению SELinux можно ознакомиться на *официальном сайте* РЕД ОС.
3. Создайте или дополните файл `/etc/systemd/system/postgresql-12.service.d/override.conf` следующим содержимым:

```
[Service]
Environment=PGDATA=/u01/postgres
```

4. Для применения изменений в конфигурации сервиса выполните команду:

```
systemctl daemon-reload
```

5. Создайте директории для файлов и архивов, а затем инициализируйте базу данных:

```
mkdir -p /u01/postgres
chown postgres:postgres /u01/postgres
sudo -u postgres initdb --encoding=UTF8 --locale=en_US.UTF-8 -D /u01/postgres
mkdir -p /u01/postgres/tmp /u02/pgdata /u02/pgdata1 /u02/arch
```

6. Создайте конфигурационный файл `/u01/postgres/iwtm-postgres.conf`. Например, с помощью команды:

```
touch /u01/postgres/iwtm-postgres.conf
```

7. Добавьте в файл `/u01/postgres/iwtm-postgres.conf`:

```
# ------------------------------
# PostgreSQL configuration file
# ------------------------------
#
# IWTM custom values

listen_addresses = '*'
```

```
port = 5433
max_connections = 1000                  # Change requires restart
tcp_keepalives_idle = 60                # TCP_KEEPIDLE, in seconds
tcp_keepalives_interval = 20            # TCP_KEEPINTVL, in seconds
tcp_keepalives_count = 2                # TCP_KEEPCNT

shared_buffers = kB                     # min 128KiB

huge_pages = try                        # on, off, or try

max_locks_per_transaction = 256
temp_buffers =  MB
work_mem = MB
effective_cache_size = MB

min_wal_size = MB
max_wal_size = MB
lc_messages = 'en_US.UTF-8'             # Locale for system error message
log_directory = 'pg_log'
log_filename = 'postgresql.log'         # Log file name pattern
log_rotation_age = 0                    # Automatic rotation of logfiles will happen
after that time. 0 disables.
log_rotation_size = 0                   # Automatic rotation of logfiles will happen
after that much log output. 0 disables.
log_min_duration_statement = 120000     # -1 is disabled, 0 logs all statements
track_activity_query_size = 32768       # Change requires restart
log_autovacuum_min_duration = 30000     # -1 disables, 0 logs all actions
stats_temp_directory = '/u01/postgres/pg_stat_tmp'
autovacuum_max_workers = 5
autovacuum_naptime = 20
max_parallel_maintenance_workers = 8
maintenance_work_mem = GB
autovacuum_freeze_max_age = 1000000000
shared_preload_libraries = 'pg_stat_statements'
track_io_timing = on
track_activity_query_size = 32768
constraint_exclusion = off              # on, off, or partition
standard_conforming_strings = on
```

Важно!

В примере содержимого конфигурационного файла указаны пустые поля значений для параметров:

- `shared_buffers`
- `work_mem`
- `maintenance_work_mem`
- `effective_cache_size`
- `temp_buffers`
- `min_wal_size`
- `max_wal_size`

Настройте эти параметры в соответствии с *официальной инструкцией* (на английском).

8. Смените у конфигурационного файла владельца и группу на `postgres`:

```
chown -R postgres:postgres /u02 /u01
```

9. Добавьте в конфигурационный файл `/u01/postgres/postgresql.conf` ссылку на файл `iwtm-postgres.conf` с помощью команды:

```
echo "include = 'iwtm-postgres.conf'" >> /u01/postgres/postgresql.conf
```

10. Настройте файл доступа `pg_hba.conf` с помощью команд:

```
sed -i "s|local[[:space:]]*all[[:space:]]*all[[:space:]]*peer|local   all             all
                                  trust|" /u01/postgres/pg_hba.conf
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*127.0.0.1/32[[:space:]]*ident|host
   all             all             127.0.0.1/32            trust|" /u01/postgres/
pg_hba.conf
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*::1/128[[:space:]]*ident|host
 all             all             ::1/128                 trust|" /u01/postgres/pg_hba.conf
echo "# Enable not local access" >> /u01/postgres/pg_hba.conf
echo "host    postgres        all             0.0.0.0/0               md5" >> /u01/
postgres/pg_hba.conf
```

11. Запустите сервис `postgresql` и проверьте его статус с помощью команд:

```
systemctl enable postgresql
systemctl start postgresql
systemctl status postgresql
```

12. Измените для администратора базы данных пароль по умолчанию:

```
su - postgres
psql -p 5433
alter user postgres password 'xxXX1234';
```

13. Создайте нужные расширения, выполнив запросы:

```
create extension if not exists adminpack;
create extension if not exists dblink;
create extension if not exists lo;
create extension if not exists xml2;
create extension if not exists tablefunc;
create extension if not exists intarray;
```

```
create extension if not exists file_fdw;
create extension if not exists "uuid-ossp";
create extension if not exists pgcrypto;
create extension if not exists pgrowlocks;
create extension if not exists autoinc;
create extension if not exists hstore;
create extension if not exists pg_stat_statements;
create extension if not exists pg_buffercache;
create extension if not exists pgagent;
```

14. Для выхода введите команды:

```
\q
exit
```

15. Для настройки в ОС пользователя `pgagent` выполните команды:

```
mkdir -p /home/pgagent
touch /home/pgagent/.pgpass
echo "127.0.0.1:5433:postgres:postgres:xxXX1234" > /home/pgagent/.pgpass
chmod 0600 /home/pgagent/.pgpass
chown -R pgagent:pgagent /home/pgagent
usermod -s /bin/bash pgagent

sed -i "s|DBPORT=5432|DBPORT=5433|" /etc/pgagent/pgagent_12.conf
```

16. Создайте или отредактируйте файл `/etc/sudoers.d/pgagent`, чтобы его содержимое соответствовало образцу:

```
# allow pgagent to execute any command
pgagent ALL = (postgres) NOPASSWD: ALL
Defaults:pgagent !requiretty
```

> **Важно!**
>
> Пустая строка в конце файла `pgagent` обязательна.

17. Измените для `/etc/sudoers.d/pgagent` права, владельца и группу, выполнив команды:

```
chmod 440 /etc/sudoers.d/pgagent
chown root:root /etc/sudoers.d/pgagent
```

18. Запустите сервис `pgagent` и проверьте его статус с помощью команд:

```
systemctl enable pgagent_12
systemctl start pgagent_12
systemctl status pgagent_12
```

По завершении настройки убедитесь в отсутствии критических ошибок в логах базы данных и `/var/log/pgagent_12.log`.

2.4.2 Настройка СУБД PostgreSQL 15

Чтобы подготовить удаленную базу данных к установке компонентов Traffic Monitor, выполните на сервере базы данных следующие действия:

1. Установите дополнительные пакеты, выполнив команды:

```
yum -y install pgagent_15* postgresql15-contrib
```

2. Остановите работу сервисов `postgresql` и `pgagent`, используя команды:

```
systemctl stop postgresql-15
systemctl stop pgagent_15
```

3. Создайте или дополните файл `/etc/systemd/system/postgresql-15.service.d/override.conf` следующим содержимым:

```
[Service]
Environment=PGDATA=/u01/postgres
```

4. Для применения изменений в конфигурации сервиса выполните команду:

```
systemctl daemon-reload
```

5. Создайте директории для файлов и архивов, инициализируйте базу данных и смените директориям владельца и группу на `postgres`:

```
mkdir -p /u01/postgres
chown postgres:postgres /u01/postgres
export PGSETUP_INITDB_OPTIONS=" --encoding=UTF8"
sudo -u postgres /usr/pgsql-15/bin/initdb --encoding=UTF8 --locale=en_US.UTF-8 -D /u01/
postgres/
mkdir -p /u01/postgres/tmp
chown postgres:postgres /u01/postgres/tmp
mkdir -p /u02/pgdata
chown postgres:postgres /u02/pgdata
mkdir -p /u02/pgdata1
chown postgres:postgres /u02/pgdata1
```

```
mkdir -p /u02/arch
chown postgres:postgres /u02/arch
```

6. Создайте конфигурационный файл `/u01/postgres/iwtm-postgres.conf`. Например, с помощью команды:

```
touch /u01/postgres/iwtm-postgres.conf
```

7. Добавьте в файл `/u01/postgres/iwtm-postgres.conf`:

```
# ----------------------------
# PostgreSQL configuration file
# ----------------------------
#
# IWTM custom values

listen_addresses = '*'
port = 5433
max_connections = 1000                          # (change requires restart)
tcp_keepalives_idle = 60                        # TCP_KEEPIDLE, in seconds'
tcp_keepalives_interval = 20                    # TCP_KEEPINTVL, in seconds'
tcp_keepalives_count = 2                        # TCP_KEEPCNT

shared_buffers = kB

huge_pages = try                                # on, off, or try
max_locks_per_transaction = 512
temp_buffers =  MB
work_mem = MB
effective_cache_size = MB

min_wal_size = MB
max_wal_size = MB
log_min_duration_statement = 120000             # -1 is disabled, 0 logs all statements
track_activity_query_size = 32768               # (change requires restart)
log_autovacuum_min_duration = 30000             # -1 disables, 0 logs all actions and
# stats_temp_directory = '/u01/postgres/pg_stat_tmp'

autovacuum_max_workers = 5
autovacuum_naptime = 20
maintenance_work_mem = GB
autovacuum_freeze_max_age = 1000000000

shared_preload_libraries = 'pg_stat_statements'
track_io_timing = on
track_activity_query_size = 32768

constraint_exclusion = off                      # on, off, or partition
```

Важно!

В примере содержимого конфигурационного файла указаны пустые поля значений для параметров:

- `shared_buffers`
- `work_mem`
- `maintenance_work_mem`
- `effective_cache_size`
- `temp_buffers`
- `min_wal_size`
- `max_wal_size`

Настройте эти параметры в соответствии с *официальной инструкцией* (на английском).

8. Смените у конфигурационного файла владельца и группу на `postgres`:

```
chown postgres:postgres /u01/postgres/iwtm-postgres.conf
```

9. Добавьте в конфигурационный файл `/u01/postgres/postgresql.conf` ссылку на файл `iwtm-postgres.conf` с помощью команды:

```
echo "include = 'iwtm-postgres.conf'" >> /u01/postgres/postgresql.conf
```

10. Настройте файл доступа `pg_hba.conf` с помощью команд:

```
sed -i "s|local[[:space:]]*all[[:space:]]*all[[:space:]]*peer|local   all             all
                                  trust|" /u01/postgres/pg_hba.conf
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*127.0.0.1/32[[:space:]]*ident|host
  all             all             127.0.0.1/32            trust|" /u01/postgres/pg_hba.conf
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*::1/128[[:space:]]*ident|host
all             all             ::1/128                 trust|" /u01/postgres/pg_hba.conf
echo "# Enable not local access" >> /u01/postgres/pg_hba.conf
echo "host    postgres        all             0.0.0.0/0               md5" >> /u01/
postgres/pg_hba.conf
```

11. Запустите сервис `postgresql` и проверьте его статус с помощью команд:

```
systemctl enable postgresql-15
systemctl start postgresql-15
systemctl status postgresql-15
```

12. Измените для администратора базы данных пароль по умолчанию:

```
su - postgres
psql -p 5433
alter user postgres password 'xxXX1234';
```

13. Создайте нужные расширения, выполнив запросы:

```
create extension if not exists adminpack;
create extension if not exists dblink;
create extension if not exists lo;
create extension if not exists xml2;
create extension if not exists tablefunc;
create extension if not exists intarray;
create extension if not exists file_fdw;
create extension if not exists "uuid-ossp";
create extension if not exists pgcrypto;
create extension if not exists pgrowlocks;
create extension if not exists autoinc;
create extension if not exists hstore;
create extension if not exists pg_stat_statements;
create extension if not exists pg_buffercache;
create extension if not exists pgagent;
```

14. Для выхода введите команды:

```
\q
exit
```

15. Для настройки в ОС пользователя `pgagent` выполните команды:

```
mkdir /home/pgagent
touch /home/pgagent/.pgpass
echo "127.0.0.1:5433:postgres:postgres:xxXX1234" > /home/pgagent/.pgpass
chmod 0600 /home/pgagent/.pgpass
chown pgagent:pgagent /home/pgagent/.pgpass
usermod -s /bin/bash pgagent
```

16. Создайте или отредактируйте файл `/etc/sudoers.d/pgagent`, чтобы его содержимое соответствовало образцу:

```
# allow pgagent to execute any command
pgagent ALL = (postgres) NOPASSWD: ALL
Defaults:pgagent !requiretty
```

> **Важно!**
>
> Пустая строка в конце файла `pgagent` обязательна.

17. Измените для `/etc/sudoers.d/pgagent` права, владельца и группу, выполнив команды:

```
chmod 440 /etc/sudoers.d/pgagent
chown root:root /etc/sudoers.d/pgagent
```

18. В конфигурационном файле `/etc/pgagent/pgagent_15.conf` измените значение параметра `DBPORT` с `5432` на `5433`:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent_15.conf
```

19. Запустите сервис `pgagent` и проверьте его статус с помощью команд:

```
systemctl enable pgagent_15
systemctl start pgagent_15
systemctl status pgagent_15
```

По завершении настройки убедитесь в отсутствии критических ошибок в логах базы данных и `/var/log/pgagent_15.log`.

2.4.3 Настройка СУБД Postgres Pro Enterprise

Чтобы подготовить удаленную базу данных к установке компонентов Traffic Monitor, выполните на сервере базы данных следующие действия:

1. Установите дополнительный пакет, выполнив команду:

```
yum -y install postgrespro-ent-15-contrib
```

2. Остановите работу сервиса `postgrespro` с помощью команды:

```
systemctl stop postgrespro-ent-15.service
```

3. Создайте или дополните файл `/etc/systemd/system/postgrespro-ent-15.service.d/override.conf` следующим содержимым:

```
[Service]
Environment=PGDATA=/u01/postgres
```

4. Для применения изменений в конфигурации сервиса выполните команду:

```
systemctl daemon-reload
```

5. Создайте директории для файлов и архивов, инициализируйте базу данных и смените директориям владельца и группу на `postgres`:

```
mkdir -p /u01/postgres
chown postgres:postgres /u01/postgres
sudo -u postgres initdb --encoding=UTF8 --locale=en_US.UTF-8 -D /u01/postgres
mkdir -p /u01/postgres/tmp
```

6. Создайте конфигурационный файл `/u01/postgres/iwtm-postgres.conf`. Например, с помощью команды:

```
touch /u01/postgres/iwtm-postgres.conf
```

7. Добавьте в файл `/u01/postgres/iwtm-postgres.conf`:

```
# ----------------------------
# Postgres Pro configuration file
# ----------------------------
#
# IWTM custom values

listen_addresses = '*'
port = 5433
max_connections = 1000                    # (change requires restart)
tcp_keepalives_idle = 60                  # TCP_KEEPIDLE, in seconds'
tcp_keepalives_interval = 20              # TCP_KEEPINTVL, in seconds'
tcp_keepalives_count = 2                  # TCP_KEEPCNT

shared_buffers = 128kB

huge_pages = try                          # on, off, or try

max_locks_per_transaction = 512
temp_buffers = 32MB
work_mem = 16MB
effective_cache_size = 4096MB

min_wal_size = 6144MB
max_wal_size = 6144MB
lc_messages = 'en_US.UTF-8'               # locale for system error message
log_directory = 'pg_log'
log_filename = 'postgresql.log'           # log file name pattern
log_rotation_age = 0                      # Automatic rotation of logfiles will happen
after that time. 0 disables.
log_rotation_size = 0                     # Automatic rotation of logfiles will happen
after that much log output. 0 disables.
log_min_duration_statement = 120000       # -1 is disabled, 0 logs all statements
track_activity_query_size = 32768         # (change requires restart)
log_autovacuum_min_duration = 30000       # -1 disables, 0 logs all actions and
# stats_temp_directory = '/var/lib/pgpro/ent-15/data/pg_stat_tmp'

autovacuum_max_workers = 5
autovacuum_naptime = 20
maintenance_work_mem = 1GB
autovacuum_freeze_max_age = 10000000000

shared_preload_libraries = 'pg_stat_statements'
track_io_timing = on
track_activity_query_size = 32768

constraint_exclusion = off                # on, off, or partition
```

```
standard_conforming_strings = on
```

Важно!

В образце содержимого конфигурационного файла указаны примерные значения этих параметров:

- `shared_buffers`
- `work_mem`
- `maintenance_work_mem`
- `effective_cache_size`
- `temp_buffers`
- `min_wal_size`
- `max_wal_size`

Настройте эти параметры под вашу систему в соответствии с *официальной инструкцией*.

8. Смените у конфигурационного файла владельца и группу на `postgres`:

```
chown postgres:postgres /u01/postgres/iwtm-postgres.conf
```

9. Добавьте в конфигурационный файл `/u01/postgres/`**`postgresql.conf`** ссылку на файл **`iwtm-postgres.conf`**.
Вы можете сделать это командой:

```
echo "include = 'iwtm-postgres.conf'" >> /u01/postgres/postgresql.conf
```

10. Отредактируйте файл доступа `/u01/postgres/`**`pg_hba.conf`**:
    a. После строк:

```
# IPv6 local connections:
host    all             all             ::1/128                 md5
```

добавьте строку:

```
host    postgres        all             0.0.0.0/0               md5
```

Примечание:

Указанные значения подходят для установки Traffic Monitor с параметрами по умолчанию. Если при установке Traffic Monitor вы будете использовать другие значения, укажите их здесь.

    b. Замените строки с помощью команд:

```
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*127.0.0.1/32[[:space:]]*md5|
host    all             all             127.0.0.1/32            trust|" /u01/
postgres/pg_hba.conf
sed -i "s|local[[:space:]]*all[[:space:]]*all[[:space:]]*peer|local   all
all                                     trust|" /u01/postgres/pg_hba.conf
```

11. **Если вы выполняете настройку на сервере под управлением РЕД ОС:**
    a. Перейдите в директорию:

    ```
    cd /usr/lib/systemd/system
    ```

    b. Переименуйте сервисный файл:

    ```
    mv postgrespro-ent-15.service postgresql-15.service
    ```

    c. Перезагрузите сервер:

    ```
    reboot
    ```

    d. Запустите сервис:

    ```
    systemctl start postgresql-15.service
    ```

    e. Перейдите в вашу рабочую директорию.
    В нашем примере:

    ```
    cd /distr
    ```

    f. Скопируйте в директорию входящий в комплект поставки архив **`iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz`** .
    g. Распакуйте архив с помощью команды:

    ```
    tar -xvf iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz
    ```

    В нашем примере:

    ```
    tar -xvf iwtm-postgresql-15.14-7.10.0.97-redos-7.3.tar.gz
    ```

    h. Перейдите в директорию с содержимым архива.
    i. Установите пакет с помощью команды:

    ```
    yum install pgagent_15-4.2.2-0.el7.iw.x86_64.rpm
    ```

Если вы выполняете настройку на сервере под управлением ОС Red Hat Enterprise Linux:

a. Запустите сервис:

```
systemctl start postgrespro-ent-15.service
```

b. Скачайте по ссылке пакет `pgagent_15-4.2.2-3.rhel7.x86_64.rpm`.
c. Установите пакет с помощью команды:

```
yum install pgagent_15-4.2.2-3.rhel7.x86_64.rpm
```

12. Измените для администратора базы данных пароль по умолчанию:

```
su - postgres
psql -p 5433
alter user postgres password 'xxXX1234';
```

13. Создайте нужные расширения, выполнив запросы:

```
create extension if not exists adminpack;
create extension if not exists dblink;
create extension if not exists lo;
create extension if not exists xml2;
create extension if not exists tablefunc;
create extension if not exists intarray;
create extension if not exists file_fdw;
create extension if not exists "uuid-ossp";
create extension if not exists pgcrypto;
create extension if not exists pgrowlocks;
create extension if not exists autoinc;
create extension if not exists hstore;
create extension if not exists pg_stat_statements;
create extension if not exists pg_buffercache;
create extension if not exists pgagent;
```

14. Для выхода введите команды:

```
\q
exit
```

15. Для настройки в ОС пользователя `pgagent` выполните команды:

```
touch /home/pgagent/.pgpass
echo "127.0.0.1:5433:postgres:postgres:xxXX1234" > /home/pgagent/.pgpass
chmod 0600 /home/pgagent/.pgpass
chown pgagent:pgagent /home/pgagent/.pgpass
```

```
usermod -s /bin/bash pgagent
```

16. Создайте `/etc/sudoers.d/iw-pgagent` со следующим содержимым:

```
# allow pgagent to execute any command
pgagent ALL = (postgres) NOPASSWD: ALL
Defaults:pgagent !requiretty
```

17. Измените для `/etc/sudoers.d/iw-pgagent` права, владельца и группу, выполнив команды:

```
chmod 440 /etc/sudoers.d/iw-pgagent
chown root:root /etc/sudoers.d/iw-pgagent
```

18. Отредактируйте конфигурационный файл `/etc/pgagent/pgagent_15.conf` с помощью команд:
    - **На ОС Red Hat Enterprise Linux**:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent_15.conf
echo "LD_LIBRARY_PATH=/opt/pgpro/ent-15/lib" >> /etc/pgagent/pgagent_15.conf
```

    - **На РЕД ОС**:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent-15.conf
echo "LD_LIBRARY_PATH=/opt/pgpro/ent-15/lib" >> /etc/pgagent/pgagent-15.conf
```

19. Включите сервис `pgagent`, запустите его, а затем проверьте его статус с помощью команд:
    - **На ОС Red Hat Enterprise Linux**:

```
systemctl enable pgagent_15
systemctl start pgagent_15
systemctl status pgagent_15
```

    - **На РЕД ОС**:

```
systemctl enable pgagent-15
systemctl start pgagent-15
systemctl status pgagent-15
```

20. Создайте директорию `/u02`:

```
mkdir /u02
```

21. Смонтируйте в директорию `/u02` дисковое хранилище.
22. Создайте директории для табличных пространств и смените владельца и группу на `postgres`:

```
mkdir /u02/pgdata
mkdir /u02/pgdata1
mkdir /u02/arch
chown -R postgres:postgres /u02
```

По завершении настройки убедитесь в отсутствии критических ошибок в логах базы данных и `/var/log/pgagent_15.log` или `/var/log/pgagent-15.log`.

2.4.4 Настройка СУБД Jatoba

Чтобы подготовить удаленную базу данных к установке компонентов Traffic Monitor, выполните на сервере базы данных следующие действия:

1. Установите дополнительный пакет, выполнив команду:

```
yum -y install jatoba5-contrib
```

2. Создайте или дополните файл `/etc/systemd/system/jatoba-5.service.d/override.conf` следующим содержимым:

```
[Service]
Environment=PGDATA=/u01/postgres
```

3. Для применения изменений в конфигурации сервиса выполните команду:

```
systemctl daemon-reload
```

4. Создайте директории для файлов и архивов, смените директориям владельца и группу на `postgres`. Используйте команды:

```
mkdir -p /u01/postgres
chown postgres:postgres /u01/postgres
mkdir -p /u02/pgdata
mkdir -p /u02/pgdata1
mkdir -p /u02/arch
chown -R postgres:postgres /u02
```

5. Инициализируйте базу данных. Для этого:
   a. Перейдите в директорию `/usr/jatoba-5/bin/`:

```
cd /usr/jatoba-5/bin/
```

   b. Используйте команду инициализации:

```
PGSETUP_INITDB_OPTIONS=" --encoding=UTF8" ./jatoba-setup initdb jatoba-5 --
encoding=UTF8 --locale=en_US.UTF-8 -D /u01/postgres
```

6. Создайте временную директорию и смените владельца и группу на `postgres`. Используйте команды:

```
mkdir -p /u01/postgres/tmp
chown postgres:postgres /u01/postgres/tmp
```

> **Важно!**
>
> Создание временной директории `tmp` допустимо только после инициализации базы данных.

7. В директории `/u01/postgres/` создайте конфигурационный файл `iwtm-postgres.conf`:

```
touch /u01/postgres/iwtm-postgres.conf
```

8. Добавьте в файл `iwtm-postgres.conf`:

```
# ------------------------------
# PostgreSQL configuration file
# ------------------------------
#
# IWTM custom values

listen_addresses = '*'
port = 5433
max_connections = 1000                  # (Change requires restart)
tcp_keepalives_idle = 60                # TCP_KEEPIDLE, in seconds'
tcp_keepalives_interval = 20            # TCP_KEEPINTVL, in seconds'
tcp_keepalives_count = 2                # TCP_KEEPCNT

shared_buffers = kB                     # min 128KiB

huge_pages = try                        # on, off, or try

max_locks_per_transaction = 256
temp_buffers = MB
work_mem = MB
effective_cache_size = MB

min_wal_size = MB
max_wal_size = MB
lc_messages = 'en_US.UTF-8'             # Locale for system error message
log_directory = 'pg_log'
log_filename = 'postgresql.log'         # Log file name pattern
log_rotation_age = 0                    # Automatic rotation of logfiles will happen
after that time. 0 disables.
```

```
log_rotation_size = 0                       # Automatic rotation of logfiles will happen
after that much log output. 0 disables.
log_min_duration_statement = 120000         # -1 is disabled, 0 logs all statements
track_activity_query_size = 32768           # (Change requires restart)
log_autovacuum_min_duration = 30000         # -1 disables, 0 logs all actions and

autovacuum_max_workers = 5
autovacuum_naptime = 20
max_parallel_maintenance_workers = 8
maintenance_work_mem = MB
autovacuum_freeze_max_age = 1000000000

shared_preload_libraries = 'pg_stat_statements'
track_io_timing = on
track_activity_query_size = 32768

constraint_exclusion = off                  # on, off, or partition
standard_conforming_strings = on
```

Важно!

В примере содержимого конфигурационного файла указаны пустые поля значений параметров:

- `shared_buffers`
- `work_mem`
- `maintenance_work_mem`
- `effective_cache_size`
- `temp_buffers`
- `min_wal_size`
- `max_wal_size`

Настройте эти параметры в соответствии с *официальной инструкцией* (на английском).

9. Смените у конфигурационного файла владельца и группу на `postgres`:

```
chown postgres:postgres /u01/postgres/iwtm-postgres.conf
```

10. Добавьте в конфигурационный файл `/u01/postgres/postgresql.conf` ссылку на файл `iwtm-postgres.conf` с помощью команды:

```
echo "include = 'iwtm-postgres.conf'" >> /u01/postgres/postgresql.conf
```

11. Настройте файл доступа `pg_hba.conf` с помощью команд:

```
sed -i "s|local[[:space:]]*all[[:space:]]*all[[:space:]]*peer|local   all             all
                                    trust|" /u01/postgres/pg_hba.conf
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*127.0.0.1/32[[:space:]]*ident|host
  all             all             127.0.0.1/32            trust|" /u01/postgres/pg_hba.conf
```

```
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*::1/128[[:space:]]*ident|host
all             all             ::1/128                 trust|" /u01/postgres/pg_hba.conf
echo "# Enable not local access" >> /u01/postgres/pg_hba.conf
echo "host    postgres        all             0.0.0.0/0               md5" >> /u01/
postgres/pg_hba.conf
```

12. Активируйте СУБД согласно руководству по установке СУБД Jatoba.
13. Запустите сервис `jatoba-5` и проверьте его статус. Используйте команды:

```
systemctl enable jatoba-5
systemctl start jatoba-5
systemctl status jatoba-5
```

14. Установите pgAgent из репозитория ОС с помощью команды:

```
yum install pgagent_15
```

15. Перенесите файлы для установки расширений из каталога **`postgresql-15`** в каталог **`jatoba`**. Для этого:
    a. Перейдите в `/usr/pgsql-15/share/`:

    ```
    cd /usr/pgsql-15/share
    ```

    b. Используйте команды смены директорий:

    ```
    cp -R pgagent_15-x.x.x /usr/jatoba-5/share/
    cp extension/* /usr/jatoba-5/share/extension/
    ```

    Важно!

    В первой команде замените имя `pgagent_15-x.x.x` на точное название каталога, расположенного в директории `/usr/jatoba-5/share/`. Например, `pgagent_15-4.0.0`.

16. Измените пароль по умолчанию для администратора базы данных. Используйте команды:

```
su - postgres
psql -p 5433
alter user postgres password 'xxXX1234';
```

17. Создайте расширения, выполнив запросы:

```
create extension if not exists adminpack;
```

```
create extension if not exists dblink;
create extension if not exists lo;
create extension if not exists xml2;
create extension if not exists tablefunc;
create extension if not exists intarray;
create extension if not exists file_fdw;
create extension if not exists "uuid-ossp";
create extension if not exists pgcrypto;
create extension if not exists pgrowlocks;
create extension if not exists autoinc;
create extension if not exists hstore;
create extension if not exists pg_stat_statements;
create extension if not exists pg_buffercache;
create extension if not exists pgagent;
```

18. Для выхода введите команды:

```
\q
exit
```

19. Для настройки в ОС пользователя pgAgent выполните команды:

```
mkdir /home/pgagent
touch /home/pgagent/.pgpass
echo "127.0.0.1:5433:postgres:postgres:xxXX1234" > /home/pgagent/.pgpass
chmod 0600 /home/pgagent/.pgpass
chown pgagent:pgagent /home/pgagent/.pgpass
usermod -s /bin/bash pgagent
```

20. Создайте или отредактируйте файл `/etc/sudoers.d/**pgagent**`, чтобы содержимое соответствовало образцу:

```
# allow pgagent to execute any command
pgagent ALL = (postgres) NOPASSWD: ALL
Defaults:pgagent !requiretty
```

21. Измените у файла `/etc/sudoers.d/**pgagent**` права, владельца и группу, выполнив команды:

```
chmod 440 /etc/sudoers.d/pgagent
chown root:root /etc/sudoers.d/pgagent
```

22. В конфигурационном файле `/etc/pgagent/**pgagent_15.conf**` измените значение параметра `DBPORT` с `5432` на `5433`:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent_15.conf
```

23. Запустите сервис `pgagent_15` и проверьте его статус с помощью команд:

```
systemctl enable pgagent_15
systemctl start pgagent_15
systemctl status pgagent_15
```

По завершении настройки убедитесь в отсутствии критических ошибок в логах базы данных и `/var/log/pgagent_15.log`.

2.4.5 Настройка СУБД Pangolin

Чтобы подготовить удаленную базу данных к установке компонентов Traffic Monitor, выполните на сервере базы данных следующие действия:

1. Установите дополнительный пакет с помощью команды:

```
dnf install postgresql-contrib
```

2. Создайте файл `/usr/lib/systemd/system/postgresql-15.service` со следующим содержимым:

```
[Unit]
Description=PostgreSQL 15 Database Server
After=network.target

[Service]
Type=simple
User=postgres
Group=postgres

# Путь к данным PostgreSQL
Environment=PGDATA=/u01/postgres

# Путь к postmaster
ExecStart=/usr/pangolin/bin/postmaster -D ${PGDATA} -p 5433

# Перезагрузка и остановка
ExecReload=/bin/kill -HUP $MAINPID
TimeoutSec=300

[Install]
WantedBy=multi-user.target
```

3. Для применения изменений в конфигурации сервиса выполните команду:

```
systemctl daemon-reload
```

4. Создайте директории для файлов и архивов, смените директориям владельца и группу на `postgres`. Используйте команды:

```
mkdir -p /u01/postgres
chown postgres:postgres /u01/postgres
mkdir -p /u02/pgdata
mkdir -p /u02/pgdata1
mkdir -p /u02/arch
chown -R postgres:postgres /u02
```

5. Инициализируйте базу данных с помощью команд:

```
export PGSETUP_INITDB_OPTIONS=" --encoding=UTF8"
sudo -u postgres /usr/pangolin/bin/initdb --encoding=UTF8 --locale=en_US.UTF-8 -D /u01/
postgres/
```

6. Создайте временную директорию и смените владельца и группу на `postgres` с помощью команды:

```
mkdir -p /u01/postgres/tmp
chown postgres:postgres /u01/postgres/tmp
```

> **Важно!**
>
> Создание временной директории `tmp` допустимо только после инициализации базы данных.

7. В директории `/u01/postgres/` создайте конфигурационный файл `iwtm-postgres.conf`:

```
touch /u01/postgres/iwtm-postgres.conf
```

8. Добавьте в файл `iwtm-postgres.conf`:

```
# -----------------------------
# PostgreSQL configuration file
# -----------------------------
#
# IWTM custom values

listen_addresses = '*'
port = 5433
max_connections = 1000                  # (Change requires restart)
tcp_keepalives_idle = 60                # TCP_KEEPIDLE, in seconds'
tcp_keepalives_interval = 20            # TCP_KEEPINTVL, in seconds'
tcp_keepalives_count = 2                # TCP_KEEPCNT

shared_buffers = kB                     # min 128KiB
```

```
huge_pages = try                        # on, off, or try

max_locks_per_transaction = 256
temp_buffers = MB
work_mem = MB
effective_cache_size = MB

min_wal_size = MB
max_wal_size = MB
lc_messages = 'en_US.UTF-8'             # Locale for system error message
log_directory = 'pg_log'
log_filename = 'postgresql.log'         # Log file name pattern
log_rotation_age = 0                    # Automatic rotation of logfiles will happen
after that time. 0 disables.
log_rotation_size = 0                   # Automatic rotation of logfiles will happen
after that much log output. 0 disables.
log_min_duration_statement = 120000     # -1 is disabled, 0 logs all statements
track_activity_query_size = 32768       # (Change requires restart)
log_autovacuum_min_duration = 30000     # -1 disables, 0 logs all actions and

autovacuum_max_workers = 5
autovacuum_naptime = 20
max_parallel_maintenance_workers = 8
maintenance_work_mem = MB
autovacuum_freeze_max_age = 1000000000

shared_preload_libraries = 'pg_stat_statements'
track_io_timing = on
track_activity_query_size = 32768

constraint_exclusion = off              # on, off, or partition
standard_conforming_strings = on

enabled_extra_auth_methods = 'peer, trust, md5'
```

Важно!

В примере содержимого конфигурационного файла указаны пустые поля значений параметров:

- `shared_buffers`
- `work_mem`
- `maintenance_work_mem`
- `effective_cache_size`
- `temp_buffers`
- `min_wal_size`
- `max_wal_size`

Настройте эти параметры в соответствии с *официальной инструкцией* (на английском).

9. Смените у конфигурационного файла владельца и группу на `postgres`:

```
chown postgres:postgres /u01/postgres/iwtm-postgres.conf
```

10. Добавьте в конфигурационный файл `/u01/postgres/postgresql.conf` ссылку на файл `iwtm-postgres.conf` с помощью команды:

```
echo "include = 'iwtm-postgres.conf'" >> /u01/postgres/postgresql.conf
```

11. Настройте файл доступа `pg_hba.conf` с помощью команд:

```
sed -i "s|local[[:space:]]*all[[:space:]]*all[[:space:]]*peer|local   all             all
                                  trust|" /u01/postgres/pg_hba.conf
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*127.0.0.1/32[[:space:]]*ident|host
  all             all             127.0.0.1/32            trust|" /u01/postgres/pg_hba.conf
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*::1/128[[:space:]]*ident|host
all             all             ::1/128                 trust|" /u01/postgres/pg_hba.conf
echo "# Enable not local access" >> /u01/postgres/pg_hba.conf
echo "host    postgres        all             0.0.0.0/0               md5" >> /u01/
postgres/pg_hba.conf
```

12. Запустите сервис `postgresql-15` и проверьте его статус с помощью команды:

```
systemctl enable postgresql-15
systemctl start postgresql-15
systemctl status postgresql-15
```

13. Установите pgAgent из репозитория ОС с помощью команды:

```
dnf install pgagent_15
```

14. Перенесите файлы для установки расширений из каталога `postgresql-15` в каталог pangolin с помощью команды:

```
cp /usr/pgsql-15/share/extension/pgagent* /usr/pangolin/share/extension
```

15. Измените пароль по умолчанию для администратора базы данных с помощью команды:

```
su - postgres
psql -p 5433
alter user postgres password 'xxXX1234';
```

16. Создайте расширения с помощью запросов:

```
create extension if not exists adminpack;
create extension if not exists dblink;
```

```
create extension if not exists lo;
create extension if not exists xml2;
create extension if not exists tablefunc;
create extension if not exists intarray;
create extension if not exists file_fdw;
create extension if not exists "uuid-ossp";
create extension if not exists pgcrypto;
create extension if not exists pgrowlocks;
create extension if not exists autoinc;
create extension if not exists hstore;
create extension if not exists pg_stat_statements;
create extension if not exists pg_buffercache;
create extension if not exists pgagent;
```

17. Для выхода введите команды:

```
\q
exit
```

18. Для настройки в ОС пользователя pgAgent выполните команды:

```
mkdir /home/pgagent
touch /home/pgagent/.pgpass
echo "127.0.0.1:5433:postgres:postgres:xxXX1234" > /home/pgagent/.pgpass
chmod 0600 /home/pgagent/.pgpass
chown pgagent:pgagent /home/pgagent/.pgpass
usermod -s /bin/bash pgagent
```

19. Создайте или отредактируйте файл `/etc/sudoers.d/pgagent`, чтобы содержимое соответствовало образцу:

```
# allow pgagent to execute any command
pgagent ALL = (postgres) NOPASSWD: ALL
Defaults:pgagent !requiretty
```

20. Измените у файла `/etc/sudoers.d/pgagent` права, владельца и группу с помощью команды:

```
chmod 440 /etc/sudoers.d/pgagent
chown root:root /etc/sudoers.d/pgagent
```

21. В конфигурационном файле `/etc/pgagent/pgagent_15.conf` измените значение параметра `DBPORT` с `5432` на `5433`:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent_15.conf
```

22. Запустите сервис `pgagent_15` и проверьте его статус с помощью команд:

```
systemctl enable pgagent_15
systemctl start pgagent_15
systemctl status pgagent_15
```

По завершении настройки убедитесь в отсутствии критических ошибок в логах базы данных и `/var/log/pgagent_15.log`.

2.4.6 Настройка СУБД Tantor

Чтобы подготовить удаленную базу данных к установке компонентов Traffic Monitor, выполните на сервере базы данных следующие действия:

1. Остановите работу сервиса `tantor-be-server-15` с помощью команды:

```
systemctl stop tantor-be-server-15.service
```

2. Скопируйте в директорию `/var/lib/postgresql/tantor-be-15/data/` имеющийся конфигурационный файл **`iwtm-postgres.conf`** или создайте там новый со следующим содержимым:

```
# ----------------------------
# Tantor configuration file
# ----------------------------
#
# IWTM custom values

listen_addresses = '*'
port = 5433
max_connections = 1000                  # (change requires restart)
tcp_keepalives_idle = 60                # TCP_KEEPIDLE, in seconds'
tcp_keepalives_interval = 20            # TCP_KEEPINTVL, in seconds'
tcp_keepalives_count = 2                # TCP_KEEPCNT

shared_buffers = 128kB

huge_pages = try                        # on, off, or try

max_locks_per_transaction = 512
temp_buffers = 32MB
work_mem = 16MB
effective_cache_size = 4096MB

min_wal_size = 6144MB
max_wal_size = 6144MB
lc_messages = 'en_US.UTF-8'             # locale for system error message
log_directory = 'pg_log'
log_filename = 'postgresql.log'         # log file name pattern
log_rotation_age = 0                    # Automatic rotation of logfiles will happen
after that time. 0 disables.
```

```
log_rotation_size = 0                       # Automatic rotation of logfiles will happen
after that much log output. 0 disables.
log_min_duration_statement = 120000         # -1 is disabled, 0 logs all statements
track_activity_query_size = 32768           # (change requires restart)
log_autovacuum_min_duration = 30000         # -1 disables, 0 logs all actions and
# stats_temp_directory = '/var/lib/postgresql/tantor-be-15/data/pg_stat_tmp'

autovacuum_max_workers = 5
autovacuum_naptime = 20
maintenance_work_mem = 1GB
autovacuum_freeze_max_age = 1000000000

#shared_preload_libraries =  'pg_stat_statements'
track_io_timing = on
track_activity_query_size = 32768

constraint_exclusion = off                  # on, off, or partition
standard_conforming_strings = on
```

Важно!

В образце содержимого конфигурационного файла указаны примерные значения параметров:

- `shared_buffers`
- `work_mem`
- `maintenance_work_mem`
- `effective_cache_size`
- `temp_buffers`
- `min_wal_size`
- `max_wal_size`

Настройте эти параметры под вашу систему в соответствии с *официальной инструкцией PostgreSQL*.

3. Выдайте пользователю **`postgres`** права на файл **`iwtm-postgres.conf`**.

```
chown postgres:postgres /var/lib/postgresql/tantor-be-15/data/iwtm-postgres.conf
```

4. Добавьте в конфигурационный файл `/var/lib/postgresql/tantor-be-15/data/` **`postgresql.conf`** ссылку на файл **`iwtm-postgres.conf`** с помощью команды:

```
echo "include = 'iwtm-postgres.conf'" >> /var/lib/postgresql/tantor-be-15/data/
postgresql.conf
```

5. Отредактируйте файл доступа `/var/lib/postgresql/tantor-be-15/data/` **`pg_hba.conf`**:
   a. После строк:

```
# IPv6 local connections:
host    all             all             ::1/128                 md5
```

добавьте строку:

```
host    postgres        all             0.0.0.0/0               md5
```

> **Примечание:**
>
> Указанные значения подходят для установки Traffic Monitor с параметрами по умолчанию. Если при установке Traffic Monitor вы будете использовать другие значения, укажите их здесь.

b. Замените строки с помощью команд:

```
sed -i "s|host[[:space:]]*all[[:space:]]*all[[:space:]]*127.0.0.1/32[[:space:]]*md5|
host    all             all             127.0.0.1/32            trust|" /var/lib/
postgresql/tantor-be-15/data/pg_hba.conf
sed -i "s|local[[:space:]]*all[[:space:]]*all[[:space:]]*peer|local   all
  all                                     trust|" /var/lib/postgresql/tantor-be-15/
data/pg_hba.conf
```

6. Создайте директорию `/var/lib/pgpro/ent-15/data/tmp` и назначьте ей владельца и группу с помощью команд:

```
mkdir –p /var/lib/postgresql/tantor-be-15/data/tmp
chown postgres:postgres /var/lib/postgresql/tantor-be-15/data/tmp
```

7. Установите pgAgent:
На сервере под управлением ОС Red Hat Enterprise Linux:

a. Запустите сервис Tantor:

```
systemctl start tantor-be-server-15.service
```

b. Скачайте пакет `pgagent_15-4.2.2-3.rhel7.x86_64.rpm` из *репозитория Yum*.
c. Установите пакет с помощью команды:

```
yum install pgagent_15-4.2.2-3.rhel7.x86_64.rpm
```

На сервере под управлением РЕД ОС:

a. Запустите сервис Tantor:

```
systemctl start tantor-be-server-15.service
```

b. Перейдите в рабочую директорию.
   В нашем примере:

```
cd /distr
```

c. Скопируйте в директорию входящий в комплект поставки архив **`iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz`**.
d. Распакуйте архив с помощью команды:

```
tar -xvf iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz
```

   В нашем примере:

```
tar -xvf iwtm-postgresql-15.14-7.14.0.97-redos-7.3.tar.gz
```

e. Перейдите в директорию с содержимым архива.
f. Установите пакет `pgagent_15-4.2.2-3.rhel7.x86_64.rpm` с помощью команды:

```
yum install pgagent_15-4.2.2-3.rhel7.x86_64.rpm
```

8. Скопируйте файлы расширения:

```
cp /usr/pgsql-15/share/extension/pgagent* /opt/tantor/db/15/share/postgresql/extension/
```

9. Смените пользователя на `postgres`:

```
su - postgres
```

10. Подключитесь к базе данных:

```
psql -p 5433
```

11. Измените для администратора базы данных пароль по умолчанию:

```
alter user postgres with password 'xxXX1234';
```

12. Создайте нужные расширения с помощью запросов:

```
create extension if not exists adminpack;
create extension if not exists dblink;
create extension if not exists lo;
create extension if not exists xml2;
```

```
create extension if not exists tablefunc;
create extension if not exists intarray;
create extension if not exists file_fdw;
create extension if not exists "uuid-ossp";
create extension if not exists pgcrypto;
create extension if not exists pgrowlocks;
create extension if not exists autoinc;
create extension if not exists hstore;
create extension if not exists pg_stat_statements;
create extension if not exists pg_buffercache;
create extension if not exists pgagent;
```

13. Для выхода введите команды:

```
\q
exit
```

14. Для настройки в ОС пользователя `pgagent` выполните команды:

```
mkdir /home/pgagent/
touch /home/pgagent/.pgpass
echo "127.0.0.1:5433:postgres:postgres:xxXX1234" > /home/pgagent/.pgpass
chmod 0600 /home/pgagent/.pgpass
chown pgagent:pgagent /home/pgagent/.pgpass
usermod -s /bin/bash pgagent
```

15. Создайте `/etc/sudoers.d/iw-pgagent` со следующим содержимым:

```
# allow pgagent to execute any command
pgagent ALL = (postgres) NOPASSWD: ALL
Defaults:pgagent !requiretty
```

Вы можете сделать это с помощью команд:

```
touch /etc/sudoers.d/iw-pgagent
echo "# allow pgagent to execute any command" > /etc/sudoers.d/iw-pgagent
echo "pgagent ALL = (postgres) NOPASSWD: ALL" >> /etc/sudoers.d/iw-pgagent
echo 'Defaults:pgagent !requiretty' >> /etc/sudoers.d/iw-pgagent
```

16. Измените для `/etc/sudoers.d/iw-pgagent` права, владельца и группу, выполнив команды:

```
chmod 440 /etc/sudoers.d/iw-pgagent
chown root:root /etc/sudoers.d/iw-pgagent
```

17. Отредактируйте конфигурационный файл `/etc/pgagent/pgagent_15.conf`:

На сервере под управлением ОС Red Hat Enterprise Linux:

Используйте команды:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent_15.conf
echo "LD_LIBRARY_PATH=/opt/tantor/db/15/lib/" >> /etc/pgagent/pgagent_15.conf
```

На сервере под управлением РЕД ОС:

Используйте команды:

```
sed -i --follow-symlinks "s/DBPORT=5432/DBPORT=5433/" /etc/pgagent/pgagent-15.conf
echo "LD_LIBRARY_PATH=/opt/tantor/db/15/lib" >> /etc/pgagent/pgagent-15.conf
```

18. Включите сервис pgAgent, запустите его, а затем проверьте его статус:
На сервере под управлением ОС Red Hat Enterprise Linux:

Используйте команды:

```
systemctl enable pgagent_15
systemctl start pgagent_15
systemctl status pgagent_15
```

На сервере под управлением РЕД ОС:

a. Включите сервис:

```
systemctl enable pgagent-15
```

b. Внесите изменения в файл `/etc/systemd/system/multi-user.target.wants/pgagent-15.service`.
В разделе `Unit` в строках:

```
After=postgresql-15.service
BindsTo=postgresql-15.service
```

замените `postgresql-15.service` на `tantor-be-server-15.service`:

```
After=tantor-be-server-15.service
BindsTo=tantor-be-server-15.service
```

c. Запустите сервис и проверьте его статус:

```
systemctl start pgagent-15
systemctl status pgagent-15
```

19. Создайте директорию `/u02`:

```
mkdir /u02
```

20. Создайте директории для табличных пространств и смените владельца и группу на `postgres`:

```
mkdir /u02/pgdata
mkdir /u02/pgdata1
mkdir /u02/arch
chown -R postgres:postgres /u02
```

По завершении настройки убедитесь в отсутствии критических ошибок в логах базы данных и `/var/log/**pgagent_15.log**` или `/var/log/**pgagent-15.log**`.

3 Установка Системы

Этот раздел содержит инструкции для каждого из типов установки Системы.

Инструкция по установке внешнего хранилища бинарных данных Data Storage есть в статье *Установка Data Storage*.

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.

Примечание:

Установка Traffic Monitor не поддерживается при подключении к серверу с помощью HP Integrated Lights Out (ILO).

Для установки с помощью инсталлятора Traffic Monitor используются шаблоны. Набор активных компонентов будет различаться в зависимости от целевого назначения сервера.
О выборе типа установки и шаблонах см. *Схемы развертывания Системы и выбор типа установки*.

Кроме установки из консоли сервера, вы можете воспользоваться графическим режимом инсталлятора. Запуск инсталлятора в графическом режиме описан в статьях по установке.

Инсталлятор также позволяет устанавливать Traffic Monitor в тихом режиме и с использованием файла параметров (файл `.options`). Вы можете подготовить файлы, в которых будут указаны все запрашиваемые в процессе установки параметры. Затем нужно скопировать их вместе с дистрибутивами Traffic Monitor на серверы, где планируется развертывание Системы. После этого вы можете запустить на серверах установку в тихом режиме, указав соответствующие файлы с параметрами. В сочетании с системой шаблонов установки, такой подход позволяет сократить участие пользователя в первичном развертывании Traffic Monitor.

Информация по типам установки доступна в статьях:

- Установка InfoWatch Traffic Monitor:
  - Установка TM Enterprise и TM Standard в режиме "Все-в-одном";
  - Распределенная установка TM Enterprise;
  - Установка в тихом режиме с файлом параметров.

Примечание:

Установка InfoWatch Device Monitor описана в документе *InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию*.

Примечание:

В процессе установки IW Traffic Monitor будут выполнены действия, требующие прав sysdba:

при использовании СУБД Oracle

- Создание триггера iwtm_logon_trg, который нужен для доступа пользователей iwtm_linux и iwtm_web к объектам схемы iwtm;
- Создание процедуры sp_iwtm_execute_os_command для выполнения команд ОС при создании, удалении, архивации и восстановлении файлов табличных пространств;
- Настройка профиля пользователя по умолчанию (срок действия пароля, максимальное количество изменений пароля и максимальное количество попыток соединения);
- Настройка служебных окон планировщика dbms_scheduler;
- Отключение доступа к XDB по HTTP-протоколу;
- Отключение диспетчера dispatcher, т. к. используется выделенный сервер;
- Выдача пользователю iwtm:
  - Прав для установки, обновления и удаления схемы БД;
  - Прав для создания, удаления, архивации и восстановления табличных пространств;
  - Прав, используемых в коде продукта InfoWatch Traffic Monitor;
  - Прав для просмотра статистики БД.

при использовании СУБД PostgreSQL или СУБД, основанной на 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).

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

После окончания установки серверных компонентов работа в Консоли управления Traffic Monitor доступна через окно браузера. При этом нужно ввести URL-адрес:

- сервера Traffic Monitor – если выполнена установка "Все-в-одном";
- сервера Traffic Monitor, установленного с помощью шаблона "Веб-консоль" (где установлен пакет `web-gui`), – если компоненты Системы установлены на разные компьютеры.

3.1 Установка Data Storage

Так как внешнее хранилище бинарных данных Data Storage является частью Платформы, то для его использования нужно установить Платформу.

Если Traffic Monitor еще не установлен:

1. Установите Платформу. Это можно сделать одним из следующих способов:
   - Установить Платформу без продуктов. Этот тип установки описан в статьях:
     a. Подготовка сервера.
     b. Установка Платформы.
   - Установить платформенный продукт. В этом случае Платформа будет установлена автоматически.
     Описание установки, а также информацию о возможности установки Traffic Monitor и платформенного продукта на один сервер можно найти в документации на этот продукт.
2. Установите Traffic Monitor. В ходе установки введите параметры соединения с Data Storage.
   Один из таких параметров – это токен авторизации Data Storage.

   > **Важно!**
   >
   > В целях повышения безопасности не рекомендуем использовать значение токена по умолчанию.

   Проверить актуальное значение токена можно:
   - На сервере Data Storage с помощью командной строки. Для этого:
     1. Перейдите в директорию, куда был распакован дистрибутив Платформы;
     2. Выполните команду:
        `./setup.py tokens list`
        В результате будет выведен список токенов для подключения к Платформе. Актуальный токен авторизации Data Storage будет указан напротив сущности DataStorageUser.
     3. Если токен имеет значение по умолчанию: `1exwo92iwpczl1hy6jxy` , обновите его с помощью команды:
        `./setup.py tokens refresh DataStorageUser`
   - В консоли управления платформенного продукта, в разделе **Основные настройки** в поле **Токен для Data Storage User**.
     Доступно, если на сервере с Data Storage установлен платформенный продукт с веб-интерфейсом, и в нем есть эта настройка.
     В этом случае токен можно обновить, нажав .
3. Если Платформа установлена на один сервер с Traffic Monitor, убедитесь, что в конфигурационном файле `/opt/iw/tm5/etc/consul/consul.json` в поле `bind_addr` указан IP-адрес сервера Traffic Monitor.

Если Traffic Monitor был установлен прежде Data Storage:

1. Установите Платформу: см. шаг 1 выше.
2. Настройте соединение между Traffic Monitor и Data Storage. Подробнее см. *InfoWatch Traffic Monitor. Руководство администратора. Настройка соединения с Data Storage*.

> **Примечание:**
>
> Соединение между Traffic Monitor и Data Storage может быть настроено в случае установки *Все-в-одном* или установки сервера с помощью шаблона "База данных".

3. Если Платформа установлена на один сервер с Traffic Monitor, убедитесь, что в конфигурационном файле `/opt/iw/tm5/etc/consul/consul.json` в поле `bind_addr` указан IP-адрес сервера Traffic Monitor.

3.1.1 Подготовка сервера

Перед установкой Платформы подготовьте сервер:

1. **На сервере под управлением МОС ОС:**

   Убедитесь, что доступны официальные репозитории ОС:

   - `software`
   - `update`
   - `oss`
2. Программа установки написана на языке Python версии 2.7, поэтому для установки Платформы установите интерпретатор этого языка. Пакет с интерпретатором не входит в состав дистрибутива.
3. **На сервере под управлением Red Hat Enterprise Linux и РЕД ОС настройте SELinux.**

   Для корректной работы используемого `containerd` **обновите** политики SELinux или **отключите** систему контроля доступа:

   - **Чтобы обновить политики SELinux**, скачайте и установите пакет `container-selinux`.
     Вы можете сделать это, выполнив команду:

     ```
     dnf install container-selinux
     ```

     > **Примечание:**
     >
     > Пакет не входит в состав дистрибутива продукта.
     >
     > Пакет может отсутствовать в репозиториях. В этом случае скачайте и установите его вручную.

   - **Чтобы отключить SELinux**:
     a. Выполните команды от имени суперпользователя `root`:

        ```
        setenforce 0
        sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config
        ```

     b. Перезагрузите сервер с помощью команды:

```
reboot
```

c. Проверьте статус системы SELinux с помощью команды:

```
sestatus
```

4. Настройте правила POD сети или отключите межсетевой экран (см. *Конфликты при взаимодействии службы firewalld и Kubernetes* и *Полное отключение межсетевого экрана*). В противном случае установка Платформы будет невозможна.
5. Если вы используете антивирус, настройте его для совместной работы с Платформой (см. *Настройка антивируса для продуктов Платформы*).
6. Платформа использует компонент Kubernetes. Для корректной установки Платформы и работы Kubernetes на сервере должен быть установлен пакет *conntrack*.
   Убедитесь, что пакет установлен. Для этого введите в командной строке:

   ```
   conntrack
   ```

   В результате будут выведены сведения о работе с модулем *conntrack* и его установленная версия.

```
Command line interface for the connection tracking system. Version 1.4.4
Usage: conntrack [commands] [options]

Commands:
  -L [table] [options]          List conntrack or expectation table
  -G [table] parameters         Get conntrack or expectation
  -D [table] parameters         Delete conntrack or expectation
  -I [table] parameters         Create a conntrack or expectation
  -U [table] parameters         Update a conntrack
  -E [table] [options]          Show events
  -F [table]                    Flush table
  -C [table]                    Show counter
  -S                            Show statistics

Tables: conntrack, expect, dying, unconfirmed

Conntrack parameters and options:
  -n, --src-nat ip                      source NAT ip
  -g, --dst-nat ip                      destination NAT ip
  -j, --any-nat ip                      source or destination NAT ip
  -m, --mark mark                       Set mark
  -c, --secmark secmark                 Set selinux secmark
  -e, --event-mask eventmask            Event mask, eg. NEW,DESTROY
  -z, --zero                            Zero counters while listing
  -o, --output type[,...]               Output format, eg. xml
  -l, --label label[,...]               conntrack labels

Expectation parameters and options:
  --tuple-src ip        Source address in expect tuple
  --tuple-dst ip        Destination address in expect tuple

Updating parameters and options:
  --label-add label     Add label
  --label-del label     Delete label

Common parameters and options:
  -s, --src, --orig-src ip              Source address from original direction
  -d, --dst, --orig-dst ip              Destination address from original direct
ion
  -r, --reply-src ip            Source addres from reply direction
  -q, --reply-dst ip            Destination address from reply direction
  -p, --protonum proto          Layer 4 Protocol, eg. 'tcp'
  -f, --family proto            Layer 3 Protocol, eg. 'ipv6'
  -t, --timeout timeout         Set timeout
  -u, --status status           Set status, eg. ASSURED
  -w, --zone value              Set conntrack zone
  --orig-zone value             Set zone for original direction
  --reply-zone value            Set zone for reply direction
  -b, --buffer-size             Netlink socket buffer size
  --mask-src ip                 Source mask address
  --mask-dst ip                 Destination mask address
```

Если *conntrack* не установлен, установите его с помощью команды:

- **Red Hat Enterprise Linux, Oracle Linux, РЕД ОС:**

```
dnf install conntrack
```

- **ОС Альт Сервер**:

```
apt-get install conntrack-tools
```

- **МОС ОС**:

```
zypper install conntrack-tools
```

Если пакет недоступен в репозитории, скачайте его, перейдите в директорию с пакетом и установите вручную с помощью команды вида:

- **Red Hat Enterprise Linux, Oracle Linux, РЕД ОС:**

```
rpm -Uhv ./<имя_пакета>
```

- **ОС Альт Сервер**:

```
rpm -Uhv ./<имя_пакета>
```

- **МОС ОС**:

```
zypper install <имя_пакета>
```

7. **На сервере под управлением МОС ОС:**

   Установите пакеты `socat`, `ethtool`, `app_armor` и `sysctl` с зависимостями:

```
zypper install socat
zypper install ethtool
zypper install patterns-base-apparmor
zypper install procps
zypper install libprocps7
```

8. **На сервере под управлением ОС Альт Сервер:**

   Установите пакеты:

   - `python-modules-json`
   - `python-modules-distutils`
   - `python-modules-sqlite3`

9. **Если вы устанавливаете Платформу на сервер, где уже установлен Traffic Monitor с локальной базой данных, отключите Huge Pages. Для этого:**

   a. Остановите Систему, выполнив команду:

```
iwtm stop
```

   b. Остановите работу СУБД.

   - Если вы используете СУБД PostgreSQL на компьютере под управлением ОС Red Hat Enterprise Linux, РЕД ОС или Oracle, выполните команды следующего вида:

```
systemctl stop pgagent-15
systemctl stop postgresql-15
```

   - Если вы используете СУБД PostgreSQL на компьютере под управлением ОС Альт Сервер, выполните команды следующего вида:

```
systemctl stop pgagent
systemctl stop postgresql
```

   - Если вы используете СУБД Oracle:

     i. Откройте Oracle SQL*Plus и подключитесь как пользователь **sysdba**:

```
sqlplus / as sysdba
```

ii. Выполните команду:

```
dbshut $ORACLE_HOME
```

c. Задайте нулевое значение параметру *Huge Pages*.

- В файле `/etc/sysctl.conf` вставьте строку:

```
vm.nr_hugepages=0
```

- Сохраните и примените изменения, выполнив команду:

```
sysctl -p
```

> **Примечание:**
>
> Посмотреть текущее значение *Huge Pages* можно с помощью команды:
>
> ```
> sysctl -a | grep 'huge*page'
> ```

d. Запустите СУБД.

- Если вы используете СУБД PostgreSQL на компьютере под управлением ОС Red Hat Enterprise Linux, РЕД ОС или Oracle, выполните команды следующего вида:

```
systemctl start pgagent-15
systemctl start postgresql-15
```

- Если вы используете СУБД PostgreSQL на компьютере под управлением ОС Альт Сервер, выполните команды следующего вида:

```
systemctl start pgagent
systemctl start postgresql
```

- Если вы используете СУБД Oracle:
  i. Откройте Oracle SQL*Plus и подключитесь как пользователь **sysdba**:

```
sqlplus / as sysdba
```

  ii. Выполните команду:

```
dbstart $ORACLE_HOME
```

e. Запустите Систему:

```
iwtm start
```

3.1.2 Установка Платформы

> **Важно!**
>
> Перед установкой **обязательно** подготовьте сервер (см. *Подготовка сервера*).

Установка Платформы производится вручную, с помощью командной строки.

Для установки Платформы используется архив `iw_platform.tar.xz`, который входит в состав дистрибутива Traffic Monitor. Он содержит полный набор бинарных модулей образов контейнеров, необходимых для развертывания Платформы без доступа к интернету. Также архив содержит инсталлятор.

Платформа может быть установлена в двух режимах:

- **`central`** (центральная нода);
- **`office`** (офисная нода).

Центральная и офисные ноды Платформы объединены в кластер.

Установка в режиме central

Чтобы установить Платформу в режиме `central`:

1. Выполните шаги по подготовке сервера к установке Платформы (см. *Подготовка сервера*).

   > **Примечание:**
   >
   > В ходе установки инсталлятор проверит наличие:
   >
   > - не менее 100 ГБ на диске для директорий, которые будут указаны далее в пп. 9–12. Если директории для хранения данных находятся на разных дисках, то проверится наличие 100 ГБ свободного места на каждом из них;
   > - не менее 20 ГБ на диске для директорий с образами;
   > - не менее 8 ГБ ОЗУ;
   > - не менее 2 ядер процессора;
   > - поддержки инструкции SSE 4.2;
   > - установленного пакета **`conntrack`**.

2. Создайте новую директорию на диске (например, Platform):
   `mkdir Platform`

3. Скопируйте архив `iw_platform.tar.xz` в созданную директорию.
4. Перейдите в директорию, в которую был скопирован архив.
5. Распакуйте архив с дистрибутивом Платформы в эту директорию:
   ```
   tar -xvf iw_platform.tar.xz
   ```
6. Запустите инсталлятор Платформы:
   ```
   ./setup.py install
   ```
   При необходимости укажите дополнительные параметры:
   - Для архивирования ежедневных табличных пространств задайте путь к медленному диску сервера Data Storage. Туда Система будет перемещать бинарные данные при архивировании. Для этого запустите установку Платформы с параметром `--dsslowdatapath`:
     `./setup.py install --dsslowdatapath=/root/slowdisk`
     где `/root/slowdisk` – путь к медленному диску.
     Подробнее об архивировании табличных пространств см. *InfoWatch Traffic Monitor. Руководство администратора. Архивирование ежедневных табличных пространств*.
   - Для возможности резервного копирования Data Storage запустите установку Платформы с параметром `--dsbackupspath`:
     `./setup.py install --dsbackupspath=/opt/dsbackups`
     где `/opt/dsbackups` – путь к хранилищу резервных копий.
     Подробнее о резервном копировании Data Storage см. *InfoWatch Traffic Monitor. Руководство администратора. Создание резервной копии Data Storage*.
7. Введите IP-адрес сетевого интерфейса для взаимодействия с кластером в формате IPv4: "xxx.xxx.xxx.xxx" и нажмите **Enter**.

   > **Примечание:**
   >
   > Если указать `0.0.0.0`, будут использованы все доступные сетевые интерфейсы.
   >
   > Здесь и далее для использования значений по умолчанию нажмите **Enter** без ввода значений.

8. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию: `80%`) и нажмите **Enter**.
9. Укажите путь для размещения данных Clickhouse (по умолчанию: `/opt/chdata`) и нажмите **Enter**.
10. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/opt/pgdata`) и нажмите **Enter**.
11. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
12. Укажите путь для размещения бинарных данных (по умолчанию: `/opt/dsdata`) и нажмите **Enter**.
13. Укажите путь для временного размещения событий Traffic Monitor перед их загрузкой в Платформу (по умолчанию: `/opt/factsldrtmdata`) и нажмите **Enter**.
14. Укажите порт подключения к веб-интерфейсу Платформы и нажмите **Enter**.

> **Важно!**
>
> При установке на один сервер с Traffic Monitor укажите порт, отличный от 443: по умолчанию порт 443 используется как порт подключения к веб-интерфейсу Traffic Monitor.

15. Дождитесь окончания установки Платформы.
16. Ознакомьтесь с отчетом об установке Платформы. В графе **`web ui`** указаны адрес и порт для подключения к веб-интерфейсу Платформы:

```
###Result###
Install product: Infowatch Platform(platform)
Install manifest section: central
Install node label: central
installed 41 components
updated   0 components
add ref   0 components
web ui:
https://10.60.25.54:444
```

17. Чтобы вывести на экран информацию о Платформе, выполните команду:
`./setup.py showproducts`
18. Убедитесь, что все сервисы запущены, выполнив команду:
`kubectl get pods -n infowatch`

    Команда выведет список сервисов. Каждый сервис должен иметь статус `Running`.

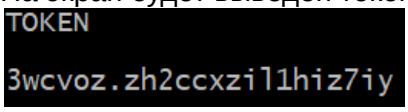
Установка в режиме office

Чтобы установить Платформу в режиме `office`:

1. Выполните шаги по подготовке сервера к установке Платформы (см. *Подготовка сервера*).

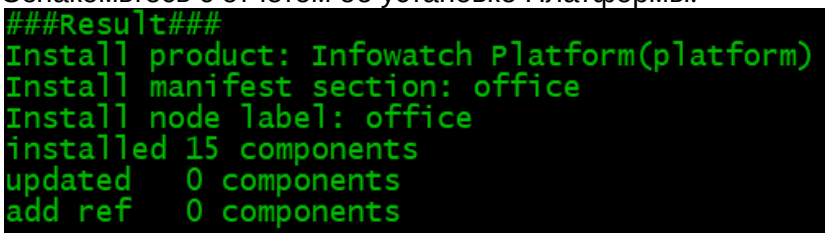
> **Примечание:**
>
> В ходе установки инсталлятор проверит наличие:
>
> - не менее 100 ГБ на диске для директорий, которые будут указаны далее в пп. 11–14. Если директории для хранения данных находятся на разных дисках, то проверится наличие 100 ГБ свободного места на каждом из них;
> - не менее 20 ГБ на диске для директорий с образами;
> - не менее 8 ГБ ОЗУ;
> - не менее 2 ядер процессора;
> - поддержки инструкции SSE 4.2;
> - установленного пакета **`conntrack`**.

2. Создайте новую директорию на диске (например, Platform):
`mkdir Platform`
3. Скопируйте архив **`iw_platform.tar.xz`** в созданную директорию.
4. Перейдите в директорию, в которую был скопирован архив.

5. Распакуйте архив с дистрибутивом Платформы в эту директорию:
   `tar -xvf iw_platform.tar.xz`
6. Запустите инсталлятор Платформы:
   `./setup.py install --nodemode=office`
   При необходимости укажите дополнительные параметры:
   - Для архивирования ежедневных табличных пространств задайте путь к медленному диску сервера Data Storage. Туда Система будет перемещать бинарные данные при архивировании. Для этого запустите установку Платформы с параметром `--dsslowdatapath`:
     `./setup.py install --nodemode=office --dsslowdatapath=/root/slowdisk`
     где `/root/slowdisk` – путь к медленному диску.
     Подробнее об архивировании табличных пространств см. *InfoWatch Traffic Monitor. Руководство администратора. Архивирование ежедневных табличных пространств*.
   - Для возможности резервного копирования Data Storage запустите установку Платформы с параметром `--dsbackupspath`:
     `./setup.py install --nodemode=office --dsbackupspath=/opt/dsbackups`
     где `/opt/dsbackups` – путь к хранилищу резервных копий.
     Подробнее о резервном копировании Data Storage см. *InfoWatch Traffic Monitor. Руководство администратора. Создание резервной копии Data Storage*.
7. Укажите адрес центральной ноды кластера в формате IP-адреса или доменного имени (например: `192.0.2.0` или `host.example.com`).
8. Укажите токен для подключения к центральной ноде.
   Чтобы получить токен:
   a. Подключитесь к серверу центральной ноды.
   b. В командной строке сервера выполните команду для получения токена:
      `kubeadm token list`
      На экран будет выведен токен:
      

      Токен в нашем примере: `3wcvoz.zh2ccxzil1hiz7iy`
9. Укажите лейбл ноды (по умолчанию: `office`) и нажмите **Enter**.
   Лейбл может состоять из букв латинского алфавита и/или цифр. Длина лейбла не должна превышать 32 символа.
10. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию: `80%`) и нажмите **Enter**.
11. Укажите путь для размещения данных Clickhouse (по умолчанию: `/opt/chdata`) и нажмите **Enter**.
12. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/opt/pgdata`) и нажмите **Enter**.
13. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
14. Укажите путь для размещения бинарных данных (по умолчанию: `/opt/dsdata`) и нажмите **Enter**.
15. Укажите путь для временного размещения событий Traffic Monitor перед их загрузкой в Платформу (по умолчанию: `/opt/factsldrtmdata`) и нажмите **Enter**.

16. Дождитесь окончания установки Платформы.
17. Ознакомьтесь с отчетом об установке Платформы.



18. Чтобы вывести на экран информацию о Платформе, выполните команду:
`./setup.py showproducts`
19. Убедитесь, что все сервисы запущены, выполнив команду:
`kubectl get pods -n infowatch`

    Команда выведет список сервисов. Каждый сервис должен иметь статус `Running`.

После установки Платформы следуйте дальнейшим инструкциям в статье *Установка Data Storage*.

См. также в этом разделе:

- Установка Платформы с указанием параметров в командной строке.

Установка Платформы с указанием параметров в командной строке

Инсталлятор Платформы позволяет установить ее с минимальным участием пользователя. Для этого запустите его, указав все нужные параметры в командной строке.

Перед запуском инсталлятора Платформы:

1. Проверьте соответствие сервера аппаратным и программным требованиям (см. *Аппаратные и программные требования*).
2. Подготовьте сервер к установке Платформы (см. *Подготовка сервера*).
3. Создайте новую директорию на диске (например, `Platform`):

```
mkdir Platform
```

4. Скопируйте архив с дистрибутивом Платформы **`iw_platform.tar.xz`** в созданную директорию.
5. Перейдите в директорию, в которую скопировали архив.
6. Распакуйте архив в эту директорию:

```
tar -xvf iw_platform.tar.xz
```

Ниже приведен список ключей: с их помощью вы можете указать инсталлятору параметры установки продукта.

Ключ	Описание
`--nodemode`	Режим установки: центральный офис или филиал. Чтобы установить Платформу в режиме филиала, укажите этот параметр со значением `office`. В режиме центрального офиса параметр можно не указывать.

Ключ	Описание
`--chmemsize`	Объем оперативной памяти, используемой для данных ClickHouse. **Доступные значения:** • `1` – `100%` или числовое значение Если не указать `%`, указанное значение будет принято за объем в ГБ.
`--disable-check-free-disk`	Отключение проверки свободного места на диске: • 20 ГБ для размещения образов • 100 ГБ для размещения данных в указанных выше директориях **Примечание**: если директории для хранения данных находятся на разных дисках, то проверится наличие 100 ГБ свободного места на каждом из них.
`--disable-check-total-ram`	Отключение проверки наличия на компьютере 8 ГБ ОЗУ.
`--chdbpath`	Путь для размещения данных ClickHouse.
`--pgdbpath`	Путь для размещения данных PostgreSQL.
`--natspath`	Путь для размещения данных NATS.
`--dsdatapath`	Путь для размещения бинарных данных.
`--factsldrtmdatapath`	Путь для временного размещения событий Traffic Monitor перед их загрузкой в Платформу.
`--advertise`	IP-адрес сетевого интерфейса, на котором работает сервис `kubelet`. Укажите значение при установке центральной ноды Платформы.
`--guiport`	Порт, по которому будет осуществляться подключение к веб-интерфейсу. Не указывается в случае установки в режиме филиала. **Важно!** При установке на один сервер с Traffic Monitor указывайте порт, отличный от 443: по умолчанию порт 443 используется как порт подключения к веб-интерфейсу Traffic Monitor.
`--cluster`	Адрес центральной ноды Платформы в кластере. Укажите значение при установке офисной ноды Платформы.

Ключ	Описание

`--clustertoken`	Токен для подключения к центральной ноде Платформы.
	Чтобы получить токен, в терминале центральной ноды Платформы выполните команду:
	`kubeadm token list`
	Создать токен можно с помощью команды:
	`kubeadm token create`
	Указывайте значение токена при установке офисной ноды Платформы.

`--nodelabel`	Лейбл ноды Платформы; уникален в пределах кластера. Значение по умолчанию для офисной ноды – `office`. Если в кластере более одной офисной ноды, нужно задать уникальные лейблы.
`--dsslowdatapath`	Путь к медленному диску сервера Data Storage. Туда Система будет перемещать бинарные данные при архивировании ежедневных табличных пространств. Пример: `--dsslowdatapath=/root/slowdisk` Подробнее об архивировании табличных пространств см. *InfoWatch Traffic Monitor. Руководство администратора. Архивирование ежедневных табличных пространств*.
`--dsbackupspath`	Путь к хранилищу резервных копий. Должен быть указан для возможности резервного копирования Data Storage. Пример: `--dsbackupspath=/opt/dsbackups` Подробнее о резервном копировании Data Storage см. *InfoWatch Traffic Monitor. Руководство администратора. Создание резервной копии Data Storage*

Чтобы установить Платформу:

1. Запустите инсталлятор Платформы с указанием параметров.
   Пример команды установки центральной ноды Платформы:

```
./setup.py install \
--advertise=0.0.0.0 \
--chmemsize=60% \
--chdbpath=/opt/chdata \
--pgdbpath=/opt/pgdata \
--natspath=/opt/natsdata \
--dsdatapath=/opt/dsdata \
--factsldrtmdatapath=/opt/factsldrtmdata \
--guiport=444 \
--dsslowdatapath=/root/slowdisk
```

Если вы не указали значения каких-либо обязательных параметров, инсталлятор запустит интерактивный режим и попросит задать их. Подробнее см. *Установка Платформы*.

2. Дождитесь завершения установки.
3. Чтобы вывести на экран информацию о Платформе, выполните команду:

```
./setup.py showproducts
```

4. Убедитесь, что все сервисы запущены, выполнив команду:

```
kubectl get pods -n infowatch
```

Команда выведет список сервисов. Каждый сервис должен иметь статус `Running`.

3.2 Установка InfoWatch Traffic Monitor

Сведения по установке InfoWatch Traffic Monitor на операционные системы Red Hat Enterprise Linux, РЕД ОС, Oracle Linux, AlmaLinux, Rocky Linux и Альт Сервер приведены в следующих разделах:

- Установка TM Enterprise и TM Standard в режиме "Все-в-одном"
- Распределенная установка TM Enterprise
- Установка в тихом режиме с файлом параметров

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

При установке "Все-в-одном" (All-in-one) вы можете установить все компоненты Traffic Monitor на один компьютер. Она аналогична установке всех шаблонов на один компьютер. Распаковка пакетов начнется перед процессом установки, после указания всех параметров.

Важно!

По умолчанию нельзя установить Систему на сервер, имя которого начинается с цифры. Если нужно разрешить цифры в начале имени сервера, с помощью командной строки задайте значение `1` параметру `--allow_digits_at_hostname_begin`. При этом нужно, чтобы была активирована проверка сети: параметру `--skip_check_network` задано значение `0` (эта проверка включена по умолчанию).

Инсталлятор Traffic Monitor может работать в двух режимах при установке с участием пользователя:

- текстовом, в консоли сервера;
- графический.

Этапы установки и их последовательность аналогичны в обоих режимах.

Независимо от выбранного режима работы инсталлятора, выполните общие действия:

1. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя `root`).

Важно!

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

Важно!

Если вы планируете использовать удаленную базу данных (развернутую локально или на отдельном сервере), то нужно провести *предварительную подготовку*.

Перед установкой рекомендуем перезагрузить сервер, на котором будет развернута база данных, чтобы очистить память.

2. Подключите внешние или локальные репозитории ОС.
Например, с инструкцией по настройке локального репозитория в Red Hat Enterprise Linux можно ознакомиться на *официальном сайте* (на английском).
Если вы устанавливаете Traffic Monitor на РЕД ОС без доступа в интернет:

   a. Выключите внешние репозитории:
   На сервере под управлением РЕД ОС версии 7.3.3 и ниже:

   Выполните команды:
   ```
   echo "enabled=0" >> /etc/yum.repos.d/RedOS-Base.repo
   echo "enabled=0" >> /etc/yum.repos.d/RedOS-Updates.repo
   sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-kernels.repo
   ```

   На сервере под управлением РЕД ОС версии 7.3.4 или 7.3.5:

   Выполните команду:
   ```
   sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-*.repo
   ```

   b. Подключите диск с дистрибутивом РЕД ОС к серверу.
   c. Смонтируйте диск с дистрибутивом РЕД ОС с помощью команды:
   `mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/`
   d. Создайте файл `/etc/yum.repos.d/cdrom.repo` с указанием смонтированного диска в качестве репозитория. Для этого выполните команду:
   ```
   cat << EOF > /etc/yum.repos.d/cdrom.repo
   [cdrom]
   name=cdrom
   baseurl=file:///media/cdrom/
   enabled=1
   gpgcheck=0
   EOF
   ```
   e. Удалите временные файлы и удостоверьтесь, что в списке репозиториев указан репозиторий с диска:
   `yum clean all && yum repolist`
   f. Установите библиотеку `libpq-14` и пакет `python2`:
   `yum install libpq-14 python2`

g. Установите перечисленные ниже пакеты. Используйте репозиторий в зависимости от редакции РЕД ОС, на которую вы устанавливаете Traffic Monitor.

Название пакета	Официальный репозиторий
`lshw-B.02.19.2-1.el7.x86_64.rpm`	*РЕД ОС Стандартная редакция – Updates* *РЕД ОС Сертифицированная редакция – Updates*
`lz4-1.9.4-1.el7.x86_64.rpm`	
`python3-psycopg2-2.9.3-1.el7.x86_64.rpm`	
`urw-base35-fonts-legacy-20170801-11.el7.noarch.rpm`	*РЕД ОС Стандартная редакция – OS* *РЕД ОС Сертифицированная редакция – OS*
`libxslt-1.1.34-1.el7.x86_64.rpm`	

Для этого:

i. Скачайте указанные пакеты из официального репозитория РЕД ОС.
ii. Скопируйте их на сервер, куда будет установлен Traffic Monitor.
iii. Перейдите в каталог, куда были скопированы указанные пакеты.
iv. Для каждого пакета выполните команду:
`yum localinstall <package>`

> **Примечание:**
>
> Дополнительно вы можете установить утилиты для работы с операционной системой с помощью команды:
> `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`
>
> Также вы можете установить утилиту *htop*, скачав ее из официального репозитория РЕД ОС:
>
> - РЕД ОС Стандартная редакция – OS
> - РЕД ОС Сертифицированная редакция – OS

h. Если вы устанавливаете Traffic Monitor на сертифицированную версию РЕД ОС, установите следующие пакеты по аналогии с предыдущим шагом:

Название пакета	Официальный репозиторий
`python2-psycopg2-2.8.3-2.el7.x86_64.rpm`	*РЕД ОС Сертифицированная редакция – Updates*
`nginx-core-1.25.4-1.el7.3.x86_64.rpm`	

Название пакета	Официальный репозиторий
`nginx-filesystem-1.25.4-1.el7.3.noarch.rpm`	
`nginx-1.25.4-1.el7.3.x86_64.rpm`	
`nginx-mod-http-push-stream-1.25.4-1.el7.3.x86_64.rpm`	
`pgagent_12-4.0.0-3.el7.x86_64.rpm`	*РЕД ОС Сертифицированная редакция – OS*

i. Убедитесь, что сетевые настройки выполнены корректно (см. *Требования к настройкам ОС и сети сервера*) и файл `/etc/hosts` содержит инструкцию преобразования имени сервера в IP-адрес. Если она отсутствует, выполните команду:
```
sh -c "echo '<IP_адрес> `hostname -f` `hostname -s`' >> /etc/hosts"
```

Если вы устанавливаете Traffic Monitor на ОС Oracle Linux 7 без доступа в интернет:

a. Убедитесь, что в операционной системе в качестве текущего выбрано ядро Red Hat Compatible Kernel (RHCK), а именно Oracle Linux Server Kernel `3.10.0-xxxx.el7.x86_64`, а ядро UEK удалено. Подробнее см. *Требования к настройкам ОС и сети сервера*.
b. Выключите внешние репозитории, выполнив следующую команду:
```
find /etc/yum.repos.d/ -iname "*.repo" -exec sed -i -e "s/enabled=.*/enabled=0/g" {} \;
```
c. Подключите диск с дистрибутивом ОС Oracle Linux к серверу.
d. Смонтируйте диск с дистрибутивом ОС Oracle Linux с помощью команды:
```
mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/
```
e. Создайте файл `/etc/yum.repos.d/cdrom.repo` с указанием смонтированного диска в качестве репозитория. Для этого выполните команду:
```
cat << EOF > /etc/yum.repos.d/cdrom.repo
[cdrom]
name=cdrom
baseurl=file:///media/cdrom/
enabled=1
gpgcheck=0
EOF
```
f. Удалите временные файлы и удостоверьтесь, что в списке репозиториев указан репозиторий с диска:
```
yum clean all && yum repolist
```
g. Установите `Perl`:
```
yum install perl
```
h. Установите следующие пакеты:
- `perl-List-MoreUtils-0.33-9.el7.x86_64.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 Latest*)
- `perl-Dist-CheckConflicts-0.06-2.el7.noarch.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 Optional Latest*)

- `urw-base35-fonts-legacy-20170801-10.el7.noarch.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 Optional Latest*)
- `python3-psycopg2-2.7.7-2.el7.x86_64.rpm (` пакет можно скачать из *официального репозитория Oracle Linux 7 EPEL*)
- `libzstd-1.5.5-1.el7.x86_64.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 EPEL*)

Для этого:

i. Скачайте перечисленные пакеты из официальных репозиториев Oracle Linux.
ii. Скопируйте их на сервер, куда будет установлен Traffic Monitor.
iii. Перейдите в каталог, куда были скопированы пакеты.
iv. Выполните следующую команду для каждого пакета:
`rpm -ivh <имя_пакета>`

> **Примечание:**
>
> Дополнительно вы можете установить утилиты для работы с операционной системой с помощью команды:
> `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`

i. Убедитесь, что сетевые настройки выполнены корректно (см. *Требования к настройкам ОС и сети сервера*) и файл `/etc/hosts` содержит инструкцию преобразования имени сервера в IP-адрес. Если она отсутствует, выполните команду:
`sh -c "echo '<IP_адрес> `hostname -f` `hostname -s`' >> /etc/hosts"`

3. **Если вы устанавливаете Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8:**

> **Важно!**
>
> Убедитесь, что в операционной системе Oracle Linux 8.10 в качестве текущего выбрано ядро Red Hat Compatible Kernel (RHCK), к примеру Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, а ядро UEK удалено. Подробнее см. *Требования к настройкам ОС и сети сервера*.

a. Установите пакет `redhat-lsb-core` с помощью команды:

```
dnf install redhat-lsb-core
```

b. Создайте резервную копию файла выпуска ОС и замените содержимое исходного файла. Для этого выполните команды в зависимости от ОС:
- на ОС Oracle Linux 8:

```
cp /etc/oracle-release /etc/release.bak

echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/oracle-release
```

- на ОС AlmaLinux 8 или Rocky Linux 8:

```
cp /etc/redhat-release /etc/release.bak
echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/
redhat-release
```

c. Выполните команду:

```
lsb_release -a
```

В результате должна быть выведена следующая информация:

```
Distributor ID: RedHatEnterprise
Description:    Red Hat Enterprise Linux release 8.10 (Ootpa)
Release:        8.10
Codename:       Ootpa
```

> **Примечание:**
>
> После установки Traffic Monitor восстановите исходный файл выпуска ОС. Подробнее см. *ниже*.

4. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой системы выполните команду:
`mkdir /distr`
5. Скопируйте в созданную директорию файлы из дистрибутива InfoWatch Traffic Monitor: инсталлятор и архив с компонентами СУБД.

ОС	Файлы дистрибутива
Red Hat Enterprise Linux 7 Oracle Linux 7[4]	**Инсталлятор:** `iwtm-installer-x.x.x.xxx-rhel7` **Архив с компонентами СУБД[1][2]:** • PostgreSQL: `iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz` • Oracle[3]: `iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`

РЕД ОС	**Инсталлятор:**
	`iwtm-installer-x.x.x.xxx-redos-7.3`
	Архив с компонентами СУБД[1][2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz`

Red Hat Enterprise Linux 8	**Инсталлятор:**
	`iwtm-installer-x.x.x.xxx-rhel8`
	Архив с компонентами СУБД[1][2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-rhel8.tar.gz`

ОС	Файлы дистрибутива
Oracle Linux 8	
AlmaLinux 8	
Rocky Linux 8	
Альт Сервер	**Инсталлятор:** `iwtm-installer-x.x.x.xxx-altlinux-10` **Архив с компонентами СУБД[1][2]:** `iwtm-postgresql-15.10-x.x.x.xxx-altlinux-10.tar.gz.md5`

Важно!

[1] Архив с компонентами СУБД нужен как при установке поставляемой в дистрибутиве СУБД (режим `local`), так и при использовании уже развернутой СУБД в удаленном режиме. Подробнее см. *Схемы развертывания Системы и выбор типа установки*.

[2] Если вы планируете использовать уже развернутую СУБД на основе PostgreSQL, используйте архив из столбца PostgreSQL. Список поддерживаемых PostgreSQL-подобных СУБД см. в статье *Аппаратные и программные требования*.

[3] Если используется СУБД Oracle и сетевая файловая система (NFS), перед запуском инсталлятора:

- **при использовании Oracle Real Application Clusters (RAC):**

  Установите опции монтирования в соответствии со *статьей на официальном сайте* (на английском).

- **если RAC не используется:**

  Откройте настройки точки монтирования (по умолчанию `/etc/fstab`) и убедитесь, что опция `noac` не используется, а параметру `actimeo` не присвоено значение `0`.

  Подробнее смотрите в *статье на официальном сайте* (на английском).

[4] При установке Traffic Monitor на сервер под управлением Oracle Linux 7 не поддерживается работа с СУБД Postgres Pro Enterprise.

Далее будет описана установка с использованием инсталлятора для ОС Red Hat Enterprise Linux 7. В нашем примере нужно скопировать файл инсталлятора и архив с компонентами СУБД:

- инсталлятор:
  `iwtm-installer-7.14.0.97-rhel7`
  где `7.14.0.97` – номер сборки, `rhel7` – обозначение ОС;
- архив с компонентами СУБД:

- если будет использована PostgreSQL (или одна из поддерживаемых СУБД на ее базе):
  `iwtm-postgresql-15.14-7.14.0.97-rhel7.tar.gz`
  где `postgresql-15.14` – обозначение СУБД, `7.14.0.97` – номер сборки, `rhel7` – обозначение ОС;
- если будет использована СУБД Oracle:
  `iwtm-oracle-19.0.0.0.0-7.14.0.97.tar.gz`
  где `oracle-19.0.0.0.0` – обозначение СУБД, `7.14.0.97` – номер сборки.

Данная инструкция актуальна и для других поддерживаемых ОС: Oracle Linux, РЕД ОС, AlmaLinux, Rocky Linux и Альт Сервер.

6. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
   `cd /distr`
7. Перед запуском установки сделайте файл инсталлятора исполняемым. Для этого используйте команду вида:

   ```
   chmod u+x ./iwtm-installer-x.x.x.xxx-rhel7
   ```

   В нашем примере команда будет следующей:

   ```
   chmod u+x ./iwtm-installer-7.14.0.97-rhel7
   ```

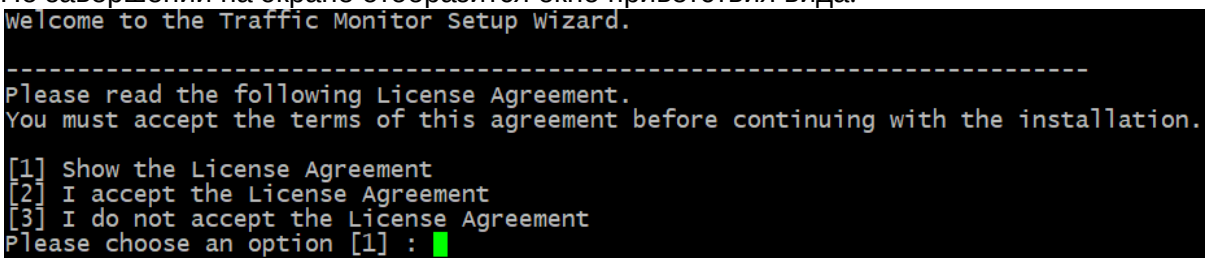
Установка в текстовом режиме в консоли сервера

Чтобы установить Traffic Monitor Enterprise или Traffic Monitor Standard в режиме "Все-в-одном" в консоли сервера, выполните следующие действия:

1. Для установки Traffic Monitor запустите инсталлятор, выполнив команду:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   В нашем примере команда будет следующей:
   `./iwtm-installer-7.14.0.97-rhel7`
   Начнется подготовка к запуску инсталлятора. На этом этапе не производится распаковка файлов.

> **Важно!**
>
> При отсутствии настроенных и доступных репозиториев ОС запуск инсталлятора прервется со следующей ошибкой:
>
> ```
> Preparing installation.../Warning: Failed to prepare installation:
> Missing OS repos or unsupported OS. Please mount and/or enable OS packages
> repository and try once again.
>
> For details refer to
> /var/log/infowatch/install/iwtm-installation_20211007114106.log or
> /tmp/installbuilder_installer_11672.log if the first doesn't exist
> Press [Enter] to continue:
> ```
>
> При возникновении данной ошибки нажмите **Enter** для завершения работы инсталлятора, а затем подключите стандартный репозиторий ОС, репозиторий EPEL и повторно запустите инсталлятор.
>
> Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

По завершении на экране отобразится окно приветствия вида:



2. Для продолжения установки нужно принять условия Лицензионного соглашения. Выберите один из предложенных вариантов. Для этого введите цифру, указанную напротив него, и нажмите **Enter**:
   - `Show the License Agreement` – для просмотра Лицензионного соглашения;
     При выборе этого варианта:
     a. Выберите язык, на котором будет выведен текст Лицензионного соглашения:
        - `English` – английский;
        - `Russian` – русский;
     b. Прочитайте Лицензионное соглашение. Для перехода к следующей странице нажимайте **Enter**.
     c. Примите Лицензионное соглашение. Для этого введите **y** и нажмите **Enter**.
   - `I accept the License Agreement` – чтобы принять Лицензионное соглашение без предварительного просмотра;
   - `I do not accept the License Agreement` – чтобы не принимать Лицензионное соглашение и прервать процесс установки.

   > **Примечание:**
   >
   > При установке в консоли сервера перед полем ввода в квадратных скобках указано значение по умолчанию. Оно будет использовано, если оставить поле ввода пустым и нажать **Enter**.
   >
   > **Пример:**
   >
   > Если на изображении выше не вводить значение, а только нажать Enter, будет выбран пункт `[1] Show the License Agreement`.

3. Выберите редакцию Traffic Monitor:
   - `Traffic Monitor Enterprise (TME)` – для установки редакции Enterprise;
   - `Traffic Monitor Standard (TMS)` – для установки редакции Standard.

Важно!

При установке редакции `Traffic Monitor Standard (TMS)` доступна только СУБД PostgreSQL.

4. Если вы выбрали редакцию `Traffic Monitor Enterprise (TME)`, при выборе типа установки укажите `All in one`.
5. Затем выберите основной язык пользовательского интерфейса консоли управления, а также формат отображения даты, времени и язык предустановленных настроек:
   - `Russian` – для русскоязычного интерфейса;
   - `English` – для англоязычного интерфейса.
6. Выберите язык базы классификации. База классификации включает в себя предустановленные политики, элементы настройки технологий и объекты защиты. Для выбора доступны:
   - `Russian` – русский;
   - `English` – английский.

   Вы можете выбрать оба языка. Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.
   Варианты будут предложены последовательно. Для использования предлагаемого варианта введите **Y**, для отказа – **N**, а для подтверждения решения нажмите **Enter**.

Примечание:

При установке в консоли сервера в квадратных скобках заглавной буквой указано значение по умолчанию. Оно будет использовано, если оставить поле ввода пустым и нажать **Enter**.

Пример использования значений по умолчанию

```
Select database classification language


Russian [Y/n]:



English [y/N]:
```

7. Выберите расположение базы данных:
   - `Install database server locally` – для локальной установки на текущем сервере;
   - `Use remote database server` – для использования уже

развернутой удаленной базы данных. В этом случае в удаленную базу данных будет добавлена схема Traffic Monitor.

> **Примечание:**
>
> Вариант `Install database server locally` поддерживается только при использовании СУБД Oracle или PostgreSQL, поставляемых в дистрибутиве.

8. Если устанавливается редакция **Enterprise** на сервер под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux или Rocky Linux, выберите одну из СУБД, с которой будет работать Система:
   - `Oracle Database Enterprise Edition`
   - `PostgreSQL`

   > **Важно!**
   >
   > Выберите вариант `PostgreSQL`:
   >
   > - если вы устанавливаете Traffic Monitor на ОС Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8
   >
   > и/или
   >
   > - если вы будете использовать СУБД Postgres Pro Enterprise, Jatoba, Tantor или Pangolin.

9. Если выбрано использование удаленной базы данных, последовательно введите:
   a. IP-адрес или доменное имя сервера с базой данных.

   > **Важно!**
   >
   > Чтобы установить Traffic Monitor на одном сервере с уже развернутой СУБД, укажите адрес `127.0.0.1`.

   b. Порт подключения.
   c. Имя используемой базы данных, в которую будет добавлена схема.
10. При необходимости вы можете изменить значения по умолчанию для параметров аутентификации в базе данных.
    В случае утвердительного ответа будет предложено поменять следующие параметры:
    - Пароль пользователя с правами `sysdba`;
    - Имя владельца схемы базы данных;
    - Пароль владельца схемы базы данных;
    - Имя пользователя сервисов Linux;
    - Пароль пользователя сервисов Linux;
    - Имя пользователя веб-сервисов;
    - Пароль пользователя веб-сервисов;
    - Имя пользователя Nagios;
    - Пароль пользователя Nagios.
11. Выберите один из режимов хранения данных:

- **Normal** (обычный) – переключение на следующий раздел, если он указан, происходит при переполнении предыдущего.
- **Fast/Slow disks** – разделение пулов на быстрый и медленный. Новые данные сохраняются в быстром разделе и через указанное количество дней перемещаются на медленные разделы. Медленный пул работает при этом в режиме `normal`.
- **Rotate** – переход к следующему разделу происходит ежедневно и при переполнении предыдущего.

12. Вы можете изменить значения по умолчанию для параметров хранения в базе данных.
В случае утвердительного ответа вы можете поменять следующие параметры:
    - **Main tablespaces path** – директориия хранения данных основного табличного пространства;
    - Если выбран режим **Fast/Slow disks**:
        - **Fast disk path** – директория хранения данных ежедневных табличных пространств в быстром разделе в режиме **Fast/Slow disks**;
        - **Number of days to store daily tablespaces on fast disk** – период хранения данных ежедневных табличных пространств в быстром разделе в режиме **Fast/Slow disks**;
    - **Number of daily tablespaces paths** – количество директорий для файлов ежедневных табличных пространств, число от 1 до 10;

      > **Примечание:**
      >
      > Если указать значение больше 1, дальше нужно будет последовательно указать соответствующее количество директорий ежедневных табличных пространств.

    - **Daily tablespaces paths** – директория данных ежедневных табличных пространств.
13. Для ежедневных табличных пространств вы можете изменить значения по умолчанию для параметров архивирования.
В случае утвердительного ответа:
    - **Path to archiving** – директория файлов архивированных табличных пространств.

Для каждого следующего параметра предварительно будет выведен запрос на использование:

- **`Archive non-violation events`** – включить автоматическое архивирование событий, которые не являются нарушениям. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.
- **`Archive violation events`** – включить автоматическое архивирование событий, которые являются нарушениями. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.
- **`Archive screenshots`** – включить автоматическое архивирование снимков экрана, полученных от Агентов Device Monitor. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.

> **Примечание:**
>
> Если вы будете использовать Data Storage, то для архивирования табличных пространств необходимо во время установки хранилища указать путь к его медленному диску. Подробнее см. *Установка Платформы*.

14. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию – 90.
15. Вы можете включить использование внешнего хранилища бинарных данных Data Storage.
    В случае утвердительного ответа укажите параметры подключения к внешнему хранилищу:
    - **`Data Storage hostname`** – имя хоста или IP-адрес сервера, на котором установлено хранилище;
    - **`Data Storage port`** – порт подключения к Data Storage, по умолчанию используется порт 40731;
    - **`Data Storage access token`** – токен авторизации Data Storage.

    Узнать актуальное значение токена можно:
    - На сервере Data Storage с помощью командной строки. Для этого:
      a. Перейдите в директорию, куда был распакован дистрибутив Платформы;
      b. Выполните команду:
      `./setup.py tokens list`
      В результате будет выведен список токенов для подключения к Платформе. Актуальный токен авторизации Data Storage будет указан напротив сущности *DataStorageUser*.
    - В консоли управления платформенного продукта, в разделе **Основные настройки** в поле **Токен для Data Storage User**. Доступно, если на сервере с Data Storage установлен платформенный продукт с веб-интерфейсом и в нем есть данная настройка.
16. Укажите параметры подключения к службе Consul:
    a. **`Network interface address`** – выберите IP-адрес сетевого интерфейса.

b. `Datacenter name` – введите название дата-центра Consul.

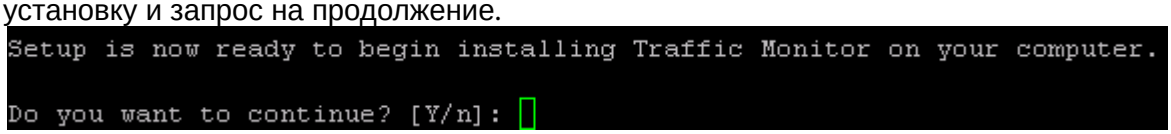
17. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:
    - `Use system NTP-server` – использовать системный NTP-сервер;
    - `Set manually` – указать NTP-сервер вручную. При выборе этого варианта нужно будет ввести IP-адрес или имя доступного NTP-сервера.
18. Далее для службы Sphinx вы можете включить индексацию на точное совпадение слов.

> **Важно!**
>
> Включение индексации на точное совпадение увеличит размер индекса минимум в 2 раза.

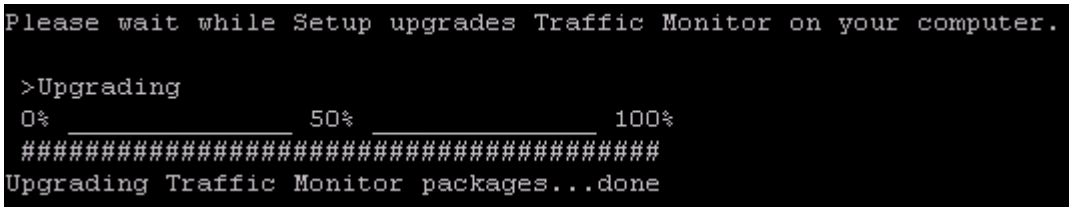
19. При необходимости вы можете изменить стандартные параметры работы службы Sphinx.
    В этом случае будет предложено задать список языков с поддержкой морфологии. По этим языкам будет проводиться индексация.
    Вы можете указать несколько языков, используя пробел в качестве разделителя.

> **Примечание:**
>
> Приоритет языков соответствует последовательности их выбора. Английский будет добавлен по умолчанию, он имеет самый высокий приоритет.

20. Вы можете включить использование технологии OCR.
    В случае включения нужно выбрать для использования одну из систем:
    - `Content AI ContentReader Engine`;
    - `Tesseract`.
21. Если выбран OCR-экстрактор Content AI ContentReader Engine:
    a. Выберите один из режимов распознавания:
        - `Quick` – быстрый режим;
        - `Quality` – тщательный режим, обеспечивающий более высокое качество распознавания.
    b. Подтвердите наличие у вас активной лицензии на использование **Content AI ContentReader Engine**.
    Если у вас отсутствует лицензия, введите **N** и нажмите **Enter**. В этом случае ContentReader Engine будет установлен без лицензии. Для возможности работы ContentReader Engine активную лицензию нужно будет добавить позже вручную.
    Подробнее смотрите в документе *InfoWatch Traffic Monitor. Руководство администратора. Настройка OCR-экстракторов*.
22. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.



Для начала установки введите **Y** и нажмите **Enter**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



Процесс может занять некоторое время.

23. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
    Если установка прошла успешно, данные рекомендуется удалить.

> **Примечание:**
>
> В случае некорректной настройки службы Consul в консоли будет выведено предупреждение:
>
> 
>
>
> Для завершения работы инсталлятора нажмите **Enter**.
>
> **Для корректной работы Системы выполните проверку и настройку кластера службы Consul**
>
> a. Запустите службу Consul с помощью команды:
> `service iwtm-consul start`
> Проверить статус службы можно командой:
> `service iwtm-consul status`
>
> b. Чтобы проверить службу Consul, выполните команды:
> i. Для вывода IP-адреса основного сервера (лидера) кластера:
> `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
> ii. Для вывода информации о членах кластера:
> `consul members`
>
> c. Если не будет выведен IP-адрес лидера кластера, выполните *конфигурирование кластера службы Consul*.
> После настройки повторите проверку (действие ii).
>
> При данной ошибке инсталлятор не запустит сервисы Traffic Monitor по завершении работы – их нужно будет запустить вручную.

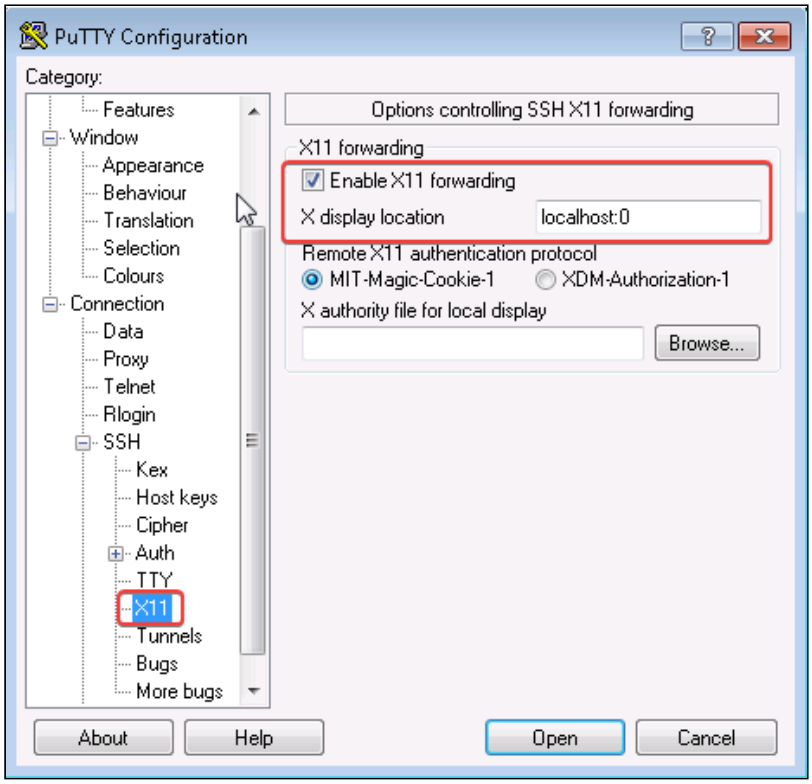
24. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
25. Если нужно вывести список сервисов Traffic Monitor и их статусы, введите команду:
    `iwtm status`

Установка с использованием графического режима инсталлятора

В ОС оконная система X Window System использует клиент-серверную модель. Для запуска инсталлятора в графическом режиме используется перенаправление графического вывода удаленной подсистемы (**X11 Forwarding**). Это позволит работать напрямую с графическими приложениями среды Linux на компьютере, с которого осуществляется подключение к серверу. Этот режим реализуется с помощью SSH-подключения.

Чтобы установить Traffic Monitor Enterprise или Traffic Monitor Standard в режиме "Все-в-одном" с использованием графического режима инсталлятора, выполните следующие действия:

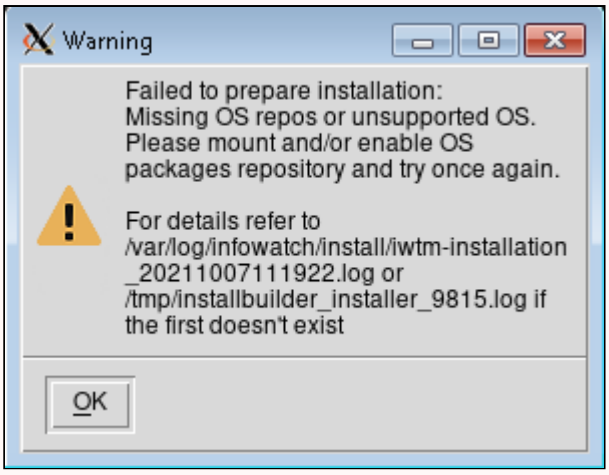
1. На сервере, на котором планируется установка компонентов Traffic Monitor:
   a. Установите утилиту xauth с помощью команды:
      - На сервере под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux, Rocky Linux или РЕД ОС:
        ```
        yum install xauth
        ```
      - На сервере под управлением ОС Альт Сервер:
        ```
        sudo apt-get install xauth
        ```
   b. Убедитесь, что в конфигурационном файле `/etc/ssh/sshd_config`:
      - для параметра `X11Forwarding` установлено значение `yes`;
      - строка с параметром `X11Forwarding` раскомментирована, то есть не содержит символ `#`.
   c. Сохраните изменения в конфигурационном файле.
   d. Перезапустите службу SSH с помощью команды:
      `systemctl restart sshd`
2. На компьютере, на котором будет использован графический режим:
   a. Для подключения к серверу установки Traffic Monitor вам потребуется SSH-клиент с включенной опцией X11 Forwarding, например PuTTY.
   b. Для запуска инсталлятора в графическом режиме вам потребуется настроенное приложение-клиент для обращения к X Window System, например:
      - приложение Xming – для ОС семейства MS Windows;
      - оболочка Gnome 3 – для ОС семейства Linux.
3. Запустите настроенное приложение-клиент для обращения к X Window System.
4. Подключитесь к серверу, на котором планируется установка компонентов Traffic Monitor, с помощью выбранного SSH-клиента.
   Пример окна настройки PuTTY при подключении



5. Для установки Traffic Monitor запустите инсталлятор с помощью команды:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   В нашем примере команда будет:
   `./iwtm-installer-7.14.0.97-rhel7`
   Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

   Важно!

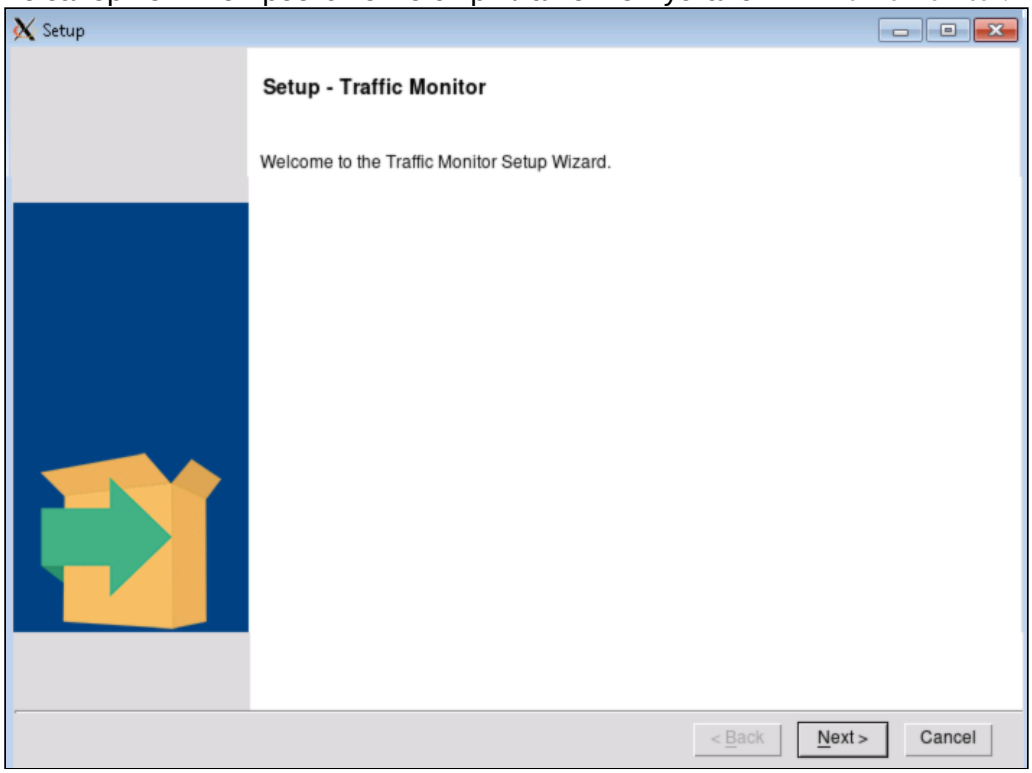
   При отсутствии настроенных и доступных репозиториев ОС запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите **OK** для завершения работы инсталлятора, а затем подключите стандартный репозиторий ОС, репозиторий EPEL и повторно запустите инсталлятор.

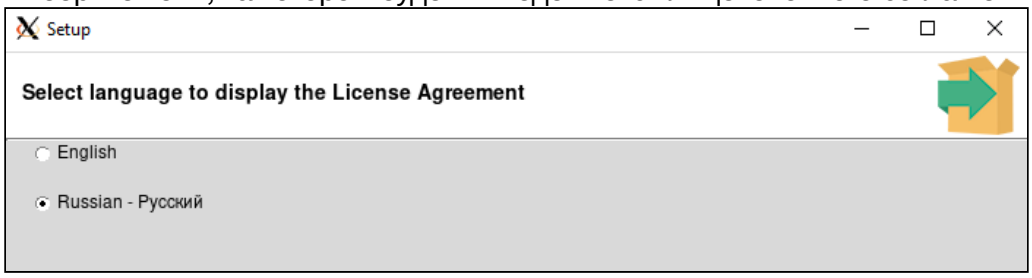
Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

По завершении откроется окно с приглашением установить Traffic Monitor:



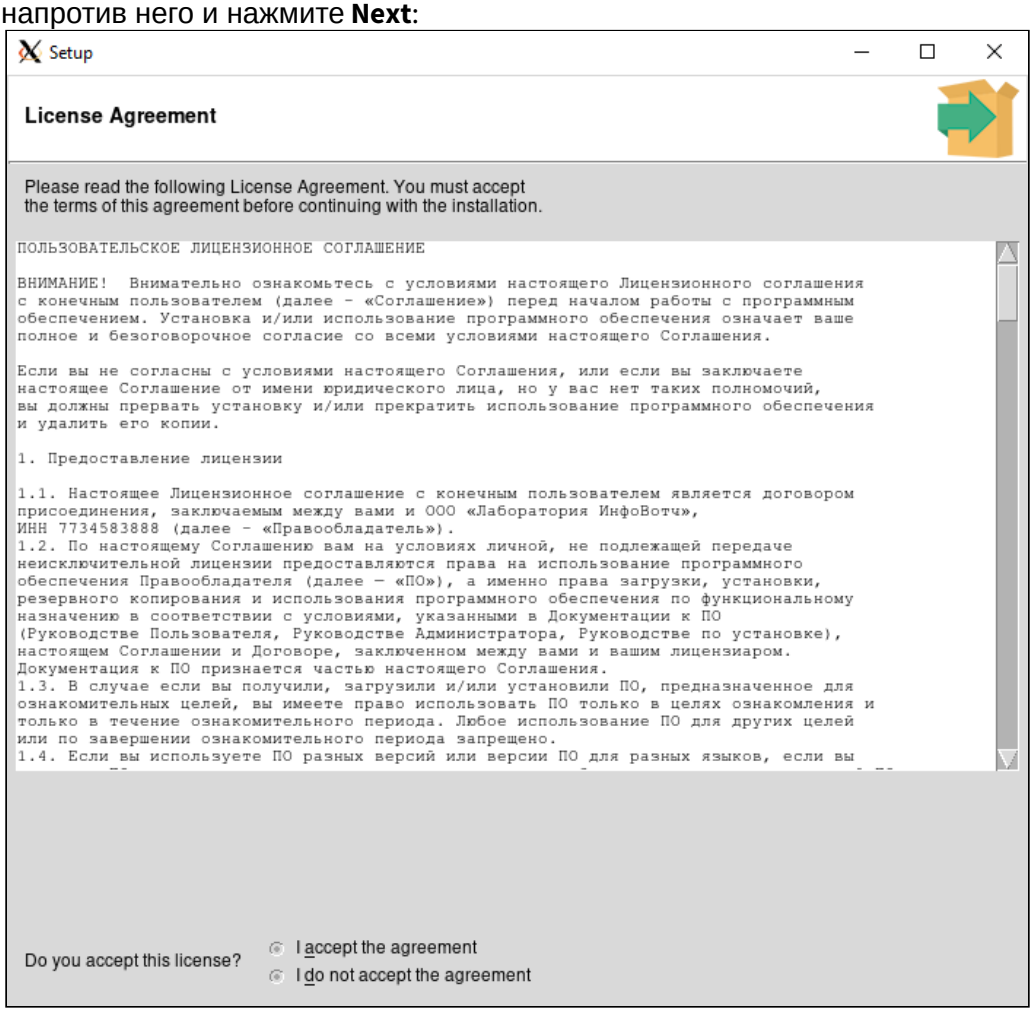
Для перехода к следующему параметру нажмите **Next**, для возврата к предыдущему – **Back**. Для выхода из инсталлятора нажмите **Cancel**.

6. Для продолжения установки нужно принять условия Лицензионного соглашения. Для этого:
   a. Выберите язык, на котором будет выведен текст Лицензионного соглашения:



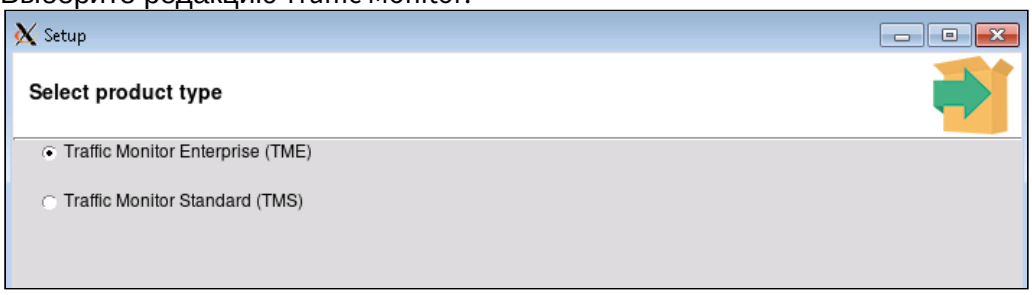
- `English` – английский;
- `Russian` – русский;

b. Выберите один из предложенных вариантов. Для этого установите флажок напротив него и нажмите **Next**:



- **`I accept the agreement`** – чтобы принять Лицензионное соглашение и продолжить процесс установки;
- **`I do not accept the agreement`** – чтобы не принимать Лицензионное соглашение и прервать процесс установки.

7. Выберите редакцию Traffic Monitor:

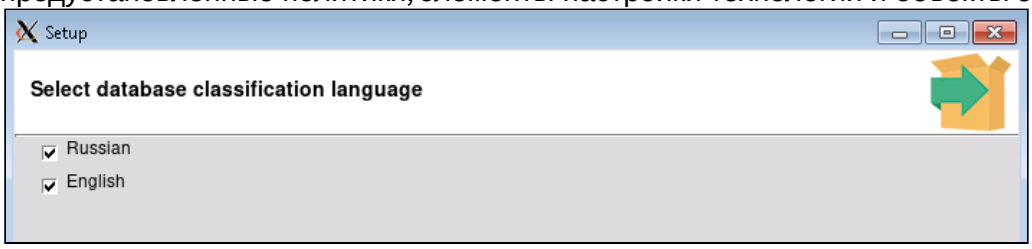


- **`Traffic Monitor Enterprise (TME)`** – для установки редакции Enterprise;
- **`Traffic Monitor Standard (TMS)`** – для установки редакции Standard.

Важно!

При установке редакции `Traffic Monitor Standard (TMS)` доступна только СУБД PostgreSQL.

8. Если вы выбрали редакцию `Traffic Monitor Enterprise (TME)`, при выборе типа установки укажите `All in one`.
9. Далее выберите основной язык пользовательского интерфейса консоли управления, а также формат отображения даты, времени и язык предустановленных настроек:
   - `Russian` – для русскоязычного интерфейса;
   - `English` – для англоязычного интерфейса.
10. Выберите язык базы классификации. База классификации включает в себя предустановленные политики, элементы настройки технологий и объекты защиты.

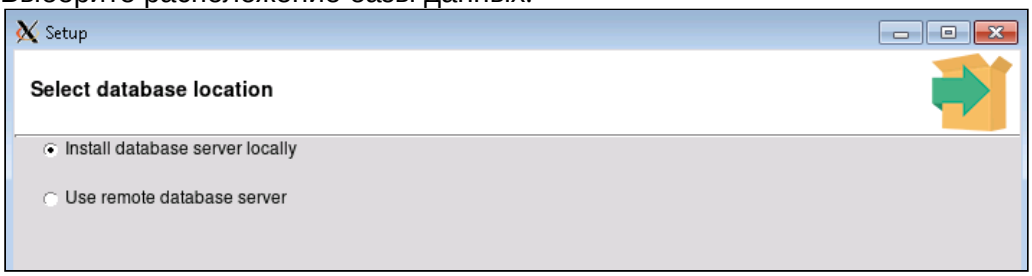


Для выбора доступны:

- `Russian` – русский;
- `English` – английский.

Чтобы выбрать оба значения, отметьте их флажками и нажмите **Next**. Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.

11. Выберите расположение базы данных:



- `Install database server locally` – для локальной установки на текущем сервере;
- `Use remote database server` – для использования уже развернутой удаленной базы данных. В этом случае в удаленную базу данных будет добавлена схема Traffic Monitor.

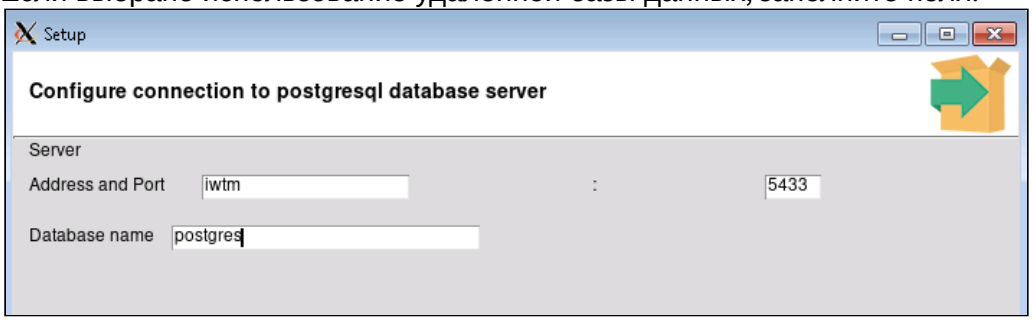
Примечание:

Вариант **`Install database server locally`** поддерживается только при использовании СУБД Oracle или PostgreSQL, поставляемых в дистрибутиве.

12. Если устанавливается редакция **Enterprise** на сервер под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux или Rocky Linux, выберите одну из СУБД, с которой будет работать Система:
    - **`Oracle Database Enterprise Edition`**
    - **`PostgreSQL`**

> **Важно!**
>
> Выберите вариант **`PostgreSQL`**:
>
> - если вы устанавливаете Traffic Monitor на ОС Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8
>
> и/или
>
> - если вы будете использовать СУБД Postgres Pro Enterprise, Jatoba, Tantor или Pangolin.

13. Если выбрано использование удаленной базы данных, заполните поля:



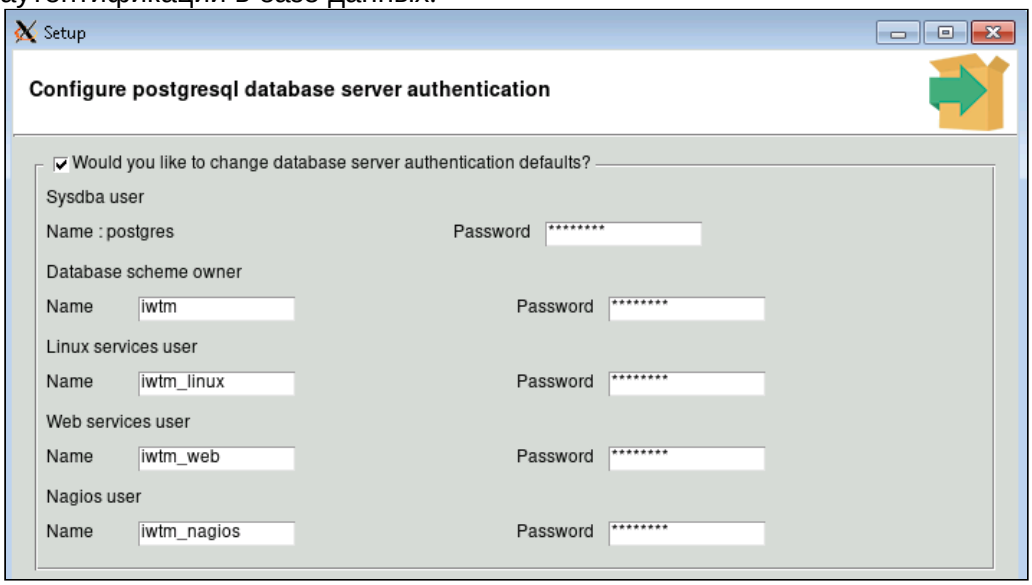
    a. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.

> **Важно!**
>
> Чтобы установить Traffic Monitor на одном сервере с уже развернутой СУБД, укажите адрес `127.0.0.1`.

    b. **`Database name`** – Имя используемой базы данных, в которую будет добавлена схема.

> **Примечание:**
>
> В графическом режиме в активных полях указаны значения по умолчанию.

14. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.

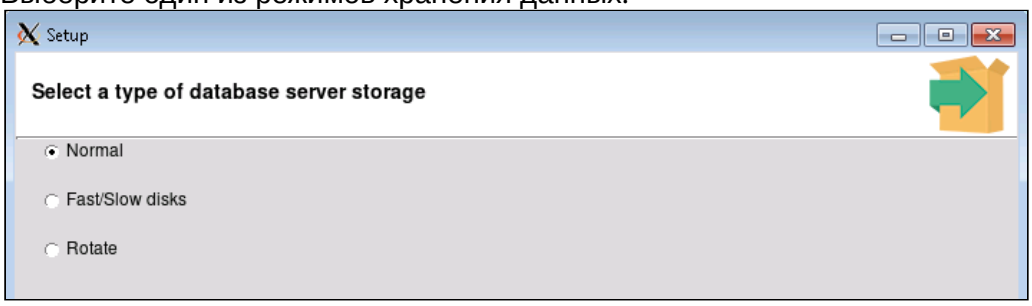


Чтобы отредактировать значения, установите флажок напротив поля с вопросом. Это сделает доступными для редактирования следующие разделы:

- **`Sysdba user`** – пароль пользователя с правами sysdba;
- **`Database scheme owner`** – имя и пароль владельца схемы базы данных;
- **`Linux services user`** – имя и пароль пользователя сервисов Linux;
- **`Web services user`** – имя и пароль пользователя веб-сервисов;
- **`Nagios user`** – имя и пароль пользователя Nagios.

Чтобы оставить значения по умолчанию, не устанавливайте флажок и нажмите **Next**. В этом случае поля останутся недоступны для редактирования, а инсталлятор использует значения по умолчанию.

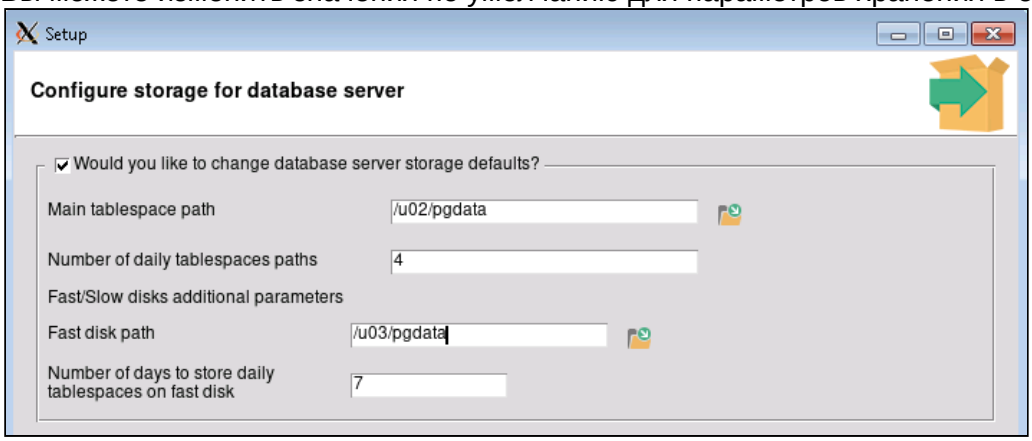
15. Выберите один из режимов хранения данных:



- **`Norma l`** (обычный) – переключение на следующий раздел, если он указан, происходит при переполнении предыдущего.
- **`Fast/Slow disks`** – разделение пулов на быстрый и медленный. Новые данные сохраняются в быстром разделе и через указанное количество дней перемещаются на медленные разделы. Медленный пул работает при этом в режиме `normal`.

- **Rotate** – переход к следующему разделу происходит ежедневно и при переполнении предыдущего.

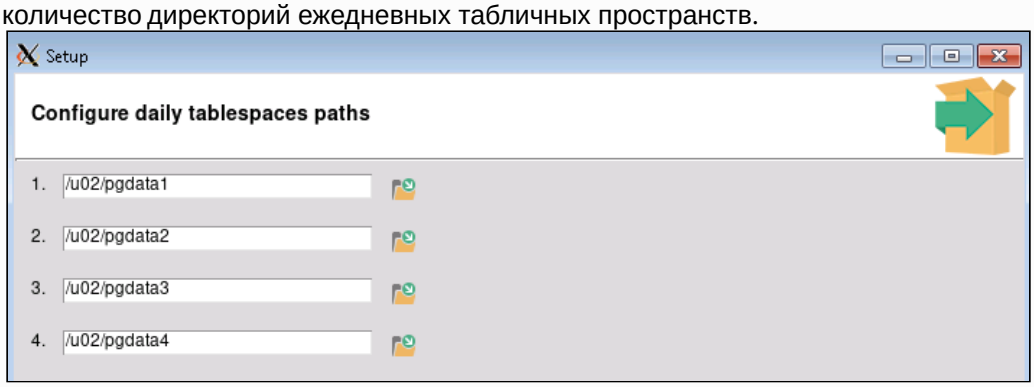
16. Вы можете изменить значения по умолчанию для параметров хранения в базе данных.



- **Main tablespaces path** – директория хранения данных основного табличного пространства;
  Вы можете вписать директорию в поле или указать ее в окне файлового менеджера с помощью кнопки .
- Если выбран режим **Fast/Slow disks**:
  - **Fast disk path** – директория хранения данных ежедневных табличных пространств в быстром разделе в режиме **Fast/Slow disks**;
  - **Number of days to store daily tablespaces on fast disk** – период хранения данных ежедневных табличных пространств в быстром разделе в режиме **Fast/Slow disks**;
- **Number of daily tablespaces paths** – количество директорий для файлов ежедневных табличных пространств, число от 1 до 10;

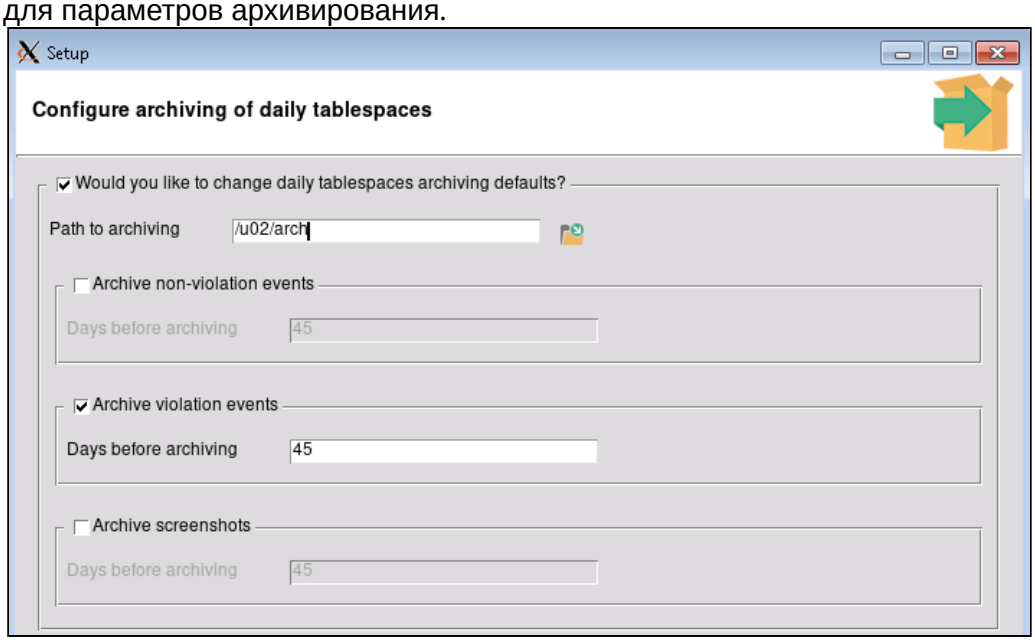
> **Примечание:**

Если указать значение больше 1, дальше нужно будет указать соответствующее количество директорий ежедневных табличных пространств.



- **Daily tablespaces paths** – директория хранения данных ежедневных табличных пространств.

17. Для ежедневных табличных пространств вы можете изменить значения по умолчанию для параметров архивирования.



- **Path to archiving** – директория хранения файлов архивированных табличных пространств.

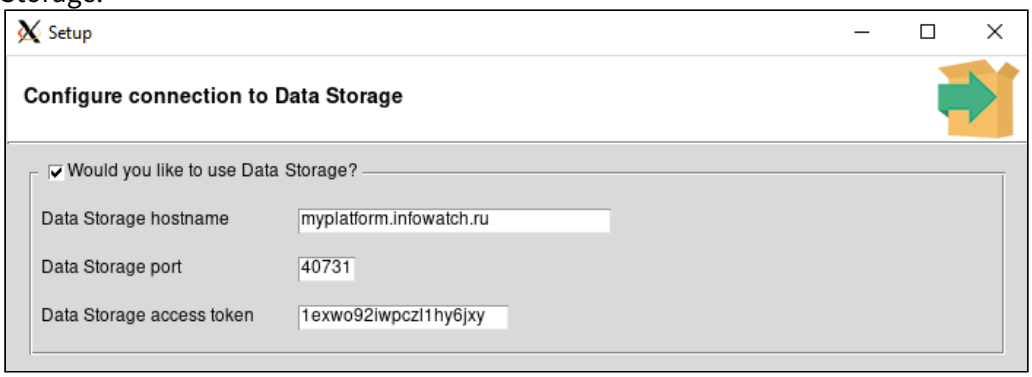
Каждый параметр включается отдельно:

- **Archive non-violation events** – включить автоматическое архивирование событий, которые не являются нарушениям. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.
- **Archive violation events** – включить автоматическое архивирование событий, которые являются нарушениями. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.
- **Archive screenshots** – включить автоматическое архивирование снимков экрана, полученных от

Агентов Device Monitor. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.

> **Примечание:**
>
> Если вы будете использовать Data Storage, то для архивирования табличных пространств необходимо во время установки хранилища указать путь к его медленному диску. Подробнее см. *Установка Платформы*.

18. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию – 90.
19. Вы можете включить использование внешнего хранилища бинарных данных Data Storage.



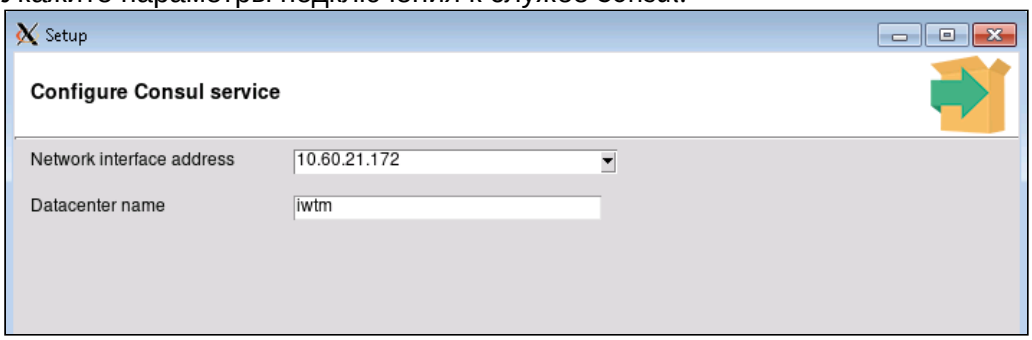
Для этого установите флажок напротив поля с вопросом и укажите параметры подключения к внешнему хранилищу:

- `Data Storage hostname` – имя хоста или IP-адрес сервера, на котором установлено хранилище;
- `Data Storage port` – порт подключения к Data Storage, по умолчанию используется порт 40731;
- `Data Storage access token` – токен авторизации Data Storage.

Узнать актуальное значение токена можно:

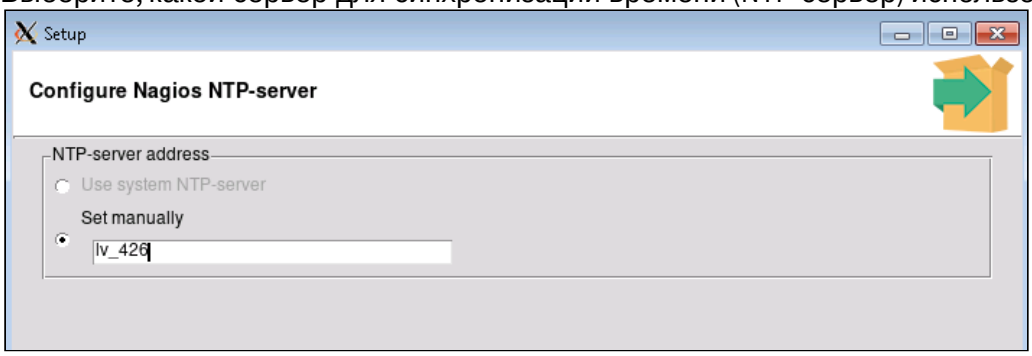
- На сервере Data Storage с помощью командной строки. Для этого:
  a. Перейдите в директорию, куда был распакован дистрибутив Платформы;
  b. Выполните команду:
  `./setup.py tokens list`
  В результате будет выведен список токенов для подключения к Платформе. Актуальный токен авторизации Data Storage будет указан напротив сущности *DataStorageUser*.
- В консоли управления платформенного продукта, в разделе **Основные настройки** в поле **Токен для Data Storage User**. Доступно, если на сервере с Data Storage установлен платформенный продукт с веб-интерфейсом и в нем есть данная настройка.

20. Укажите параметры подключения к службе Consul:



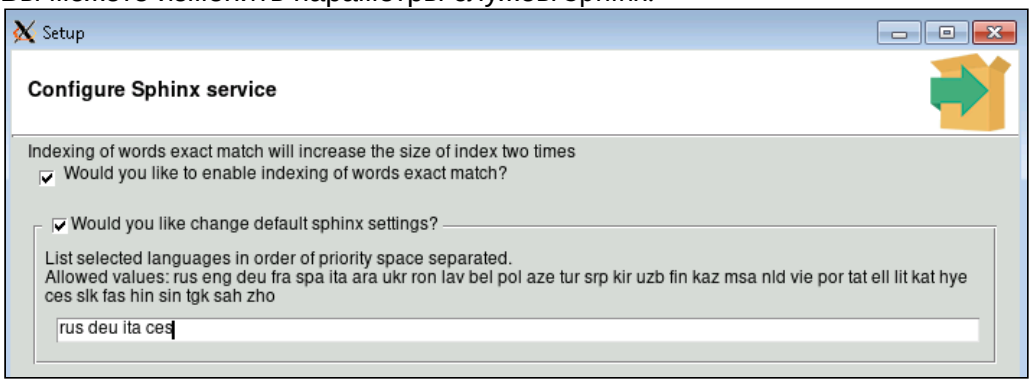
    a. **`Network interface address`** – выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите ▼ и в раскрывшемся списке выберите требуемое значение.
    b. **`Datacenter name`** – введите название дата-центра Consul.

21. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:



- **`Use system NTP-server`** – использовать системный NTP-сервер;
- **`Set manually`** – указать NTP-сервер вручную. При выборе этого варианта укажите IP-адрес или имя доступного NTP-сервера.

22. Вы можете изменить параметры службы Sphinx:



- **`Enable indexing of words exact match`** – включить индексацию на точное совпадение слов;

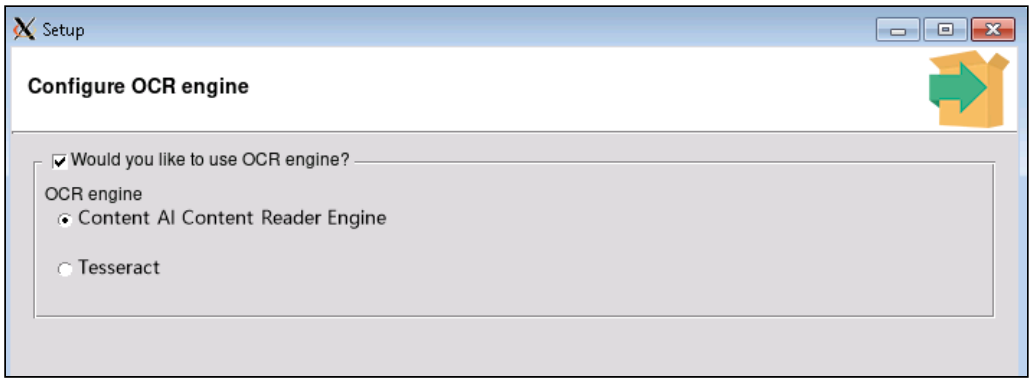
> **Важно!**

Включение индексации на точное совпадение увеличит размер индекса минимум в 2 раза.

- При необходимости вы можете изменить стандартные параметры работы службы Sphinx (**`default sphinx settings`**). В этом случае укажите список языков с поддержкой морфологии. По этим языкам будет проводиться индексация. Вы можете указать несколько языков, используя пробел в качестве разделителя.

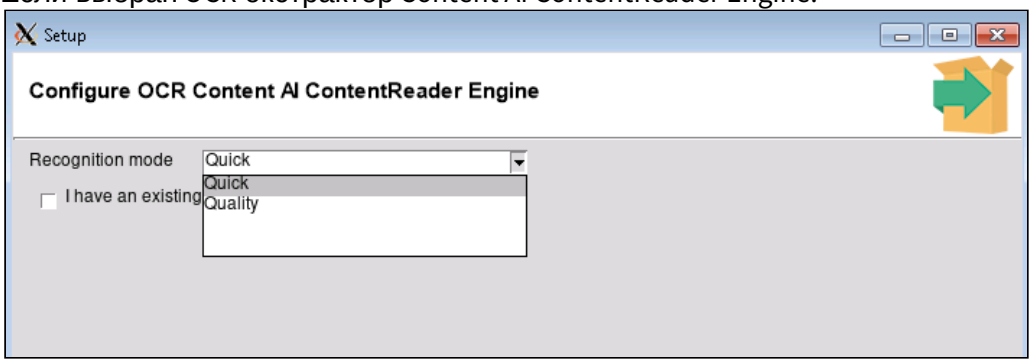
> **Примечание:**
>
> Приоритет языков соответствует последовательности их выбора. Английский будет добавлен по умолчанию, он имеет самый высокий приоритет.

23. Вы можете включить использование технологии OCR.



В случае включения нужно выбрать для использования одну из систем:
- **`Content AI ContentReader Engine`** ;
- **`Tesseract`** .

24. Если выбран OCR-экстрактор Content AI ContentReader Engine:

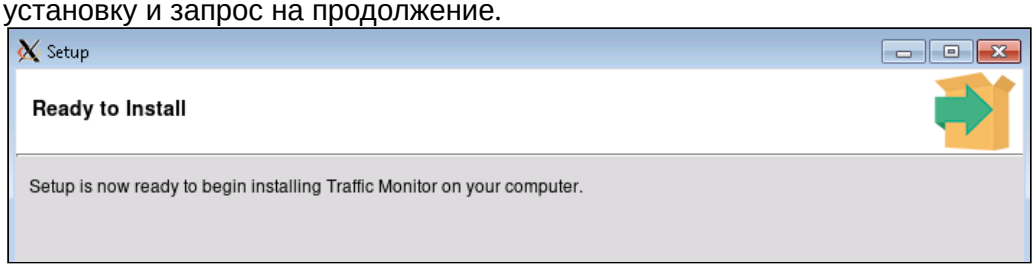


a. Выберите один из режимов распознавания (**`Recognition mode`**):
   - **`Quick`** – быстрый режим;
   - **`Quality`** – тщательный режим, обеспечивающий более высокое качество распознавания.

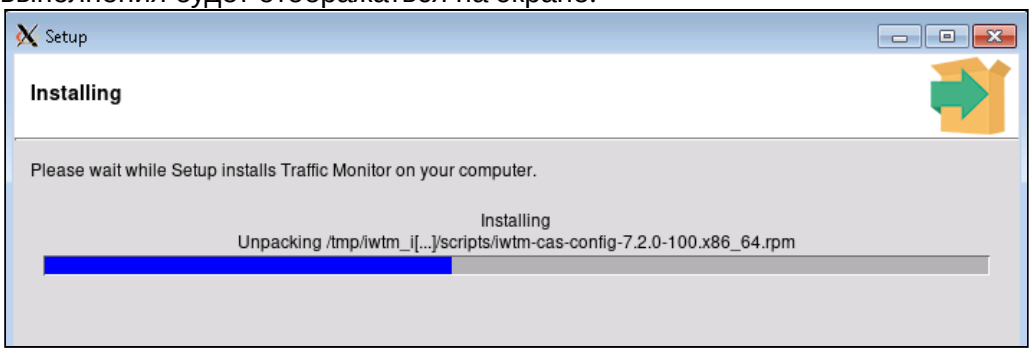
b. Подтвердите наличие у вас активной лицензии на использование ContentReader Engine.
   Если у вас отсутствует лицензия, не ставьте флажок в этом поле. В этом случае ContentReader Engine будет установлен без лицензии. Для возможности работы ContentReader Engine активную лицензию нужно будет добавить позже вручную.

Подробнее смотрите в документе *InfoWatch Traffic Monitor. Руководство администратора. Настройка OCR-экстракторов*.

25. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.



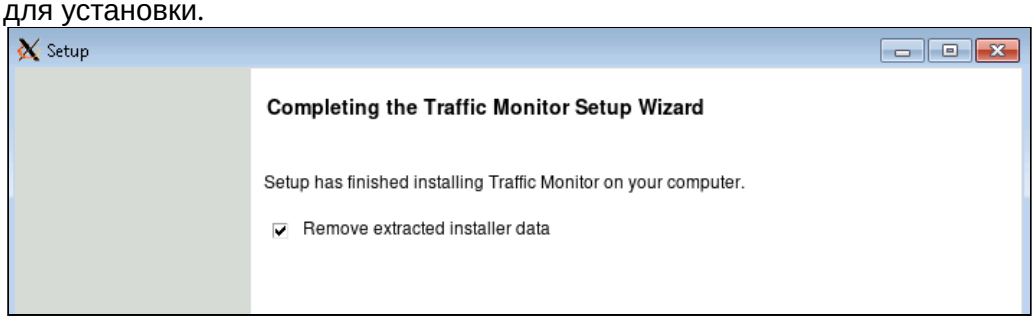
Для начала установки нажмите **Next**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



Процесс может занять некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

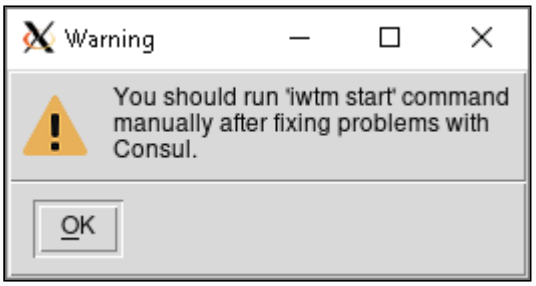
26. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.



Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта `Remove extracted installer data`.

> **Примечание:**

В случае некорректной настройки службы Consul в консоли будет выведено предупреждение:



Чтобы закрыть окно и завершить работу инсталлятора, нажмите **OK**.

Для корректной работы Системы выполните проверку и настройку кластера службы Consul

a. Запустите службу Consul с помощью команды:
`service iwtm-consul start`
Проверить статус службы можно командой:
`service iwtm-consul status`

b. Чтобы проверить службу Consul, выполните команды:
   i. Для вывода IP-адреса основного сервера (лидера) кластера:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. Для вывода информации о членах кластера:
   `consul members`

c. Если не будет выведен IP-адрес лидера кластера, выполните *конфигурирование кластера службы Consul*.
После настройки повторите проверку (действие ii).

При данной ошибке инсталлятор не запустит сервисы Traffic Monitor по завершении работы – их нужно будет запустить вручную.

27. Для завершения нажмите **Finish**.
28. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
29. Если нужно вывести список сервисов Traffic Monitor и их статусы, в консоли сервера введите команду:
`iwtm status`

Если вы установили Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8, восстановите исходный файл выпуска ОС.

Для этого:

1. Выполните команду в зависимости от ОС:
   - в ОС Oracle Linux 8:
     ```
     mv /etc/release.bak /etc/oracle-release
     ```
   - в ОС AlmaLinux 8 или Rocky Linux 8:
     ```
     mv /etc/release.bak /etc/redhat-release
     ```
2. Подтвердите перезапись файла. Для этого введите `yes` и нажмите **Enter**.
3. Убедитесь, что исходный файл выпуска успешно восстановлен. Для этого выполните команду:
   ```
   lsb_release -a
   ```
   В результате должна быть выведена информация о вашей операционной системе. Например, для ОС AlmaLinux 8 будет выведено:
   ```
   Distributor ID: AlmaLinux
   Description:    AlmaLinux release 8.10 (Cerulean Leopard)
   Release:        8.10
   Codename:       CeruleanLeopard
   ```

В результате установки в системе будут созданы учетные записи. Подробнее см. *Предустановленные серверные параметры*.

После окончания установки работа в Консоли управления Traffic Monitor доступна через окно браузера. Для этого в адресной строке браузера введите URL-адрес сервера Traffic Monitor.

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

3.2.2 Распределенная установка TM Enterprise

Traffic Monitor в редакции Enterprise позволяет развернуть Систему так, чтобы различные компоненты Traffic Monitor, например СУБД, модули или веб-консоль, были установлены на разные серверы. Такая установка используется, если с учетом предполагаемой нагрузки все компоненты Traffic Monitor, включая СУБД, не смогут эффективно работать на одном сервере.

> **Важно!**
>
> По умолчанию нельзя установить Систему на сервер, имя которого начинается с цифры. Если нужно разрешить цифры в начале имени сервера, с помощью командной строки задайте значение `1` параметру `--allow_digits_at_hostname_begin`. При этом нужно, чтобы была активирована проверка сети: параметру `--skip_check_network` задано значение `0` (эта проверка включена по умолчанию).

Для упрощения установки компонентов Traffic Monitor на несколько серверов в инсталляторе реализованы шаблоны установки, с помощью которых можно эффективно распределить нагрузку между серверами и спланировать Систему. Подробнее о шаблонах см. в статье *Схемы развертывания Системы и выбор типа установки*.
Доступны четыре шаблона установки:

- **База данных** (`Database`);
- **Индексер** (`Indexer service`);
- **Веб-консоль** (`Web console`);

- **Перехватчики** (`Traffic interceptors`).

Допускается установка шаблонов в произвольном порядке.

> **Примечание:**
>
> В одном кластере рекомендуется устанавливать шаблоны в следующей последовательности:
>
> 1. База данных
> 2. Индексер
> 3. Веб-консоль
> 4. Перехватчики

На один сервер можно одновременно установить несколько шаблонов.
Установка всех шаблонов на один сервер соответствует *установке в режиме "Все-в-одном"*.

> **Важно!**
>
> Шаблоны **База данных**, **Индексер** и **Веб-консоль** в одном кластере должны быть в единственном экземпляре. Шаблон **Перехватчики** в одном кластере может быть использован больше одного раза с учетом планируемой нагрузки на Систему.

Инсталлятор Traffic Monitor может работать в двух режимах при установке с участием пользователя:

- текстовом, в консоли сервера;
- графическом.

Этапы установки и их последовательность аналогичны в обоих режимах.

Независимо от выбранного режима работы инсталлятора, выполните общие действия:

1. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя `root`).

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

   > **Важно!**
   >
   > Если вы планируете использовать удаленную базу данных (развернутую локально или на отдельном сервере), то нужно провести *предварительную подготовку*.
   >
   > Перед установкой рекомендуем перезагрузить сервер, на котором будет развернута база данных, чтобы очистить память.

2. Подключите внешние или локальные репозитории ОС.
   Например, с инструкцией по настройке локального репозитория в Red Hat Enterprise Linux можно ознакомиться на *официальном сайте* (на английском).

Если вы устанавливаете Traffic Monitor на РЕД ОС без доступа в Интернет:

a. Выключите внешние репозитории:
На рабочей станции под управлением РЕД ОС версии 7.3.3 и ниже:

Выполните следующие команды:
```
echo "enabled=0" >> /etc/yum.repos.d/RedOS-Base.repo
echo "enabled=0" >> /etc/yum.repos.d/RedOS-Updates.repo
sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-kernels.repo
```

На рабочей станции под управлением РЕД ОС версии 7.3.4 или 7.3.5:

Выполните команду:
```
sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-*.repo
```

b. Подключите диск с дистрибутивом РЕД ОС к серверу.
c. Смонтируйте диск с дистрибутивом РЕД ОС с помощью команды:
```
mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/
```
d. Создайте файл `/etc/yum.repos.d/cdrom.repo` с указанием смонтированного диска в качестве репозитория. Для этого выполните команду:
```
cat << EOF > /etc/yum.repos.d/cdrom.repo
[cdrom]
name=cdrom
baseurl=file:///media/cdrom/
enabled=1
gpgcheck=0
EOF
```
e. Удалите временные файлы и удостоверьтесь, что в списке репозиториев указан репозиторий с диска:
```
yum clean all && yum repolist
```
f. Установите библиотеку `libpq` и пакет `python2`:
```
yum install libpq python2
```
g. Установите следующие пакеты:

Название пакета	Официальный репозиторий
`lshw-B.02.19.2-1.el7.x86_64.rpm`	*РЕД ОС – Updates*
`lz4-1.9.4-1.el7.x86_64.rpm`	
`python3-psycopg2-2.9.3-1.el7.x86_64.rpm`	
`urw-base35-fonts-legacy-20170801-11.el7.noarch.rpm`	*РЕД ОС – OS*
`libxslt-1.1.34-1.el7.x86_64.rpm`	

Для этого:
   i. Скачайте указанные пакеты из официального репозитория РЕД ОС.
   ii. Скопируйте их на сервер, куда будет установлен Traffic Monitor.
   iii. Перейдите в каталог, куда были скопированы указанные пакеты.

iv. Выполните команду:
`yum localinstall lshw-B.02.19.2-1.el7.x86_64.rpm lz4-1.9.4-1.el7.x86_64.rpm python3-psycopg2-2.9.3-1.el7.x86_64.rpm urw-base35-fonts-legacy-20170801-11.el7.noarch.rpm libxslt-1.1.34-1.el7.x86_64.rpm`

> **Примечание:**
>
> Дополнительно вы можете установить утилиты для работы с операционной системой с помощью команды:
> `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`
>
> Также вы можете установить утилиту *htop*, скачав ее из *официального репозитория РЕД ОС*.

h. Убедитесь, что сетевые настройки выполнены корректно (см. *Требования к настройкам ОС и сети сервера*) и файл `/etc/hosts` содержит инструкцию преобразования имени сервера в IP-адрес. Если она отсутствует, выполните команду:
`sh -c "echo '<IP_адрес> `hostname -f` `hostname -s`' >> /etc/hosts"`

Если вы устанавливаете Traffic Monitor на ОС Oracle Linux 7 без доступа в Интернет:

a. Убедитесь, что в операционной системе в качестве текущего выбрано ядро Red Hat Compatible Kernel (RHCK), а именно Oracle Linux Server Kernel `3.10.0-xxxx.el7.x86_64`, а ядро UEK удалено. Подробнее см. *Требования к настройкам ОС и сети сервера*.
b. Выключите внешние репозитории с помощью команды:
`find /etc/yum.repos.d/ -iname "*.repo" -exec sed -i -e "s/enabled=.*/enabled=0/g" {} \;`
c. Подключите диск с дистрибутивом ОС Oracle Linux к серверу.
d. Смонтируйте диск с дистрибутивом ОС Oracle Linux с помощью команды:
`mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/`
e. Создайте файл `/etc/yum.repos.d/cdrom.repo` с указанием смонтированного диска в качестве репозитория. Для этого выполните команду:
```
cat << EOF > /etc/yum.repos.d/cdrom.repo
[cdrom]
name=cdrom
baseurl=file:///media/cdrom/
enabled=1
gpgcheck=0
EOF
```
f. Удалите временные файлы и удостоверьтесь, что в списке репозиториев указан репозиторий с диска:
`yum clean all && yum repolist`
g. Установите `Perl`:
`yum install perl`
h. Установите следующие пакеты:
- `perl-List-MoreUtils-0.33-9.el7.x86_64.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 Latest*)

- `perl-Dist-CheckConflicts-0.06-2.el7.noarch.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 Optional Latest*)
- `urw-base35-fonts-legacy-20170801-10.el7.noarch.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 Optional Latest*)
- `python3-psycopg2-2.7.7-2.el7.x86_64.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 EPEL*)
- `libzstd-1.5.5-1.el7.x86_64.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 EPEL*)

Для этого:

i. Скачайте перечисленные пакеты из официальных репозиториев Oracle Linux.
ii. Скопируйте их на сервер, куда будет установлен Traffic Monitor.
iii. Перейдите в каталог, куда были скопированы пакеты.
iv. Выполните следующую команду для каждого пакета:
`rpm -ivh <имя_пакета>`

> **Примечание:**
>
> Дополнительно вы можете установить утилиты для работы с операционной системой с помощью команды:
> `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`

i. Убедитесь, что сетевые настройки выполнены корректно (см. *Требования к настройкам ОС и сети сервера*) и файл `/etc/hosts` содержит инструкцию преобразования имени сервера в IP-адрес. Если она отсутствует, выполните команду:
`sh -c "echo '<IP_адрес> `hostname -f` `hostname -s`' >> /etc/hosts"`

3. **Если вы устанавливаете компоненты Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8:**

> **Важно!**
>
> Убедитесь, что в операционной системе Oracle Linux 8.10 в качестве текущего выбрано ядро Red Hat Compatible Kernel (RHCK), к примеру Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, а ядро UEK удалено. Подробнее см. *Требования к настройкам ОС и сети сервера*.

a. Установите пакет `redhat-lsb-core` с помощью команды:

```
dnf install redhat-lsb-core
```

b. Создайте резервную копию файла выпуска ОС и замените содержимое исходного файла. Для этого выполните команды в зависимости от ОС:
- на ОС Oracle Linux 8:

```
cp /etc/oracle-release /etc/release.bak
```

```
                    echo "Red Hat Enterprise Linux release 8.10
(Ootpa)" > /etc/oracle-release
```

- на ОС AlmaLinux 8 или Rocky Linux 8:

```
cp /etc/redhat-release /etc/release.bak
echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/
redhat-release
```

c. Выполните команду:

```
lsb_release -a
```

В результате должна быть выведена следующая информация:

```
Distributor ID: RedHatEnterprise
Description:    Red Hat Enterprise Linux release 8.10 (Ootpa)
Release:        8.10
Codename:       Ootpa
```

> **Примечание:**
>
> После установки Traffic Monitor восстановите исходный файл выпуска ОС. Подробнее см. *ниже*.

4. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой системы выполните команду:
   `mkdir /distr`
5. Скопируйте в созданную директорию файлы из дистрибутива InfoWatch Traffic Monitor: инсталлятор и архив с компонентами СУБД.

ОС	Файлы дистрибутива
Red Hat Enterprise Linux 7 Oracle Linux 7 [4]	**Инсталлятор:** `iwtm-installer-x.x.x.xxx-rhel7` **Архив с компонентами СУБД [1] [2]:** • PostgreSQL: `iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz` • Oracle[3]: `iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`

РЕД ОС	**Инсталлятор:**
	`iwtm-installer-x.x.x.xxx-redos-7.3`
	Архив с компонентами СУБД [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz`

ОС	Файлы дистрибутива

Red Hat Enterprise Linux 8
Oracle Linux 8
AlmaLinux 8
Rocky Linux 8
	Инсталлятор:
	`iwtm-installer-x.x.x.xxx-rhel8`
	Архив с компонентами СУБД [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-rhel8.tar.gz`

Альт Сервер	**Инсталлятор:**
	`iwtm-installer-x.x.x.xxx-altlinux-10`
	Архив с компонентами СУБД [1] [2]:
	`iwtm-postgresql-15.10-x.x.x.xxx-altlinux-10.tar.gz.md5`

Важно!

[1] Архив с компонентами СУБД необходим как при установке поставляемой в дистрибутиве СУБД (режим `local`), так и при использовании уже развернутой СУБД в удаленном режиме. Подробнее см. *Схемы развертывания Системы и выбор типа установки*.

[2] Если вы планируете использовать уже развернутую СУБД на основе PostgreSQL, используйте архив из столбца PostgreSQL. Список поддерживаемых PostgreSQL-подобных СУБД см. в статье *Аппаратные и программные требования*.

[3] Если используется СУБД Oracle и сетевая файловая система (NFS), перед запуском инсталлятора:

- **если RAC не используется:**

  Откройте настройки точки монтирования (по умолчанию `/etc/fstab`) и убедитесь, что опция `noac` не используется, а параметру `actimeo` не присвоено значение `0`.

  Подробнее см. в *статье на официальном сайте* (на английском).

- **при использовании Oracle Real Application Clusters (RAC):**

  Установите опции монтирования в соответствии со *статьей на официальном сайте* (на английском).

[4] При установке Traffic Monitor на сервер под управлением Oracle Linux 7 не поддерживается работа с СУБД Postgres Pro Enterprise.

Далее будет описана установка с использованием инсталлятора для ОС Red Hat Enterprise Linux 7. В нашем примере нужно скопировать файл инсталлятора и архив с компонентами СУБД:

- инсталлятор:
  `iwtm-installer-7.14.0.97-rhel7`
  где `7.14.0.97` – номер сборки, `rhel7` – обозначение ОС;
- архив с компонентами СУБД:
  - если будет использована PostgreSQL (или одна из поддерживаемых СУБД на ее базе):
    `iwtm-postgresql-15.14-7.14.0.97-rhel7.tar.gz`
    где `postgresql-15.14` – обозначение СУБД, `7.14.0.97` – номер сборки, `rhel7` – обозначение ОС;
  - если будет использована СУБД Oracle:
    `iwtm-oracle-19.0.0.0.0-7.14.0.97.tar.gz`
    где `oracle-19.0.0.0.0` – обозначение СУБД, `7.14.0.97` – номер сборки.

Эта инструкция актуальна и для других поддерживаемых ОС: Oracle Linux, РЕД ОС, AlmaLinux, Rocky Linux и Альт Сервер.

6. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
   `cd /distr`
7. Перед запуском установки сделайте файл инсталлятора исполняемым. Для этого используйте команду вида:
   `chmod u+x ./iwtm-installer-x.x.x.xxx-rhel7`
   В нашем примере команда будет следующей:
   `chmod u+x ./iwtm-installer-7.14.0.97-rhel7`

Установка в текстовом режиме в консоли сервера

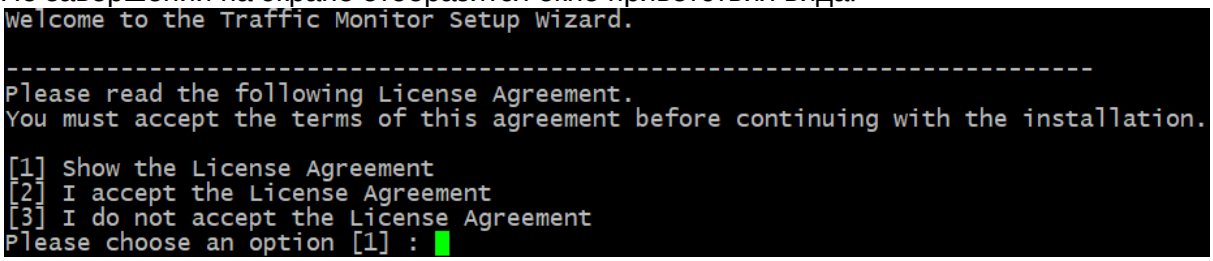
Чтобы установить компоненты Traffic Monitor Enterprise в текстовом режиме в консоли серверов, выполните следующие действия:

1. Для установки Traffic Monitor запустите инсталлятор, выполнив команду:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   В нашем примере команда будет следующей:
   `./iwtm-installer-7.14.0.97-rhel7`
   Начнется подготовка к запуску инсталлятора. На этом этапе не производится распаковка файлов.

> **Важно!**
>
> При отсутствии настроенных и доступных репозиториев ОС запуск инсталлятора прервется ошибкой:
>
> ```
> Preparing installation.../Warning: Failed to prepare installation:
> Missing OS repos or unsupported OS. Please mount and/or enable OS packages
> repository and try once again.
>
> For details refer to
> /var/log/infowatch/install/iwtm-installation_20211007114106.log or
> /tmp/installbuilder_installer_11672.log if the first doesn't exist
> Press [Enter] to continue:
> ```
>
> При возникновении этой ошибки нажмите **Enter** для завершения работы инсталлятора, затем подключите стандартный репозиторий ОС, репозиторий EPEL и повторно запустите инсталлятор.

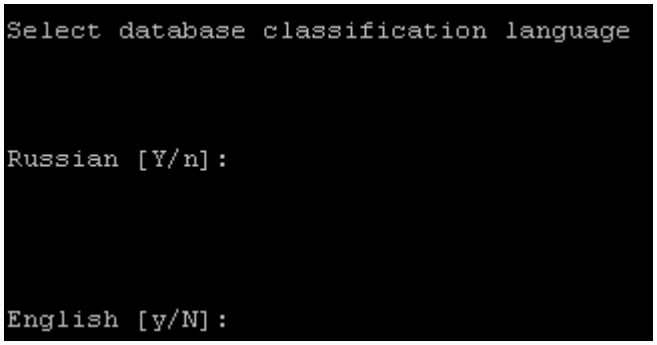
Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

По завершении на экране отобразится окно приветствия вида:



2. Для продолжения установки нужно принять условия Лицензионного соглашения. Выберите один из предложенных вариантов. Для этого введите цифру, указанную напротив него, и нажмите **Enter**:
   - `Show the License Agreement` – для просмотра Лицензионного соглашения;
     При выборе этого варианта:
     a. Выберите язык, на котором будет выведен текст Лицензионного соглашения:
        - `English` – английский;
        - `Russian` – русский;
     b. Прочитайте Лицензионное соглашение. Для перехода к следующей странице нажимайте **Enter**.
     c. Примите Лицензионное соглашение. Для этого введите **y** и нажмите **Enter**.
   - `I accept the License Agreement` – чтобы принять Лицензионное соглашение без предварительного просмотра;
   - `I do not accept the License Agreement` – чтобы не принимать Лицензионное соглашение и прервать процесс установки.

> **Примечание:**
>
> При установке в консоли сервера перед полем ввода в квадратных скобках указано значение по умолчанию. Оно будет использовано, если оставить поле ввода пустым и нажать **Enter**.
>
> **Пример:**
>
> Если на изображении выше не вводить значение, а только нажать Enter, будет выбран пункт `[1] Show the License Agreement`.
> Также значение по умолчанию в квадратных скобках может быть указано заглавной буквой.
>
> **Пример:**



3. Выберите для установки редакцию **`Traffic Monitor Enterprise (TME)`**.
4. На этапе выбора типа установки выберите **`Distributed`**.
5. Далее с помощью выбора шаблонов вы можете последовательно указать, какие наборы компонентов нужно будет использовать после установки на текущем сервере.

> **Важно!**
>
> Наборы требуемых компонентов, комбинации шаблонов и количество серверов определяются при планировании Системы в зависимости от предполагаемой нагрузки и окружения. Если вы будете пользоваться удаленной базой данных, устанавливайте шаблон "База данных" вместе с ещё хотя бы одним другим шаблоном.

> **Примечание:**
>
> В случае некорректной настройки службы Consul по завершении установки в консоли будет выведено предупреждение:
>
> 
>
>
> Для завершения работы инсталлятора нажмите **Enter**.
>
> **Для корректной работы Системы выполните проверку и настройку кластера службы Consul**
>
> a. Запустите службу Consul с помощью команды:
> `service iwtm-consul start`
> Проверьте статус службы командой:
> `service iwtm-consul status`
> b. Чтобы проверить службу Consul, выполните команды:
> i. Для вывода IP-адреса основного сервера (лидера) кластера:
> `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
> ii. Для вывода информации о членах кластера:
> `consul members`

c. Если не будет выведен IP-адрес лидера кластера, выполните *конфигурирование кластера службы Consul*.
После настройки повторите проверку (действие ii).

При данной ошибке инсталлятор не запустит сервисы Traffic Monitor по завершении работы – их нужно будет запустить вручную.

Ниже будет рассмотрена установка каждого шаблона на отдельный сервер.

Установка шаблона База данных

Если для установки выбран шаблон "База данных" (`Database`):

1. Выберите основной язык пользовательского интерфейса консоли управления, а также формат отображения даты, времени и язык предустановленных настроек:
   - **`Russian`** – для русскоязычного интерфейса;
   - **`English`** – для англоязычного интерфейса.
2. Выберите язык базы классификации. База классификации включает в себя предустановленные политики, элементы настройки технологий и объекты защиты. Для выбора доступны:
   - **`Russian`** – русский;
   - **`English`** – английский.

   Варианты будут предложены последовательно. Вы можете выбрать оба языка. Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.
3. Выберите расположение базы данных:
   - **`Install database server locally`** – для локальной установки на текущем сервере;
   - **`Use remote database server`** – для использования уже развернутой удаленной базы данных. В этом случае в удаленную базу данных будет добавлена схема Traffic Monitor.

   > **Примечание:**
   >
   > Вариант **`Install database server locally`** поддерживается только при использовании СУБД Oracle или PostgreSQL, поставляемых в дистрибутиве.

4. В случае установки на сервер под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux или Rocky Linux выберите одну из СУБД, с которой будет работать Система:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

> **Важно!**
>
> Выберите вариант **`PostgreSQL`** :
>
> - если вы устанавливаете Traffic Monitor на ОС Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8
> и/или
> - если вы будете использовать СУБД Postgres Pro Enterprise, Jatoba, Tantor или Pangolin.

5. Если вы выбрали использование удаленной базы данных, последовательно введите:
   a. IP-адрес или доменное имя сервера с базой данных.

      > **Важно!**
      >
      > Чтобы установить Traffic Monitor на одном сервере с уже развернутой СУБД, укажите адрес `127.0.0.1`.

   b. Порт подключения.
   c. Имя используемой базы данных, в которую будет добавлена схема.
6. При необходимости вы можете изменить значения по умолчанию для параметров аутентификации в базе данных.
   В случае утвердительного ответа будет предложено поменять следующие параметры:
   - Пароль пользователя с правами `sysdba`;
   - Имя владельца схемы базы данных;
   - Пароль владельца схемы базы данных;
   - Имя пользователя сервисов Linux;
   - Пароль пользователя сервисов Linux;
   - Имя пользователя веб-сервисов;
   - Пароль пользователя веб-сервисов;
   - Имя пользователя Nagios;
   - Пароль пользователя Nagios.
7. Выберите один из режимов хранения данных:
   - **`Norma l`** (обычный) – переключение на следующий раздел, если он указан, происходит при переполнении предыдущего.
   - **`Fast/Slow disks`** – разделение пулов на быстрый и медленный. Новые данные сохраняются в быстром разделе и через указанное количество дней перемещаются на медленные разделы. Медленный пул работает при этом в режиме `normal`.
   - **`Rotate`** – переход к следующему разделу происходит ежедневно и при переполнении предыдущего.
8. Вы можете изменить значения по умолчанию параметров хранения в базе данных.
   В случае утвердительного ответа вы можете поменять следующие параметры:
   - **`Main tablespaces path`** – путь к директории хранения данных основного табличного пространства;
   - Если выбран режим **`Fast/Slow disks`**:
     - **`Fast disk path`** – путь к директории хранения данных ежедневных табличных пространств в быстром разделе в режиме **`F ast/Slow disks`**;
     - **`Number of days to store daily  tablespaces on fast disk`** – период хранения данных ежедневных табличных пространств в быстром разделе в режиме **`F ast/Slow disks`**;
   - **`Number of daily tablespaces paths`** – количество путей для файлов ежедневных табличных пространств, число от 1 до 10;

     > **Примечание:**

Если указать значение больше 1, далее нужно будет последовательно указать пути к соответствующему числу ежедневных табличных пространств.

- **`Daily tablespaces paths`** – путь к директории хранения данных ежедневных табличных пространств.

9. Для ежедневных табличных пространств вы можете изменить значения по умолчанию для параметров архивирования.
В случае утвердительного ответа:
   - **`Path to archiving`** – путь к директории хранения файлов архивированных табличных пространств.

   Для каждого следующего параметра предварительно будет выведен запрос на использование:
   - **`Archive non-violation events`** – включить автоматическое архивирование событий, которые не являются нарушениям. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.
   - **`Archive violation events`** – включить автоматическое архивирование событий, которые являются нарушениями. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.
   - **`Archive screenshots`** – включить автоматическое архивирование снимков экрана, полученных от Агентов Device Monitor. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.

   Примечание:

   Если вы будете использовать Data Storage, то для архивирования табличных пространств необходимо во время установки хранилища указать путь к его медленному диску. Подробнее см. *Установка Платформы*.

10. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию – 90.
11. Вы можете включить использование внешнего хранилища бинарных данных Data Storage.
В случае утвердительного ответа укажите параметры подключения к внешнему хранилищу:
    - **`Data Storage hostname`** – имя хоста или IP-адрес сервера, на котором установлено хранилище;
    - **`Data Storage port`** – порт подключения к Data Storage, по умолчанию используется порт 40731;
    - **`Data Storage access token`** – токен авторизации Data Storage.

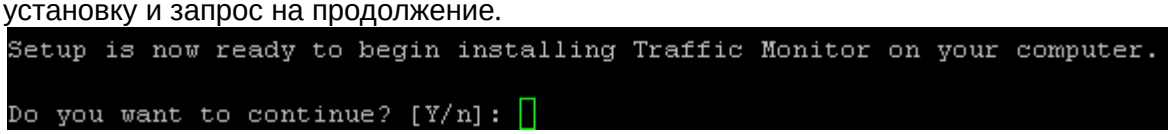
    Узнать актуальное значение токена можно:
    - На сервере Data Storage с помощью командной строки. Для этого:
      a. Перейдите в директорию, куда был распакован дистрибутив Платформы;
      b. Выполните команду:
      `./setup.py tokens list`
      В результате будет выведен список токенов для подключения к Платформе. Актуальный токен авторизации Data Storage будет указан напротив сущности *DataStorageUser*.

- В консоли управления платформенного продукта, в разделе **Основные настройки** в поле **Токен для Data Storage User**. Доступно, если на сервере с Data Storage установлен платформенный продукт с веб-интерфейсом и в нем есть данная настройка.

12. Укажите параметры подключения к службе Consul:
    a. **`Network interface address`** – выберите IP-адрес сетевого интерфейса.
    b. Режим работы Consul. Доступны два режима:
        - **`Server`**
        - **`Client`**

    > **Важно!**
    >
    > В одном кластере должно быть нечетное число серверов Consul – не больше 5.

    c. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.
    d. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
    e. **`Consul retryjoin servers`** – список серверов Consul, к которым нужно подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущем компьютере, оставьте поле пустым.
    f. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.
13. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:
    - **`Use system NTP-server`** – использовать системный NTP-сервер;
    - **`Set manually`** – указать NTP-сервер вручную. При выборе этого варианта нужно будет ввести IP-адрес или имя доступного NTP-сервера.
14. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.



Для начала установки введите **Y** и нажмите **Enter**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



Процесс может занять некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

15. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
Если установка прошла успешно, данные рекомендуется удалить.

16. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
17. Если нужно вывести список сервисов Traffic Monitor и их статусы, введите команду: `iwtm status`

Установка шаблона Индексер

Если для установки выбран шаблон "Индексер" (`Indexer service`):

1. Выберите одну из СУБД, с которой будет работать Система:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

   > **Примечание:**
   >
   > Тип СУБД должен соответствовать выбранному для шаблона "База данных".

2. Последовательно укажите параметры подключения к базе данных:
   a. IP-адрес или доменное имя сервера с базой данных.
   b. Порт подключения.
   c. Имя используемой базы данных.
3. При необходимости вы можете изменить значения по умолчанию для параметров аутентификации в базе данных.
   В случае утвердительного ответа будет предложено поменять следующие параметры:
   - Пароль пользователя с правами `sysdba` ;
   - Имя пользователя сервисов Linux;
   - Пароль пользователя сервисов Linux;
   - Имя пользователя веб-сервисов;
   - Пароль пользователя веб-сервисов;
   - Имя пользователя Nagios;
   - Пароль пользователя Nagios.
4. Укажите параметры подключения к службе Consul:
   a. **`Network interface address`** – выберите IP-адрес сетевого интерфейса.
   b. Режим работы Consul. Доступны два режима:
      - **`Server`**
      - **`Client`**

      > **Важно!**
      >
      > В одном кластере должно быть нечетное число серверов Consul – не больше 5.

   c. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm` .
   d. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
   e. **`Consul retryjoin servers`** – список серверов Consul, к которым нужно подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущем компьютере, оставьте поле пустым.
   f. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.
5. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:
   - **`Use system NTP-server`** – использовать системный NTP-сервер;

- `Set manually` – указать NTP-сервер вручную. При выборе этого варианта нужно будет ввести IP-адрес или имя доступного NTP-сервера.

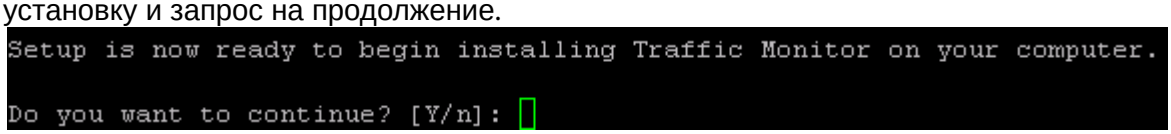
6. Далее для службы Sphinx вы можете включить индексацию на точное совпадение слов.

> **Важно!**
>
> Включение индексации на точное совпадение увеличит размер индекса минимум в 2 раза.

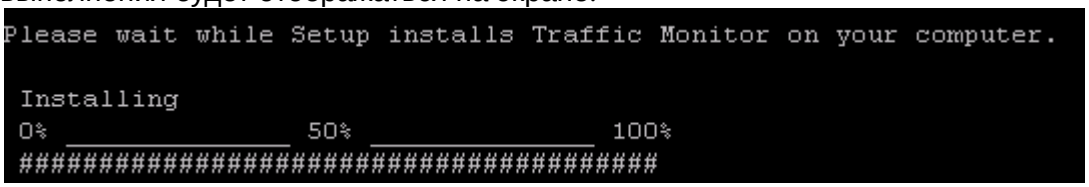
7. При необходимости вы можете изменить стандартные параметры работы службы Sphinx.
   В этом случае будет предложено задать список языков с поддержкой морфологии. По этим языкам будет проводиться индексация.
   Вы можете указать несколько языков, используя пробел в качестве разделителя.

> **Примечание:**
>
> Приоритет языков соответствует последовательности их выбора. Английский язык будет добавлен по умолчанию, он имеет самый высокий приоритет.

8. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.



   Для начала установки введите **Y** и нажмите **Enter**.
   Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



   Процесс может занять некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

9. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
   Если установка прошла успешно, данные рекомендуется удалить.
10. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
11. Если нужно вывести список сервисов Traffic Monitor и их статусы, введите команду:
    `iwtm status`

Установка шаблона Веб-консоль

Если для установки выбран шаблон "Веб-консоль" (`Web console`):

1. В случае установки на сервер под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux или Rocky Linux выберите одну из СУБД, с которой будет работать Система:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

   > **Примечание:**
   >
   > Тип СУБД должен соответствовать выбранному для шаблона "База данных".

2. Последовательно укажите параметры подключения к базе данных:
   a. IP-адрес или доменное имя сервера с базой данных.
   b. Порт подключения.
   c. Имя используемой базы данных.
3. При необходимости вы можете изменить значения по умолчанию для параметров аутентификации в базе данных.
   В случае утвердительного ответа будет предложено поменять следующие параметры:
   - Пароль пользователя с правами `sysdba` ;
   - Имя владельца схемы базы данных;
   - Имя пользователя сервисов Linux;
   - Пароль пользователя сервисов Linux;
   - Имя пользователя веб-сервисов;
   - Пароль пользователя веб-сервисов;
   - Имя пользователя Nagios;
   - Пароль пользователя Nagios.
4. Укажите параметры подключения к службе Consul:
   a. **`Network interface address`** – выберите IP-адрес сетевого интерфейса.
   b. Режим работы Consul. Доступны два режима:
      - **`Server`**
      - **`Client`**

      > **Важно!**
      >
      > В одном кластере должно быть нечетное число серверов Consul – не больше 5.

   c. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm` .
   d. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
   e. **`Consul retryjoin servers`** – список серверов Consul, к которым нужно подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущем компьютере, оставьте поле пустым.
   f. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.
5. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:
   - **`Use system NTP-server`** – использовать системный NTP-сервер;
   - **`Set manually`** – указать NTP-сервер вручную. При выборе этого варианта нужно будет ввести IP-адрес или имя доступного NTP-сервера.

6. Укажите адрес сервера, на котором функционирует служба Sphinx (шаблон "Индексер").

> **Примечание:**
>
> Если шаблоны "Индексер" и "Веб-консоль" устанавливаются на один сервер, инсталлятор не будет запрашивать этот параметр.

7. Вы можете включить использование технологии OCR.

> **Примечание:**
>
> OCR-экстрактор выбирается при установке шаблона "Перехватчики".

8. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.

```
Setup is now ready to begin installing Traffic Monitor on your computer.

Do you want to continue? [Y/n]:
```

Для начала установки введите **Y** и нажмите **Enter**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.

```
Please wait while Setup installs Traffic Monitor on your computer.

 Installing
 0% _____________ 50% _____________ 100%
 ########################################
```

Процесс может занять некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

9. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
   Если установка прошла успешно, данные рекомендуется удалить.
10. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
11. Если нужно вывести список сервисов Traffic Monitor и их статусы, введите команду: `iwtm status`

Установка шаблона Перехватчики

Если для установки выбран шаблон "Перехватчики" (`Interceptors`):

1. В случае установки на сервер под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux или Rocky Linux выберите одну из СУБД, с которой будет работать Система:
   - **`Oracle Database Enterprise Edition`**

- **PostgreSQL**

> **Примечание:**
>
> Тип СУБД должен соответствовать выбранному для шаблона "База данных".

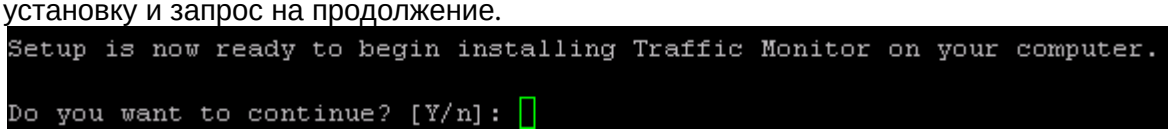
2. Последовательно укажите параметры подключения к базе данных:
   a. IP-адрес или доменное имя сервера с базой данных.
   b. Порт подключения.
   c. Имя используемой базы данных.
3. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.
   В случае утвердительного ответа будет предложено поменять следующие параметры:
   - Пароль пользователя с правами sysdba;
   - Имя пользователя сервисов Linux;
   - Пароль пользователя сервисов Linux;
   - Имя пользователя веб-сервисов;
   - Пароль пользователя веб-сервисов;
   - Имя пользователя nagios;
   - Пароль пользователя nagios.
4. Укажите параметры подключения к службе Consul:
   a. **Network interface address** – выберите IP-адрес сетевого интерфейса.
   b. Режим работы Consul. Доступны два режима:
      - **Server**
      - **Client**

      > **Важно!**
      >
      > В одном кластере должно быть нечетное число серверов Consul – не больше 5.

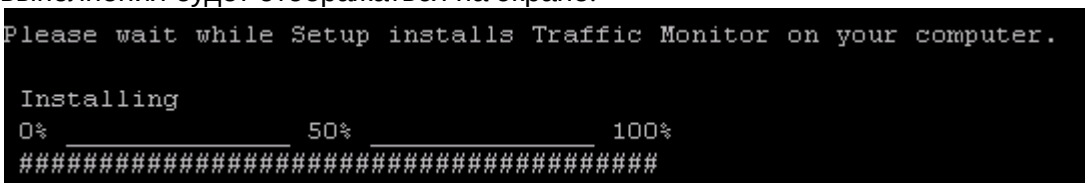
   c. **Datacenter name** – введите название дата-центра Consul. По умолчанию – `iwtm`.
   d. **Node name** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
   e. **Consul retryjoin servers** – список серверов Consul, к которым нужно подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущем компьютере, оставьте поле пустым.
   f. **Consul retryjoin port** – порт подключения к указанным серверам Consul.
5. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:
   - **Use system NTP-server** – использовать системный NTP-сервер;
   - **Set manually** – указать NTP-сервер вручную. При выборе этого варианта нужно будет ввести IP-адрес или имя доступного NTP-сервера.
6. Вы можете включить использование технологии OCR.
   В случае включения нужно выбрать для использования одну из систем:
   - **Content AI ContentReader Engine**;
   - **Tesseract**.

> **Примечание:**
>
> Для работы OCR включите использование технологии при установке шаблона "Веб-консоль".

7. Если выбран OCR-экстрактор Content AI ContentReader Engine:
   a. Выберите один из режимов распознавания:
      - `Quick` – быстрый режим;
      - `Quality` – тщательный режим, обеспечивающий более высокое качество распознавания.
   b. Подтвердите наличие у вас активной лицензии на использование Content AI ContentReader Engine.
      Если у вас отсутствует лицензия, введите **N** и нажмите **Enter**. В этом случае ContentReader Engine будет установлен без лицензии. Для возможности работы ContentReader Engine активную лицензию нужно будет добавить позже вручную.
      Подробнее см. в документе *InfoWatch Traffic Monitor. Руководство администратора. Настройка OCR-экстракторов*.
8. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.



   Для начала установки введите **Y** и нажмите **Enter**.
   Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



   Процесс может занять некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

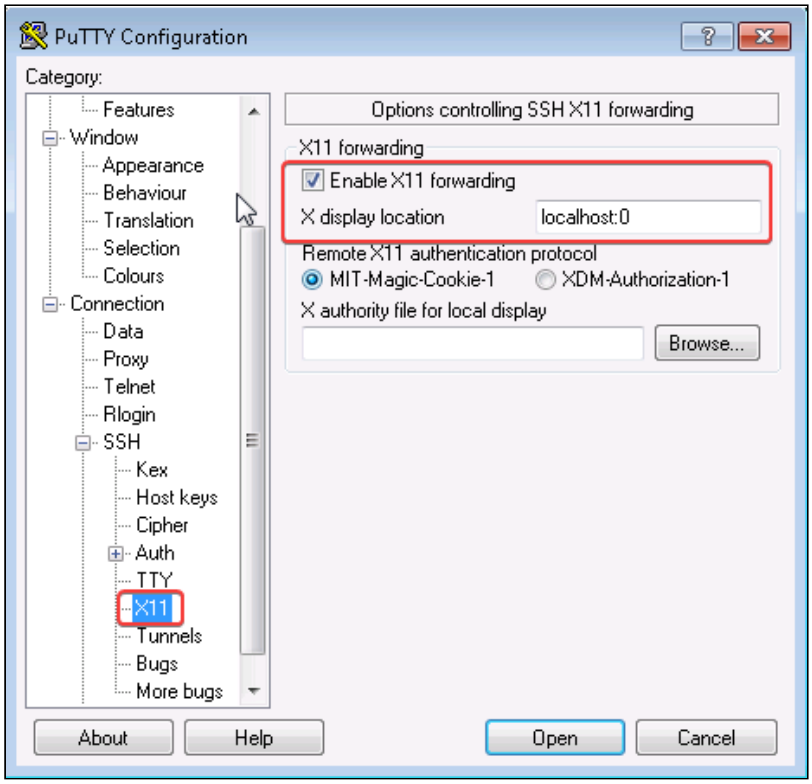
9. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
   Если установка прошла успешно, данные рекомендуется удалить.
10. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
11. Если нужно вывести список сервисов Traffic Monitor и их статусы, введите команду:
    `iwtm status`

Установка с использованием графического режима инсталлятора

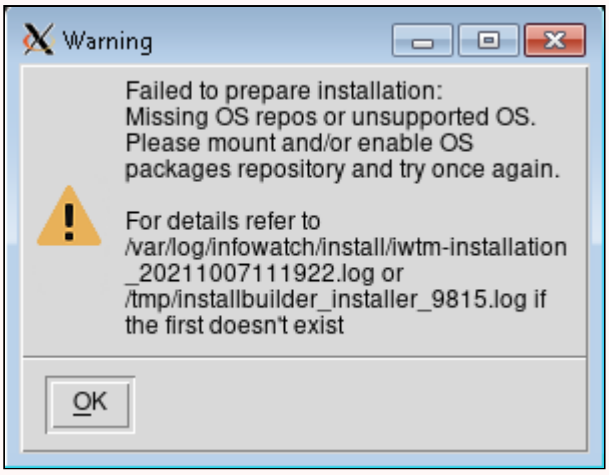
В ОС оконная система X Window System использует клиент-серверную модель. Для запуска инсталлятора в графическом режиме используется перенаправление графического вывода удаленной подсистемы (**X11 Forwarding**). Это позволит работать напрямую с графическими приложениями среды Linux на компьютере, с которого осуществляется подключение к серверу. Этот режим реализуется с помощью SSH-подключения.

Чтобы установить компоненты Traffic Monitor Enterprise с использованием графического режима инсталлятора, выполните следующие действия:

1. На сервере, на котором планируется установка компонентов Traffic Monitor:
   a. Установите утилиту xauth с помощью команды:
      - На сервере под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux, Rocky Linux или РЕД ОС:
        `yum install xauth`
      - На сервере под управлением ОС Альт Сервер:
        `sudo apt-get install xauth`
   b. Убедитесь, что в конфигурационном файле `/etc/ssh/sshd_config`:
      - для параметра `X11Forwarding` установлено значение `yes`;
      - строка с параметром `X11Forwarding` раскомментирована, то есть не содержит символ `#`.
   c. Сохраните изменения в конфигурационном файле.
   d. Перезапустите службу SSH с помощью команды:
      `systemctl restart sshd`
2. На компьютере, на котором будет использован графический режим:
   a. Для подключения к серверу установки Traffic Monitor вам потребуется SSH-клиент с включенной опцией X11 Forwarding, например PuTTY.
   b. Для запуска инсталлятора в графическом режиме вам потребуется настроенное приложение-клиент для обращения к X Window System, например:
      - приложение Xming – для ОС семейства MS Windows;
      - оболочка Gnome 3 – для ОС семейства Linux.
3. Запустите настроенное приложение-клиент для обращения к X Window System.
4. Подключитесь к серверу, на котором планируется установка компонентов Traffic Monitor, с помощью выбранного SSH-клиента.
   Пример окна настройки PuTTY при подключении



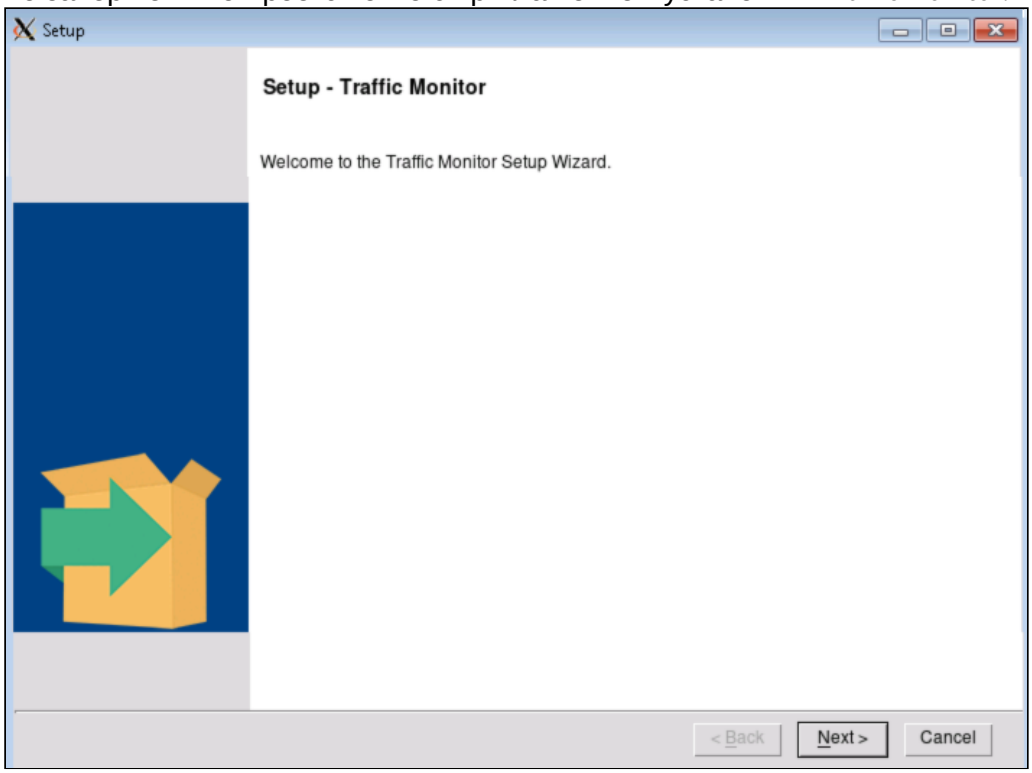
5. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
   `./iwtm-installer-x.x.x.xxx-rhel7`
   В нашем примере команда будет следующей:
   `./iwtm-installer-7.14.0.97-rhel7`
   Начнется подготовка к запуску инсталлятора. На этом этапе не производится распаковка файлов.

> **Важно!**
>
> При отсутствии настроенных и доступных репозиториев ОС запуск инсталлятора прервется со следующей ошибкой:
>
> 
>

При возникновении этой ошибки нажмите кнопку **OK** для закрытия окна и завершения работы инсталлятора, подключите стандартный репозиторий ОС, репозиторий EPEL, а затем повторно запустите инсталлятор.

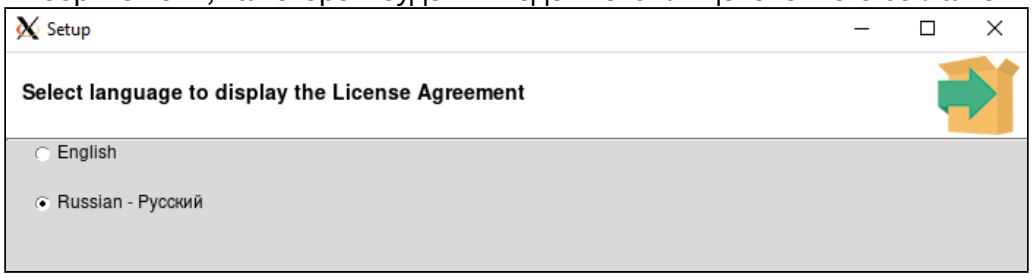
Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

По завершении откроется окно с приглашением установить Traffic Monitor:



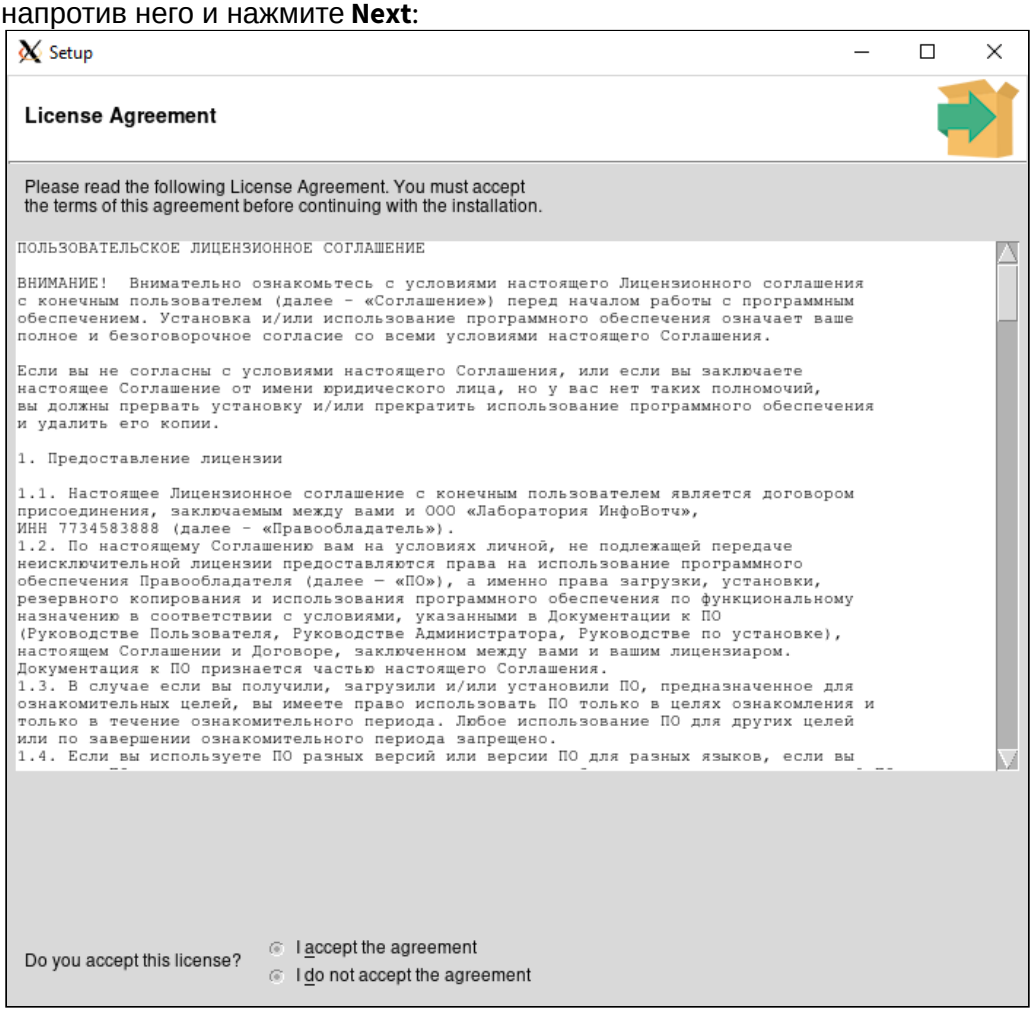
Для перехода к следующему параметру нажмите **Next**, для возврата к предыдущему – **Back**. Для выхода из инсталлятора нажмите **Cancel**.

6. Для продолжения установки нужно принять условия Лицензионного соглашения. Для этого:
   a. Выберите язык, на котором будет выведен текст Лицензионного соглашения:



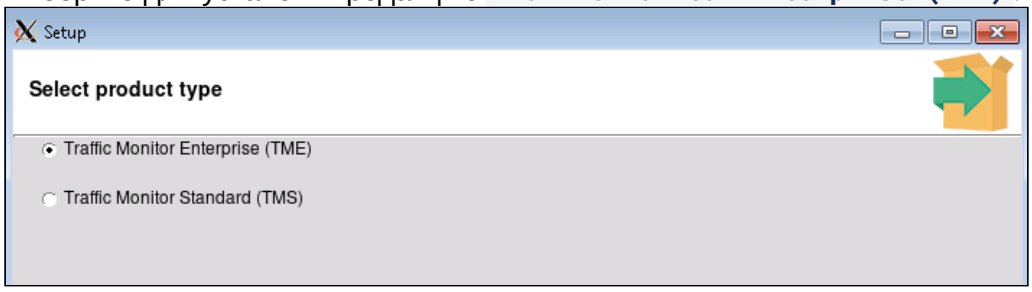
- `English` – английский;
- `Russian` – русский;

b. Выберите один из предложенных вариантов. Для этого установите флажок напротив него и нажмите **Next**:



- **`I accept the agreement`** – чтобы принять Лицензионное соглашение и продолжить процесс установки;
- **`I do not accept the agreement`** – чтобы не принимать Лицензионное соглашение и прервать процесс установки.

7. Выберите для установки редакцию **`Traffic Monitor Enterprise (TME)`**.



8. На этапе выбора типа установки выберите **`Distributed`**.
9. Далее с помощью выбора шаблонов вы можете указать, какие наборы компонентов нужно будет использовать после установки на текущем сервере.



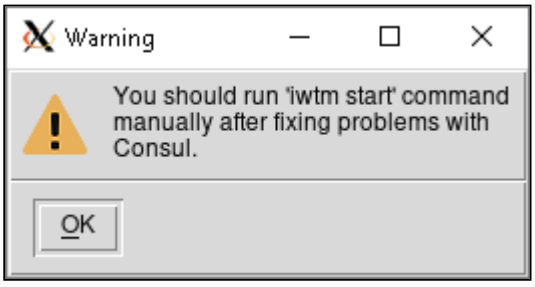
Чтобы выбрать сразу несколько значений, отметьте их флажками и нажмите **Next**.

Важно!

Наборы требуемых компонентов, комбинации шаблонов и количество серверов определяются при планировании Системы в зависимости от предполагаемой нагрузки и окружения.
Если будет использована удаленная база данных, устанавливайте шаблон "База данных" вместе с ещё хотя бы одним другим шаблоном.

Примечание:

В случае некорректной настройки службы Consul по завершении установки в консоли будет выведено предупреждение:



Для закрытия окна и завершения работы инсталлятора нажмите **OK**.

Для корректной работы Системы выполните проверку и настройку кластера службы Consul

a. Запустите службу Consul, выполнив команду:
`service iwtm-consul start`
Проверить статус службы можно командой:
`service iwtm-consul status`
b. Чтобы проверить службу Consul, выполните команды:
   i. Для вывода IP-адреса основного сервера (лидера) кластера:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. Для вывода информации о членах кластера:
   `consul members`
c. Если не будет выведен IP-адрес лидера кластера, выполните *конфигурирование кластера службы Consul*.
После настройки повторите проверку (действие ii).

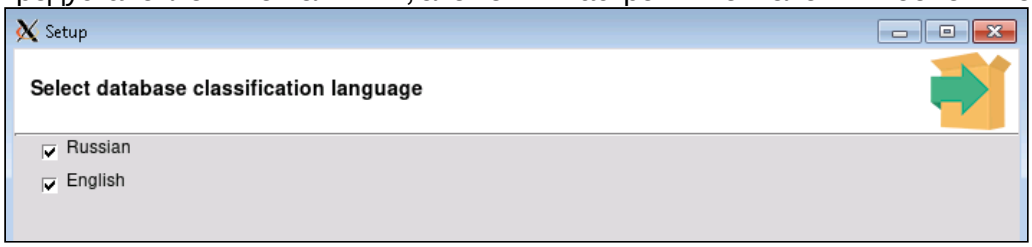
При данной ошибке инсталлятор не запустит сервисы Traffic Monitor по завершении работы – их нужно будет запустить вручную.

Ниже будет рассмотрена установка каждого шаблона на отдельный сервер.

Установка шаблона База данных

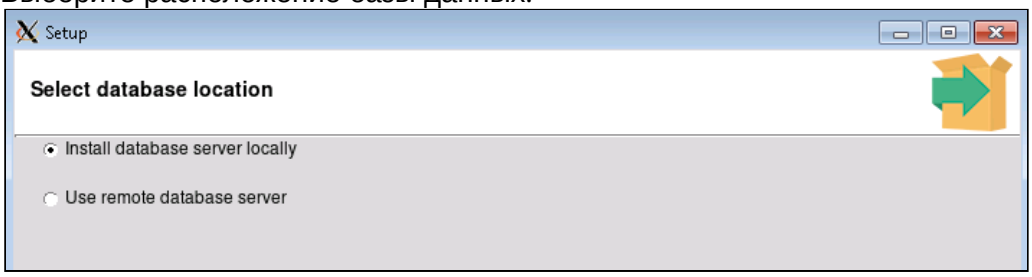
Если для установки выбран шаблон "База данных" (`Database`):

1. Выберите основной язык пользовательского интерфейса консоли управления, а также формат отображения даты, времени и язык предустановленных настроек:
   - **`Russian`** – для русскоязычного интерфейса;
   - **`English`** – для англоязычного интерфейса.
2. Выберите язык базы классификации. База классификации включает в себя предустановленные политики, элементы настройки технологий и объекты защиты.



   Для выбора доступны:
   - **`Russian`** – русский;
   - **`English`** – английский.

   Чтобы выбрать оба значения, отметьте их флажками и нажмите **Next**. Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.
3. Выберите расположение базы данных:



   - **`Install database server locally`** – для локальной установки на текущем сервере;
   - **`Use remote database server`** – для использования уже развернутой удаленной базы данных. В этом случае в удаленную базу данных будет добавлена схема Traffic Monitor.

     Примечание:

     Вариант **`Install database server locally`** поддерживается только при использовании СУБД Oracle или PostgreSQL, поставляемых в дистрибутиве.

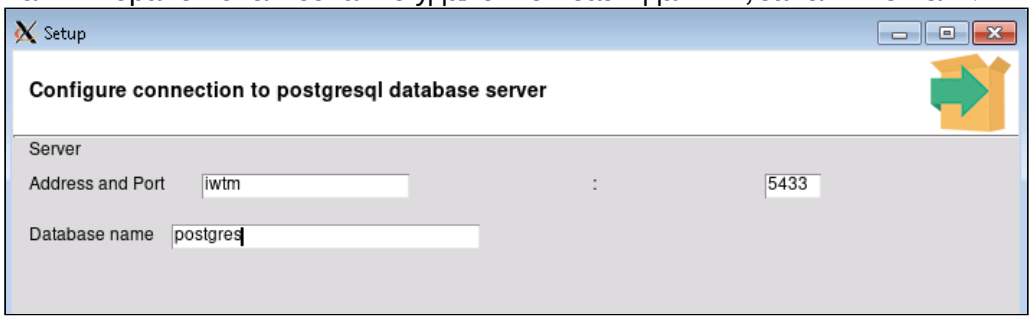
4. В случае установки на сервер под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux или Rocky Linux выберите одну из СУБД, с которой будет работать Система:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

Важно!

Выберите вариант **`PostgreSQL`**:

- если вы устанавливаете Traffic Monitor на ОС Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8
  и/или
- если вы будете использовать СУБД Postgres Pro Enterprise, Jatoba, Tantor или Pangolin.

5. Если выбрано использование удаленной базы данных, заполните поля:



   a. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.

   Важно!

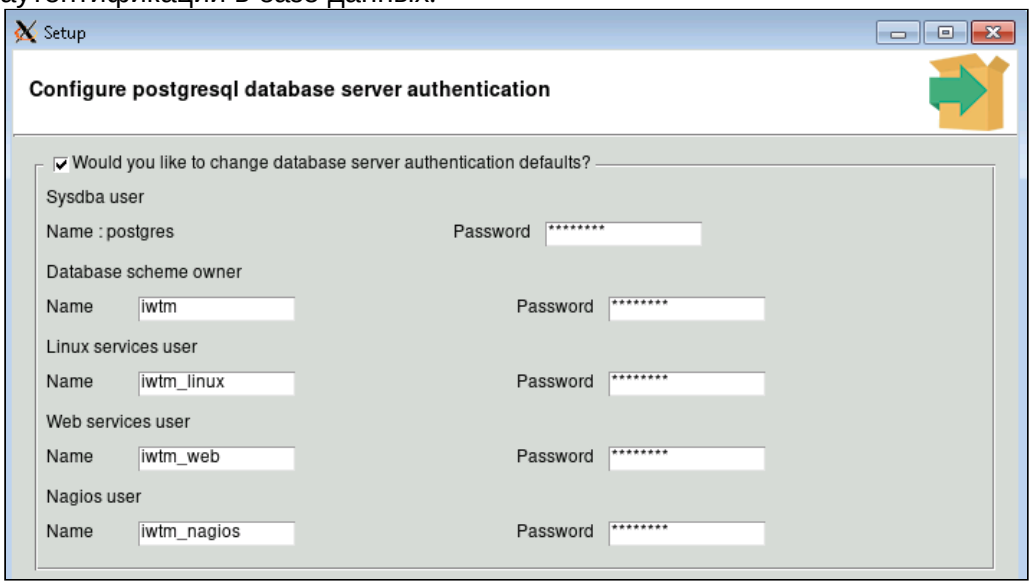
   Чтобы установить Traffic Monitor на одном сервере с уже развернутой СУБД, укажите адрес `127.0.0.1`.

   b. **`Database name`** – имя используемой базы данных, в которую будет добавлена схема.

Примечание:

В графическом режиме в активных полях указаны значения по умолчанию.

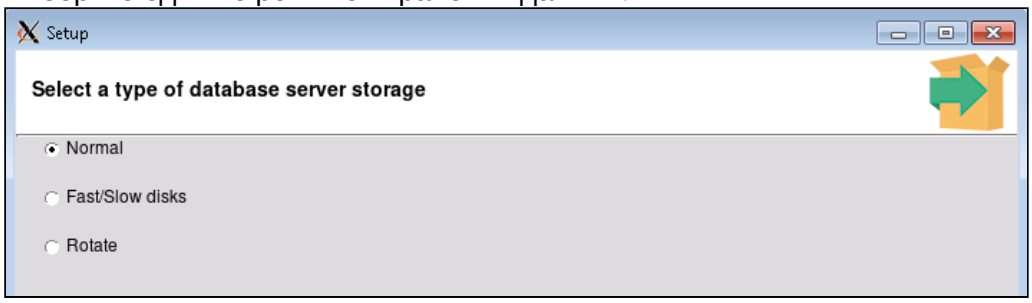
6. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



Чтобы отредактировать значения, установите флажок напротив поля с вопросом. Это сделает доступными для редактирования следующие разделы:

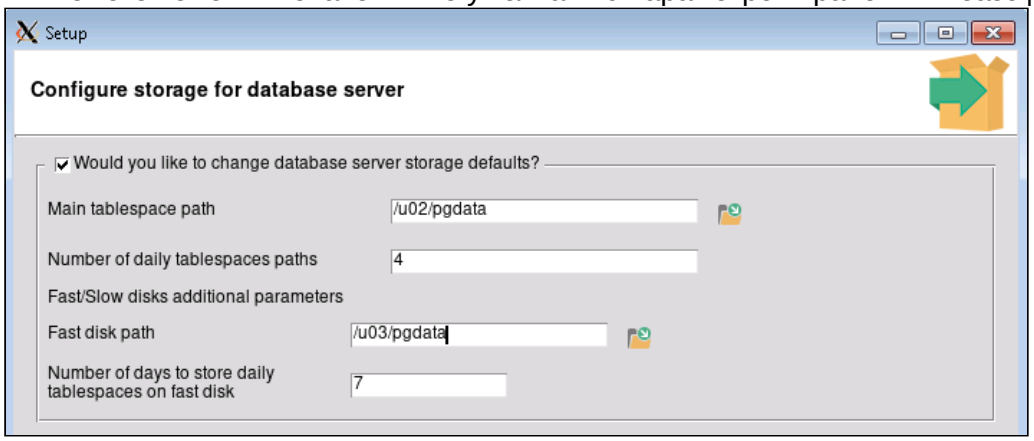
- **`Sysdba user`** – пароль пользователя с правами sysdba;
- **`Database scheme owner`** – имя и пароль владельца схемы базы данных;
- **`Linux services user`** – имя и пароль пользователя сервисов Linux;
- **`Web services user`** – имя и пароль пользователя веб-сервисов;
- **`Nagios user`** – имя и пароль пользователя nagios.

7. Выберите один из режимов хранения данных:

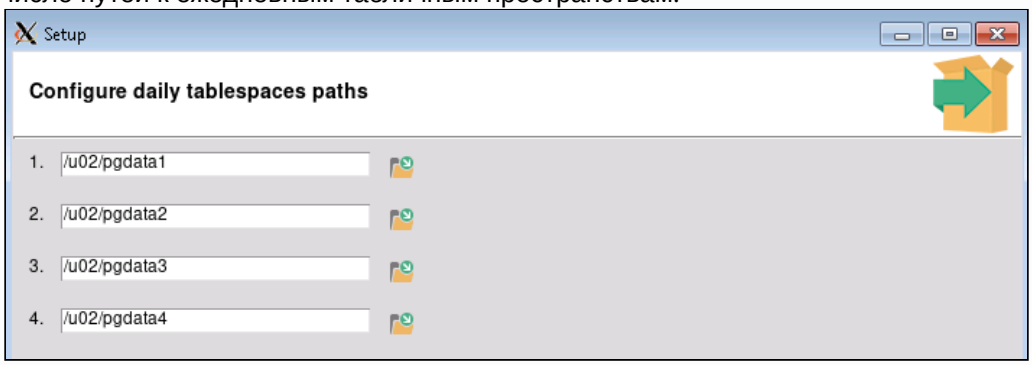


- **`Norma l`** (обычный) – переключение на следующий раздел, если он указан, происходит при переполнении предыдущего.
- **`Fast/Slow disks`** – разделение пулов на быстрый и медленный. Новые данные сохраняются в быстром разделе и через указанное количество дней перемещаются на медленные разделы. Медленный пул работает при этом в режиме `normal`.
- **`Rotate`** – переход к следующему разделу происходит ежедневно и при переполнении предыдущего.

8. Вы можете изменить значения по умолчанию параметров хранения в базе данных.

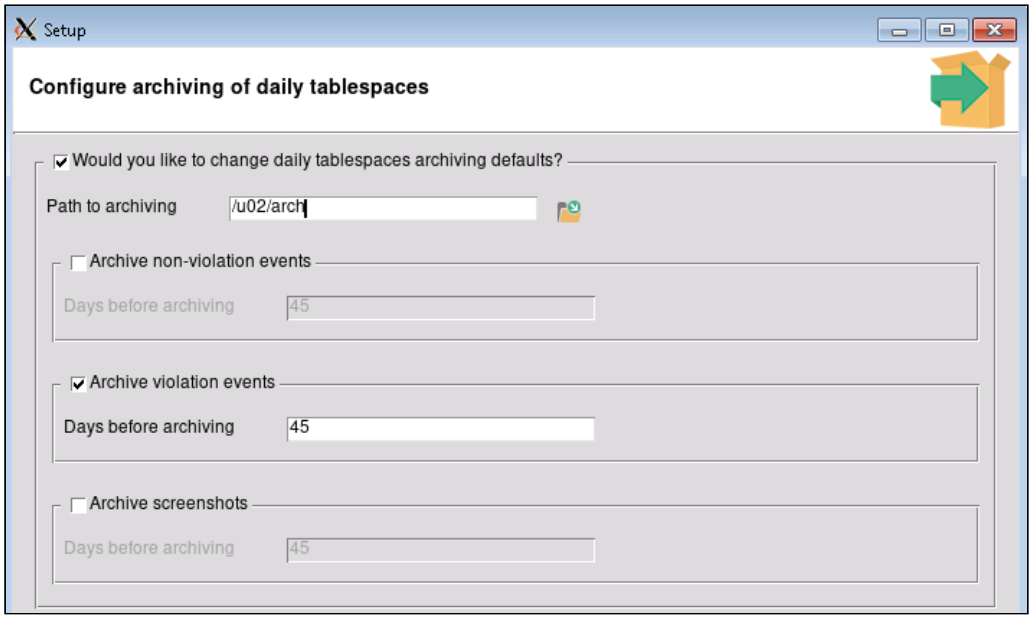


- **`Main tablespaces path`** – путь к директории хранения данных основного табличного пространства;
  Вы можете вписать путь в поле или указать его в окне файлового менеджера с помощью кнопки .
- Если выбран режим **`Fast/Slow disks`**:
  - **`Fast disk path`** – путь к директории хранения данных ежедневных табличных пространств в быстром разделе в режиме **`F ast/Slow disks`**;
  - **`Number of days to store daily  tablespaces on fast disk`** – период хранения данных ежедневных табличных пространств в быстром разделе в режиме **`F ast/Slow disks`**;
- **`Number of daily tablespaces paths`** – количество путей для файлов ежедневных табличных пространств, число от 1 до 10;

> **Примечание:**
>
> Если указать значение больше 1, далее нужно будет указать соответствующее число путей к ежедневным табличным пространствам.
>
> 
>

- **`Daily tablespaces paths`** – путь к директории хранения данных ежедневных табличных пространств.

9. Для ежедневных табличных пространств вы можете изменить значения по умолчанию для параметров архивирования.



- **`Path to archiving`** – путь к директории хранения файлов архивированных табличных пространств.

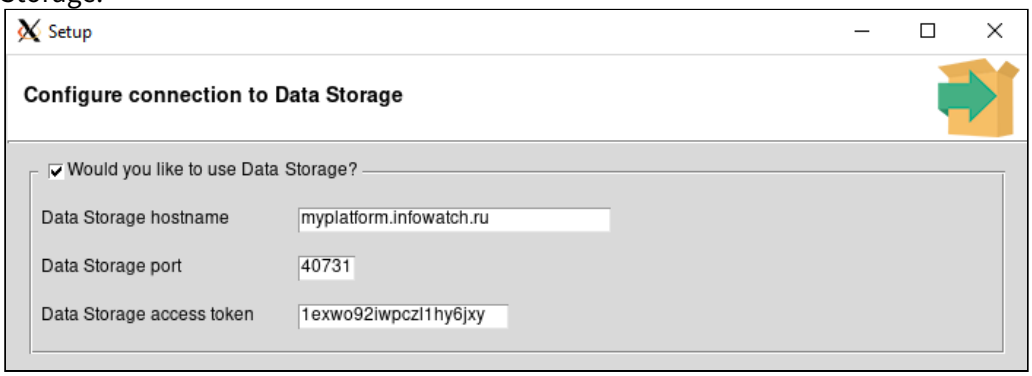
Каждый параметр включается отдельно:

- **`Archive non-violation events`** – включить автоматическое архивирование событий, которые не являются нарушениям. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.
- **`Archive violation events`** – включить автоматическое архивирование событий, которые являются нарушениями. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.
- **`Archive screenshots`** – включить автоматическое архивирование снимков экрана, полученных от Агентов Device Monitor. В случае включения укажите число дней до архивирования. Значение по умолчанию – 45.

> **Примечание:**
>
> Если вы будете использовать Data Storage, то для архивирования табличных пространств необходимо во время установки хранилища указать путь к его медленному диску. Подробнее см. *Установка Платформы*.

10. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию – 90.

11. Вы можете включить использование внешнего хранилища бинарных данных Data Storage.



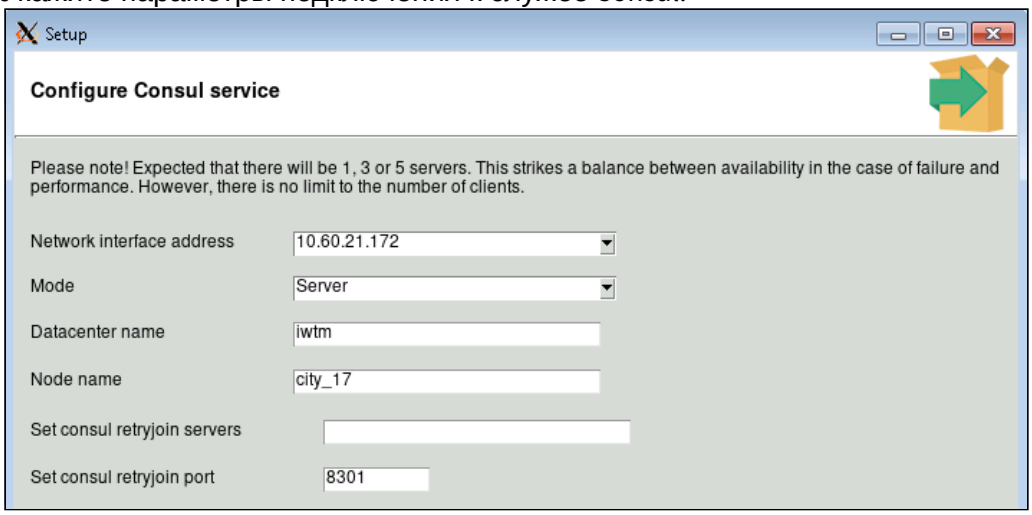
Для этого установите флажок напротив поля с вопросом и укажите параметры подключения к внешнему хранилищу:

- **`Data Storage hostname`** – имя хоста или IP-адрес сервера, на котором установлено хранилище;
- **`Data Storage port`** – порт подключения к Data Storage, по умолчанию используется порт 40731;
- **`Data Storage access token`** – токен авторизации Data Storage.

Узнать актуальное значение токена можно:

- На сервере Data Storage с помощью командной строки. Для этого:
  a. Перейдите в директорию, куда был распакован дистрибутив Платформы;
  b. Выполните команду:
  `./setup.py tokens list`
  В результате будет выведен список токенов для подключения к Платформе. Актуальный токен авторизации Data Storage будет указан напротив сущности *DataStorageUser*.
- В консоли управления платформенного продукта, в разделе **Основные настройки** в поле **Токен для Data Storage User**. Доступно, если на сервере с Data Storage установлен платформенный продукт с веб-интерфейсом и в нем есть данная настройка.

12. Укажите параметры подключения к службе Consul:



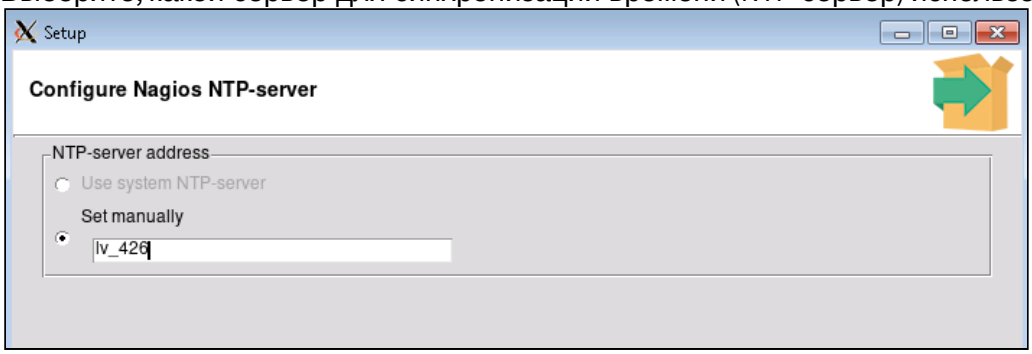
a. **`Network interface address`** – выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите ▼ и в раскрывшемся списке выберите нужное значение.

b. Доступны два режима работы Consul:
   - `Server`
   - `Client`

> **Важно!**
>
> В одном кластере должно быть нечетное число серверов Consul – не больше 5.

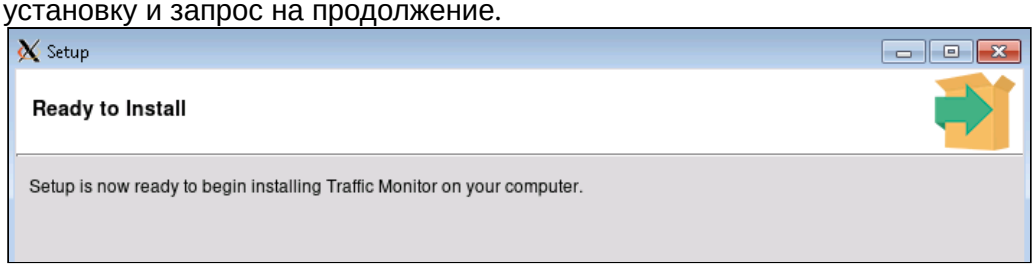
c. `Datacenter name` – введите название дата-центра Consul. По умолчанию – `iwtm`.
d. `Node name` – имя сервера, на который устанавливаются компоненты Traffic Monitor.
e. `Consul retryjoin servers` – список серверов Consul, к которым нужно подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущем компьютере, оставьте поле пустым.
f. `Consul retryjoin port` – порт подключения к указанным серверам Consul.

13. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:

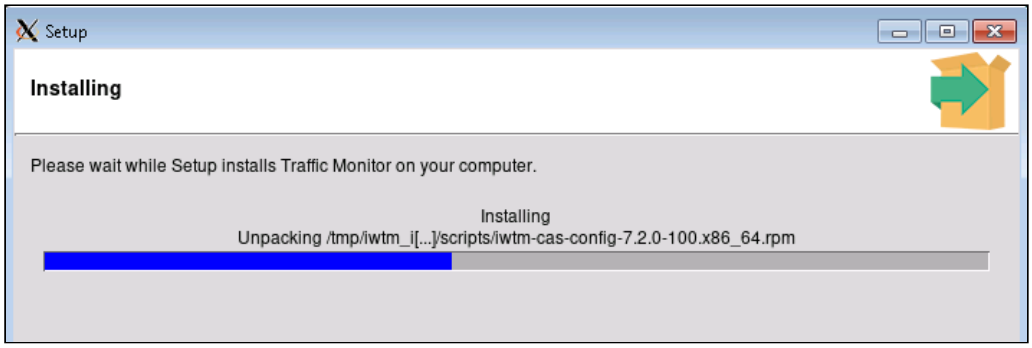


- `Use system NTP-server` – использовать системный NTP-сервер;
- `Set manually` – указать NTP-сервер вручную. При выборе этого варианта укажите IP-адрес или имя доступного NTP-сервера.

14. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.



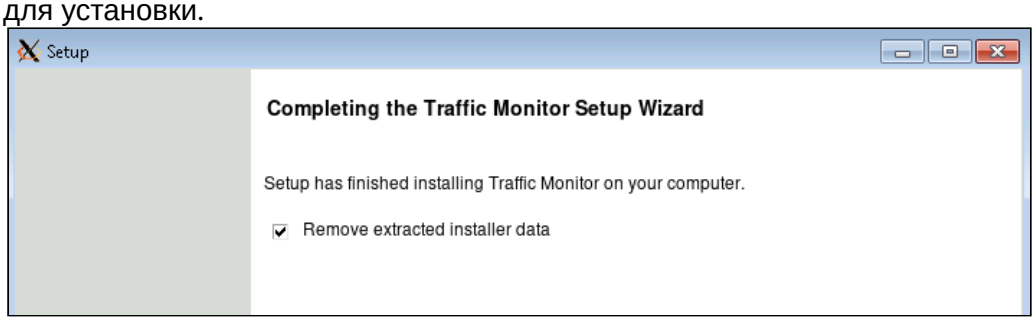
Для начала установки нажмите **Next**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



Процесс может занять некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

15. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.



Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove extracted installer data`**.

16. Для завершения нажмите **Finish**.
17. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
18. Если нужно вывести список сервисов Traffic Monitor и их статусы, введите команду: `iwtm status`

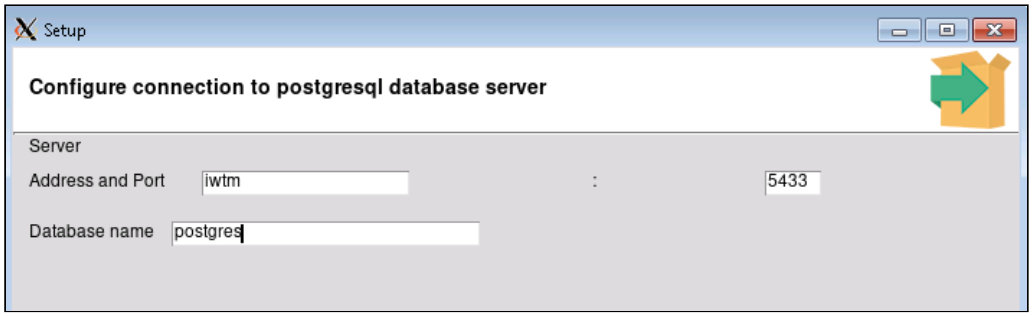
Установка шаблона Индексер

Если для установки выбран шаблон "Индексер" (Indexer service):

1. В случае установки на сервер под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux или Rocky Linux выберите одну из СУБД, с которой будет работать Система:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

> **Примечание:**
>
> Тип СУБД должен соответствовать выбранному для шаблона "База данных".

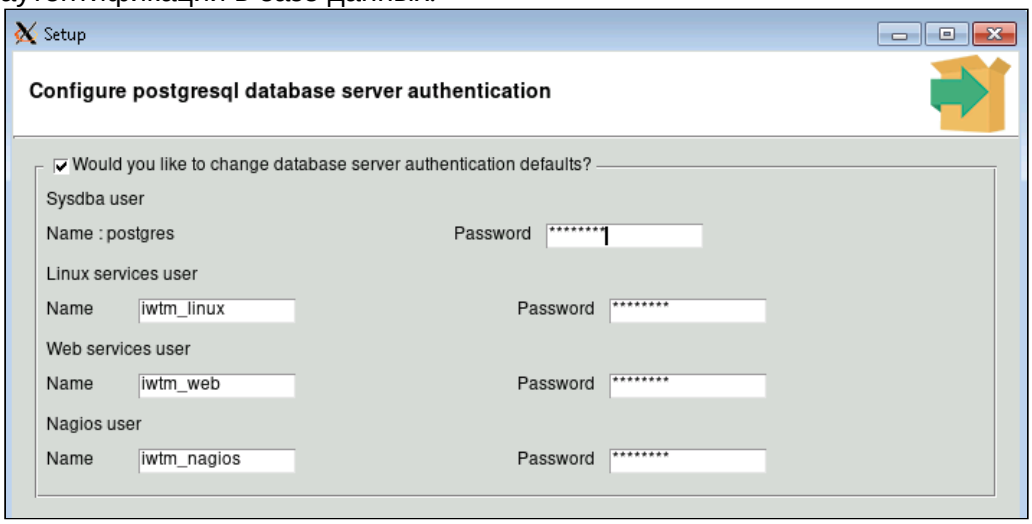
2. Укажите параметры подключения к базе данных:



a. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.
b. **`Database name`** – имя используемой базы данных.

> **Примечание:**
>
> В графическом режиме в активных полях указаны значения по умолчанию.

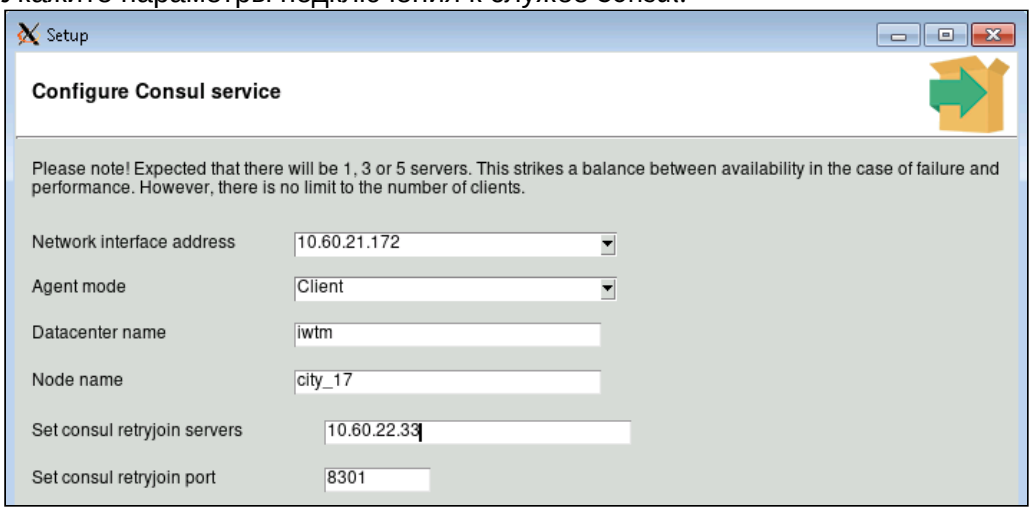
3. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



Чтобы отредактировать значения, установите флажок напротив поля с вопросом. Это сделает доступными для редактирования следующие разделы:

- **`Sysdba user`** – пароль пользователя с правами `sysdba`;
- **`Linux services user`** – имя и пароль пользователя сервисов Linux;
- **`Web services user`** – имя и пароль пользователя веб-сервисов;
- **`Nagios user`** – имя и пароль пользователя Nagios.

4. Укажите параметры подключения к службе Consul:

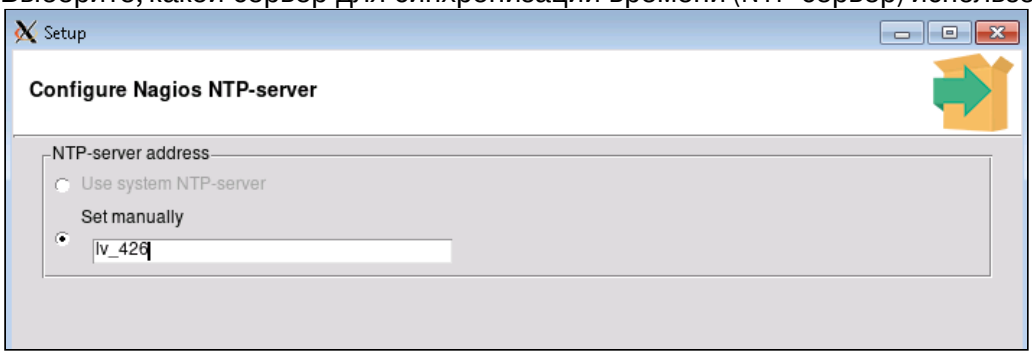


   a. **`Network interface address`** – выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите ▾ и в раскрывшемся списке выберите нужное значение.
   b. Доступны два режима работы Consul:
      - **`Server`**
      - **`Client`**

> **Важно!**
>
> В одном кластере должно быть нечетное число серверов Consul – не больше 5.

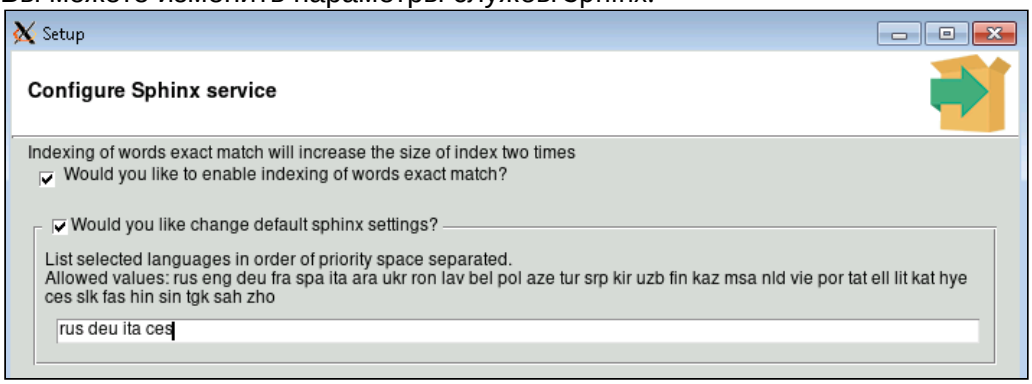
   c. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.
   d. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
   e. **`Consul retryjoin servers`** – список серверов Consul, к которым нужно подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущем компьютере, оставьте поле пустым.
   f. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

5. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:



   - **`Use system NTP-server`** – использовать системный NTP-сервер;
   - **`Set manually`** – указать NTP-сервер вручную. При выборе этого варианта нужно будет ввести IP-адрес или имя доступного NTP-сервера.

6. Вы можете изменить параметры службы Sphinx:



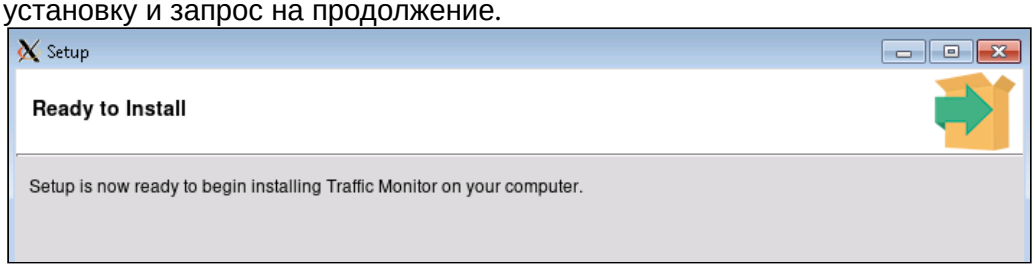
- `Enable indexing of words exact match` – включить индексацию на точное совпадение слов;

> **Важно!**
>
> Включение индексации на точное совпадение увеличит размер индекса минимум в 2 раза.

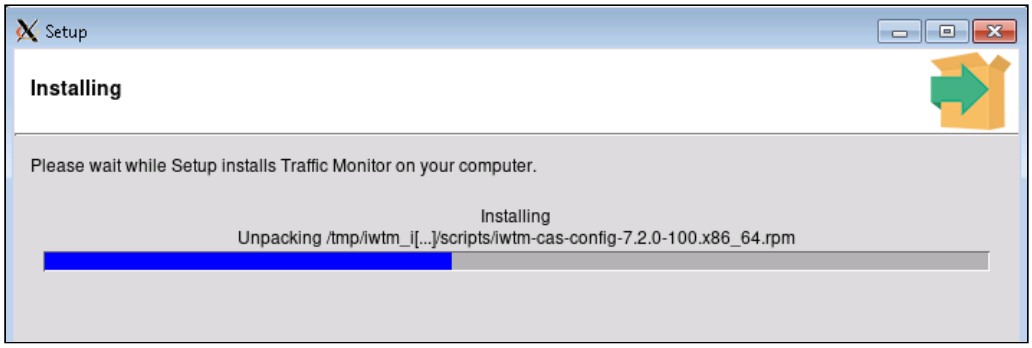
- При необходимости вы можете изменить стандартные параметры работы службы Sphinx (`default sphinx settings`). В этом случае укажите список языков с поддержкой морфологии. По этим языкам будет проводиться индексация. Вы можете указать несколько языков, используя пробел в качестве разделителя.

> **Примечание:**
>
> Приоритет языков соответствует последовательности их выбора. Английский язык будет добавлен по умолчанию, он имеет самый высокий приоритет.

7. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.



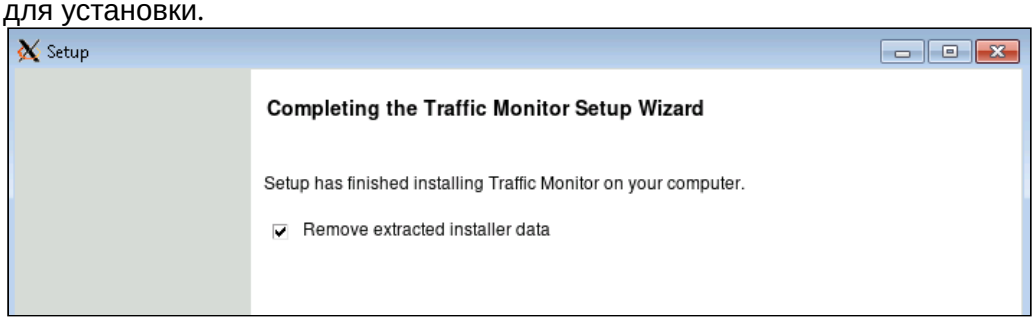
Для начала установки нажмите **Next**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



Процесс может занять некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

8. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.



Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove extracted installer data`**.

9. Для завершения нажмите **Finish**.
10. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
11. Если нужно вывести список сервисов Traffic Monitor и их статусы, введите команду: `iwtm status`

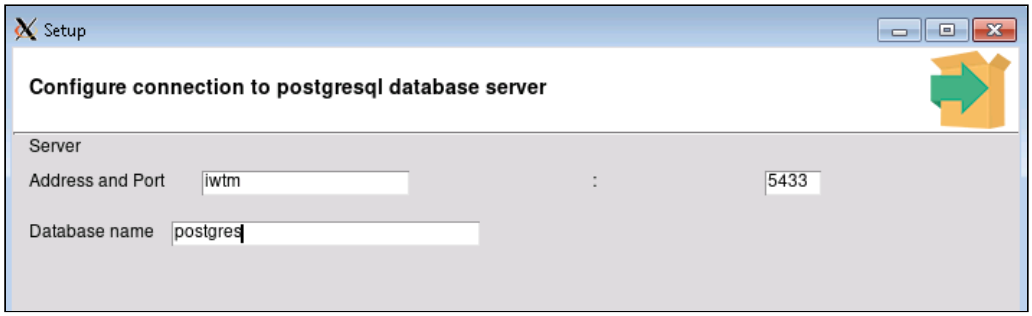
Установка шаблона Веб-консоль

Если для установки выбран шаблон "Веб-консоль" (Web console):

1. В случае установки на сервер под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux или Rocky Linux выберите одну из СУБД, с которой будет работать Система:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

> **Примечание:**
>
> Тип СУБД должен соответствовать выбранному для шаблона "База данных".

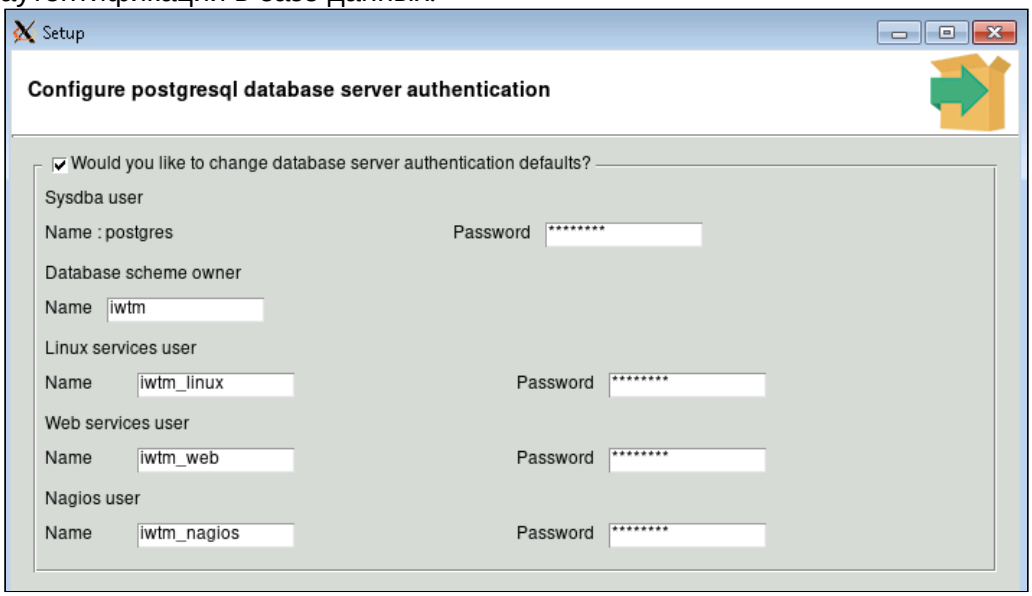
2. Укажите параметры подключения к базе данных:



a. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.
b. **`Database name`** – имя используемой базы данных.

> **Примечание:**
>
> В графическом режиме в активных полях указаны значения по умолчанию.

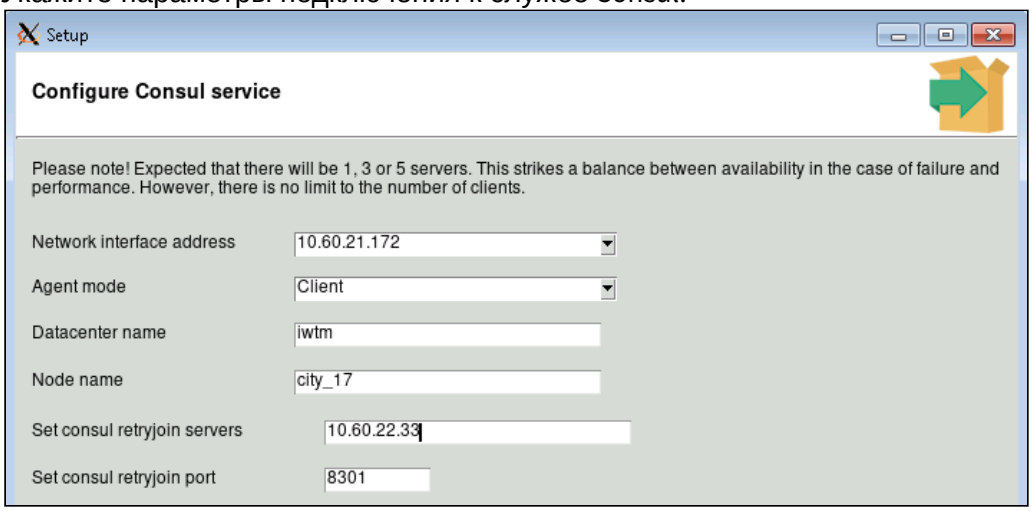
3. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



Чтобы отредактировать значения, установите флажок напротив поля с вопросом. Это сделает доступными для редактирования следующие разделы:

- **`Sysdba user`** – пароль пользователя с правами `sysdba`;
- **`Database scheme owner`** – имя владельца схемы базы данных;
- **`Linux services user`** – имя и пароль пользователя сервисов Linux;
- **`Web services user`** – имя и пароль пользователя веб-сервисов;
- **`Nagios user`** – имя и пароль пользователя Nagios.

4. Укажите параметры подключения к службе Consul:

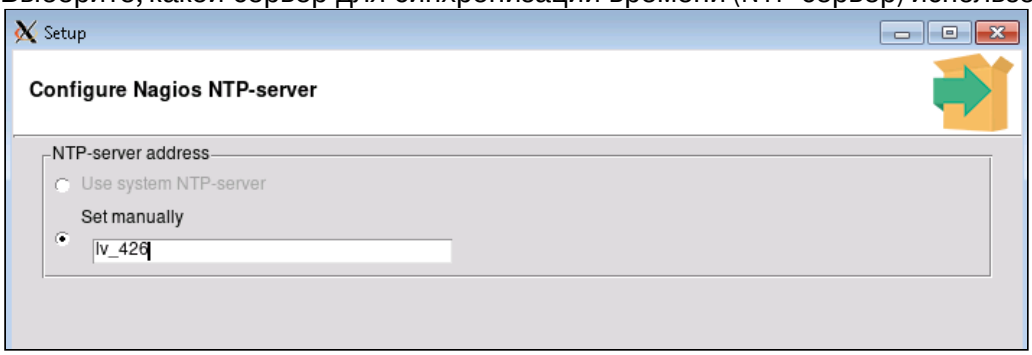


   a. **`Network interface address`** – выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите ▾ и в раскрывшемся списке выберите нужное значение.
   b. Доступны два режима работы Consul:
      - **`Server`**
      - **`Client`**

> **Важно!**
>
> В одном кластере должно быть нечетное число серверов Consul – не больше 5.

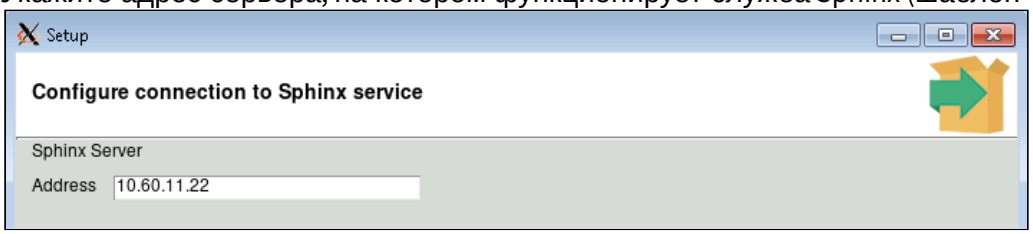
   c. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.
   d. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
   e. **`Consul retryjoin servers`** – список серверов Consul, к которым нужно подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущем компьютере, оставьте поле пустым.
   f. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

5. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:



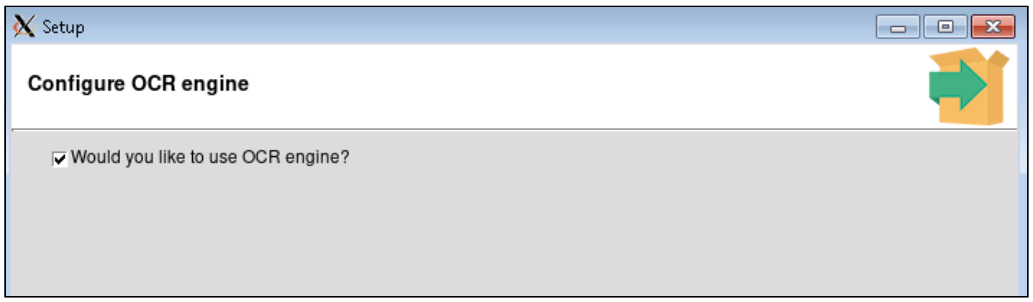
   - **`Use system NTP-server`** – использовать системный NTP-сервер;
   - **`Set manually`** – указать NTP-сервер вручную. При выборе этого варианта нужно будет ввести IP-адрес или имя доступного NTP-сервера.

6. Укажите адрес сервера, на котором функционирует служба Sphinx (шаблон "Индексер").



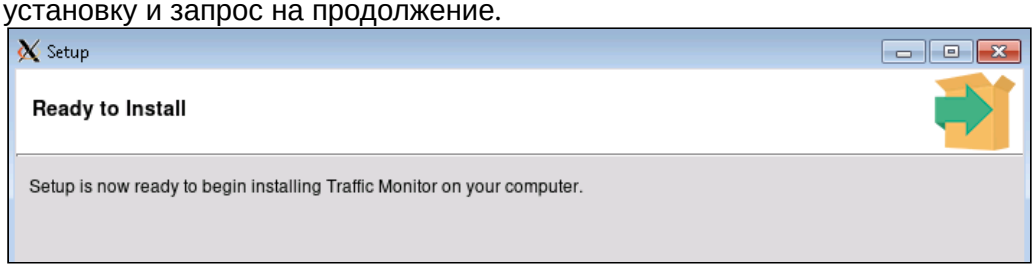
> **Примечание:**
>
> Если шаблоны "Индексер" и "Веб-консоль" устанавливаются на один сервер, этот параметр не будет запрошен инсталлятором.

7. Вы можете включить использование технологии OCR.

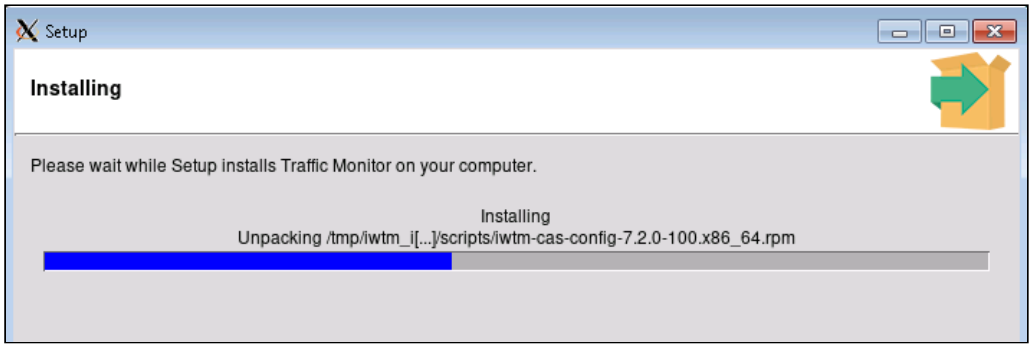


> **Примечание:**
>
> OCR-экстрактор выбирается при установке шаблона "Перехватчики".

8. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.



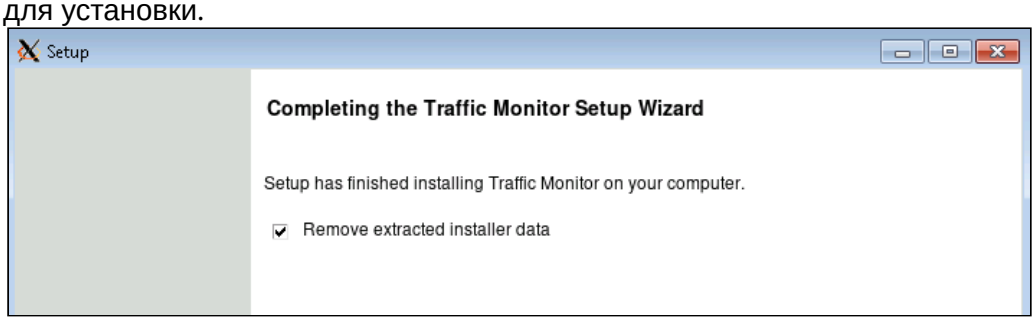
Для начала установки нажмите **Next**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



Процесс может занять некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

9. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.



Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove extracted installer data`**.

10. Для завершения нажмите **Finish**.
11. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
12. Если нужно вывести список сервисов Traffic Monitor и их статусы, введите команду: `iwtm status`

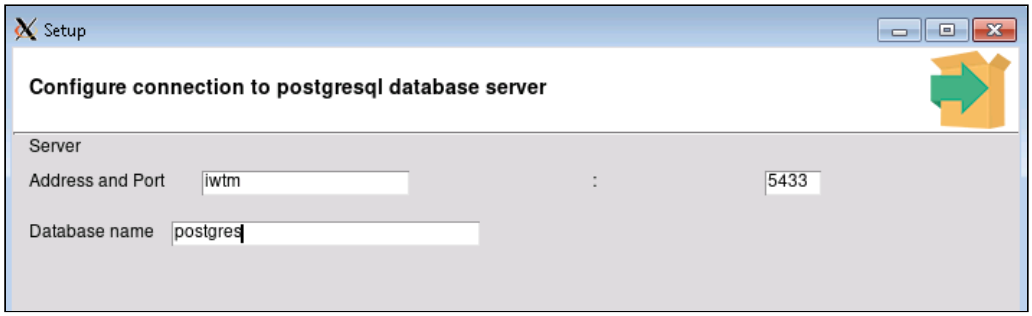
Установка шаблона Перехватчики

Если для установки выбран шаблон "Перехватчики" (Interceptors):

1. В случае установки на сервер под управлением ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux или Rocky Linux выберите одну из СУБД, с которой будет работать Система:
   - **`Oracle Database Enterprise Edition`**
   - **`PostgreSQL`**

> **Примечание:**
>
> Тип СУБД должен соответствовать выбранному для шаблона "База данных".

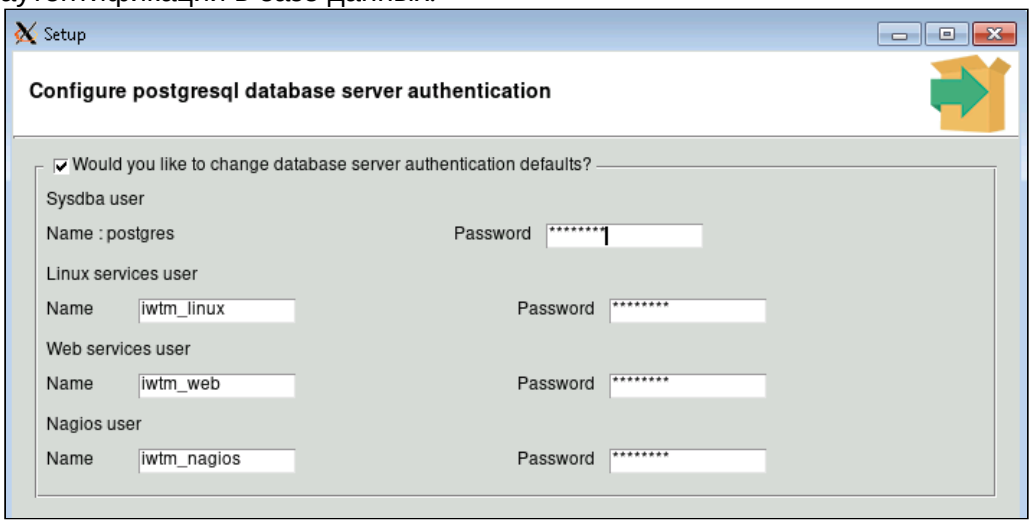
2. Укажите параметры подключения к базе данных:



a. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.
b. **`Database name`** – имя используемой базы данных.

> **Примечание:**
>
> В графическом режиме в активных полях указаны значения по умолчанию.

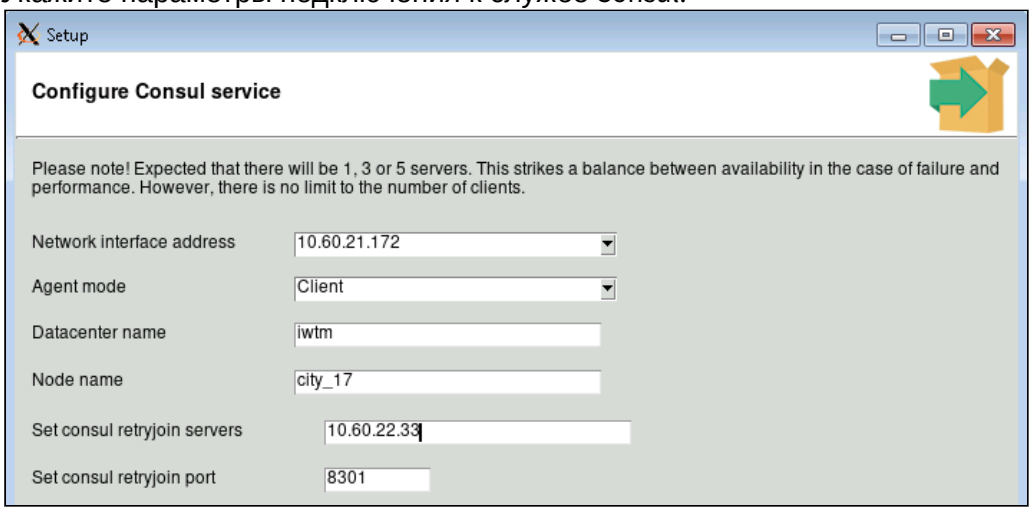
3. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



Чтобы отредактировать значения, установите флажок напротив поля с вопросом. Это сделает доступными для редактирования следующие разделы:

- **`Sysdba user`** – пароль пользователя с правами sysdba;
- **`Linux services user`** – имя и пароль пользователя сервисов Linux;
- **`Web services user`** – имя и пароль пользователя веб-сервисов;
- **`Nagios user`** – имя и пароль пользователя nagios.

4. Укажите параметры подключения к службе Consul:

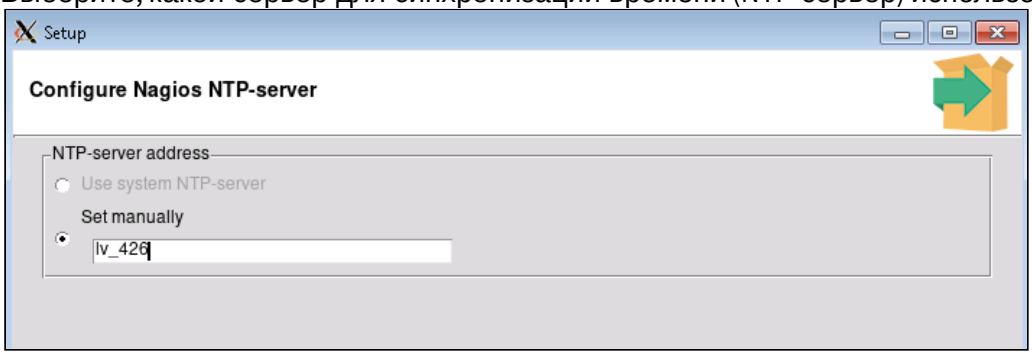


   a. **`Network interface address`** – выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите ▼ и в раскрывшемся списке выберите нужное значение.
   b. Доступны два режима работы Consul:
      - **`Server`**
      - **`Client`**

> **Важно!**
>
> В одном кластере должно быть нечетное число серверов Consul – не больше 5.

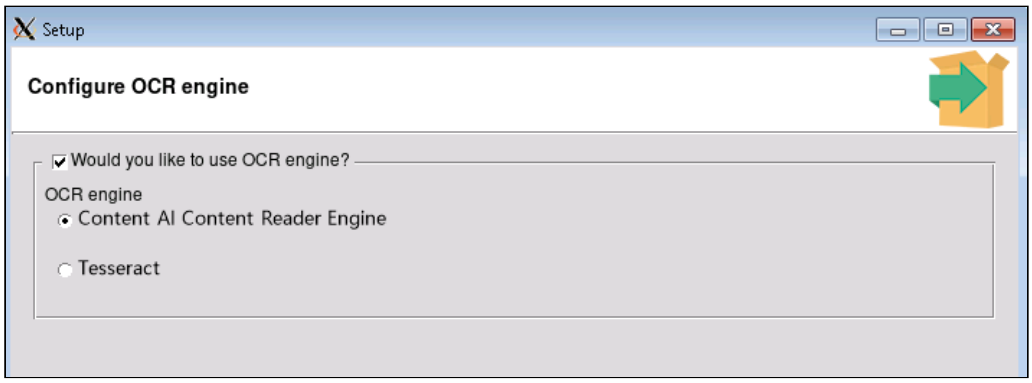
   c. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.
   d. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
   e. **`Consul retryjoin servers`** – список серверов Consul, к которым нужно подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущем компьютере, оставьте поле пустым.
   f. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

5. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:



   - **`Use system NTP-server`** – использовать системный NTP-сервер;
   - **`Set manually`** – указать NTP-сервер вручную. При выборе этого варианта нужно будет ввести IP-адрес или имя доступного NTP-сервера.

6. Вы можете включить использование технологии OCR.

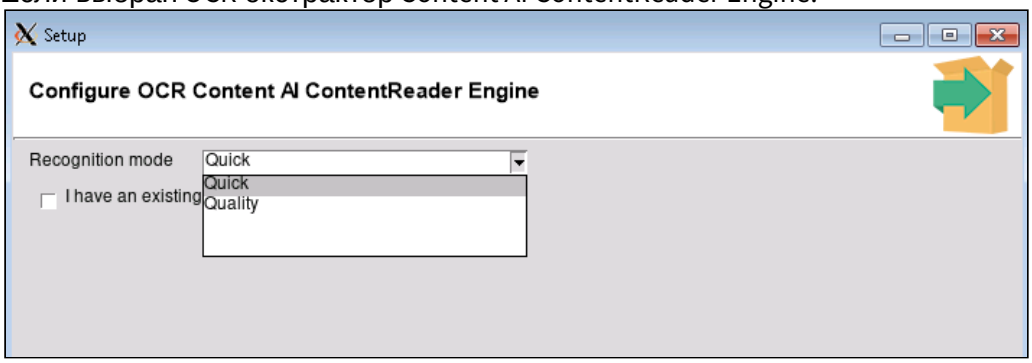


В случае включения нужно выбрать для использования одну из систем:

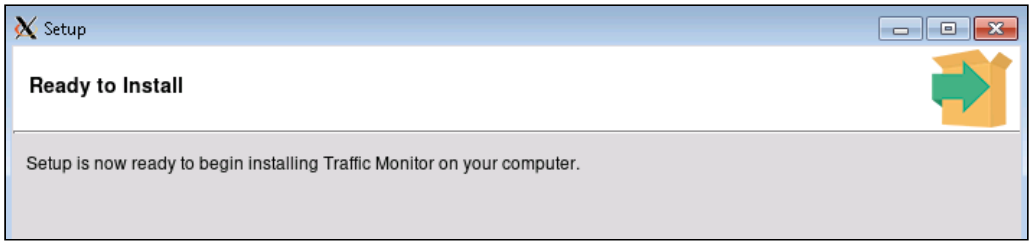
- **`Content AI ContentReader Engine`**;
- **`Tesseract`**.

> **Примечание:**
>
> Для работы OCR включите использование технологии при установке шаблона "Веб-консоль".

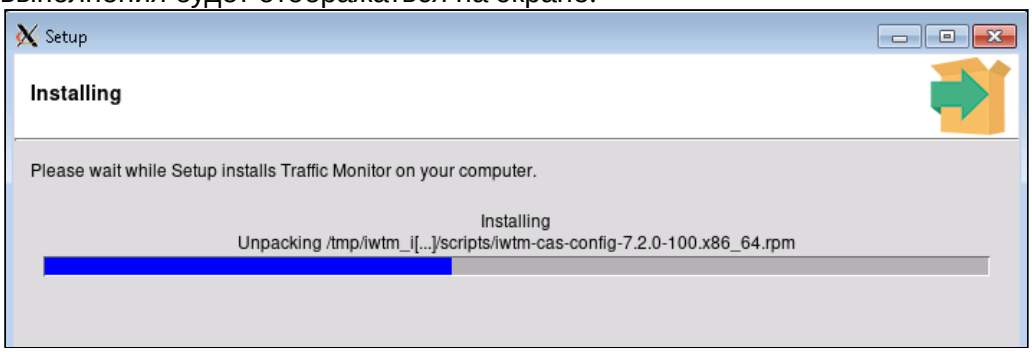
7. Если выбран OCR-экстрактор Content AI ContentReader Engine:



   a. Выберите один из режимов распознавания (**`Recognition mode`**):
      - **`Quick`** – быстрый режим;
      - **`Quality`** – тщательный режим, обеспечивающий более высокое качество распознавания.
   b. Подтвердите наличие у вас активной лицензии на использование Content AI ContentReader Engine.
      Если у вас отсутствует лицензия, не ставьте флажок в этом поле. В этом случае ContentReader Engine будет установлен без лицензии. Для возможности работы ContentReader Engine активную лицензию нужно будет добавить позже вручную. Подробнее смотрите в документе *InfoWatch Traffic Monitor. Руководство администратора. Настройка OCR-экстракторов*.
8. После задания всех параметров будет выведено сообщение о готовности начать установку и запрос на продолжение.



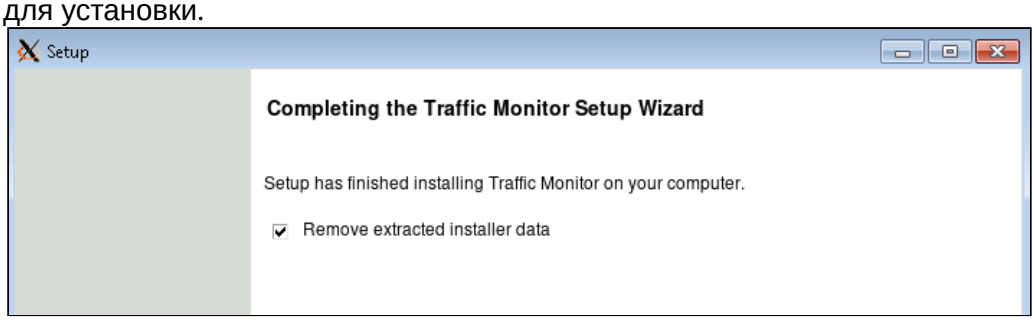
Для начала установки нажмите **Next**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



Процесс может занять некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

9. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.



Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта `Remove extracted installer data`.
10. Для завершения нажмите **Finish**.
11. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
12. Если нужно вывести список сервисов Traffic Monitor и их статусы, введите команду:
`iwtm status`

Если вы установили компоненты Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8, восстановите исходный файл выпуска ОС.

Для этого:

1. Выполните команду в зависимости от ОС:
   - в ОС Oracle Linux 8:
     ```
     mv /etc/release.bak /etc/oracle-release
     ```
   - в ОС AlmaLinux 8 или Rocky Linux 8:
     ```
     mv /etc/release.bak /etc/redhat-release
     ```
2. Подтвердите перезапись файла. Для этого введите `yes` и нажмите **Enter**.
3. Убедитесь, что исходный файл выпуска успешно восстановлен. Для этого выполните команду:
   ```
   lsb_release -a
   ```
   В результате должна быть выведена информация о вашей операционной системе. Например, для ОС AlmaLinux 8 будет выведено:
   ```
   Distributor ID: AlmaLinux
   Description:    AlmaLinux release 8.10 (Cerulean Leopard)
   Release:        8.10
   Codename:       CeruleanLeopard
   ```

В результате установки в системе будут созданы учетные записи. Подробнее см. *Предустановленные серверные параметры*.

После окончания установки вы можете работать в консоли управления через окно браузера. Для этого в адресной строке браузера введите URL-адрес сервера, на котором установлен шаблон "Веб-консоль".

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

> **Примечание:**
>
> Если после установки вы решите расширить Систему и добавить дополнительные серверы, их нужно будет зарегистрировать в кластере Consul. См. *InfoWatch Traffic Monitor. Руководство администратора. Распределенная установка*.

Список процессов, которые должны быть запущены только на одном из серверов, приведен в статье *InfoWatch Traffic Monitor. Руководство администратора. Проверка автозапуска процессов*. О том, как включить и выключить автозапуск процессов, см. *InfoWatch Traffic Monitor. Руководство администратора. Включение и выключение автозапуска процессов*. С описанием процессов можно ознакомиться также в статье *InfoWatch Traffic Monitor. Руководство администратора. Список процессов серверной части Traffic Monitor*.

3.2.3 Установка в тихом режиме с файлом параметров

Чтобы минимизировать участие пользователя в установке Системы, в инсталляторе предусмотрен тихий режим. В нем инсталлятор может установить Traffic Monitor, используя параметры по умолчанию.

В инсталляторе есть возможность использования файла параметров (option file). В нем вы можете задать нужные особенности установки. При запуске инсталлятора с файлом параметров указанные в нем значения будут считаться параметрами по умолчанию.

Таким образом, использование тихого режима и подготовленного файла параметров позволяет установить Traffic Monitor практически без участия пользователя.

> **Важно!**
>
> По умолчанию установка Системы не разрешена на сервере, имя которого начинается с цифры. Если нужно разрешить наличие цифр в начале имени сервера, с помощью командной строки задайте значение `1` параметру `--allow_digits_at_hostname_begin`. При этом нужно, чтобы проверка сети была активирована – параметру `--skip_check_network` задано значение `0` (эта проверка включена по умолчанию).

Перед установкой выполните общие действия:

1. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя `root`).

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

   > **Важно!**
   >
   > Если вы планируете пользоваться удаленной базой данных (развернутой локально или на отдельном сервере), нужно провести *предварительную подготовку*.
   >
   > Перед установкой для очистки памяти рекомендуем перезагрузить сервер, на котором будет развернута база данных.

2. Подключите внешние или локальные репозитории ОС.
   Например, с инструкцией по настройке локального репозитория в Red Hat Enterprise Linux можно ознакомиться на *официальном сайте* (на английском).
   Если вы устанавливаете Traffic Monitor на РЕД ОС без доступа в Интернет:

   a. Выключите внешние репозитории:
   На рабочей станции под управлением РЕД ОС версии 7.3.3 и ниже:

   Выполните следующие команды:
   ```
   echo "enabled=0" >> /etc/yum.repos.d/RedOS-Base.repo
   echo "enabled=0" >> /etc/yum.repos.d/RedOS-Updates.repo
   sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-kernels.repo
   ```

   На рабочей станции под управлением РЕД ОС версии 7.3.4 или 7.3.5:

   Выполните команду:
   ```
   sed -i -e "s/enabled=.*/enabled=0/g" /etc/yum.repos.d/RedOS-*.repo
   ```

   b. Подключите диск с дистрибутивом РЕД ОС к серверу.
   c. Смонтируйте диск с дистрибутивом РЕД ОС с помощью команды:
   ```
   mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/
   ```
   d. Создайте файл `/etc/yum.repos.d/cdrom.repo` с указанием смонтированного диска в качестве репозитория. Для этого выполните команду:

```
cat << EOF > /etc/yum.repos.d/cdrom.repo
[cdrom]
name=cdrom
baseurl=file:///media/cdrom/
enabled=1
gpgcheck=0
EOF
```

e. Удалите временные файлы и удостоверьтесь, что в списке репозиториев указан репозиторий с диска:
`yum clean all && yum repolist`

f. Установите библиотеку `libpq` и пакет `python2`:
`yum install libpq python2`

g. Установите следующие пакеты:

Название пакета	Официальный репозиторий
`lshw-B.02.19.2-1.el7.x86_64.rpm`	*РЕД ОС – Updates*
`lz4-1.9.4-1.el7.x86_64.rpm`	
`python3-psycopg2-2.9.3-1.el7.x86_64.rpm`	
`urw-base35-fonts-legacy-20170801-11.el7.noarch.rpm`	*РЕД ОС – OS*
`libxslt-1.1.34-1.el7.x86_64.rpm`	

Для этого:

i. Скачайте указанные пакеты из официального репозитория РЕД ОС.
ii. Скопируйте их на сервер, куда будет установлен Traffic Monitor.
iii. Перейдите в каталог, куда были скопированы пакеты.
iv. Выполните команду:
`yum localinstall lshw-B.02.19.2-1.el7.x86_64.rpm lz4-1.9.4-1.el7.x86_64.rpm python3-psycopg2-2.9.3-1.el7.x86_64.rpm urw-base35-fonts-legacy-20170801-11.el7.noarch.rpm libxslt-1.1.34-1.el7.x86_64.rpm`

> **Примечание:**
>
> Дополнительно вы можете установить утилиты для работы с операционной системой с помощью команды:
> `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`
>
> Также вы можете установить утилиту *htop*, скачав ее из *официального репозитория РЕД ОС*.

h. Убедитесь, что сетевые настройки выполнены корректно (см. *Требования к настройкам ОС и сети сервера*) и файл `/etc/hosts` содержит инструкцию преобразования имени сервера в IP-адрес. Если она отсутствует, выполните

команду:
`sh -c "echo '<IP_адрес> `hostname -f` `hostname -s`' >> /etc/hosts"`

Если вы устанавливаете Traffic Monitor на ОС Oracle Linux без доступа в Интернет:

a. Убедитесь, что в операционной системе в качестве текущего выбрано ядро Red Hat Compatible Kernel (RHCK), к примеру Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, а ядро UEK удалено. Подробнее см. *Требования к настройкам ОС и сети сервера*.
b. Выключите внешние репозитории с помощью команды:
`find /etc/yum.repos.d/ -iname "*.repo" -exec sed -i -e "s/enabled=.*/enabled=0/g" {} \;`
c. Подключите диск с дистрибутивом ОС Oracle Linux к серверу.
d. Смонтируйте диск с дистрибутивом ОС Oracle Linux с помощью команды:
`mkdir -p /media/cdrom/ && mount /dev/cdrom /media/cdrom/`
e. Создайте файл `/etc/yum.repos.d/cdrom.repo` с указанием смонтированного диска в качестве репозитория. Для этого выполните команду:
```
cat << EOF > /etc/yum.repos.d/cdrom.repo
[cdrom]
name=cdrom
baseurl=file:///media/cdrom/
enabled=1
gpgcheck=0
EOF
```
f. Удалите временные файлы и удостоверьтесь, что в списке репозиториев указан репозиторий с диска:
`yum clean all && yum repolist`
g. Установите `Perl`:
`yum install perl`
h. Установите пакеты:
   - `perl-List-MoreUtils-0.33-9.el7.x86_64.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 Latest*)
   - `perl-Dist-CheckConflicts-0.06-2.el7.noarch.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 Optional Latest*)
   - `urw-base35-fonts-legacy-20170801-10.el7.noarch.rpm` (пакет можно скачать из *официального репозитория Oracle Linux 7 Optional Latest*)

   Для этого:
   i. Скачайте перечисленные пакеты из официальных репозиториев Oracle Linux.
   ii. Скопируйте их на сервер, куда будет установлен Traffic Monitor.
   iii. Перейдите в каталог, куда были скопированы пакеты.
   iv. Выполните следующую команду для каждого пакета:
   `rpm -ivh <имя_пакета>`

> **Примечание:**
>
> Дополнительно вы можете установить утилиты для работы с операционной системой с помощью команды:
> `yum install mc vim screen telnet bind-utils mlocate net-tools iptraf sysstat iotop rsync`

i. Убедитесь, что сетевые настройки выполнены корректно (см. *Требования к настройкам ОС и сети сервера*) и файл `/etc/hosts` содержит инструкцию преобразования имени сервера в IP-адрес. Если она отсутствует, выполните команду:

```
sh -c "echo '<IP_адрес> `hostname -f` `hostname -s`' >> /etc/hosts"
```

3. **Если вы устанавливаете Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8:**

> **Важно!**
>
> Убедитесь, что в операционной системе Oracle Linux 8.10 в качестве текущего выбрано ядро Red Hat Compatible Kernel (RHCK), к примеру Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, а ядро UEK удалено. Подробнее см. *Требования к настройкам ОС и сети сервера*.

a. Установите пакет `redhat-lsb-core` с помощью следующей команды:

```
dnf install redhat-lsb-core
```

b. Создайте резервную копию файла выпуска ОС и замените содержимое исходного файла. Для этого выполните команды в зависимости от ОС:

- на ОС Oracle Linux 8:

```
cp /etc/oracle-release /etc/release.bak

echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/oracle-release
```

- на ОС AlmaLinux 8 или Rocky Linux 8:

```
cp /etc/redhat-release /etc/release.bak
echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/redhat-release
```

c. Выполните команду:

```
lsb_release -a
```

В результате должна быть выведена следующая информация:

```
Distributor ID: RedHatEnterprise
Description:    Red Hat Enterprise Linux release 8.10 (Ootpa)
Release:        8.10
Codename:       Ootpa
```

> **Примечание:**
>
> После установки Traffic Monitor восстановите исходный файл выпуска ОС. Подробнее см. *ниже*.

4. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой системы выполните команду:
   `mkdir /distr`
5. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor: инсталлятор и архив с компонентами СУБД.

ОС	Файлы дистрибутива
Red Hat Enterprise Linux 7 Oracle Linux 7 [4]	**Инсталлятор:** `iwtm-installer-x.x.x.xxx-rhel7` **Архив с компонентами СУБД [1] [2]:** • PostgreSQL: `iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz` • Oracle[3]: `iwtm-oracle-19.0.0.0.0-x.xx.x.tar.gz`

РЕД ОС	**Инсталлятор:**
	`iwtm-installer-x.x.x.xxx-redos-7.3`
	Архив с компонентами СУБД [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-redos-7.3.tar.gz`

Red Hat Enterprise Linux 8
Oracle Linux 8
AlmaLinux 8
Rocky Linux 8
	Инсталлятор:
	`iwtm-installer-x.x.x.xxx-rhel8`
	Архив с компонентами СУБД [1] [2]:
	`iwtm-postgresql-15.14-x.x.x.xxx-rhel8.tar.gz`

Альт Сервер	**Инсталлятор:**
	`iwtm-installer-x.x.x.xxx-altlinux-10`
	Архив с компонентами СУБД [1] [2]:
	`iwtm-postgresql-15.10-x.x.x.xxx-altlinux-10.tar.gz.md5`

Важно!

[1] Архив с компонентами СУБД нужен как при установке поставляемой в дистрибутиве СУБД (режим `local`), так и при использовании уже развернутой СУБД в удаленном режиме. Подробнее см. *Схемы развертывания Системы и выбор типа установки*.

[2] Если вы планируете использовать уже развернутую СУБД на основе PostgreSQL, используйте архив из столбца PostgreSQL. Список поддерживаемых PostgreSQL-подобных СУБД см. в статье *Аппаратные и программные требования*.

[3] Если используется СУБД Oracle и сетевая файловая система (NFS), перед запуском инсталлятора:

- **если RAC не используется:**

  Откройте настройки точки монтирования (по умолчанию `/etc/fstab`) и убедитесь, что опция `noac` не используется, а параметру `actimeo` не присвоено значение `0`.

  Подробнее смотрите в *статье на официальном сайте* (на английском).

- **при использовании Oracle Real Application Clusters (RAC):**

  Установите опции монтирования в соответствии со *статьей на официальном сайте* (на английском).

[4] При установке Traffic Monitor на сервер под управлением Oracle Linux 7 не поддерживается работа с СУБД Postgres Pro Enterprise.

Далее будет описана установка с использованием инсталлятора для ОС Red Hat Enterprise Linux 7. В нашем примере нужно скопировать файл инсталлятора и архив с компонентами СУБД:

- инсталлятор:
  `iwtm-installer-7.14.0.97-rhel7`
  где `7.14.0.97` – номер сборки, `rhel7` – обозначение ОС;
- архив с компонентами СУБД:
  - если будет использована PostgreSQL (или одна из поддерживаемых СУБД на ее базе):
    `iwtm-postgresql-15.14-7.14.0.97-rhel7.tar.gz`
    где `postgresql-15.14` – обозначение СУБД, `7.14.0.97` – номер сборки, `rhel7` – обозначение ОС;
  - если будет использована СУБД Oracle:
    `iwtm-oracle-19.0.0.0.0-7.14.0.97.tar.gz`
    где `oracle-19.0.0.0.0` – обозначение СУБД, `7.14.0.97` – номер сборки.

Данная инструкция актуальна и для других поддерживаемых ОС: Oracle Linux, РЕД ОС, AlmaLinux, Rocky Linux и Альт Сервер.

6. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
   `cd /distr`
7. Перед запуском установки сделайте файл инсталлятора исполняемым. Для этого используйте команду вида:
   `chmod u+x ./iwtm-installer-x.x.x.xxx-rhel7`
   В нашем примере команда будет:
   `chmod u+x ./iwtm-installer-7.14.0.97-rhel7`

Файл параметров (option file)

В файле описание параметров имеет вид:

`<имя_параметра>=<значение_параметра>`

Вы можете оставлять комментарии с помощью символа `#`.

Пример файла параметров:

```
# This file is just an example
product_type=tme
installation_type=distributed
template_database=1
template_indexer=1
template_web=1
template_interceptors=0
product_language=rus
use_data_storage=1
ds_set_host=example.host.com
ds_set_port=40731
ds_set_token=hcb90t4it745zl1hycg43
```

В данном примере указаны параметры:

- редакция продукта – Traffic Monitor Enterprise (TME);
- тип установки – распределенная;
- для установки на сервер выбраны шаблоны:
  - База данных;
  - Индексер;
  - Веб-консоль.
- основной язык продукта – русский;
- соединение с внешним хранилищем бинарных данных.

Важно!

Для параметров, которые не указаны в файле, будут использованы значения по умолчанию. Полный набор параметров указан в таблице ниже.

Чтобы использовать файл параметров, перейдите в директорию с инсталлятором и запустите его с опцией `--optionfile` и с указанием созданного ранее файла.

Пример команды использования файла параметров:

```
./iwtm-installer-7.14.0.97-rhel7 --optionfile /some_directory/option-file-example
```

Альтернативный способ: назовите файл параметров тем же именем, каким назван инсталлятор, но с расширением `.options`, и скопируйте его в директорию к инсталлятору. В этом случае при запуске инсталлятор также будет считать параметры из файла значениями по умолчанию.

Тихий режим установки

Для установки в тихом режиме используйте опцию `--mode unattended`.

Уровень взаимодействия с пользователем задается параметром `--unattendedmodeui`, который имеет следующие значения:

- `none` – в процессе установки инсталлятор не выводит на экран никакую информацию и не требует взаимодействия с пользователем;

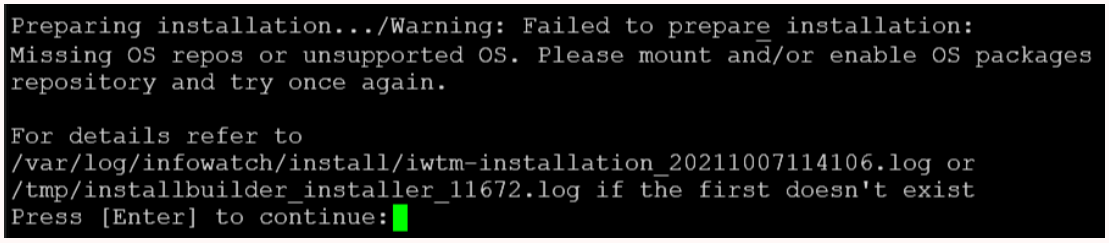
- `minimal` – в процессе отображается ход выполнения установки, не требует взаимодействия с пользователем;
- `minimalWithDialogs` – отображает ход выполнения установки, также в процессе могут появляться всплывающие окна и может потребоваться взаимодействие с пользователем.

Пример команды запуска инсталлятора в тихом режиме без участия пользователя и с файлом параметров:

```
./iwtm-installer-7.14.0.97-rhel7 --optionfile /some_directory/option-file-example --mode unattended --unattendedmodeui minimal
```

Важно!

При отсутствии настроенных и доступных репозиториев ОС запуск инсталлятора прервется со следующей ошибкой:



При возникновении этой ошибки нажмите **Enter** для завершения работы инсталлятора, подключите стандартный репозиторий ОС, репозиторий EPEL, а затем повторно запустите инсталлятор.

Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

Примечание:

В случае некорректной настройки службы Consul в консоли будет выведено предупреждение:



Для завершения работы инсталлятора нажмите **Enter**.

Для корректной работы Системы выполните проверку и настройку кластера службы Consul

1. Запустите службу Consul с помощью команды:
   `service iwtm-consul start`
   Проверить статус службы можно командой:
   `service iwtm-consul status`
2. Чтобы проверить службу Consul, выполните команды:
   a. Для вывода IP-адреса основного сервера (лидера) кластера:
      `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`

b. Для вывода информации о членах кластера:
`consul members`

3. Если не будет выведен IP-адрес лидера кластера, выполните *конфигурирование кластера службы Consul*.
После настройки повторите проверку (действие ii).

При данной ошибке инсталлятор не запустит сервисы Traffic Monitor при завершении работы — их нужно будет запустить вручную.

Примечание:

Если процесс установки был прерван по какой-то причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.
Когда процесс завершится без ошибок, инсталлятор удалит пакеты, созданные для установки.

После окончания установки Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8, восстановите исходный файл выпуска ОС.

Для этого:

1. Выполните команду в зависимости от ОС:
   - в ОС Oracle Linux 8:
     `mv /etc/release.bak /etc/oracle-release`
   - в ОС AlmaLinux 8 или Rocky Linux 8:
     `mv /etc/release.bak /etc/redhat-release`
2. Подтвердите перезапись файла. Для этого введите `yes` и нажмите **Enter**.
3. Убедитесь, что исходный файл выпуска успешно восстановлен. Для этого выполните команду:
   `lsb_release -a`
   В результате должна быть выведена информация о вашей операционной системе. Например, для ОС AlmaLinux 8 будет выведено:
   ```
   Distributor ID: AlmaLinux
   Description:    AlmaLinux release 8.10 (Cerulean Leopard)
   Release:        8.10
   Codename:       CeruleanLeopard
   ```

Полный состав файла параметров

В таблице приведен полный список возможных параметров и их значения по умолчанию.

Примечание:

В значениях по умолчанию `<ora|pg>` означает, что должно быть выбрано одно из значений в зависимости от указанной ранее СУБД:

- `ora` – для СУБД Oracle;
- `pg` – для СУБД PostgreSQL, Postgres Pro, Jatoba, Tantor или Pangolin.

Название	Описание
`use_debug`	Включение режима отладки для скриптов, входящих в состав инсталлятора Параметр используется для сбора расширенной диагностической информации в случае ошибок при работе инсталлятора Допустимые значения: `0` (по умолчанию), `1`
`skip_check_swap`	Отключение проверки объема Swap-пространства Допустимые значения: `0` (по умолчанию), `1`
`skip_check_space`	Отключение проверки объема свободного пространства на диске Допустимые значения: `0` (по умолчанию), `1`
`skip_check_ram`	Отключение проверки объема оперативной памяти (RAM) Допустимые значения: `0` (по умолчанию), `1`
`skip_check_network`	Отключение проверки доступности сети Допустимые значения: `0` (по умолчанию), `1`
`skip_check_tmp`	Отключение проверки временной директории Допустимые значения: `0` (по умолчанию), `1`
`skip_check_home`	Отключение проверки домашней директории Допустимые значения: `0` (по умолчанию), `1`
`setup_cron_jobs`	Установить задания для планировщика cron Допустимые значения: `0` , `1` (по умолчанию)
`log_dir`	Путь к директории для лог-файлов Значение по умолчанию: `/var/log/infowatch/install`
`eula`	Допустимые значения: • `show` (вывести текст Лицензионного соглашения) • accept (принять Лицензионное соглашение без предварительного просмотра) Если вы запускаете установку не в тихом режиме и параметр не указан, то будет выведен текст Лицензионного соглашения и будет предложено принять его. При установке в тихом режиме значение параметра игнорируется и Лицензионное соглашение принимается по умолчанию.

Название	Описание
`product_type`	Редакция Traffic Monitor Допустимые значения: `tme` (по умолчанию), `tms`
`product_language`	Основной язык продукта Допустимые значения: `rus` (по умолчанию), `eng`
`installation_type`	Тип установки Параметр используется, если выбрана редакция Traffic Monitor Enterprise (`product_type=tme`). Допустимые значения: `all_in_one` (по умолчанию), `distributed`
`template_database`	Установить шаблон "База данных" Параметр используется, если выбрана распределенная установка (`installation_type=distributed`). Допустимые значения: `0` (по умолчанию), `1`
`template_indexer`	Установить шаблон "Индексер" Параметр используется, если выбрана распределенная установка (`installation_type=distributed`). Допустимые значения: `0` (по умолчанию), `1`
`template_web`	Установить шаблон "Веб-консоль" Параметр используется, если выбрана распределенная установка (`installation_type=distributed`). Допустимые значения: `0` (по умолчанию), `1`
`template_interceptors`	Установить шаблон "Перехватчики" Параметр используется, если выбрана распределенная установка (`installation_type=distributed`). Допустимые значения: `0` (по умолчанию), `1`
`db classification_lang_ru`	Установить русский язык для базы классификации Параметр используется, если выбран тип установки "Все-в-одном" (All-in-one) (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) Допустимые значения: `0`, `1` (по умолчанию)
`db classification_lang_en`	Установить английский язык для базы классификации Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`)

Название	Описание
	Допустимые значения: `0` (по умолчанию), `1`
`db_installation_type`	Расположение базы данных Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) Допустимые значения: `local` (по умолчанию), `remote` Вариант `local` поддерживается только при использовании СУБД Oracle или PostgreSQL, поставляемых в дистрибутиве.
`db_type`	Выбор СУБД Доступно при установке на ОС Red Hat Enterprise Linux, Oracle Linux, AlmaLinux, Rocky Linux и редакции Traffic Monitor Enterprise (`product_type=tme`). Допустимые значения: `postgresql` (по умолчанию), `oracle` Выберите вариант `postgresql`: • если вы устанавливаете Traffic Monitor на ОС Red Hat Enterprise Linux 8, Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8 и/или • если вы будете использовать СУБД Postgres Pro Enterprise, Jatoba, Tantor или Pangolin.
`db_server_address`	Адрес сервера с шаблоном "База данных" или адрес сервера удаленной базой данных Параметр используется: • для шаблонов "Индексер", "Перехватчики", "Веб-консоль"; • для типа установки All-in-one или шаблона "База данных" при использовании удаленной базы данных (`db_installation_type=remote`). Значение по умолчанию: `iwtm` Чтобы установить Traffic Monitor на одном сервере с уже развернутой СУБД, укажите адрес `127.0.0.1`.
`db_server_port`	Порт сервера с базой данных Параметр используется: • для шаблонов "Индексер", "Перехватчики", "Веб-консоль"; • для типа установки All-in-one или шаблона "База данных" при использовании удаленной базы данных (`db_installation_type=remote`).
`db_name`	Имя базы данных Параметр используется:

Название	Описание
	• для шаблонов "Индексер", "Перехватчики", "Веб-консоль"; • для типа установки All-in-one или шаблона "База данных" при использовании удаленной базы данных (`db_installation_type=remote`). Значение по умолчанию: `postgres` или `iwtm` (в зависимости от параметра `db_type`)
`db_sysdba_password`	Пароль пользователя с правами SYSDBA Значение по умолчанию: `xxXX1234`
`db_scheme_owner_name`	Имя владельца схемы базы данных Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`), шаблон "База данных" (`template_database=1`) или шаблон "Веб-консоль" (`template_web=1`). Значение по умолчанию: `iwtm`
`db_scheme_owner_password`	Пароль владельца схемы базы данных Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) Значение по умолчанию: `xxXX1234`
`db_linux_user_name`	Имя пользователя сервисов Linux Значение по умолчанию: `iwtm_linux`
`db_linux_user_password`	Пароль пользователя сервисов Linux Значение по умолчанию: `xxXX1234`
`db_web_user_name`	Имя пользователя веб-сервисов Значение по умолчанию: `iwtm_web`
`db_web_user_password`	Пароль пользователя веб-сервисов Значение по умолчанию: `xxXX1234`
`db_nagios_user`	Имя пользователя Nagios Значение по умолчанию: `iwtm_nagios`
`db_nagios_password`	Пароль пользователя Nagios Значение по умолчанию: `xxXX1234`

Название	Описание
`db_auth_change_defaults`	Изменить параметры подключения к базе данных по умолчанию Допустимые значения: `0` (по умолчанию), `1`
`db_storage_type`	Режим хранения данных Допустимые значения: `normal` (по умолчанию), `fast_slow`, `rotate`
`db_storage_main_tbs_path`	Путь к основному табличному пространству Значение по умолчанию: `/u02/<ora|pg>data`
`db_storage_dtbs_paths_number`	Количество путей к ежедневным табличным пространствам Допустимые значения: `1` - `10` Значение по умолчанию: `1`
`db_storage_fast_disk_path`	Путь к директории хранения данных ежедневных табличных пространств в быстром разделе Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) и режим хранения данных `fast_slow` (`db_storage_type=fast_slow`) Значение по умолчанию: `/u03/<ora|pg>data`
`db_storage_dtbs_days_on_fast_disk`	Период хранения данных ежедневных табличных пространств в быстром разделе, в днях Значение по умолчанию: `7`
`db_storage_change_defaults`	Изменить параметры хранения в базе данных Допустимые значения: `0` (по умолчанию), `1`
`db_storage_dtbs_path_1`	Путь к ежедневному табличному пространству №1 Параметр (а также прочие параметры, задающие пути к табличным пространствам) зависит от значения параметра `db_storage_dtbs_paths_number` и используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`). Значение по умолчанию: `/u02/<ora|pg>data1`
`db_storage_dtbs_path_2`	Путь к ежедневному табличному пространству №2 Значение по умолчанию: `/u02/<ora|pg>data2`

Название	Описание
`db_storage_dtbs_path_3`	Путь к ежедневному табличному пространству №3 Значение по умолчанию: `/u02/<ora|pg>data3`
`db_storage_dtbs_path_4`	Путь к ежедневному табличному пространству №4 Значение по умолчанию: `/u02/<ora|pg>data4`
`db_storage_dtbs_path_5`	Путь к ежедневному табличному пространству №5 Значение по умолчанию: `/u02/<ora|pg>data5`
`db_storage_dtbs_path_6`	Путь к ежедневному табличному пространству №6 Значение по умолчанию: `/u02/<ora|pg>data6`
`db_storage_dtbs_path_7`	Путь к ежедневному табличному пространству №7 Значение по умолчанию: `/u02/<ora|pg>data7`
`db_storage_dtbs_path_8`	Путь к ежедневному табличному пространству №8 Значение по умолчанию: `/u02/<ora|pg>data8`
`db_storage_dtbs_path_9`	Путь к ежедневному табличному пространству №9 Значение по умолчанию: `/u02/<ora|pg>data9`
`db_storage_dtbs_path_10`	Путь к ежедневному табличному пространству №10 Значение по умолчанию: `/u02/<ora|pg>data10`
`db_archiving_dtbs_path`	Путь к директории хранения архивированных табличных пространств Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`). Значение по умолчанию: `/u02/arch` **Примечание:** Если вы будете использовать Data Storage, то для архивирования табличных пространств необходимо во время установки хранилища указать путь к его медленному диску. Подробнее см. *Установка Платформы*.
`db_days_before_archiving_nonviolations`	Сколько дней хранить события без нарушений до архивирования Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`), а также `db_archive_nonviolations=1`

Название	Описание
	Значение по умолчанию: `45`
`db_archive_nonviolations`	Архивировать события без нарушений Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) Допустимые значения: `0` (по умолчанию), `1`
`db_days_before_archiving_violations`	Сколько дней хранить события с нарушением до архивирования Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных (`template_database=1`), а также `db_archive_violations=1` Значение по умолчанию: `45`
`db_archive_violations`	Архивировать события с нарушениями Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) Допустимые значения: `0` (по умолчанию), `1`
`db_days_before_archiving_screenshots`	Сколько дней хранить события скриншотов до архивирования Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`), а также `db_archive_screenshots=1` Значение по умолчанию: `45`
`db_archive_screenshots`	Архивировать события скриншотов Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) Допустимые значения: `0` (по умолчанию), `1`
`db_archiving_dtbs_change_defaults`	Изменить параметры архивирования по умолчанию Допустимые значения: `0` (по умолчанию), `1`
`db_days_before_removing_nonviolations`	Сколько дней хранить события без нарушений до удаления Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`), а также `db_remove_nonviolations=1` Значение по умолчанию: `90`

Название	Описание
`db_remove_nonviolations`	Удалять события без нарушений Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) Допустимые значения: `0` (по умолчанию), `1`
`db_days_before_removing_violations`	Сколько дней хранить события с нарушением до удаления Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`), а также `db_remove_violations=1` Значение по умолчанию: `90`
`db_remove_violations`	Удалять события с нарушением Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) Допустимые значения: `0` (по умолчанию), `1`
`db_days_before_removing_screenshots`	Сколько дней хранить события скриншотов до удаления Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`), а также `db_remove_screenshots=1` Значение по умолчанию: `90`
`db_remove_screenshots`	Удалять события скриншотов Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`) Допустимые значения: `0` (по умолчанию), `1`
`db_removing_dtbs_change_defaults`	Изменить параметры удаления по умолчанию Допустимые значения: `0` (по умолчанию), `1`
`use_data_storage`	Использовать внешнее хранилище бинарных данных Data Storage Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`). Допустимые значения: `0` , `1` (по умолчанию) **Важно!** Убедитесь в корректности вводимых значений параметров подключения к хранилищу (адрес, порт и токен; описание см. ниже).

Название	Описание
`ds_set_host`	Имя хоста или IP-адрес сервера, на котором установлено хранилище Data Storage Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`). **Важно!** Параметр **обязателен**. Если вы не планируете использовать хранилище Data Storage, укажите значение `any_data` .
`ds_set_port`	Порт подключения к Data Storage Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`). Значение по умолчанию: `40731`
`ds_set_token`	Токен авторизации Data Storage Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "База данных" (`template_database=1`). Значение по умолчанию: `1exwo92iwpczl1hy6jxy` Узнать актуальное значение токена авторизации можно: • На сервере Data Storage с помощью командной строки. Для этого: 1. Перейдите в директорию, куда был распакован дистрибутив Платформы; 2. Выполните команду: `./setup.py tokens list` В результате будет выведен список токенов для подключения к Платформе. Актуальный токен авторизации Data Storage будет указан напротив сущности *DataStorageUser*. • В консоли управления платформенного продукта, в разделе **Основные настройки** в поле **Токен для Data Storage User**. Доступно, если на сервере с Data Storage установлен платформенный продукт с веб-интерфейсом и в нем есть данная настройка.
`consul_bind_addr`	Адрес сетевого интерфейса Consul Значение по умолчанию: `<список_ip_адресов>`
`consul_mode`	Режим работы Consul: сервер или клиент Доступные значения: • `server` – для шаблона "База данных" и установки All-in-one • `client` – для остальных шаблонов
`consul_datacenter_name`	Имя дата-центра Consul Значение по умолчанию: `iwtm`

Название	Описание
`consul_node_name`	Имя ноды Значение по умолчанию: `<hostname>`
`consul_retryjoin_manual`	Список серверов Consul для подключения агентов
`consul_retryjoin_port`	Порт для подключения агентов Consul Значение по умолчанию: `8301`
`ntp_manual_addr`	Адрес NTP сервера Параметр используется, если выбрано указание NTP-сервера вручную (`ntp_mode=ntp_manual_addr`)
`ntp_mode`	Тип NTP-сервера: • `ntp_use_system` – использовать системный NTP-сервер (по умолчанию); • `ntp_manual_addr` – указать NTP-сервер вручную.
`sphinx_server_address`	Адрес Sphinx-сервера Параметр используется, если выбран шаблон "Веб-консоль" (`template_web=1`) и не выбран шаблон "Индексер" (`template_indexer=0`)
`sphinx_exact_match_words`	Включить индексацию на точное совпадение слов Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "Индексер" (`template_indexer=1`) Допустимые значения: `0` (по умолчанию), `1`
`sphinx_change_language_settings`	Изменить список языков Sphinx Допустимые значения: `0` (по умолчанию), `1`
`sphinx_langs`	Список языков Sphinx Последовательность языков определяет их приоритет. Допустимые значения: `rus eng deu fra spa ita ara ukr ron lav bel pol aze tur srp kir uzb fin kaz msa nld vie por tat ell lit kat hye ces slk fas hin sin tgk sah zho` Значение по умолчанию: `rus`
`ocr_enabled`	Включить использование OCR

Название	Описание
	Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`), шаблон "Перехватчики" (`template_interceptors=1`) или шаблон "Веб-консоль" (`template_web=1`). Допустимые значения: `0` , `1` (по умолчанию)
`ocr_type`	Выбор OCR-экстрактора: • `fre` – Content AI ContentReader Engine; • `ts` – Tesseract (по умолчанию). Параметр используется, если выбран тип установки All-in-one (`installation_type=all_in_one`) или шаблон "Перехватчики". (`template_interceptors=1`)
`ocr_contentai_mode`	Режим работы Content AI ContentReader Engine Параметр используется, если выбран Content AI ContentReader Engine (`ocr_type=fre`). Допустимые значения: `quick` , `quality` (по умолчанию)
`ocr_contentai_have_license`	Наличие лицензии на OCR Content AI ContentReader Engine Параметр используется, если выбран OCR Content AI ContentReader Engine (`ocr_type=fre`). Допустимые значения: `0` , `1` (по умолчанию)
`db_unpack_dir`	В директорию будет распакован архив БД Директория будет создана автоматически. Вы можете указать существующую директорию. Если установка завершится без ошибок, директория будет автоматически удалена. Значение по умолчанию: `/tmp/iwtm_installer/database`
`packages_unpack_dir`	В директорию будут распакованы установочные пакеты Traffic Monitor Директория будет создана автоматически. Вы можете указать существующую директорию. Если установка завершится без ошибок, директория будет автоматически удалена. Значение по умолчанию: `/tmp/iwtm_installer/packages`

3.3 Предустановленные серверные параметры

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

Директории установки Системы:

- компоненты Traffic Monitor – `/opt/iw`
- компоненты базы данных – `/u01` и `/u02`

> **Примечание:**
>
> Директории могут располагаться на разных серверах.

После установки Системы **смените пароли**:

- пользователя `oracle` или пользователя `postgres`, в зависимости от используемой БД;
- учетной записи Linux (подробнее см. *InfoWatch Traffic Monitor. Руководство администратора. Изменение предустановленного пароля*).

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

Параметры базы данных Traffic Monitor:

`oinstall` – группа владельца инстанса клиента СУБД, в состав которой включены пользователи:

- `iwtm`, `oracle` – для базы данных Oracle;
- `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`	Не задан*
Пользователь, от имени которого будут запускаться серверные процессы базы данных Oracle **Примечание:** при установке базы данных PostgreSQL учетная запись не создается	`oracle`	Не задан*
Пользователь, от имени которого будут запускаться серверные процессы базы данных PostgreSQL **Примечание:** при установке базы данных Oracle учетная запись не создается	`postgres`	Не задан*

Учетные записи баз данных:

Примечание:

Учетные записи доступны после запуска:

- `sqlplus` – для Oracle;
- `psql` – для PostgreSQL.

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

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

Назначение	Имя	Пароль
Пользователь Linux, от имени которого будут запускаться бинарные файлы и индексы Sphinx	`iwtm`	Не задан*

Примечание:

* Доступ пользователей к Системе ограничен:

- Права учетной записи `iwtm` ограничены запуском процессов Traffic Monitor, бинарных файлов и индексов Sphinx. Редактирование учетной записи недоступно.
- Список групп, в которые входит пользователь `postgres` / `oracle`, ограничен группами этого пользователя.

Учетные записи Веб-консоли:

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

4 Обновление Системы

Важно!

- Обновление до версии 7.14.x поддерживается с версий 7.12.x и 7.13.x. Порядок выпуска версий Системы указан в статье *Документация InfoWatch Traffic Monitor*.
- Обновление Traffic Monitor не поддерживается при подключении к серверу с помощью HP Integrated Lights Out (ILO).
- Во время обновления Системы перехват и анализ событий работать не будут.

Примечание:

Обновление Системы происходит с использованием подключаемого репозитория.

Репозиторий – это папка, содержащая файлы и другие папки и предоставляющая их по запросу ОС. Другими словами, репозиторий – это хранилище, из которого устанавливаются и обновляются программы. Перед использованием нужно подключить репозиторий, чтобы ОС могла к нему обращаться.Инструкция по работе с репозиториями доступна на *официальном сайте Red Hat Enterprise Linux* (на английском).

Примечание:

В процессе обновления IW Traffic Monitor будут выполнены действия, требующие прав `sysdba`:

при использовании СУБД Oracle

- создание триггера `iwtm_logon_trg`, который нужен для доступа пользователей `iwtm_linux` и `iwtm_web` к объектам схемы `iwtm`;
- создание процедуры `sp_iwtm_execute_os_command` для выполнения команд ОС при создании, удалении, архивации и восстановлении файлов табличных пространств;
- настройка профиля пользователя по умолчанию (время жизни пароля, максимальное количество изменений пароля и максимальное количество попыток соединения);
- настройка служебных окон планировщика `dbms_scheduler`;
- отключение доступа к XDB по HTTP-протоколу;
- отключение диспетчера `dispatcher`, т. к. используется выделенный сервер;
- выдача пользователю `iwtm`:
  - прав для установки, обновления и удаления схемы БД;
  - прав для создания, удаления, архивации и восстановления табличных пространств;
  - прав, используемых в коде продукта InfoWatch Traffic Monitor;
  - прав для просмотра статистики БД.

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`).

4.1 Перед обновлением

До начала обновления:

- Примените конфигурацию. Если не применить конфигурацию перед обновлением, она будет применена принудительно.
- Если в Системе установлен и запущен адаптер Password Disclosure Adapter (PDA), перед обновлением ТМ остановите его процессы. Подробнее см. *InfoWatch Password Disclosure Adapter. Руководство по установке и конфигурированию. Диагностика и удаление InfoWatch Password Disclosure Adapter*.

- Убедитесь в наличии:
  - ISO-образа дистрибутивного диска ОС, на которой установлен Traffic Monitor. Версии поддерживаемых ОС можно посмотреть в статье *Аппаратные и программные требования*;
  - дистрибутива InfoWatch Traffic Monitor той версии, до которой планируется обновление;
  - доступа к физическому или виртуальному серверу (серверам), которые нужно обновить;
  - пароля пользователя `root`.
- Выясните:
  - тип установки в Системе: *Все-в-одном (All-in-One)* или *Распределенная (Distributed)* (эта информация понадобится для выбора инструкции по обновлению);
  - тип используемой СУБД: Oracle или PostgreSQL (эта информация понадобится при обновлении схемы БД и серверных компонентов);
  - на каком сервере установлен пакет `web-gui` (эта информация понадобится для очистки кеша сервера после обновления схемы БД). **Подсказка:** пакет установлен на том сервере, к которому подключается Консоль управления Traffic Monitor.

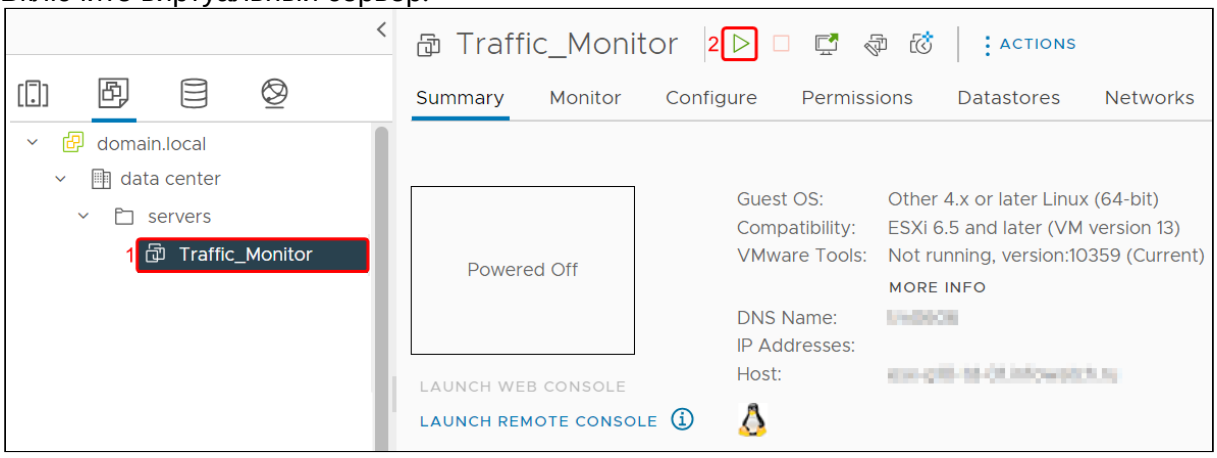
> **Примечание:**
>
> Если ранее продукт был установлен с использованием команды `sudo -i`, примените эту команду во время обновления Системы на РЕД ОС.

- Запустите скрипт, позволяющий определить наличие дубликатов графических объектов и инициирующий их удаление.
- Включите все серверы, предназначенные для обновления (если они были выключены):
  - в случае физического сервера нажмите кнопку включения на корпусе сервера (подробнее см. в инструкции к серверу);
  - в случае виртуального сервера выполните команду **Power On** (см. пример ниже).

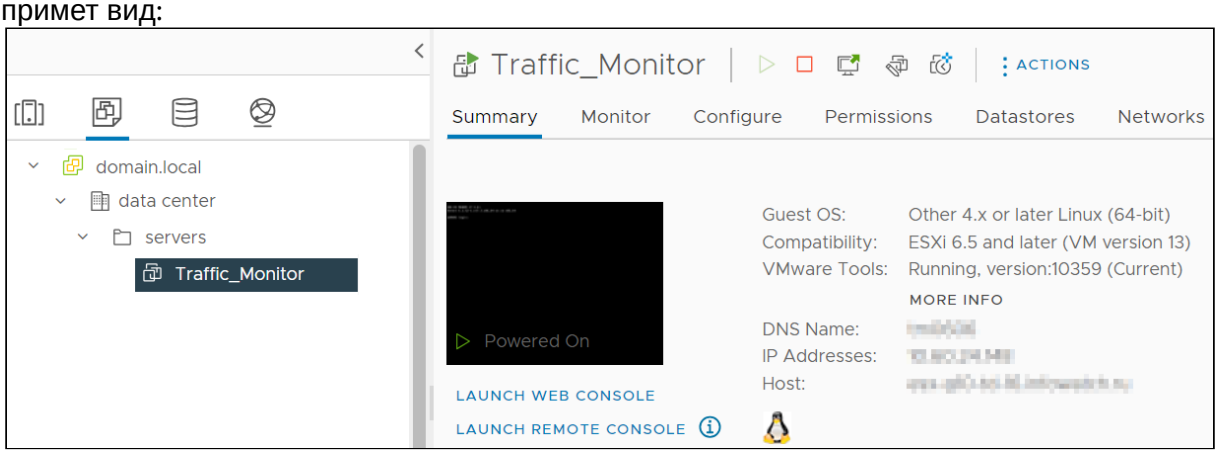
Пример запуска виртуального сервера:

> **Примечание:**
>
> В этой инструкции приводятся примеры по работе с виртуальным сервером в веб-версии клиентского приложения 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.

1. Запустите веб-версию клиентского приложения VMware vSphere Client. Войдите в приложение, используя логин и пароль, выданные администратором вашей информационной сети.
2. Последовательно раскройте все узлы в левой части рабочей области, пока не дойдете до нужного виртуального сервера.
3. Включите виртуальный сервер:



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



4.2 Обновление Системы

Обновите серверы согласно инструкциям:

- *Обновление ТМ Все-в-одном (All-in-one) Enterprise и Standard* – обновление сервера с типом установки "Все-в-одном";
- *Обновление ТМ при распределенной установке* – обновление сервера с распределенным типом установки.

Если вы используете Data Storage, рекомендуем обновить его. Инструкция: *Обновление Data Storage*.

Сведения по обновлению подсистемы Device Monitor смотрите в документе *InfoWatch Device Monitor for Windows. Руководство по установке, конфигурированию и администрированию* или *InfoWatch Device Monitor for Linux. Руководство по установке*.

После обновления

Учитывайте особенности работы Системы:

- после обновления предустановленные привилегии на полное управление запросами и отчетами для пользователей с ролями *Офицер безопасности* и *Администратор* в Системе отсутствуют;
- при наличии выгрузок из БД нужно будет подождать до 7 минут после обновления Системы для корректной работы технологии анализа. Если ждать нельзя, добавьте любой элемент технологии выгрузок из БД и примените конфигурацию. После этого добавленный элемент может быть удален.

4.3 Удаление дубликатов графических объектов

Перед тем, как приступить к обновлению Системы до версии 7.14.x, запустите скрипт, позволяющий определить наличие дубликатов графических объектов и инициирующий их удаление. Для этого в используемой консоли СУБД PostgreSQL выполните запрос:

```
//Автоматическое удаление дублирующихся отпечатков графических объектов
with fingerprint_to_delete as (
   with duplicate_contents as (
     select content_id, count(f2c.fingerprint_id) cnt
     from fingerprint_to_content_sb f2c
     left join fingerprint_sb f on f.fingerprint_id=f2c.fingerprint_id
     where f.type =  'image_classifier'
     group by content_id
     having count(f2c.fingerprint_id) >  1
   )
   select f2c.fingerprint_id
   from duplicate_contents dc
   left join fingerprint_to_content_sb f2c on f2c.content_id = dc.content_id
   where f2c.fingerprint_id not in (
     select (select fingerprint_id from fingerprint_to_content_sb where content_id=dc.content_id limit  1 )
     from duplicate_contents dc
   )
order by dc.content_id
)
delete from fingerprint_sb
```

```
where fingerprint_id in (select fingerprint_id from fingerprint_to_delete);
```

При отсутствии дубликатов Система уведомит вас об этом и вы сможете приступить к обновлению.

После завершения работы скрипта осуществите выход пользователя из базы данных.

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

> **Важно!**
>
> Перед обновлением Traffic Monitor обновите сервер Device Monitor.

Инсталлятор Traffic Monitor при обновлении с участием пользователя может работать в двух режимах:

- текстовый в консоли сервера;
- графический.

Шаги установки и их последовательность аналогичны в обоих режимах.

Также доступен тихий режим работы инсталлятора без участия пользователя.

Независимо от выбранного режима работы инсталлятора, для обновления понадобится использовать консоль (или терминал) сервера.

В процессе обновления на сервер будут установлены все пакеты Traffic Monitor, но при завершении работы инсталлятор запустит только те сервисы, которые до обновления не были отключены.

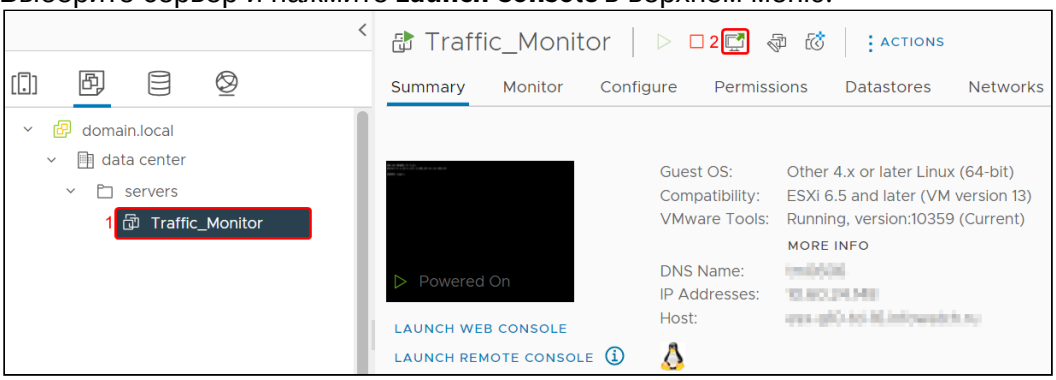
> **Примечание:**
>
> Если сервис был отключен, после обновления он **не** будет запущен.
>
> Если сервис был остановлен, после обновления он будет запущен.
>
> Статусы новых сервисов будут соответствовать первичной установке.

Распаковка пакетов начнется не при запуске инсталлятора, а непосредственно перед обновлением.

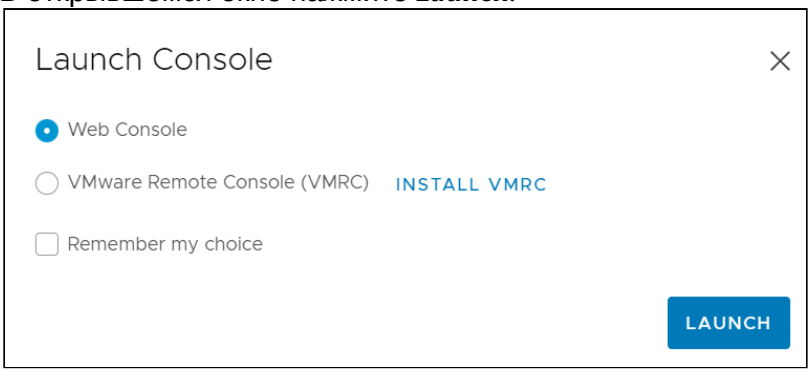
Перед обновлением Системы выполните следующие действия:

1. Откройте консоль обновляемого сервера:
   - в случае физического сервера – консоль отображается на экране монитора, подключенного к серверу;
   - в случае виртуального сервера – выполните команду **Launch Console** (см. пример ниже):
     Пример запуска консоли виртуального сервера в веб-версии клиентского приложения VMware vSphere Client:

a. Выберите сервер и нажмите **Launch Console** в верхнем меню:



b. В открывшемся окне нажмите **Launch**.



Откроется окно с консолью сервера, в котором вам нужно ввести пароль пользователя.

2. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя `root`).

> **Подсказка:**
>
> Команды в консоли вводятся с помощью клавиатуры и обязательно подтверждаются нажатием клавиши **Enter**, поэтому в данной инструкции под "введите команду `command`" подразумевается "введите команду `command` и нажмите **Enter**". После выполнения команды снова отображается приглашение – оно заканчивается знаком `#` или `$` (в зависимости от того, от имени какого пользователя выполнен вход). Прежде чем вводить следующую команду, нужно убедиться, что в командной строке отображается приглашение.

3. **Если вы обновляете Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8:**

> **Важно!**
>
> Убедитесь, что в операционной системе Oracle Linux 8.10 в качестве текущего выбрано ядро Red Hat Compatible Kernel (RHCK), например Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, а ядро UEK удалено. Подробнее см. *Требования к настройкам ОС и сети сервера*.

a. Установите пакет `redhat-lsb-core` с помощью следующей команды:

```
dnf install redhat-lsb-core
```

b. Создайте резервную копию файла выпуска ОС и замените содержимое исходного файла. Для этого выполните команды в зависимости от ОС:
   - на ОС Oracle Linux 8:

     ```
     cp /etc/oracle-release /etc/release.bak

     echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/oracle-release
     ```
   - на ОС AlmaLinux 8 или Rocky Linux 8:

     ```
     cp /etc/redhat-release /etc/release.bak
     echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/redhat-release
     ```

c. Выполните команду:

   ```
   lsb_release -a
   ```

   В результате должна быть выведена следующая информация:

   ```
   Distributor ID: RedHatEnterprise
   Description:    Red Hat Enterprise Linux release 8.10 (Ootpa)
   Release:        8.10
   Codename:       Ootpa
   ```

   > **Примечание:**
   >
   > После обновления Traffic Monitor восстановите исходный файл выпуска ОС. Подробнее см. ниже.

4. Проверьте версию, редакцию и тип установки обновляемого сервера при помощи команды:
   `cat /opt/iw/tm5/install_mode`

Пример содержимого файла install_mode

```
{
  "product_type": "tme",
  "version": "7.13.0.150",
  "all_in_one": true,
  "templates": {
    "db": {
      "local": true
    },
    "indexer": {},
    "web": {},
```

```
    "interceptors": {}
  },
  "upgrade": {
    "previous_version": "7.12.0.136",
    "state": "done"
  }
}
```

Запись из примера соответствует серверу Traffic Monitor с типом установки *All-in-One* редакции *Enterprise* и версии *7.13.0.150*.

5. Обновите ОС на сервере, если ее версия отсутствует в списке поддерживаемых версий ОС в статье *Аппаратные и программные требования*.

Важно!

Перед обновлением Системы убедитесь, что сервер соответствует *требованиям к настройкам ОС и сети сервера*.

После обновления параметры unit-файлов системы инициализации `systemd` вернутся к значениями по умолчанию.

Внимание!

Чтобы в случае ошибки иметь возможность восстановить базу данных и возобновить процесс обновления с последнего успешного этапа, рекомендуется выполнить:

1. **Резервное копирование базы данных и индексов**

   Важно!

   Для успешного восстановления файлы обязательно должны быть скопированы с сохранением их **прав, пользователей и групп**.
   Для этого копируйте файлы только на **файловую систему Linux** (например, Ext4 или XFS).
   Храните резервные копии либо на другом разделе сервера, либо на другом сервере, либо на внешнем устройстве. Убедитесь, что данные не будут потеряны.
   Для восстановления нужно будет скопировать резервные копии **по адресам исходных файлов, не изменяя прав, пользователей и групп**.

   a. Для остановки сервисов Traffic Monitor введите команду:
      `iwtm stop`
   b. Выполните резервное копирование:
      i. В зависимости от используемой СУБД введите команду для остановки Базы данных:
         - для **СУБД Oracle**:
           `systemctl stop oracle`
         - для **СУБД PostgreSQL** версии 13:
           `systemctl stop postgresql-13`

- для **СУБД PostgreSQL** версии 15:
  `systemctl stop postgresql-15`

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

> **Примечание:**
>
> Для уточнения директорий, содержащих Базу данных, проверьте также содержимое файла:
>
> - `/opt/iw/tm5/csw/oracle/database.conf` (для **СУБД Oracle**)
> - `/opt/iw/tm5/csw/postgres/database.conf` (для **СУБД PostgreSQL**)

iii. Создайте резервную копию индексов. Для этого:
   1. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на просмотр файл **`indexer.conf`**.
   2. В параметре `"SphinxBaseDir"` указан путь к директории с индексами. В параметре `"ArchiveDir"` указан относительный путь к архивам индексов. Путь к архивам указывается относительно содержимого параметра `"NookDir"`.
      Скопируйте директории с индексами и архивами индексов либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство.

iv. Создайте резервную копию конфигурации службы `iw_adlibitum`. Для этого:
   1. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на просмотр файл **`adlibitum. conf`**.
   2. В параметре `"ConfigDir"` указан относительный путь к директории с конфигурации службы `iw_adlibitum`. Путь к директории указывается относительно содержимого параметра `"NookDir"`.
      Скопируйте директорию с конфигурацией либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство.

2. **Резервное копирование настроек окружения**

   Обязательно учитывайте особенности копирования из предупреждения в предыдущем шаге. Перейдите по адресам и скопируйте указанные файлы:

   - **Для СУБД Oracle:**
     - `/opt/iw/tm5/etc/oracle/` – все файлы в директории
     - `/etc/default/iwtm`
     - `/etc/profile.d/iw-oracle-env.sh`
     - `/etc/logrotate.d/iwtm-oracle-conf-server`
     - `/opt/iw/tm5/etc/oracle.conf`
   - **Для СУБД PostgreSQL:**
     - `/etc/default/iwtm`

- `/etc/profile.d/iw-postgresql-env.sh`
- `/etc/profile.d/iw-postgresql-client-env.sh`
- `/etc/sudoers.d/iw-pgagent`
- `/etc/pgagent/pgagent-13.conf` или `/etc/pgagent/pgagent-15.conf`, в зависимости от версии СУБД
- `/opt/iw/tm5/etc/postgresql/` – все файлы в директории
- `/opt/iw/tm5/etc/postgresql.conf`

> **Примечание:**
>
> Также инсталлятор автоматически создает копии файлов настроек окружения в директории `/tmp/iwtm_db_configs_backup`. Для удобства пользователя инсталлятор воссоздает в директории пути оригинальных файлов, по которым их нужно будет скопировать для восстановления исходного состояния.
> Созданные инсталлятором резервные копии хранятся только до успешного обновления. По завершении они будут удалены.

Выберите инструкцию в зависимости от варианта обновления:

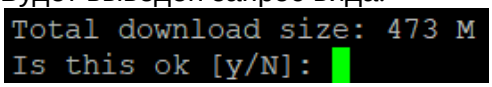
- Обновление Системы поверх установленной
- Обновление Системы путем чистой установки и восстановления данных из резервной копии (для СУБД PostgreSQL)

Обновление Системы поверх установленной

> **Важно!**
>
> Крайне рекомендуем выполнить резервное копирование Системы, а также клонировать ее и провести обновление на этой тестовой машине.

Чтобы обновить Систему, выполните следующие действия:

1. Скопируйте в директорию `/root` файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor. Список файлов для различных ОС и СУБД см. в статье *Установка TM Enterprise и TM Standard в режиме "Все-в-одном"*, шаг 5. Далее будет описано обновление с использованием инсталлятора для ОС Red Hat Enterprise Linux. Данная инструкция актуальна и для других поддерживаемых ОС: Oracle Linux, РЕД ОС, AlmaLinux, Rocky Linux и Альт Сервер.
2. Чтобы сделать файл **`iwtm-installer-x.x.x.xxx-rhel7`** исполняемым, введите команду:
   `chmod u+x /root/iwtm-installer-x.x.x.xxx-rhel7`
   В нашем примере команда будет следующей:
   `chmod u+x /root/iwtm-installer-7.14.0.97-rhel7`
3. Подключите внешние или локальные репозитории ОС.
   Например, с инструкцией по настройке локального репозитория в Red Hat Enterprise Linux можно ознакомиться на *официальном сайте* (на английском).

4. Для обновления пакетов введите команду:
   `yum upgrade`
   Будет выведен запрос вида:
   

   Для продолжения введите **Y** на клавиатуре и нажмите **Enter**.
5. Установите дополнительные пакеты `python3-psycopg2` и `libzstd` с помощью команды:
   `yum install python3-psycopg2 libzstd`
   В случае ошибки скачайте эти пакеты из репозитория EPEL и установите вручную.
6. Если вы используете удаленную базу данных:
   a. Убедитесь, что версия вашей СУБД поддерживается Traffic Monitor (см. *Аппаратные и программные требования*).
   b. Если версия СУБД актуальна, пропустите это действие.
   Если СУБД нужно обновить:
      i. Остановите сервисы Traffic Monitor с помощью команды:
      `iwtm stop`
      ii. Остановите СУБД.
      iii. Обновите СУБД до поддерживаемой версии, используя официальную инструкцию.

      > **Примечание:**
      >
      > Для СУБД PostgreSQL и PostgreSQL Pro также обновите используемый сервис `pgagent`.

      iv. После обновления запустите СУБД, но не запускайте сервисы Traffic Monitor.
7. Если обновляемый сервер Traffic Monitor взаимодействует с Data Discovery 2.0 и более новыми, остановите под (pod) `technologies`, который создает соединения с базой данных для доступа к конфигурации.
   Чтобы остановить под:
   a. Подключитесь к терминалу любой ноды кластера Центра расследований, в котором установлен Data Discovery, подключающийся к базе данных Traffic Monitor.
   b. Имя пода (pod) содержит лейбл ноды, на которой он установлен. Для определения имени пода выполните команду:
   `kubectl get pods -A -o wide | grep technolog`

   Пример вывода в командной строке после команды:

   ```
   root@lv-426:~# kubectl get pods -A -o wide | grep technolog
   infowatch      technologies-central-71cb89dd54-bgwn6      3/3     Running   0
   18h   10.244.0.86   lv-426   <none>           <none>
   ```

   В нашем примере лейбл ноды `central`.
   c. Для остановки пода на ноде с лейблом `central` выполните команду:
   `kubectl scale -n infowatch --replicas=0 deployment/technologies-central`
   d. Подключитесь обратно к терминалу сервера с Traffic Monitor.

8. Если в Системе установлен и запущен адаптер Password Disclosure Adapter, перед обновлением Traffic Monitor остановите его процессы. Подробнее см. документ *InfoWatch Password Disclosure Adapter. Руководство по установке и конфигурированию. Диагностика и удаление InfoWatch Password Disclosure Adapter*.
9. Если у вас установлена система Prometheus, для остановки службы выполните команду:
   `systemctl stop iwtm-postgres_exporter` – для **СУБД PostgreSQL**
   `systemctl stop iwtm-oracledb_exporter` – для **СУБД Oracle**
10. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor:
    `cd /root`

> **Примечание:**
>
> Перед обновлением рекомендуем запустить сервис базы данных, если ранее он был остановлен. В зависимости от используемой СУБД введите команду для запуска:
>
> - для **СУБД Oracle**:
>   `systemctl start oracle`
> - для **СУБД PostgreSQL** версии 13:
>   `systemctl start postgresql-13`
> - для **СУБД PostgreSQL** версии 15:
>   `systemctl start postgresql-15`

11. В инсталляторе реализован механизм автоматического объединения конфигурационных файлов Traffic Monitor старой и новой версии.

> **Важно!**
>
> Автоматическое объединение затрагивает только конфигурационные файлы Traffic Monitor с расширением **`.conf`**, расположенные в директории `/opt/iw/tm5/etc`.
> Перед объединением в директории `/opt/iw/tm5/etc_conf_backup_<дата_время>` будут созданы резервные копии исходных конфигурационных файлов. Пример названия директории: `/opt/iw/tm5/etc_conf_backup_05.06.2024_09:26:33`.
> После успешного объединения файлы с расширением **`.rpmnew`**, которые относятся к затрагиваемым конфигурационным файлам, будут удалены.
> Все выполненные действия будут отражены в лог-файле `/var/log/infowatch/iwtm-install-<версия>-<дата>_<время>.log`. Пример названия лог-файла: `/var/log/iwtm-install-7.14.0.97-2024-09-06_09-56-25.log`.
> Также информацию о процессе можно найти в директории `/var/log/infowatch/config_merge/`.
> Если во время действий с конфигурационным файлом будут обнаружены ошибки, процесс будет остановлен до исправления ошибок пользователем. После исправления ошибок повторно запустите обновление.

Запустите инсталлятор в одном из режимов:

- **обновление в текстовом режиме в консоли сервера**

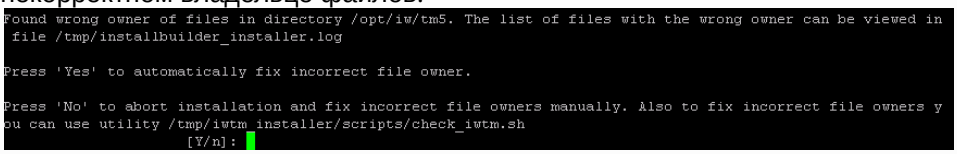
  Чтобы обновить Traffic Monitor в консоли сервера, выполните следующие действия:

  a. Для обновления Traffic Monitor запустите инсталлятор, выполнив команду вида:
     `./iwtm-installer-x.x.x.xxx-rhel7`

В нашем примере команда будет:
`./iwtm-installer-7.14.0.97-rhel7`
Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

Примечание:

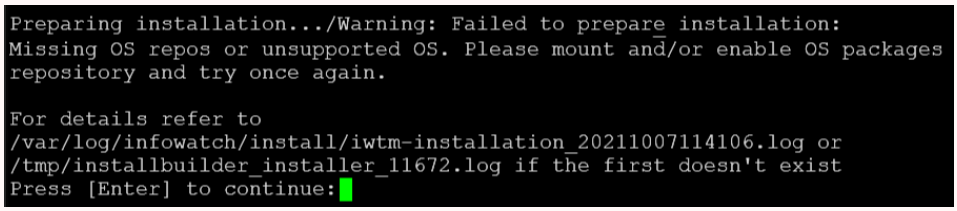
Перед запуском инсталлятора может быть выведено предупреждение о некорректном владельце файлов.



Введите **Y** и нажмите **Enter**, чтобы инсталлятор исправил владельца файлов и продолжил запуск.
В противном случае введите **N**, нажмите **Enter**, исправьте несоответствие вручную или с помощью скрипта `/tmp/iwtm_installer/scripts/check_iwtm.sh` и повторно запустите инсталлятор.

Важно!

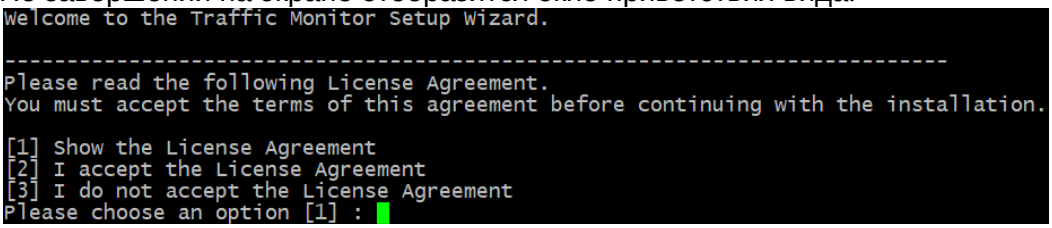
При отсутствии настроенных и доступных репозиториев ОС запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите **Enter** для завершения работы инсталлятора, затем подключите стандартный репозиторий RHEL, репозиторий EPEL и повторно запустите инсталлятор.

Подробную информацию об ошибке можно найти в лог-файлах, указанных в предупреждении.

По завершении на экране отобразится окно приветствия вида:



b. Для продолжения обновления нужно принять условия Лицензионного соглашения. Выберите один из предложенных вариантов. Для этого введите цифру, указанную напротив него, и нажмите **Enter**:

- `Show the License Agreement` – для просмотра Лицензионного соглашения;

  При выборе этого варианта:

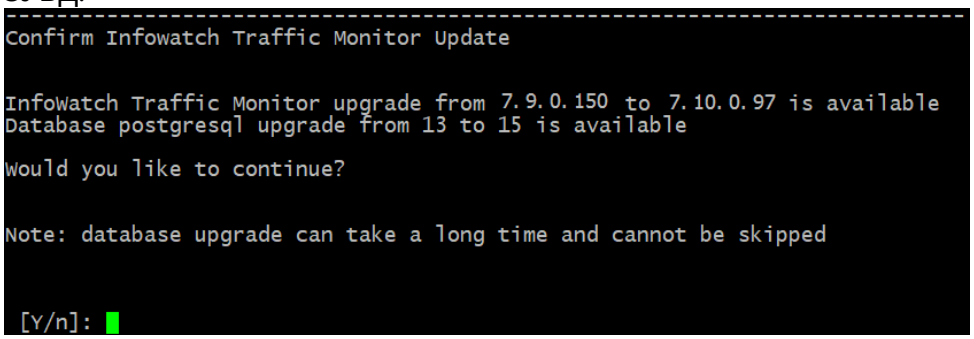
  i. Выберите язык, на котором будет выведен текст Лицензионного соглашения:
     - `English` – английский;
     - `Russian` – русский.

  ii. Прочитайте Лицензионное соглашение. Для перехода к следующей странице нажимайте **Enter**.

  iii. Примите Лицензионное соглашение. Для этого введите **y** и нажмите **Enter**.
- `I accept the License Agreement` – чтобы принять Лицензионное соглашение без предварительного просмотра;
- `I do not accept the License Agreement` – чтобы не принимать Лицензионное соглашение и прервать процесс обновления.

> **Примечание:**
>
> При обновлении в консоли сервера перед полем ввода в квадратных скобках указано значение по умолчанию. Оно будет использовано, если оставить поле ввода пустым и нажать **Enter**.
>
> **Пример:**
>
> Если на изображении выше не вводить значение, а только нажать **Enter**, будет выбран пункт `[1] Show the License Agreement`.

Далее на экране отобразится окно подтверждения обновления, в котором будут указаны доступные обновления для Traffic Monitor и СУБД:



c. Для продолжения введите **Y** и нажмите **Enter**. Для выхода из инсталлятора введите **N** и нажмите **Enter**.

d. Подтвердите остановку сервисов Traffic Monitor и Базы данных. Шаги подтверждения и выбора режима остановки будут пропущены, если сервисы были остановлены вручную до запуска инсталлятора.

e. Выберите режим остановки Traffic Monitor:
   - `Quick stop` – быстрая остановка без обработки событий;

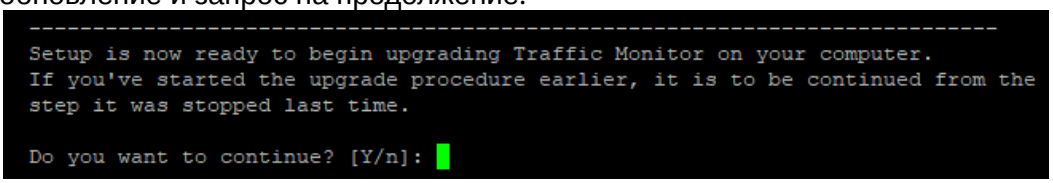
- `Waiting for stop` – перед остановкой дождаться завершения текущей обработки событий;
- `Waiting for emptying file queues` – перед остановкой дождаться обработки всех событий и очистки файловых очередей.

Для выбора введите цифру, указанную напротив выбранного варианта, и нажмите **Enter**.

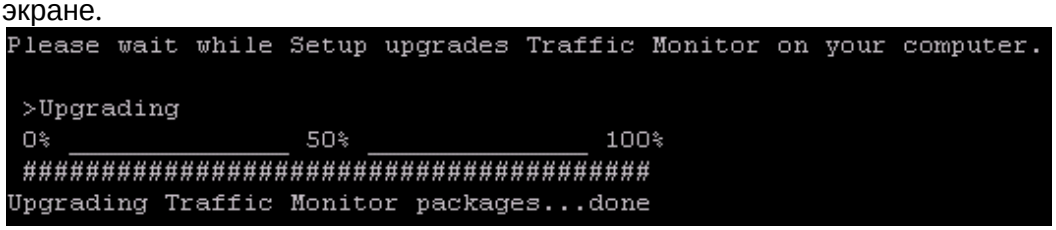
> **Примечание:**
>
> Если выбран `Quick stop`, остановленные сервисы до запуска будут иметь статус `failed (failed)`.

f. Если выбран `Quick stop` или `Waiting for stop`, после возобновления работы Traffic Monitor необработанные события могут попасть в очередь ошибок обработки.
Для продолжения введите **Y** и нажмите **Enter**.
В процессе остановки на экране будет информация о ходе обработки событий.

g. После остановки сервисов будет выведено сообщение о готовности начать обновление и запрос на продолжение.



Для начала обновления введите **Y** и нажмите **Enter**.
Начнется распаковка пакетов, обновление имеющихся и установка новых компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



Процесс займет некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-либо причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

h. После обновления инсталлятор предложит запустить остановленные сервисы.

Важно!

После обновления настройки системы мониторинга Nagios будут изменены на значения по умолчанию. Если до обновления конфигурационные файлы Nagios редактировались, в директории `/etc/infowatch/nagios/iwmon` будут созданы их копии с расширением `.saved`. Перед запуском сервисов Traffic Monitor перенесите настройки из файлов `.saved` в соответствующие новые конфигурационные файлы.

После обновления для управления системой мониторинга используйте службу `iwtm-nagios`.
Например, для просмотра статуса Nagios используйте команду:
`systemctl status iwtm-nagios`

Важно!

Если в конфигурационном файле `luaengined.conf` указан параметр `SmtpTmBccList`, перед запуском сервисов убедитесь, что значение параметра не содержит угловых скобок (`<` и `>`). В противном случае удалите скобки.

Если не запустить сервисы, то для восстановления работоспособности Системы их придется запустить позже вручную.

Примечание:

В случае некорректной настройки службы Consul в консоли будет выведено предупреждение:

```
\Warning: You should run 'iwtm start' command manually after fixing problems with
Consul.
Press [Enter] to continue:
```

Для завершения работы инсталлятора нажмите **Enter**.

Для корректной работы Системы выполните проверку и настройку кластера службы Consul

i. Запустите службу Consul, выполнив команду:
`systemctl start iwtm-consul`
Проверить статус службы можно командой:
`systemctl status iwtm-consul`

ii. Чтобы проверить службу Consul, выполните команды:
   1. Для вывода IP-адреса основного сервера (лидера) кластера:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   2. Для вывода информации о членах кластера:
   `consul members`

iii. Если не будет выведен IP-адрес лидера кластера, выполните *конфигурирование кластера службы Consul*.
После настройки повторите проверку (действие ii).

При данной ошибке инсталлятор не запустит сервисы Traffic Monitor по завершении работы – их нужно будет запустить вручную.

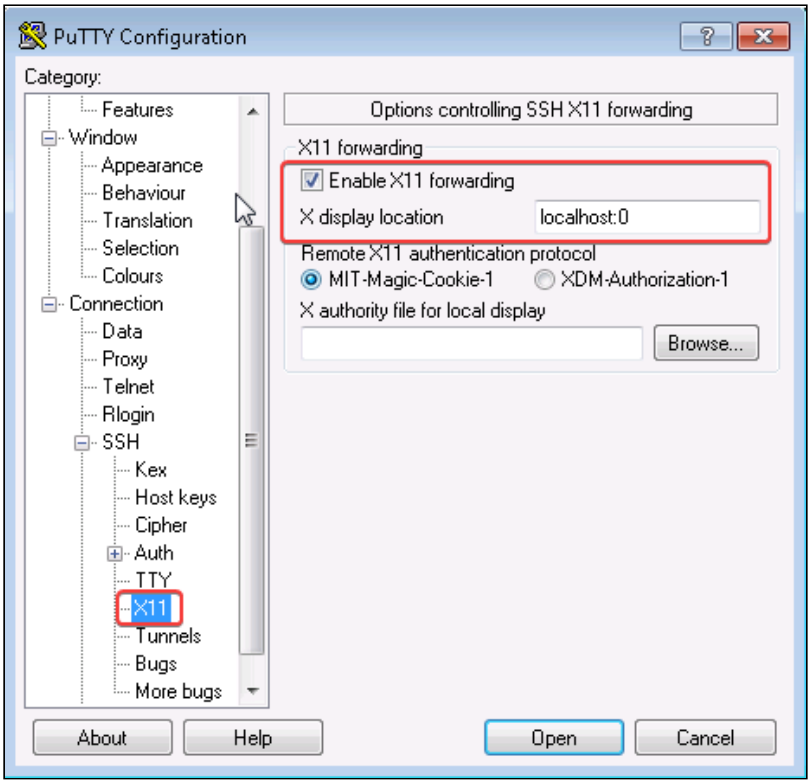
i. Перед завершением работы инсталлятор предложит удалить пакеты, созданные для обновления.
Если обновление прошло успешно, данные рекомендуется удалить.
j. Дождитесь завершения работы инсталлятора.

- **обновление с использованием графического режима инсталлятора**

В ОС оконная система X Window System использует клиент-серверную модель. Для запуска инсталлятора в графическом режиме используется перенаправление графического вывода удаленной подсистемы (**X11 Forwarding**). Это позволит работать напрямую с графическими приложениями среды Linux на компьютере, с которого осуществляется подключение к серверу. Данный режим реализуется с помощью SSH-подключения.

Чтобы обновить Traffic Monitor с использованием графического режима инсталлятора, выполните следующие действия:

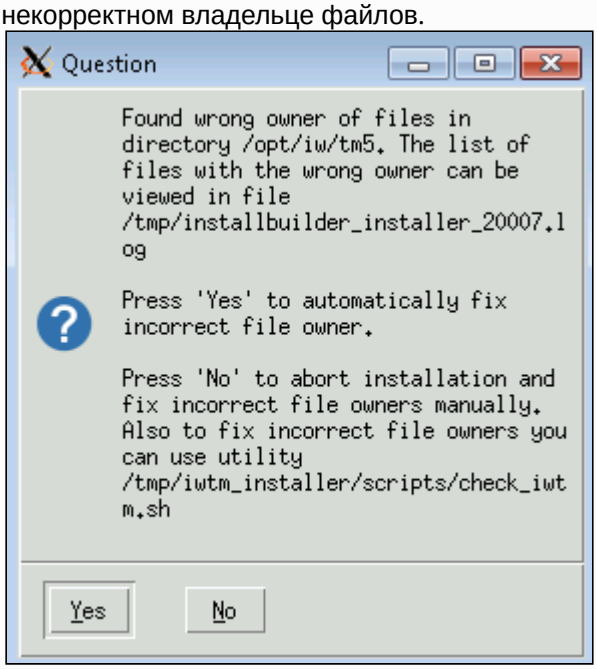
a. На обновляемом сервере:
   i. Установите утилиту XAuth с помощью команды:
   `yum install xauth`
   ii. В конфигурационном файле `/etc/ssh/sshd_config` раскомментируйте строку "`X11Forwarding yes`". Для этого удалите перед строкой символ `#`.
   iii. Сохраните изменения в конфигурационном файле.
   iv. Перезапустите службу SSH с помощью команды:
   `systemctl restart sshd`
b. На компьютере, на котором будет использован графический режим:
   i. Для подключения к обновляемому серверу вам потребуется SSH-клиент с включенной опцией X11 Forwarding, например PuTTY.
   ii. Для запуска инсталлятора в графическом режиме вам потребуется настроенное приложение-клиент для обращения к X Window System, например:
      - приложение Xming – для ОС семейства MS Windows;
      - оболочка Gnome 3 – для ОС семейства Linux.
c. Запустите настроенное приложение-клиент для обращения к X Window System.
d. Подключитесь к серверу, на котором планируется обновление Traffic Monitor, с помощью выбранного SSH-клиента.
Пример окна настройки PuTTY при подключении



e. Запустите инсталлятор, выполнив следующую команду:
`./iwtm-installer-x.x.x.xxx-rhel7`
В нашем примере команда будет следующей:
`./iwtm-installer-7.14.0.97-rhel7`
Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

> **Примечание:**

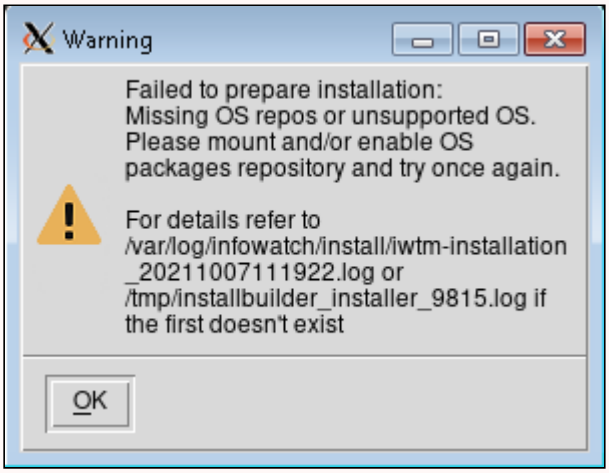
Перед запуском инсталлятора может быть выведено предупреждение о некорректном владельце файлов.



Нажмите кнопку **Yes**, чтобы инсталлятор исправил владельца файлов и продолжил запуск.
В противном случае нажмите кнопку **No**, исправьте несоответствие вручную или с помощью скрипта `/tmp/iwtm_installer/scripts/check_iwtm.sh` и повторно запустите инсталлятор.

Важно!

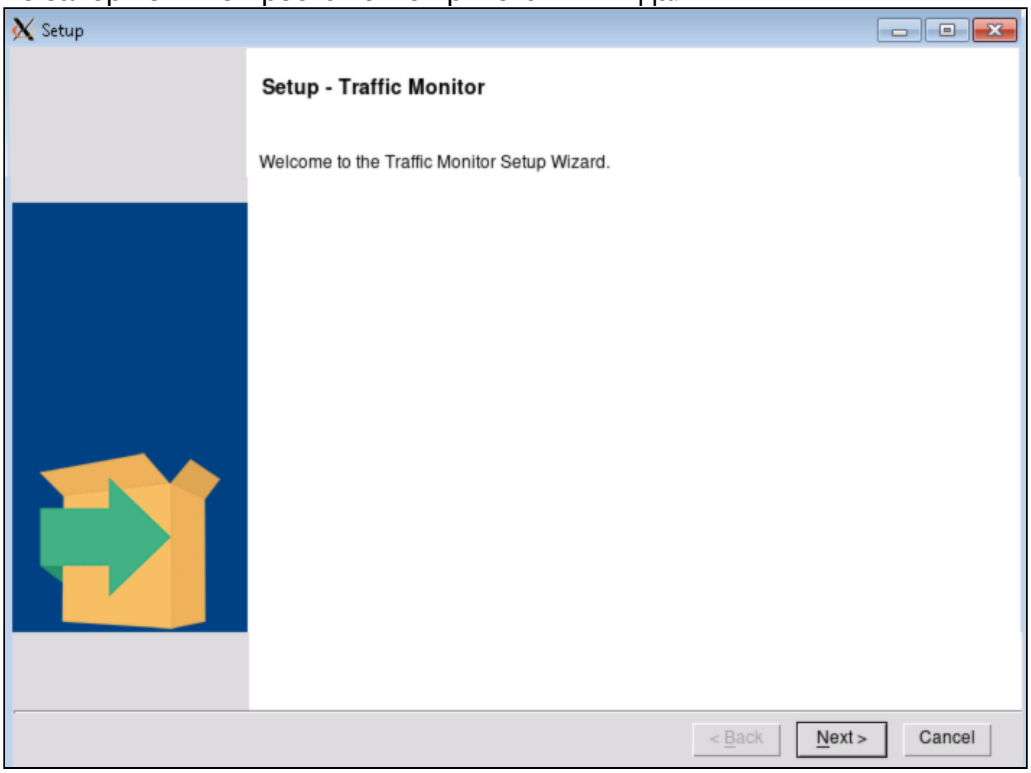
При отсутствии настроенных и доступных репозиториев ОС запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите кнопку **OK** для закрытия окна и завершения работы инсталлятора, затем подключите стандартный репозиторий RHEL, репозиторий EPEL и повторно запустите инсталлятор.

Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

По завершении откроется окно приветствия вида:



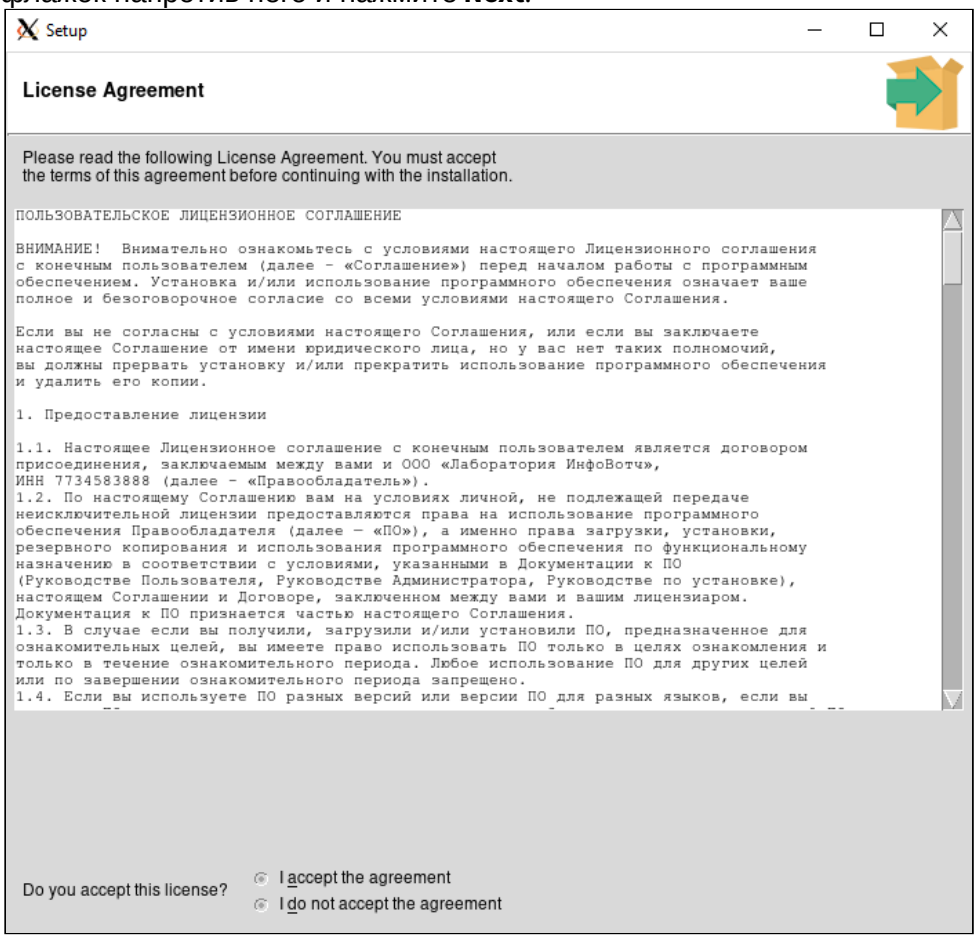
Для перехода к следующему окну нажмите **Next**, для возврата к предыдущему – **Back**. Для выхода из инсталлятора нажмите **Cancel**.

f. Для продолжения обновления нужно принять условия Лицензионного соглашения. Для этого:
   i. Выберите язык, на котором будет выведен текст Лицензионного соглашения:



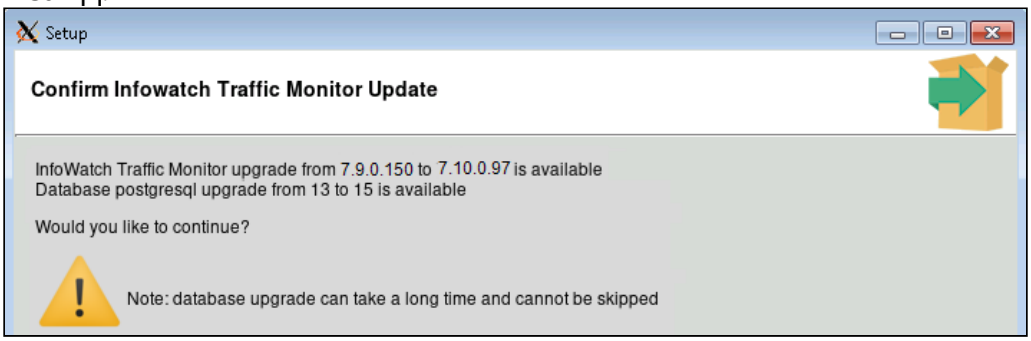
- `English` – английский;
- `Russian` – русский.

ii. Выберите один из предложенных вариантов. Для этого установите флажок напротив него и нажмите **Next**:



- `I accept the agreement` – чтобы принять Лицензионное соглашение и продолжить процесс обновления;
- `I do not accept the agreement` – чтобы не принимать Лицензионное соглашение и прервать процесс обновления.

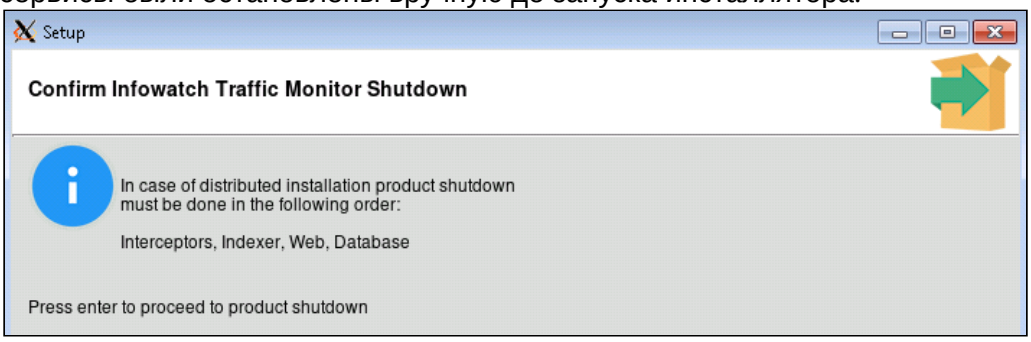
g. В следующем окне будут указаны доступные обновления для Traffic Monitor и СУБД.



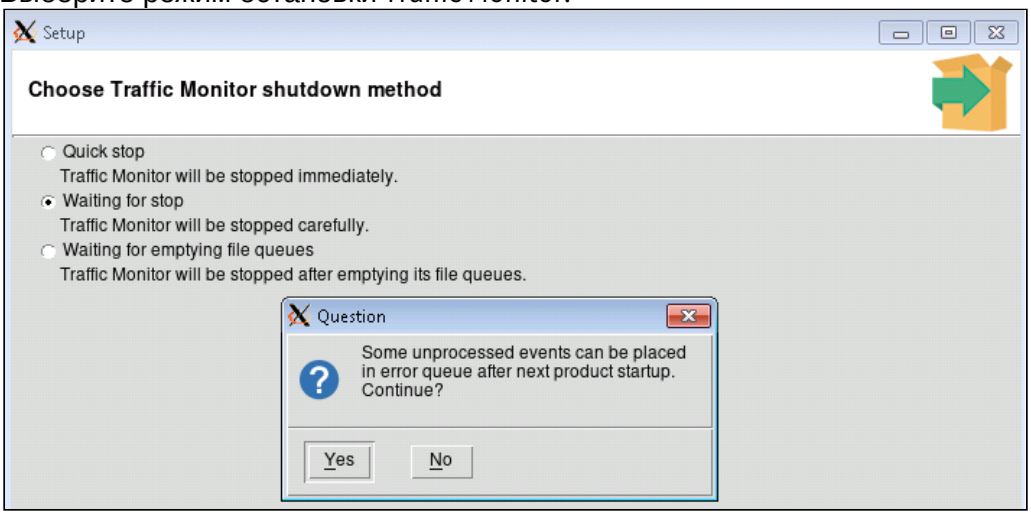
Для продолжения нажмите **Next**.

h. Подтвердите остановку сервисов Traffic Monitor и Базы данных. Шаги подтверждения и выбора режима остановки будут пропущены, если

сервисы были остановлены вручную до запуска инсталлятора.



i. Выберите режим остановки Traffic Monitor:



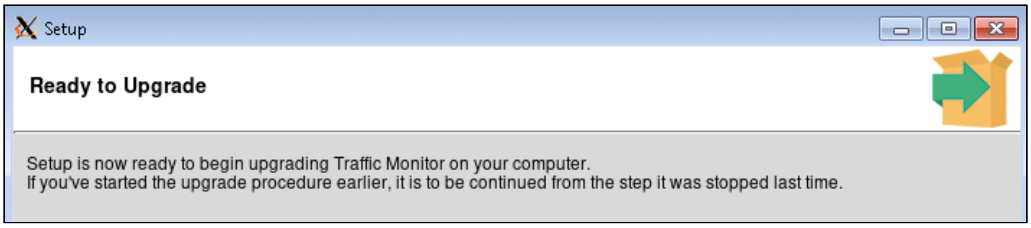
- `Quick stop` – быстрая остановка без обработки событий;
- `Waiting for stop` – перед остановкой дождаться завершения текущей обработки событий;
- `Waiting for emptying file queues` – перед остановкой дождаться обработки всех событий и очистки файловых очередей.

Для выбора установите флажок напротив соответствующего значения и нажмите **Next**.

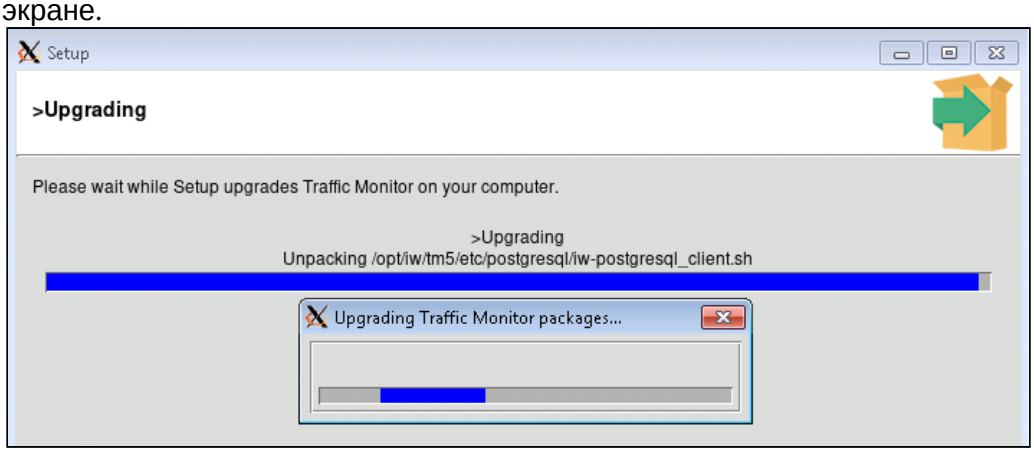
> **Примечание:**
>
> Если выбран `Quick stop`, остановленные сервисы до запуска будут иметь статус `failed(failed)`.

j. Если выбран `Quick stop` или `Waiting for stop`, после возобновления работы Traffic Monitor необработанные события могут попасть в очередь ошибок обработки.
Для продолжения нажмите **Yes**.
В процессе остановки на экране будет информация о ходе обработки событий.

k. После остановки сервисов будет выведено сообщение о готовности начать установку и запрос на продолжение.



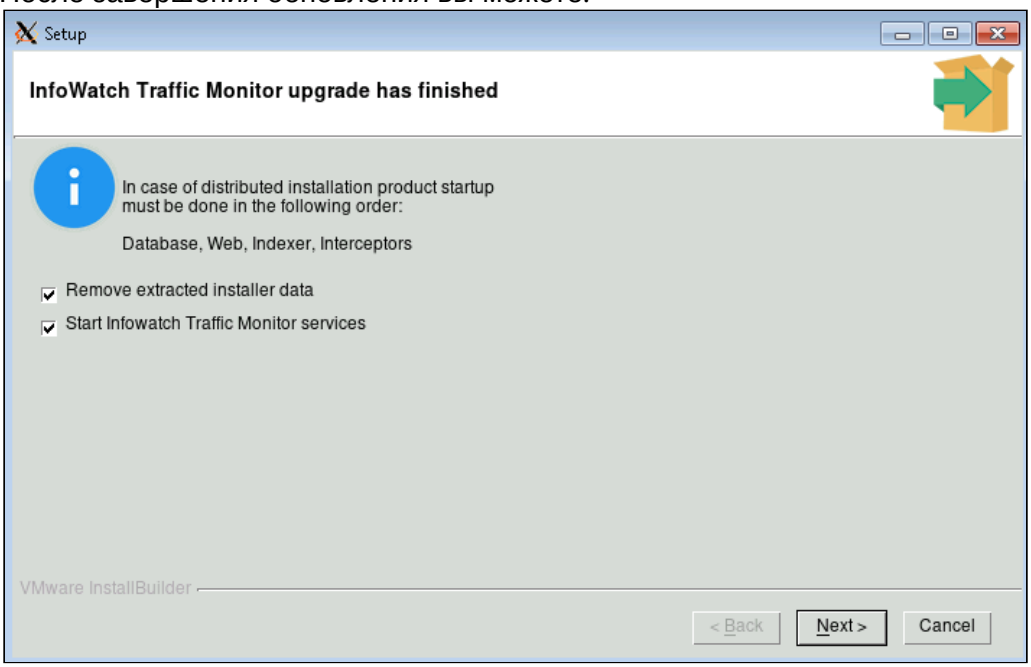
Для начала обновления нажмите **Next**.
Начнется распаковка пакетов, обновление имеющихся и установка новых компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



Процесс займет некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-либо причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

l. После завершения обновления вы можете:

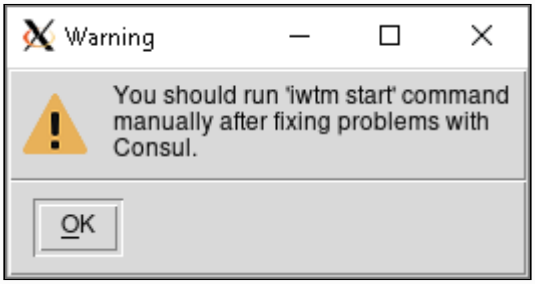


- **`Remove exctracted installer data`** – удалить пакеты, созданные инсталлятором для установки. Если установка прошла успешно, данные рекомендуется удалить;
- **`Start Infowatch Traffic Monitor services`** – запустить остановленные сервисы. Если не запустить сервисы, то для восстановления работоспособности Системы их придется запустить позже вручную.

> **Важно!**
>
> После обновления настройки системы мониторинга Nagios будут изменены на значения по умолчанию. Если до обновления конфигурационные файлы Nagios редактировались, в директории `/etc/infowatch/nagios/iwmon` будут созданы их копии с расширением `.saved`. Перед запуском сервисов Traffic Monitor перенесите настройки из файлов `.saved` в соответствующие новые конфигурационные файлы.
>
> После обновления для управления системой мониторинга используйте службу `iwtm-nagios`.
> Например, для просмотра статуса Nagios используйте команду:
> `systemctl status iwtm-nagios`

> **Важно!**
>
> Если в конфигурационном файле `luaengined.conf` указан параметр `SmtpTmBccList`, перед запуском сервисов убедитесь, что значение параметра не содержит угловых скобок (`<` и `>`). В противном случае удалите скобки.

Для выбора действий поставьте галочки напротив соответствующих пунктов.

> **Примечание:**
>
> В случае некорректной настройки службы Consul в консоли будет выведено предупреждение:
>
> 
>
>
> Для закрытия окна и завершения работы инсталлятора нажмите **OK**.
>
> **Для корректной работы Системы выполните проверку и настройку кластера службы Consul**
>
> i. Запустите службу Consul, выполнив команду:
> `systemctl start iwtm-consul`
> Проверить статус службы можно командой:
> `systemctl status iwtm-consul`
> ii. Чтобы проверить службу Consul, выполните команды:
> 1. Для вывода IP-адреса основного сервера (лидера) кластера:
> `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
> 2. Для вывода информации о членах кластера:
> `consul members`
> iii. Если не будет выведен IP-адрес лидера кластера, выполните *конфигурирование кластера службы Consul*. После настройки повторите проверку (действие ii).
>
> При данной ошибке инсталлятор не запустит сервисы Traffic Monitor по завершении работы – их нужно будет запустить вручную.

m. Для завершения работы инсталлятора нажмите **Next**.

- **обновление в тихом режиме**

  Чтобы сократить участие пользователя в процессе обновления Системы, в инсталляторе предусмотрена работа в тихом режиме. В нем инсталлятор может обновить Traffic Monitor, используя параметры по умолчанию.

  В инсталляторе реализована возможность использования файла параметров (option file). В нем вы можете задать требуемые особенности установки. При запуске инсталлятора с файлом параметров указанные в нем значения будут считаться параметрами по умолчанию.

4.4.1 Файл параметров (option file)

В файле описание параметров имеет вид:

`<имя_параметра>=<значение_параметра>`

Вы можете оставлять комментарии, используя символ `#`.

Пример файла параметров:

```
# This file is just an example
fix_incorrect_file_owners=1
cleanup_way=clean_fq
start_services_after_upgrade=1
```

В данном примере указаны параметры:

- исправить некорректного владельца файлов;
- перед остановкой сервисов дождаться обработки всех событий и очистки файловых очередей;
- после обновления запустить сервисы.

Важно!

Для параметров, которые не указаны в файле, будут использованы значения по умолчанию. Полный набор параметров указан в таблице ниже.

Чтобы использовать файл параметров, перейдите в директорию с инсталлятором и запустите его с опцией `--optionfile` и с указанием созданного ранее файла.

Пример команды использования файла параметров:

```
./iwtm-installer-7.14.0.97-rhel7 --optionfile /some_directory/option-file-example
```

Альтернативный способ использования: назовите файл параметров тем же именем, что назван инсталлятор, но с расширением `.options`, и скопируйте его в директорию к инсталлятору. В этом случае при запуске инсталлятор также будет считать параметры из файла значениями по умолчанию.

4.4.2 Тихий режим обновления

Для обновления в тихом режиме используйте опцию `--mode unattended`.

Уровень взаимодействия с пользователем задается параметром `--unattendedmodeui`, который имеет следующие значения:

- `none` – в процессе работы инсталлятор не выводит на экран никакую информацию и не требует взаимодействия с пользователем;
- `minimal` – отображает прогресс обновления, не требует взаимодействия с пользователем;

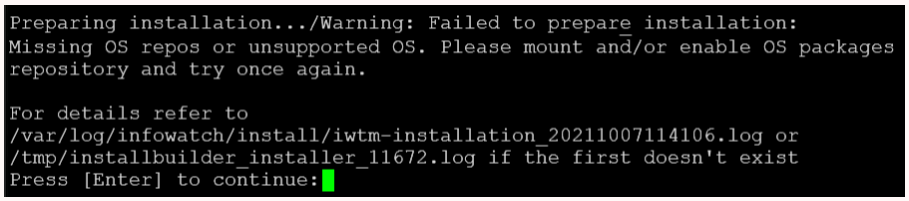
- `minimalWithDialogs` – отображает прогресс обновления, в процессе могут появляться всплывающие окна, может потребоваться взаимодействие с пользователем.

Пример команды запуска инсталлятора в тихом режиме без участия пользователя и с файлом параметров:

```
./iwtm-installer-7.14.0.97-rhel7 --optionfile /some_directory/option-file-example --mode unattended --unattendedmodeui minimal
```

Важно!

При отсутствии настроенных и доступных репозиториев ОС запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите **Enter** для завершения работы инсталлятора, затем подключите стандартный репозиторий RHEL, репозиторий EPEL и повторно запустите инсталлятор.

Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

Примечание:

Если процесс завершится без ошибок, инсталлятор удалит пакеты, созданные для установки. Если процесс установки был прерван по какой-либо причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

Примечание:

В случае некорректной настройки службы Consul в консоли будет выведено предупреждение:



Для завершения работы инсталлятора нажмите **Enter**.

Для корректной работы Системы выполните проверку и настройку кластера службы Consul

a. Запустите службу Consul, выполнив команду:
   `systemctl start iwtm-consul`

Проверить статус службы можно командой:
`systemctl status iwtm-consul`

b. Чтобы проверить службу Consul, выполните команды:
   i. Для вывода IP-адреса основного сервера (лидера) кластера:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. Для вывода информации о членах кластера:
   `consul members`
c. Если не будет выведен IP-адрес лидера кластера, выполните *конфигурирование кластера службы Consul*.
   После настройки повторите проверку (действие ii).

При данной ошибке инсталлятор не запустит сервисы Traffic Monitor по завершении работы – их нужно будет запустить вручную.

4.4.3 Полный состав файла параметров

В таблице приведен полный список возможных параметров для обновления и их значения по умолчанию.

Название	Описание
`force_upgrade`	Принудительно переключает инсталлятор в режим обновления, даже если совпадают версии. Значения: `0` (по умолчанию), `1.`
`fix_incorrect_file_owners`	Параметр определяет, должен ли инсталлятор по умолчанию исправить некорректного владельца файлов перед обновлением. Если у обновляемых файлов будет некорректный владелец, инсталлятор прервет обновление. Значения: `0` (по умолчанию), `1.`
`cleanup_way`	Выбор режим остановки сервисов: • `quick_stop` – быстрая остановка без обработки событий; • `wait_stop` (по умолчанию) – перед остановкой дождаться завершения текущей обработки событий; • `clean_fq` – перед остановкой дождаться обработки всех событий и очистки файловых очередей. Режим обработки всех событий и очистки файловых очередей (`clean_fq`) доступен, только если на сервере установлены компоненты перехвата. Если был указан этот режим, но на сервере отсутствуют компоненты перехвата, будет использован режим текущей обработки событий (`wait_stop`).

Название	Описание
`start_services_after_upgrade`	Параметр определяет, должен ли инсталлятор запустить сервисы после обновления. Значения: `0`, `1` (по умолчанию). После обновления настройки системы мониторинга Nagios будут изменены на значения по умолчанию. Если до обновления конфигурационные файлы Nagios редактировались, в директории `/etc/infowatch/nagios/iwmon` будут созданы их копии с расширением `.saved`. Перед запуском сервисов Traffic Monitor перенесите настройки из файлов `.saved` в соответствующие новые конфигурационные файлы. После обновления для управления системой мониторинга используйте службу iwtm-nagios. Например, для просмотра статуса Nagios используйте команду: `systemctl status iwtm-nagios` Если в конфигурационном файле `luaengined.conf` указан параметр `SmtpTmBccList`, и при этом значение параметра содержит угловые скобки (`<` и `>`), перед запуском сервисов нужно удалить скобки. В таком случае не следует включать запуск сервисов в файле параметров.
`eula`	Значения: • `show` – вывести текст Лицензионного соглашения; • `accept` – принять Лицензионное соглашение без предварительного просмотра. Если вы запускаете установку не в тихом режиме и параметр не указан, то будет выведен текст Лицензионного соглашения и будет предложено принять его. При установке в тихом режиме значение параметра игнорируется и Лицензионное соглашение принимается по умолчанию.

12. Введите команду для поиска файлов с расширением `.rpmnew`, за исключением резервных копий конфигурационных файлов:
`find / -name "*rpmnew*" -not -path "/opt/iw/tm5/etc_conf_backup*" -print`
Если такие файлы найдены, они будут выведены на экран консоли. В таком случае их нужно корректно объединить с конфигурационными файлами (см. статью *Объединение конфигурационных файлов*).

> **Примечание:**
>
> Для успешного объединения конфигурационных файлов рекомендуем ознакомиться со статьями на официальном сайте (на английском):
>
> - *Файлы rpmnew и rpmsave*
> - *Рекомендации по обработке файлов rpmnew и rpmsave после обновления системы Red Hat Enterpries Linux*

13. Проверьте содержимое файла `/opt/iw/tm5/etc/scripts/iwssid.lua`. Его рекомендуется оставить без изменений, если до обновления он не редактировался.

В противном случае его нужно корректно объединить с конфигурационным файлом **`iwssid.lua.rpmnew`** (см. *Объединение конфигурационных файлов*).

14. Traffic Monitor, начиная с версии 7.8.0, поддерживает OCR-экстрактор Content AI ContentReader Engine. После обновления режимы работы экстрактора будут настраиваться в новых файлах профилей `/opt/iw/tm5/etc/CRProfile.ini` и `/opt/iw/tm5/etc/CRProfile_fast.ini`.
    Если до обновления Системы вы использовали OCR-экстрактор ABBYY FineReader и вносили изменения в старые файлы профилей `FRProfile.ini` или `FRProfile_fast.ini`, для сохранения этих настроек перенесите их в новые файлы. При этом учитывайте возможные изменения названий и значений параметров в новой версии экстрактора.
15. Если ранее работа инсталлятора не была завершена, выберите запуск сервисов и завершите обновление.
    Если ранее инсталлятор завершил работу без запуска сервисов, запустите их вручную или перезагрузите сервер для запуска всех остановленных сервисов.
    Команда для перезагрузки сервера:
    `reboot`

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
4 Diagnostic information.
5 /sandbox/src/cas3/handler.cpp(682): Throw in function
 cas::Handler::LoadedConfigData
cas::Handler::GetLoadedConfigData(const prop::Property&, const Ptr&)
6 Dynamic exception type:
boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
7 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.

16. В Traffic Monitor расширен список задач по умолчанию для автоматического удаления ненужных файлов.
    Задачи для планировщика `cron` теперь по умолчанию указаны в файле `/etc/cron.d/iwtm_cleanup` (о содержимом файла см. *Автоматическое удаление ненужных файлов в Traffic Monitor*).
    Для корректной работы новых задач:
    a. Удалите старые задачи, отредактировав файл конфигурации `cron`:
       `sudo crontab -e`
    b. Сохраните изменения и выйдите из редактора файла конфигурации.
    c. Перезапустите сервис:
       `systemctl reload crond`
17. Если до обновления вы не редактировали прошлый файл с задачами `/etc/cron.d/iwtm_error_queue`, пропустите это действие.
    В противном случае `/etc/cron.d/iwtm_error_queue` будет удален, а его содержимое будет сохранено в файле `/etc/cron.d/iwtm_error_queue.rpmsave`.
    Чтобы задачи, добавленные вами ранее, снова работали, создайте файл для ваших задач в директории `/etc/cron.d/` и скопируйте в него нужные задачи из `/etc/cron.d/iwtm_error_queue.rpmsave`.

> **Примечание:**
>
> Вы можете добавить свои задачи в файл `/etc/cron.d/iwtm_cleanup`, но тогда при следующем обновлении он будет переименован в `/etc/cron.d/iwtm_cleanup.rpmnew` и заменен файлом с содержимым по умолчанию. После следующего обновления нужно будет перенести добавленные вами задачи из `/etc/cron.d/iwtm_cleanup.rpmnew` в новый `/etc/cron.d/iwtm_cleanup`.
> Чтобы каждый раз не переносить ваши задачи, вы можете создать отдельный файл с вашими задачами в директории `/etc/cron.d/`.

18. Если у вас установлена система Prometheus и если сервер не был перезагружен, для запуска службы выполните команду:
    `systemctl start iwtm-postgres_exporter` – для **СУБД PostgreSQL**
    `systemctl start iwtm-oracledb_exporter` – для **СУБД Oracle**

19. Если обновляемый сервер Traffic Monitor взаимодействует с Data Discovery 2.0 и более новыми, ранее вы остановили под (pod) `technologies`. Запустите под заново. Для этого:
    a. Подключитесь к ноде кластера Центра расследований.
    b. Для запуска пода на ноде с лейблом `central` выполните команду:
    `kubectl scale -n infowatch --replicas=1 deployment/technologies-central`
    c. Подключитесь обратно к терминалу сервера с Traffic Monitor.
20. Если ранее вы остановили процессы адаптера Password Disclosure Adapter, запустите их. Подробнее см. *InfoWatch Password Disclosure Adapter. Руководство по установке и конфигурированию. Диагностика и удаление InfoWatch Password Disclosure Adapter*.
21. Введите команду для очистки кеша менеджера пакетов:
    `yum clean all`
22. Введите команду для проверки статусов процессов:
    `iwtm status`
    На экране отобразится список процессов и их статусы.

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, которые нужно обновить, воспользуйтесь инструкциями в этом разделе.

Примечание:

После успешного обновления СУБД вы можете удалить файлы, оставшиеся от прошлой версии ПО.

Это действие допустимо **только после** завершения обновления всей Системы и проведения проверок.

Перед удалением **обязательно** проверьте, что:

- запущены и работают все сервисы, предусмотренные в данной Системе;
- в Консоли управления ТМ отсутствуют ошибки на вкладке "Состояние Системы";
- старые события находятся в БД (это можно проверить на вкладке "События" с помощью запроса с соответствующей датой перехвата);
- новые события попадают в БД.

Для удаления выполните команды:

- если используется СУБД PostgreSQL:
  `yum erase postgresql13* pgagent_13*`
  `/u01/postgres/tmp/delete_old_cluster.sh`
- если используется СУБД Oracle:
  `su - "oracle" -c "rm -rf ${ORACLE_HOME}.backup"`

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. Запуск синхронизации с сервером вручную*).

Примечание:

Для корректного отображения Консоли управления до начала работ удалите кеш в вашем браузере. Это можно сделать с помощью стандартных средств браузера.

Обновление Системы путем чистой установки и восстановления данных из резервной копии (для СУБД PostgreSQL)

Важно!

Крайне рекомендуем выполнить резервное копирование Системы, а также клонировать ее и провести обновление на тестовой машине.
Если вы планируете не копировать данные, а примонтировать диск или раздел с данными, все равно рекомендуем выполнить их резервное копирование.
После чистой установки Системы конфигурационные файлы Traffic Monitor нужно будет настроить заново. Рекомендуем сохранить их для повторной настройки после обновления.

Если в конфигурационном файле `luaengined.conf` указан параметр `SmtpTmBccList`, и при этом значение параметра содержит угловые скобки (`<` и `>`), нужно удалить скобки перед запуском сервисов.

1. Для остановки сервисов Traffic Monitor введите команду:
   `iwtm stop`
2. Проверьте количество событий в Базе данных. Для этого выполните команду:
   `psql postgres iwtm -c "select count(1) from object;"`
3. Выполните *резервное копирование БД, индексов, конфигурации службы iw_adlibitum*.
4. Начиная с версии 7.8.0, Traffic Monitor поддерживает OCR-экстрактор Content AI ContentReader Engine.
   Если до обновления Системы вы использовали OCR-экстрактор ABBYY FineReader и вносили изменения в файлы профилей `FRProfile.ini` или `FRProfile_fast.ini`, сохраните эти кастомизации, чтобы восстановить их после установки новой версии Traffic Monitor.
5. *Установите новую версию Traffic Monitor*.

   Важно!

   Если резервные копии Базы данных находятся на внешних хранилищах, не подключайте их в процессе установки. Это нужно будет сделать непосредственно перед восстановлением и обновлением Базы данных.

   По завершении установки не удаляйте пакеты, созданные инсталлятором в процессе (пункт **Remove extracted installer data**).

   Последующие действия выполняйте на сервере, где установлена новая версия Traffic Monitor.
6. Для остановки служб введите команду:
   `iwtm stop`
7. Введите команду для остановки Базы данных:
   `systemctl stop postgresql-15`

> **Примечание:**
>
> Чтобы иметь возможность восстановить исходное состояние чистой установки, вы можете скопировать директории `u01` и `u02`.

8. Для изменения прав доступа к директории введите команду:
   `chmod 777 /var/log/infowatch/update`
9. Скопируйте резервную копию Базы данных таким образом, чтобы расположение соответствовало исходному.
10. Измените владельца директорий, выполнив команды:
    ```
    chown -R postgres:postgres /u01/
    chown -R postgres:postgres /u02/
    ```
11. Введите команду для перехода в директорию со скриптами:
    `cd /tmp/iwtm_installer/scripts`
12. Находясь в директории, запустите скрипт обновления СУБД с помощью команды вида:
    `./install_postgres.sh --distrib_path=<директория_с_дистрибутивом_СУБД> --tm_version=<версия_нового_Traffic_Monitor> --update`
    В нашем примере:
    `./install_postgres.sh --distrib_path=/root --tm_version=7.14.0.97 --update`

    > **Примечание:**
    >
    > В примере дистрибутив `iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz` расположен в директории `/root`.
    > Чтобы узнать версию установленного Traffic Monitor, введите команду:
    > `cat /opt/iw/tm5/version`

13. После успешного обновления выполните команду для проверки статуса службы СУБД:
    `systemctl status postgresql-15`
14. Запустите скрипт обновления схемы данных с помощью команды вида:
    `./install_dbschema.sh --tm_version=<версия_нового_Traffic_Monitor> --db_type=postgres --update`
    В нашем примере:
    `./install_dbschema.sh --tm_version=7.14.0.97 --db_type=postgres --update`
15. Выполните действие 2 данной инструкции, чтобы сравнить количество событий в Базе данных до и после обновления.
16. Скопируйте резервные копии индексов и конфигурации службы `iw_adlibitum` таким образом, чтобы расположение соответствовало исходным директориям и файлам. Если исходное расположение не являлось расположением по умолчанию, его нужно будет указать в соответствующих разделах конфигурационных файлов (см. *действия biii и biv*).
17. Измените владельца директорий, выполнив команды:
    ```
    chown -R iwtm:iwtm /var/lib/sphinx/
    chown -R iwtm:iwtm /opt/iw/tm5/etc/adlibitum/
    ```
18. Выполните команды:
    ```
    sudo -u iwtm touch /opt/iw/tm5/www/backend/protected/runtime/first_run
    iwtm restart kicker
    ```
19. После обновления Системы режимы работы OCR-экстрактора Content AI ContentReader Engine будут настраиваться в новых файлах профилей `/opt/iw/tm5/etc/`

`CRProfile.ini` и `/opt/iw/tm5/etc/CRProfile_fast.ini`. Если до обновления Системы вы использовали OCR-экстрактор ABBYY FineReader и вносили изменения в старые файлы профилей `FRProfile.ini` или `FRProfile_fast.ini`, для сохранения этих настроек перенесите их в новые файлы. При этом учитывайте возможные изменения названий и значений параметров в новой версии экстрактора.

20. Введите команду для перезагрузки сервера:
    `reboot`
    Дождитесь загрузки сервера и повторно авторизуйтесь, выполнив действия 1–3 инструкции перед обновлением.
21. Введите команду для проверки статусов процессов:
    `iwtm status`
    На экране отобразится список процессов и их статусы.

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 подлежащие обновлению серверы или подсистемы, воспользуйтесь инструкциями этого раздела.

> **Примечание:**
>
> Для корректного отображения Консоли управления до начала работ удалите кеш в вашем браузере. Это можно сделать с помощью стандартных средств браузера.

Если вы обновили Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8, восстановите исходный файл выпуска ОС.

Для этого:

1. Выполните команду в зависимости от ОС:
   - в ОС Oracle Linux 8:
     `mv /etc/release.bak /etc/oracle-release`
   - в ОС AlmaLinux 8 или Rocky Linux 8:

     ```
     mv /etc/release.bak /etc/redhat-release
     ```
2. Подтвердите перезапись файла. Для этого введите "`yes`" и нажмите **Enter**.
3. Убедитесь, что исходный файл выпуска успешно восстановлен. Для этого выполните команду:

   ```
   lsb_release -a
   ```

   В результате должна быть выведена информация о вашей операционной системе. Например, для ОС AlmaLinux 8 будет выведено:

   ```
   Distributor ID: AlmaLinux
   Description:    AlmaLinux release 8.10 (Cerulean Leopard)
   Release:        8.10
   Codename:       CeruleanLeopard
   ```

Важно!

В Traffic Monitor 7.14 обновили поставляемые сертификаты и публичный ключ, которые используются для SSL-соединения с сервисом XAPI. По умолчанию сертификаты и ключ расположены в папке `/opt/iw/tm5/etc/cert`.

Если вы обновляете Traffic Monitor с версии 7.13 или более ранней и в вашем контуре Data Discovery, Device Monitor, адаптеры или другие сторонние сервисы взаимодействуют с Traffic Monitor с помощью сервиса XAPI, учтите замену сертификатов и публичного ключа.

Если ранее вы:

- **Использовали собственные** сертификаты и ключ **с названиями, отличными** от имен файлов по умолчанию, **обновление не повлияет** на взаимодействие сервисов, так как добавленные вами файлы не будут удалены.
- **Удалили файлы**, **поставляемые** с продуктом, и **использовали собственные** сертификаты и ключ **с аналогичными названиями**, после обновления **замените сертификаты в Traffic Monitor на сгенерированные вами**.
- **Копировали** в папки других продуктов, адаптеров или сервисов сертификаты и ключ, **поставляемые** с Traffic Monitor, после обновления **скопируйте их заново** из папки `/opt/iw/tm5/etc/cert`.

Об установке или замене сертификатов:

- в **Device Monitor Windows** см. *InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию. Настройка проверки сертификатов удаленных серверов*;
- в **Device Monitor Linux** см. *InfoWatch Device Monitor for Linux. Руководство по установке. Настройка проверки сертификатов удаленных серверов*;
- в **Data Discovery** см. *InfoWatch Data Discovery*. *Руководство администратора. Зоны и серверы*.

4.5 Обновление TM при распределенной установке

Важно!

Перед обновлением Traffic Monitor обновите сервер Device Monitor.

В инсталляторе Traffic Monitor реализована система шаблонов, представляющих из себя функциональные наборы компонентов. Подробнее о шаблонах смотрите в статье *Схемы развертывания Системы и выбор типа установки*.
Доступны четыре шаблона:

- **База данных** (`Database`);
- **Индексер** (`Indexer service`);
- **Веб-консоль** (`Web console`);
- **Перехватчики** (`Traffic interceptors`).

Обновлению подлежат все серверы, на которых установлены компоненты Traffic Monitor.

Инсталлятор Traffic Monitor при обновлении с участием пользователя может работать в двух режимах:

- текстовый в консоли сервера;

- графический.

Шаги установки и их последовательность аналогичны в обоих режимах.

Также доступен тихий режим работы инсталлятора без участия пользователя.

Независимо от выбранного режима работы инсталлятора, для обновления понадобится использовать консоль (или терминал) сервера.

В процессе обновления на сервер будут установлены все пакеты Traffic Monitor, но при завершении работы инсталлятор запустит только те сервисы, которые до обновления не были отключены.

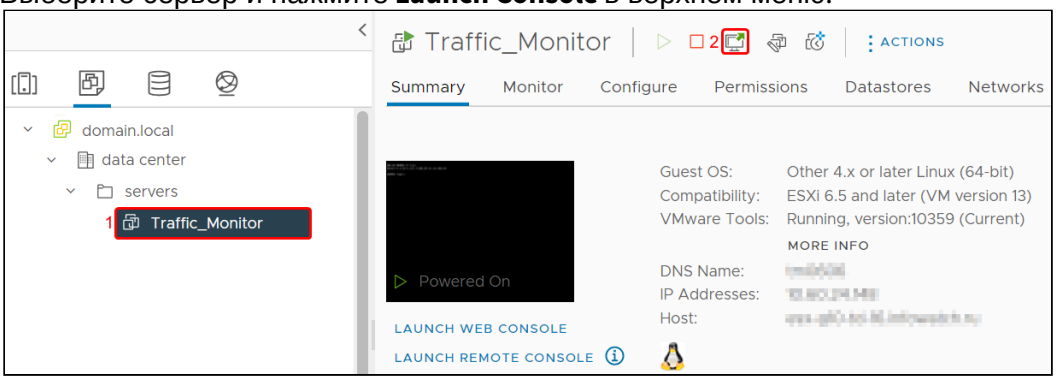
> **Примечание:**
>
> Если сервис был отключен, после обновления он **не** будет запущен.
>
> Если сервис был остановлен, после обновления он будет запущен.
>
> Статусы новых сервисов будут соответствовать первичной установке.

Распаковка пакетов начнется не при запуске инсталлятора, а непосредственно перед обновлением.

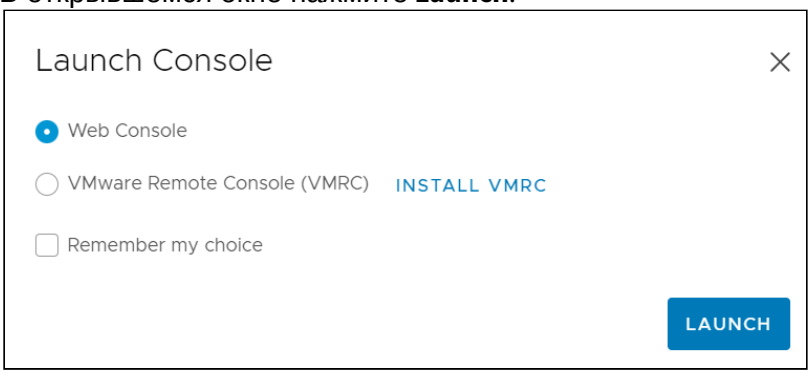
> **Важно!**
>
> Каждый сервер должен иметь уникальный корректный FQDN.

Перед обновлением Системы выполните следующие действия:

1. Откройте консоль обновляемого сервера:
   - в случае физического сервера – консоль отображается на экране монитора, подключенного к серверу;
   - в случае виртуального сервера – выполните команду **Launch Console** (см. пример ниже):
     Пример запуска консоли виртуального сервера в веб-версии клиентского приложения VMWare vSphere Client:
     a. Выберите сервер и нажмите **Launch Console** в верхнем меню:



b. В открывшемся окне нажмите **Launch**.



Откроется окно с консолью сервера, в котором вам необходимо ввести пароль пользователя.

2. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя `root`).
3. **Если вы обновляете компоненты Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8:**

> **Важно!**
>
> Убедитесь, что в операционной системе Oracle Linux 8.10 в качестве текущего выбрано ядро Red Hat Compatible Kernel (RHCK), к примеру Oracle Linux Server, Kernel `4.18.0-553.50.1.el8_10.x86_64`, а ядро UEK удалено. Подробнее см. *Требования к настройкам ОС и сети сервера*.

a. Установите пакет `redhat-lsb-core` с помощью следующей команды:

```
dnf install redhat-lsb-core
```

b. Создайте резервную копию файла выпуска ОС и замените содержимое исходного файла. Для этого выполните команды в зависимости от ОС:
   - на ОС Oracle Linux 8:

```
cp /etc/oracle-release /etc/release.bak

echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/oracle-release
```

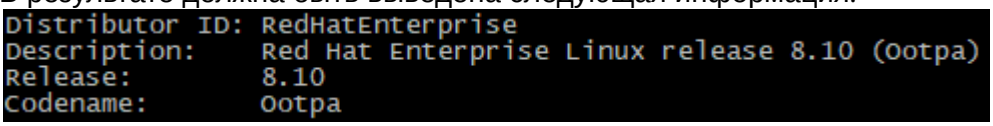
   - на ОС AlmaLinux 8 или Rocky Linux 8:

```
cp /etc/redhat-release /etc/release.bak
echo "Red Hat Enterprise Linux release 8.10 (Ootpa)" > /etc/redhat-release
```

c. Выполните команду:

```
lsb_release -a
```

В результате должна быть выведена следующая информация:



> **Примечание:**
>
> После обновления Traffic Monitor восстановите исходный файл выпуска ОС. Подробнее см. *ниже*.

4. Проверьте параметры установки обновляемого сервера при помощи команды: `cat /opt/iw/tm5/install_mode`

Пример содержимого

```
{
  "product_type": "tme",
  "version": "7.13.0.150",
  "all_in_one": false,
  "templates": {
    "db": {
      "local": true
    },
    "indexer": {},
  }
}
```

Запись из примера соответствует серверу Traffic Monitor с типом установки *Distributed* редакции *Enterprise* и версии *7.13.0.150*. На сервере из примера активированы шаблоны *База данных* и *Индексер*. Используется *локальная* база данных.

5. Обновите ОС на сервере, если ее версия отсутствует в списке поддерживаемых версий ОС в статье *Аппаратные и программные требования*.

> **Важно!**
>
> Перед обновлением Системы убедитесь, что сервер соответствует *требованиям к настройкам ОС и сети сервера*.
>
> После обновления параметры unit-файлов системы инициализации systemd вернутся к значениями по умолчанию.

> **Внимание!**
>
> Чтобы в случае ошибки иметь возможность восстановить базу данных и возобновить процесс обновления с последнего успешного этапа, рекомендуется выполнить:
>
> 1. **Резервное копирование базы данных и индексов**

Важно!

Для успешного восстановления файлы обязательно должны быть скопированы с сохранением их **прав, пользователей и групп**.
Для этого копируйте файлы только на **файловую систему Linux** (например, Ext4 или XFS).
Храните резервные копии либо на другом разделе сервера, либо на другом сервере, либо на внешнем устройстве. Убедитесь, что данные не будут потеряны.
Для восстановления резервные копии будет необходимо скопировать **по адресам исходных файлов, не изменяя прав, пользователей и групп**.

a. На всех серверах остановите сервисы Traffic Monitor:
   `iwtm stop`
b. На сервере, установленном при помощи шаблона Веб-консоль, создайте резервную копию конфигурации службы `iw_adlibitum`. Для этого:
   i. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на просмотр файл **`adlibitum. conf`**.
   ii. В параметре `"ConfigDir"` указан относительный путь к директории с конфигурации службы `iw_adlibitum`. Путь к директории указывается относительно содержимого параметра `"NookDir"`. Скопируйте директорию с конфигурацией либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство.
c. На сервере, установленном при помощи шаблона Индексер, создайте резервную копию индексов. Для этого:
   i. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на просмотр файл **`indexer.conf`**.
   ii. В параметре `"SphinxBaseDir"` указан путь к директории с индексами. В параметре `"ArchiveDir"` указан относительный путь к архивам индексов. Путь к архивам указывается относительно содержимого параметра `"NookDir"`.
   Скопируйте директории с индексами и архивами индексов либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство
d. На сервере, установленном при помощи шаблона База данных:
   i. В зависимости от используемой СУБД и установленной версии Traffic Monitor введите команду для остановки Базы данных:
      - для **СУБД Oracle**:
        `systemctl stop oracle`
      - для **СУБД PostgreSQL** версии 13:
        `systemctl stop postgresql-13`
      - для **СУБД PostgreSQL** версии 15:
        `systemctl stop postgresql-15`

        Примечание:

Для уточнения директорий, содержащих Базу данных, проверьте также содержимое файла:

- `/opt/iw/tm5/csw/oracle/database.conf` (для **СУБД Oracle**)
- `/opt/iw/tm5/csw/postgres/database.conf` (для **СУБД PostgreSQL**)

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

iii. Создайте резервную копию индексов. Для этого:

1. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на просмотр файл `indexer.conf`.
2. В параметре `"SphinxBaseDir"` указан путь к директории с индексами. В параметре " `ArchiveDir` " указан относительный путь к архивам индексов. Путь к архивам указывается относительно содержимого параметра `"NookDir"`. Скопируйте директории с индексами и архивами индексов либо на другой раздел сервера, либо на другой сервер, либо на внешнее устройство.

2. **Резервное копирование настроек окружения**

Обязательно учитывайте особенности копирования из предупреждения в предыдущем шаге. Перейдите по адресам и скопируйте указанные файлы:

- **Для СУБД Oracle:**
  - `/opt/iw/tm5/etc/oracle/` – все файлы в директории
  - `/etc/default/iwtm`
  - `/etc/profile.d/iw-oracle-env.sh`
  - `/etc/logrotate.d/iwtm-oracle-conf-server`
  - `/opt/iw/tm5/etc/oracle.conf`
- **Для СУБД PostgreSQL:**
  - `/etc/default/iwtm`
  - `/etc/profile.d/iw-postgresql-env.sh`
  - `/etc/profile.d/iw-postgresql-client-env.sh`
  - `/etc/sudoers.d/iw-pgagent`
  - `/etc/pgagent/pgagent-13.conf` или `/etc/pgagent/pgagent-15.conf` в зависимости от версии СУБД
  - `/opt/iw/tm5/etc/postgresql/` – все файлы в директории
  - `/opt/iw/tm5/etc/postgresql.conf`

> **Примечание:**
>
> Также инсталлятор автоматически создает копии файлов настроек окружения в директории `/tmp/iwtm_db_configs_backup`. Для удобства пользователя инсталлятор воссоздает в директории пути оригинальных файлов, по которым их нужно будет скопировать для восстановления исходного состояния.

Созданные инсталлятором резервные копии хранятся только до успешного обновления. По завершении они будут удалены.

Выберите инструкцию в зависимости от варианта обновления:

- Обновление Системы поверх установленной;
- Обновление Системы путем чистой установки и восстановления данных из резервной копии (для СУБД PostgreSQL).

Обновление Системы поверх установленной

Важно!

Крайне рекомендуется выполнить резервное копирование Системы, а также клонировать ее и провести обновление на этой тестовой машине.

Остановку сервисов инсталлятором и запуск обновления выполняйте в следующей последовательности шаблонов:

1. Перехватчики
2. Индексер
3. Веб-консоль
4. База данных

Процесс обновления серверов инсталлятором аналогичен для всех шаблонов. Если действие, относится только к серверу с конкретным шаблоном, это будет указано. Остальные действия относятся ко всем серверам.

Порядок обновления следующий:

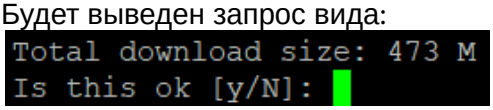
Шаг 1. Обновление всех серверов.
Шаг 2. Проверка кластера службы Consul.
Шаг 3. Проверка работоспособности внутренних сервисов Системы.
Шаг 4. Завершение обновления серверов.

ШАГ 1. ОБНОВЛЕНИЕ ВСЕХ СЕРВЕРОВ

Чтобы обновить серверы, на каждом из них выполните следующие действия:

1. Скопируйте в директорию `/root` файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor. Список файлов для различных ОС и СУБД см. в статье *Распределенная установка TM Enterprise*, шаг 5. Далее будет описано обновление с использованием инсталлятора для ОС Red Hat Enterprise Linux. Данная инструкция актуальна и для других поддерживаемых ОС: Oracle Linux, РЕД ОС, AlmaLinux, Rocky Linux и Альт Сервер.
2. Чтобы сделать файл **`iwtm-installer-x.x.x.xxx-rhel7`** исполняемым, введите команду:
   `chmod u+x /root/iwtm-installer-x.x.x.xxx-rhel7`
   В нашем примере команда будет следующей:
   `chmod u+x /root/iwtm-installer-7.14.0.97-rhel7`
3. Подключите внешние или локальные репозитории ОС.

Например, с инструкцией по настройке локального репозитория в Red Hat Enterprise Linux можно ознакомиться на *официальном сайте* (страница доступна на английском языке).

4. Для обновления пакетов введите команду:
   `yum upgrade`
   Будет выведен запрос вида:
   

   Для продолжения наберите **Y** на клавиатуре и нажмите **Enter**.
5. Установите дополнительные пакеты `python3-psycopg2` и `libzstd` с помощью команды:
   `yum install python3-psycopg2 libzstd`
   В случае ошибки, скачайте эти пакеты из репозитория EPEL и установите вручную.
6. Если вы используете удаленную базу данных:
   a. Убедитесь, что версия вашей СУБД поддерживается Traffic Monitor, см. *Аппаратные и программные требования*.
   b. Если версия СУБД актуальна, пропустите это действие.
   Если СУБД необходимо обновить:
      i. Остановите сервисы Traffic Monitor с помощью команды:
      `iwtm stop`
      ii. Остановите СУБД.
      iii. Обновите СУБД до поддерживаемой версии, для этого используйте официальную инструкцию.

      > **Примечание:**
      >
      > Для СУБД PostgreSQL и PostgreSQL Pro также обновите используемый сервис `pgagent`.

      iv. После обновления запустите СУБД, но не запускайте сервисы Traffic Monitor.
7. Если обновляемый сервер Traffic Monitor взаимодействует с Data Discovery 2.0 и более новыми, остановите под (pod) `technologies`, который создает соединения с базой данных для доступа к конфигурации.
   Чтобы остановить под:
   a. Подключитесь к терминалу любой ноды кластера Центра расследований, в котором установлен Data Discovery, подключающийся к базе данных Traffic Monitor.
   b. Имя пода (pod) содержит лейбл ноды, на которой он установлен. Для определения имени пода выполните команду:
   `kubectl get pods -A -o wide | grep technolog`

   Пример вывода в командной строке после команды:

   ```
   root@lv-426:~# kubectl get pods -A -o wide | grep technolog
   infowatch      technologies-central-71cb89dd54-bgwn6      3/3     Running   0
   18h   10.244.0.86   lv-426   <none>           <none>
   ```

   В нашем примере лейбл ноды `central`.

c. Для остановки пода на ноде с лейблом `central` выполните команду:
`kubectl scale -n infowatch --replicas=0 deployment/technologies-central`
d. Подключитесь обратно к терминалу сервера с Traffic Monitor.

8. Если в Системе установлен и запущен адаптер Password Disclosure Adapter, перед обновлением Traffic Monitor остановите процессы адаптера. Подробнее см. документ *InfoWatch Password Disclosure Adapter. Руководство по установке и конфигурированию. Диагностика и удаление InfoWatch Password Disclosure Adapter*.
9. Если используется система Prometheus, то на сервере, установленном при помощи шаблона База данных, для остановки службы выполните команду:
`systemctl stop iwtm-postgres_exporter` – для **СУБД PostgreSQL**
`systemctl stop iwtm-oracledb_exporter` – для **СУБД Oracle**
10. На сервере, установленном при помощи шаблона База данных, перед запуском инсталлятора рекомендуется запустить сервис базы данных, если ранее он был остановлен. В зависимости от используемой СУБД введите команду для запуска:
    - `systemctl start oracle` (для **СУБД Oracle**)
    - `systemctl start postgresql-13` (для **СУБД PostgreSQL** версии 13)
    - `systemctl start postgresql-15` (для **СУБД PostgreSQL** версии 15)
11. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor:
`cd /root`
12. В инсталляторе реализован механизм автоматического объединения конфигурационных файлов Traffic Monitor старой и новой версии.

> **Важно!**
>
> Автоматическое объединение затрагивает только конфигурационные файлы Traffic Monitor с расширением **`.conf`**, расположенные в директории `/opt/iw/tm5/etc`.
> Перед объединением в директории `/opt/iw/tm5/etc_conf_backup_<дата_время>` будут созданы резервные копии исходных конфигурационных файлов. Пример названия директории: `/opt/iw/tm5/etc_conf_backup_05.06.2024_09:26:33`.
> После успешного объединения файлы с расширением **`.rpmnew`**, которые относятся к затрагиваемым конфигурационным файлам, будут удалены.
> Все выполненные действия будут отражены в лог-файле `/var/log/infowatch/iwtm-install-<версия>-<дата>_<время>.log`. Пример названия лог-файла: `/var/log/iwtm-install-7.14.0.97-2024-09-06_09-56-25.log`.
> Также информацию о процессе можно найти в директории `/var/log/infowatch/config_merge/`.
> Если во время действий с конфигурационным файлом будут обнаружены ошибки, процесс будет остановлен до исправления ошибок пользователем. После исправления ошибок повторно запустите обновление.

Запустите инсталлятор в одном из режимов:

- **обновление в текстовом режиме в консоли сервера**

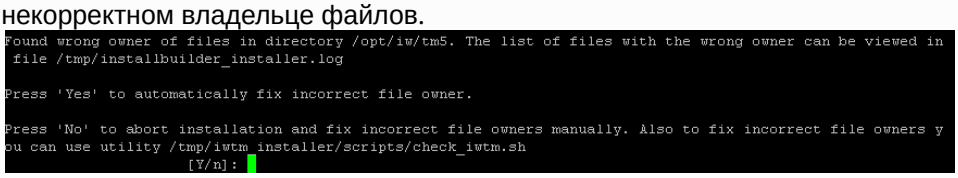
  Чтобы обновить Traffic Monitor в консоли сервера, выполните следующие действия:

  a. Для обновления Traffic Monitor запустите инсталлятор, выполнив следующую команду:
  `./iwtm-installer-x.x.x.xxx-rhel7`
  В нашем примере команда будет следующей:
  `./iwtm-installer-7.14.0.97-rhel7`

Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

Примечание:

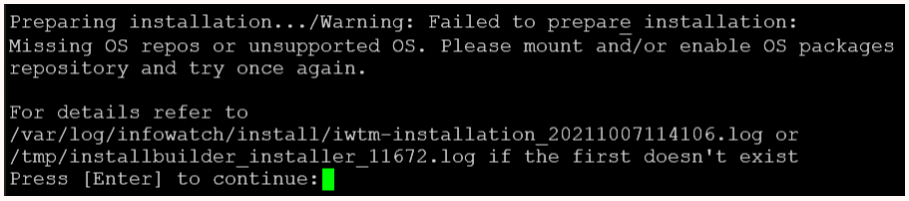
Перед запуском инсталлятора может быть выведено предупреждение о некорректном владельце файлов.



Введите **Y** и нажмите **Enter**, чтобы инсталлятор исправил владельца файлов и продолжил запуск.
В противном случае введите **N**, нажмите **Enter**, исправьте несоответствие вручную или с помощью скрипта `/tmp/iwtm_installer/scripts/check_iwtm.sh` и повторно запустите инсталлятор.

Важно!

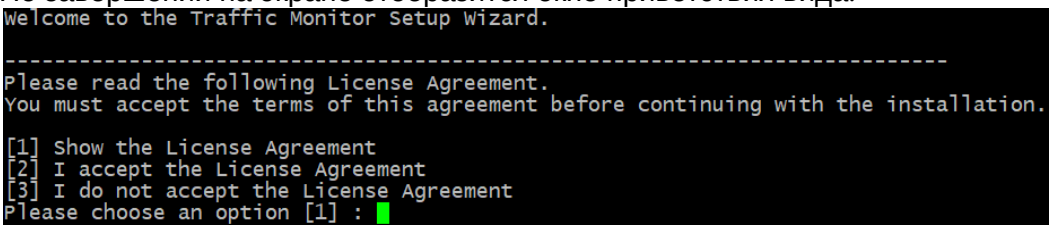
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите **Enter** для завершения работы инсталлятора, затем подключите стандартный репозиторий RHEL, репозиторий EPEL и повторно запустите инсталлятор.

Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

По завершении на экране отобразится окно приветствия вида:



b. Для продолжения обновления необходимо принять условия Лицензионного соглашения. Выберите один из предложенных вариантов. Для этого введите цифру, указанную напротив него, и нажмите **Enter**:

- `Show the License Agreement` – для просмотра Лицензионного соглашения;

При выборе этого варианта:

i. Выберите язык, на котором будет выведен текст Лицензионного соглашения:
   - `English` – английский;
   - `Russian` – русский;

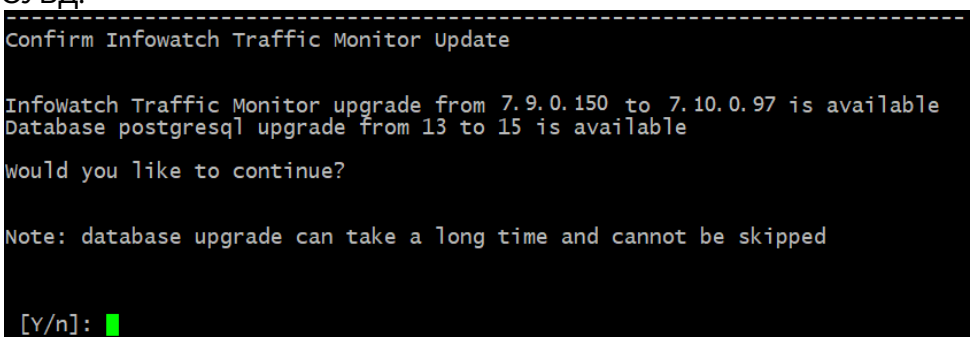
ii. Прочитайте Лицензионное соглашение. Для перехода к следующей странице нажимайте **Enter**.

iii. Примите Лицензионное соглашение. Для этого введите **y** и нажмите **Enter**.

- `I accept the License Agreement` – чтобы принять Лицензионное соглашение без предварительного просмотра;
- `I do not accept the License Agreement` – чтобы не принимать Лицензионное соглашение и прервать процесс обновления.

> **Примечание:**
>
> При обновлении в консоли сервера перед полем ввода в квадратных скобках указано значение по умолчанию. Оно будет использовано, если оставить поле ввода пустым и нажать **Enter**.
>
> **Пример:**
>
> Если на изображении выше не вводить значение, а только нажать Enter, будет выбран пункт `[1] Show the License Agreement`.

Далее на экране отобразится окно подтверждения обновления, в котором будут указаны доступные обновления для Traffic Monitor и СУБД:



c. Для продолжения введите **Y** и нажмите **Enter**. Для выхода из инсталлятора введите **N** и нажмите **Enter**.

d. Подтвердите остановку сервисов. Шаги подтверждения и выбора режима остановки будут пропущены, если сервисы были остановлены вручную до запуска инсталлятора.

> **Примечание:**

Если компоненты Traffic Monitor функционируют на нескольких серверах, они должны быть остановлены в следующей последовательности:

i. Перехватчики
ii. Индексер
iii. Веб-консоль
iv. База данных

e. Выберите режим остановки Traffic Monitor:
   - `Quick stop` – быстрая остановка без обработки событий;
   - `Waiting for stop` – перед остановкой дождаться завершения текущей обработки событий;
   - `Waiting for emptying file queues` – перед остановкой дождаться обработки всех событий и очистки файловых очередей. Режим обработки всех событий и очистки файловых очередей доступен только на серверах, установленных при помощи шаблона Перехватчики.

   Важно!

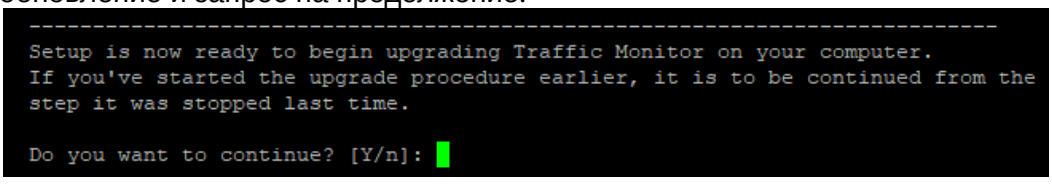
   Если компоненты перехвата и компоненты анализа (`iw_cas` , `iw_pas`) используются на разных серверах, остановка перехватчиков с очисткой файловых очередей может зависнуть. Рекомендуется использовать другие режимы или остановить компоненты вручную.

   Для выбора введите цифру, указанную напротив выбранного варианта, и нажмите **Enter**.

   Примечание:

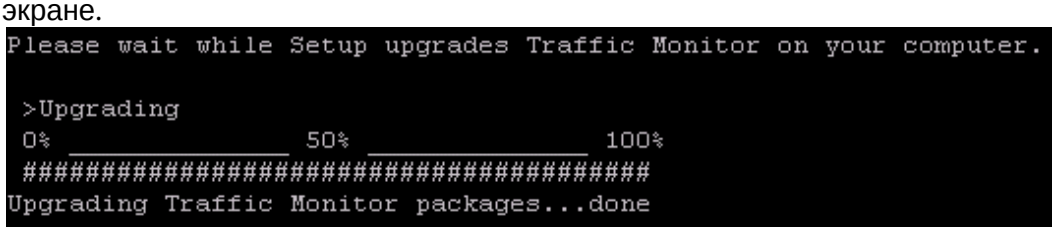
   Если выбран `Quick stop` , остановленные сервисы до запуска будут иметь статус `failed (failed)` .

f. Если выбран `Quick stop` или `Waiting for stop` , после возобновления работы Traffic Monitor необработанные события могут попасть в очередь ошибок обработки.
   Для продолжения введите **Y** и нажмите **Enter**.
   В процессе остановки на экране будет информация о ходе обработки событий.
g. После остановки сервисов будет выведено сообщение о готовности начать обновление и запрос на продолжение.



   Для начала обновления введите **Y** и нажмите **Enter**.
   Начнется распаковка пакетов, обновление имеющихся и установка новых компонентов Traffic Monitor. Прогресс выполнения будет отображаться на

экране.



Процесс займет некоторое время.

> **Примечание:**
>
> Если процесс установки был прерван по какой-либо причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

h. Перед завершением работы инсталлятор предложит удалить пакеты, созданные для обновления.
Если обновление прошло успешно, данные рекомендуется удалить.
i. После обновления инсталлятор предложит запустить остановленные сервисы.

> **Примечание:**
>
> В случае некорректной настройки службы Consul в консоли будет выведено предупреждение:
>
> 
>
>
> Для завершения работы инсталлятора нажмите **Enter**.
>
> При данной ошибке инсталлятор не запустит сервисы Traffic Monitor при завершении работы, их нужно будет запустить вручную после проверки, описанной в Шаге 3 данной инструкции.

> **Важно!**
>
> Перед запуском сервисов дождитесь завершения обновления на остальных серверах или завершайте работу инсталлятора без запуска сервисов и выполните запуск позже вручную.
> Сервисы должны быть запущены в строгой последовательности в зависимости от активированных на них шаблонов.
>
> Не запускайте сервисы Traffic Monitor до обновления и запуска сервера, установленного при помощи шаблона База данных.
>
> После обновления настройки системы мониторинга Nagios будут изменены на значения по умолчанию. Если до обновления конфигурационные файлы Nagios редактировались, в директории `/etc/infowatch/nagios/iwmon`

будут созданы их копии с расширением `.saved`. Перед запуском сервисов Traffic Monitor перенесите настройки из файлов `.saved` в соответствующие новые конфигурационные файлы.

После обновления для управления системой мониторинга используйте службу `iwtm-nagios`.
Например, для просмотра статуса Nagios используйте команду:
`systemctl status iwtm-nagios`

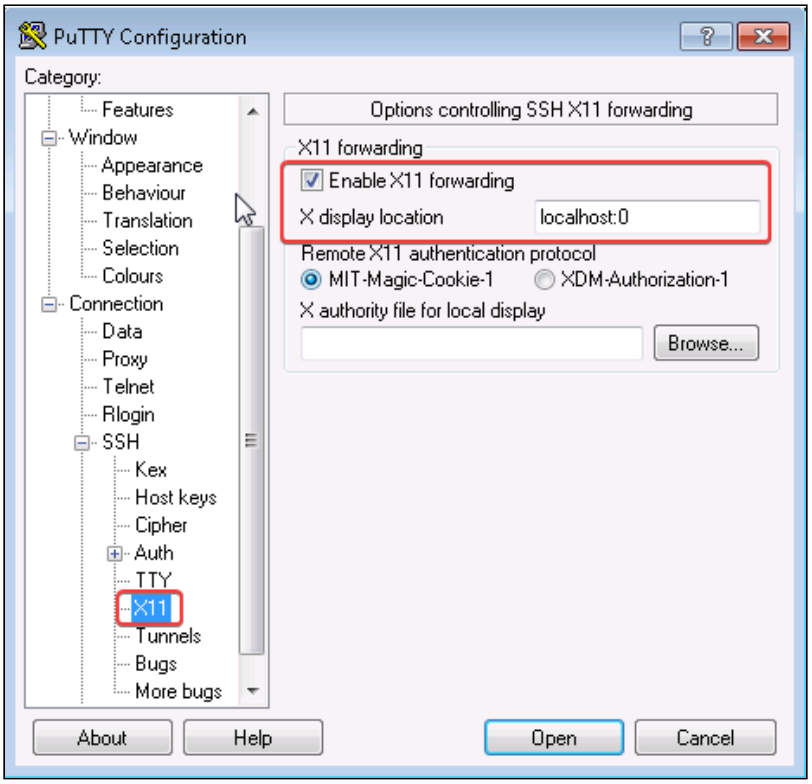
Если в конфигурационном файле `luaengined.conf` указан параметр `SmtpTmBccList`, перед запуском сервисов убедитесь, что значение параметра не содержит угловых скобок (`<` и `>`). В противном случае удалите скобки.

- **обновление с использованием графического режима инсталлятора**

  В ОС оконная система X Window System использует клиент-серверную модель. Для запуска инсталлятора в графическом режиме используется перенаправление графического вывода удаленной подсистемы (**X11 Forwarding**). Это позволит работать напрямую с графическими приложениями среды Linux на компьютере, с которого осуществляется подключение к серверу. Данный режим реализуется с помощью SSH-подключения.

  Чтобы обновить Traffic Monitor с использованием графического режима инсталлятора, выполните следующие действия:

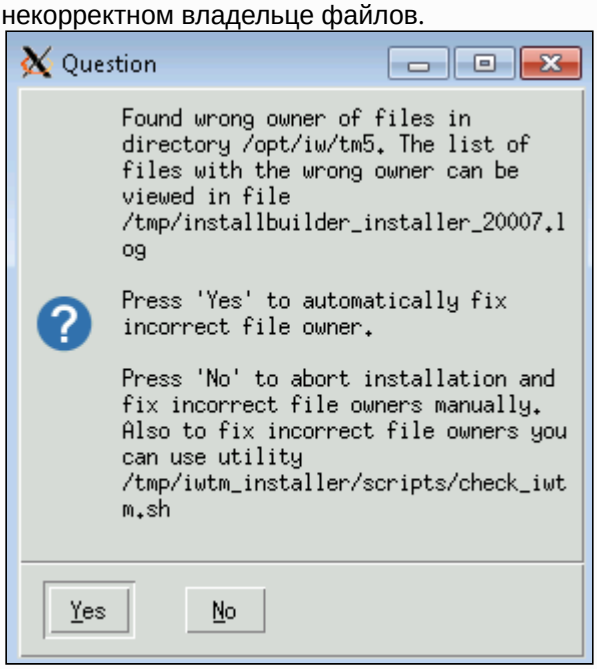
  a. На обновляемом сервере:
     i. Установите утилиту `xauth` с помощью команды:
     `yum install xauth`
     ii. В конфигурационном файле `/etc/ssh/sshd_config` раскомментируйте строку "`X11Forwarding yes`". Для этого удалите перед строкой символ `#`.
     iii. Сохраните изменения в конфигурационном файле.
     iv. Перезапустите службу SSH с помощью команды:
     `systemctl restart sshd`
  b. На компьютере, на котором будет использован графический режим:
     i. Для подключения к обновляемому вам потребуется SSH-клиент с включенной опцией X11 Forwarding, например PuTTY.
     ii. Для запуска инсталлятора в графическом режиме вам потребуется настроенное приложение-клиент для обращения к X Window System, например:
        - приложение Xming – для ОС семейства MS Windows;
        - оболочка Gnome 3 – для ОС семейства Linux.
  c. Запустите настроенное приложение-клиент для обращения к X Window System.
  d. Подключитесь к серверу, на котором планируется обновление Traffic Monitor, с помощью выбранного SSH-клиента.
     Пример окна настройки PuTTY при подключении



e. Запустите инсталлятор, выполнив следующую команду:
`./iwtm-installer-x.x.x.xxx-rhel7`
В нашем примере команда будет следующей:
`./iwtm-installer-7.14.0.97-rhel7`
Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

> **Примечание:**

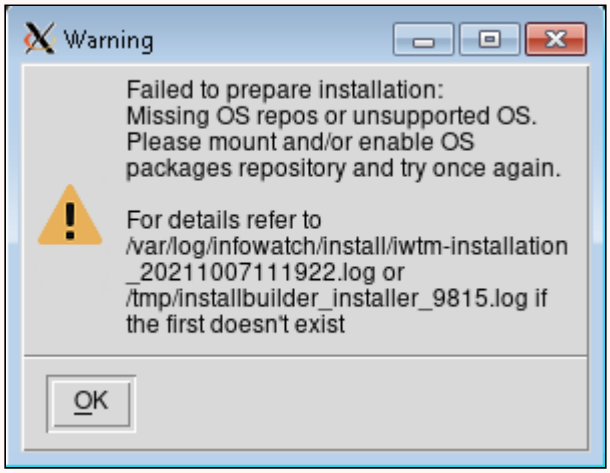
Перед запуском инсталлятора может быть выведено предупреждение о некорректном владельце файлов.



Нажмите кнопку **Yes**, чтобы инсталлятор исправил владельца файлов и продолжил запуск.
В противном случае нажмите кнопку **No**, исправьте несоответствие вручную или с помощью скрипта `/tmp/iwtm_installer/scripts/check_iwtm.sh` и повторно запустите инсталлятор.

Важно!

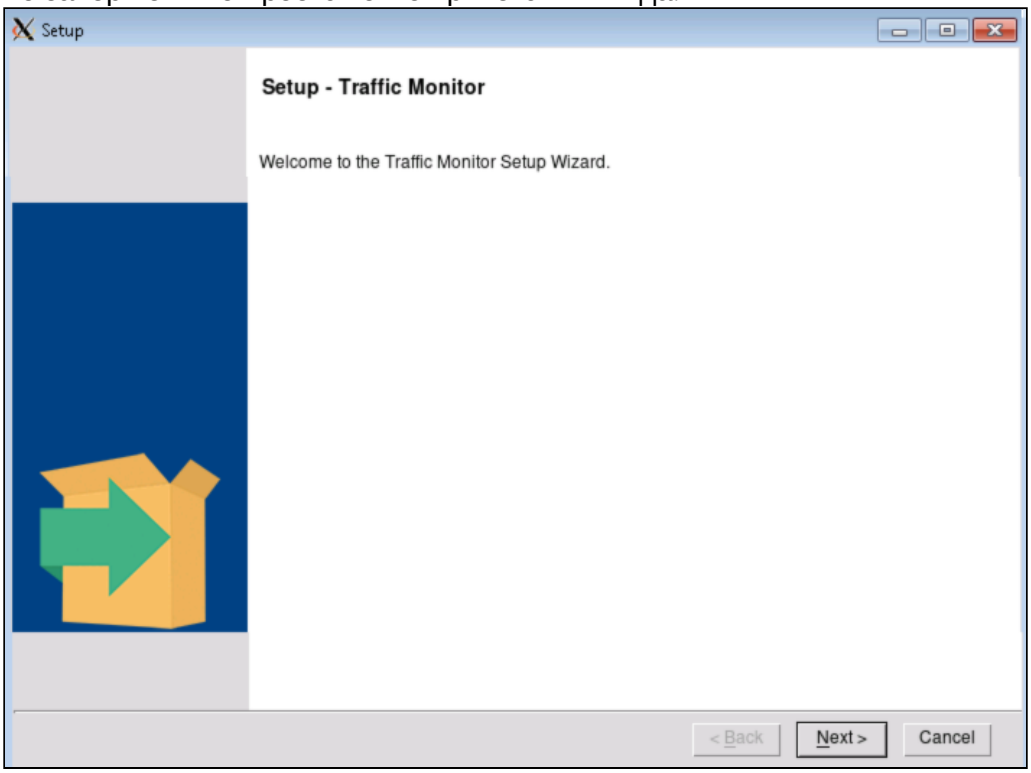
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите кнопку **OK** для закрытия окна и завершения работы инсталлятора, затем подключите стандартный репозиторий RHEL, репозиторий EPEL и повторно запустите инсталлятор.

Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

По завершении откроется окно приветствия вида:



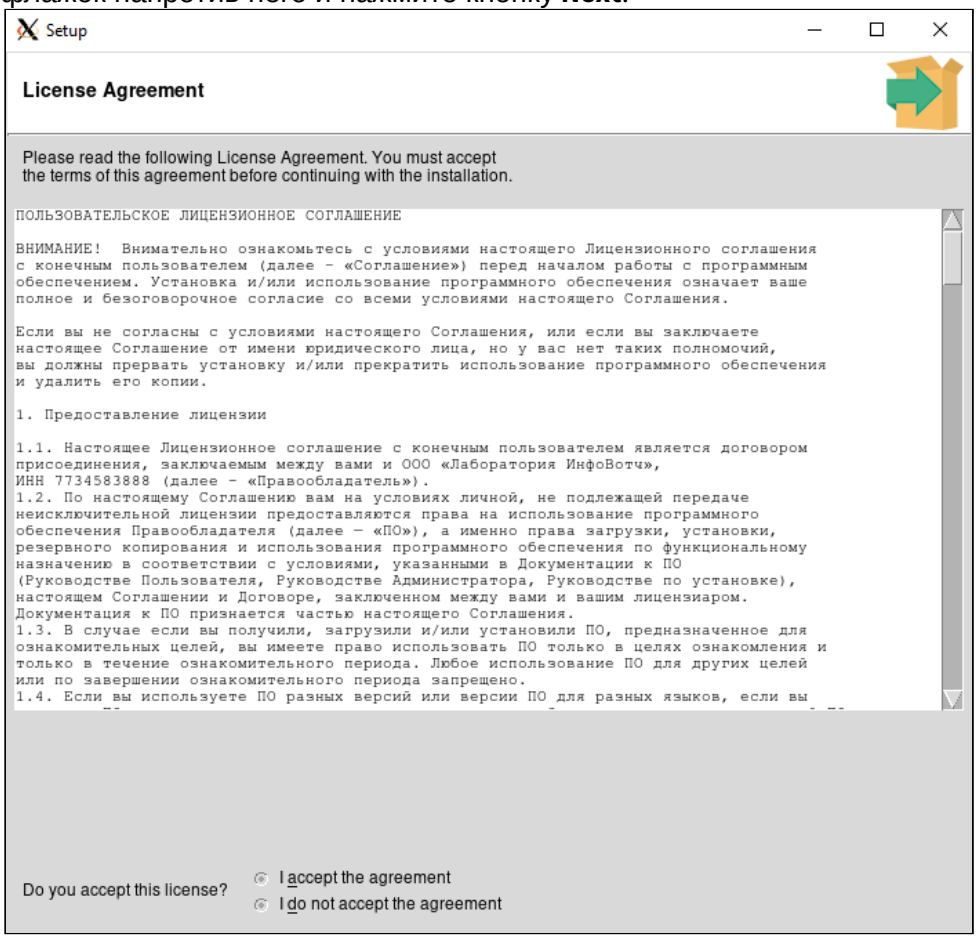
Для перехода к следующему окну используется кнопка **Next**, для возврата к предыдущему – **Back**. Для выхода из инсталлятора – кнопка **Cancel**.

f. Для продолжения обновления необходимо принять условия Лицензионного соглашения. Для этого:
   i. Выберите язык, на котором будет выведен текст Лицензионного соглашения:



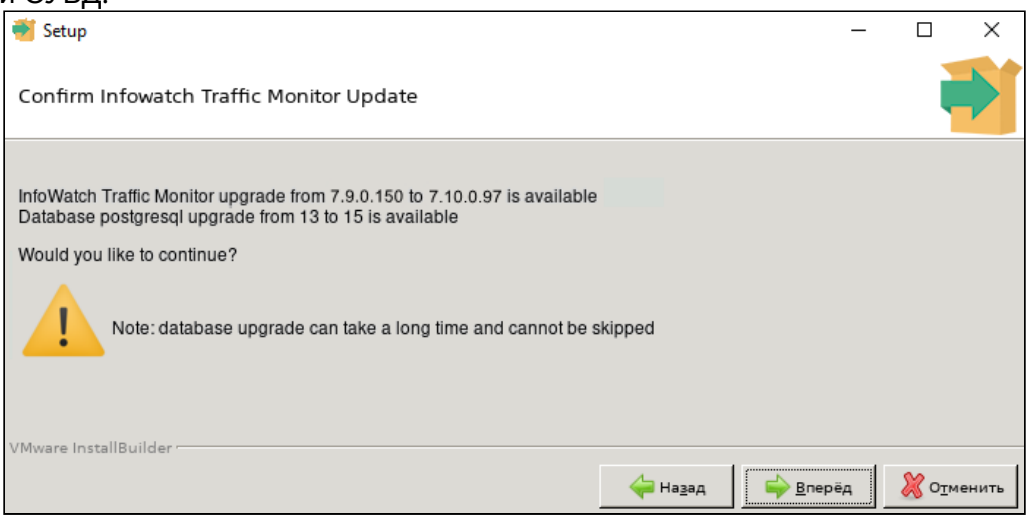
- `English` – английский;
- `Russian` – русский;

ii. Выберите один из предложенных вариантов. Для этого установите флажок напротив него и нажмите кнопку **Next**:



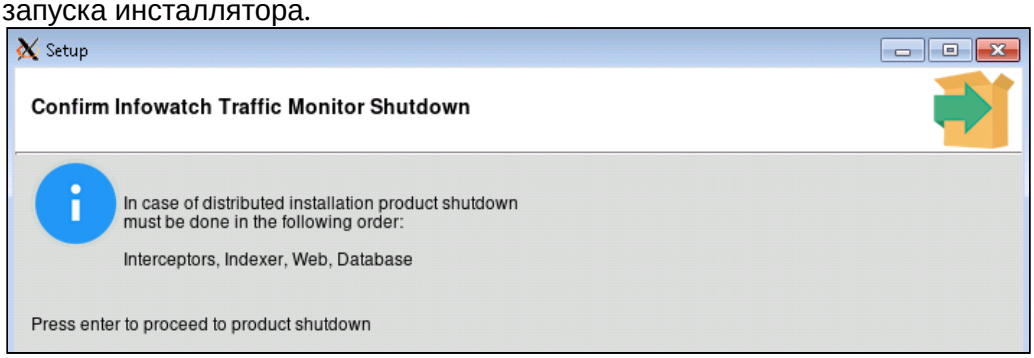
- `I accept the agreement` – чтобы принять Лицензионное соглашение и продолжить процесс обновления;
- `I do not accept the agreement` – чтобы не принимать Лицензионное соглашение и прервать процесс обновления.

g. В следующем окне будут указаны доступные обновления для Traffic Monitor и СУБД.



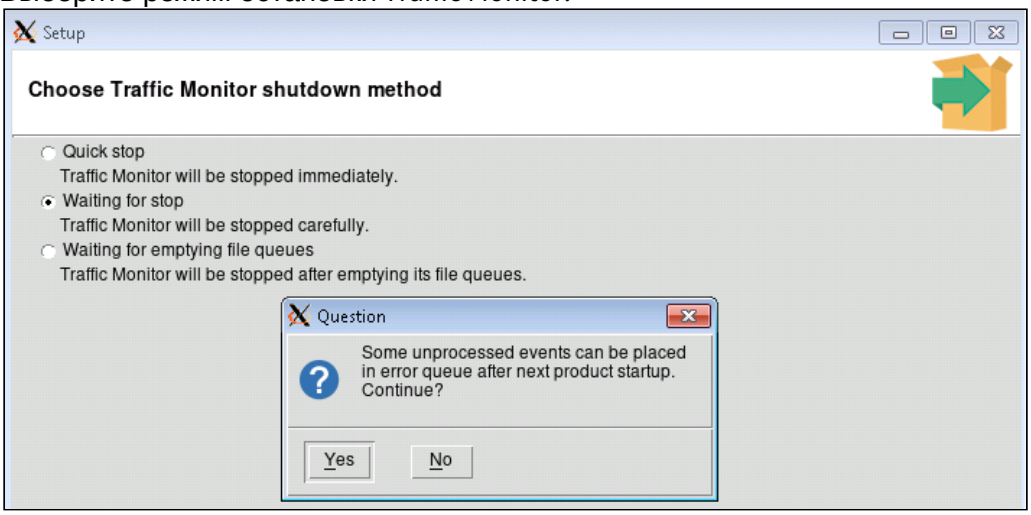
Для продолжения нажмите **Next**.

h. Подтвердите остановку сервисов. Шаги подтверждения и выбора режима остановки будут пропущены, если сервисы были остановлены вручную до запуска инсталлятора.



> **Примечание:**
>
> Если компоненты Traffic Monitor функционируют на нескольких серверах, они должны быть остановлены в следующей последовательности:
>
> i. Перехватчики
> ii. Индексер
> iii. Веб-консоль
> iv. База данных

i. Выберите режим остановки Traffic Monitor:



- `Quick stop` – быстрая остановка без обработки событий;
- `Waiting for stop` – перед остановкой дождаться завершения текущей обработки событий;
- `Waiting for emptying file queues` – перед остановкой дождаться обработки всех событий и очистки файловых очередей. Режим обработки всех событий и очистки файловых очередей доступен только на серверах, установленных при помощи шаблона Перехватчики.

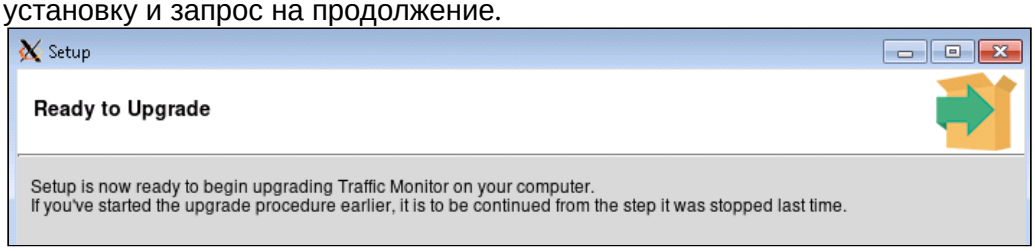
> **Важно!**
>
> Если компоненты перехвата и компоненты анализа (`iw_cas` , `iw_pas`) используются на разных серверах, остановка перехватчиков с очисткой файловых очередей может зависнуть. Рекомендуется использовать другие режимы или остановить компоненты вручную.

Для выбора установите флажок напротив соответствующего значения и нажмите кнопку **Next**

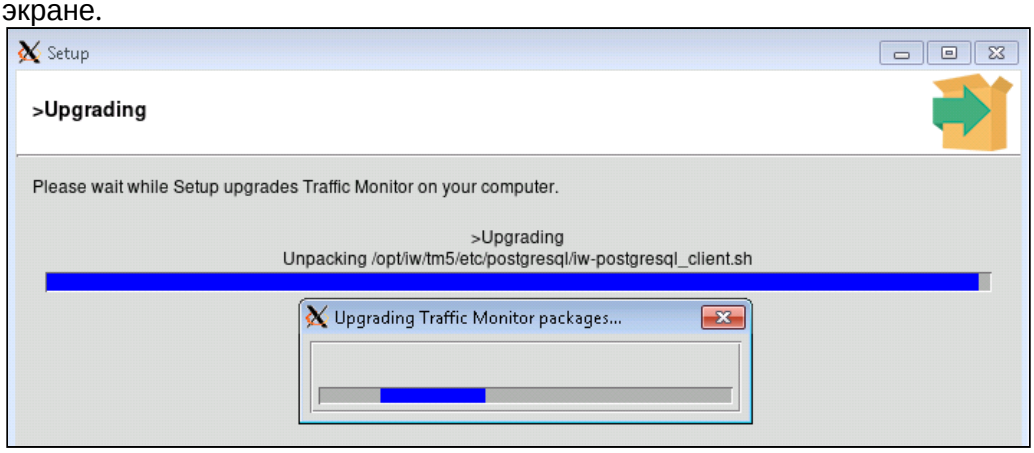
> **Примечание:**
>
> Если выбран `Quick stop` , остановленные сервисы до запуска будут иметь статус `failed (failed)` .

j. Если выбран `Quick stop` или `Waiting for stop` , после возобновления работы Traffic Monitor необработанные события могут попасть в очередь ошибок обработки.
Для продолжения нажмите кнопку **Yes**.
В процессе остановки на экране будет информация о ходе обработки событий.

k. После остановки сервисов будет выведено сообщение о готовности начать установку и запрос на продолжение.



Для начала обновления нажмите кнопку **Next**.
Начнется распаковка пакетов, обновление имеющихся и установка новых компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.

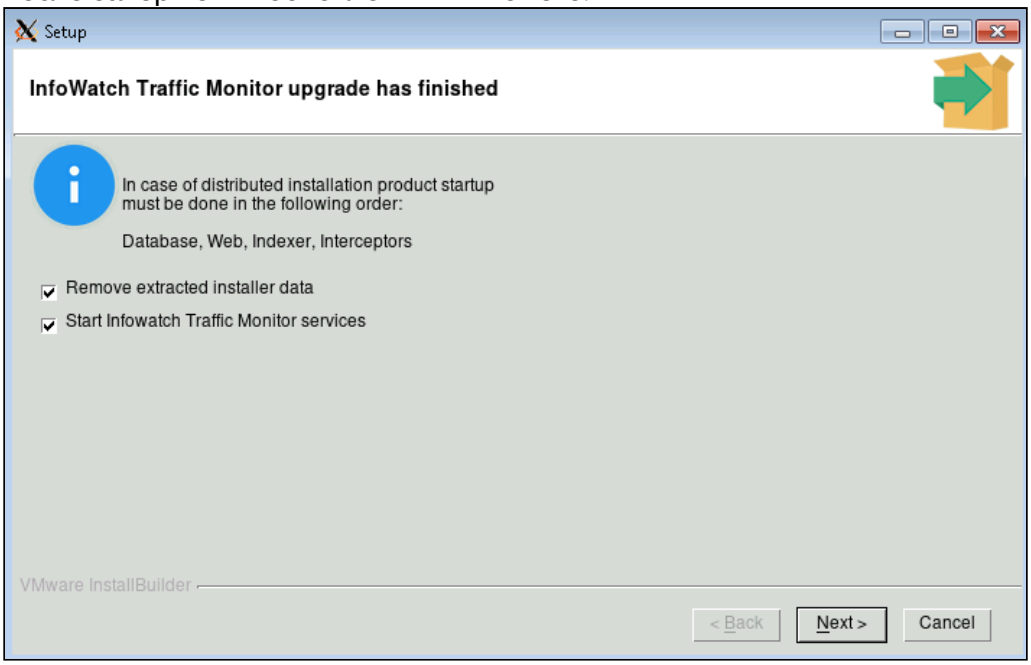


Процесс займет некоторое время.

Примечание:

Если процесс установки был прерван по какой-либо причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.

l. После завершения обновления вы можете:

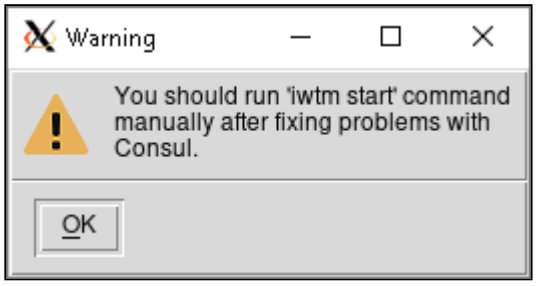


- `Remove exctracted installer data` – удалить пакеты, созданные инсталлятором для установки. Если установка прошла успешно, данные рекомендуется удалить;
- `Start Infowatch Traffic Monitor services` – запустить остановленные сервисы.

Для выбора действий поставьте галочки напротив соответствующих пунктов.

Примечание:

В случае некорректной настройки службы Consul в консоли будет выведено предупреждение:



Для закрытия окна и завершения работы инсталлятора нажмите кнопку **OK**.

При данной ошибке инсталлятор не запустит сервисы Traffic Monitor при завершении работы, их нужно будет запустить вручную после проверки, описанной в Шаге 3 данной инструкции.

Важно!

Перед запуском сервисов дождитесь завершения обновления на остальных серверах или завершайте работу инсталлятора без запуска сервисов и выполните запуск позже вручную.
Сервисы должны быть запущены в строгой последовательности в зависимости от активированных на них шаблонов.

Не запускайте сервисы Traffic Monitor до обновления и запуска сервера, установленного при помощи шаблона База данных.

После обновления настройки системы мониторинга Nagios будут изменены на значения по умолчанию. Если до обновления конфигурационные файлы Nagios редактировались, в директории `/etc/infowatch/nagios/iwmon` будут созданы их копии с расширением `.saved`. Перед запуском сервисов Traffic Monitor перенесите настройки из файлов `.saved` в соответствующие новые конфигурационные файлы.

После обновления для управления системой мониторинга используйте службу iwtm-nagios.
Например, для просмотра статуса Nagios используйте команду:
`systemctl status iwtm-nagios`

Если в конфигурационном файле `luaengined.conf` указан параметр `SmtpTmBccList`, перед запуском сервисов убедитесь, что значение параметра не содержит угловых скобок (`<` и `>`). В противном случае удалите скобки.

m. Для завершения работы инсталлятора нажмите кнопку **Next** или дождитесь завершения обновления сервера СУБД.

- **обновление в тихом режиме**

  Чтобы сократить участие в процессе обновления Системы, в инсталляторе предусмотрена работа тихом режиме. В этом режиме инсталлятор может обновить Traffic Monitor, используя параметры по умолчанию.

  В инсталляторе реализована возможность использования файла параметров (option file). В нем вы можете задать требуемые особенности установки. При запуске инсталлятора с файлом параметров, указанные в нем значения будут считаться параметрами по умолчанию.

4.5.1 Файл параметров (option file)

В файле описание параметров имеет вид:

`<имя_параметра>=<значение_параметра>`

Допускается оставлять комментарии, используя символ `#`.

Пример файла параметров:

```
# This file is just an example
fix_incorrect_file_owners=1
cleanup_way=clean_fq
start_services_after_upgrade=1
```

В данном примере указаны параметры:

- исправить некорректного владельца файлов;
- перед остановкой сервисов дождаться обработки всех событий и очистки файловых очередей;
- после обновления запустить сервисы.

Важно!

Для параметров, которые не указаны в файле, будут использованы значения по умолчанию. Полный набор параметров указан в таблице ниже.

Чтобы использовать файл параметров, перейдите в директорию с инсталлятором и запустите его с опцией `--optionfile` и с указанием созданного ранее файла.

Пример команды использования файла параметров:

```
./iwtm-installer-7.14.0.97-rhel7 --optionfile /some_directory/option-file-example
```

Альтернативный способ использования: назовите файл параметров тем же именем, что назван инсталлятор, но с расширением `.options`, и скопируйте его в директорию к инсталлятору. В этом случае при запуске инсталлятор так же будет считать параметры из файла значениями по умолчанию.

4.5.2 Тихий режим обновления

Для обновления в тихом режиме используйте опцию `--mode unattended`.

Уровень взаимодействия с пользователем задается параметром `--unattendedmodeui`, который имеет следующие значения:

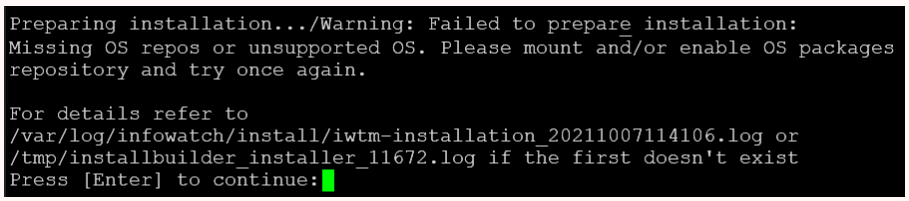
- `none` – в процессе работы инсталлятор не выводит на экран никакую информацию и не требует взаимодействия с пользователем;
- `minimal` – отображает прогресс обновления, не требует взаимодействия с пользователем;
- `minimalWithDialogs` – отображает прогресс обновления, также в процессе могут появляться всплывающие окна, может потребоваться взаимодействие с пользователем.

Пример команды запуска инсталлятора в тихом режиме без участия пользователя и с файлом параметров:

```
./iwtm-installer-7.14.0.97-rhel7 --optionfile /some_directory/option-file-example --mode unattended --unattendedmodeui minimal
```

Важно!

При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите **Enter** для завершения работы инсталлятора, затем подключите стандартный репозиторий RHEL, репозиторий EPEL и повторно запустите инсталлятор.

Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

Примечание:

Если процесс установки был прерван по какой-либо причине, устраните ее и повторно запустите инсталлятор, чтобы продолжить установку с последнего успешно завершенного этапа.
Когда процесс завершится без ошибок, инсталлятор удалит пакеты, созданные для установки.

Примечание:

В случае некорректной настройки службы Consul в консоли будет выведено предупреждение:



Для завершения работы инсталлятора нажмите **Enter**.

При данной ошибке инсталлятор не запустит сервисы Traffic Monitor при завершении работы, их нужно будет запустить вручную после проверки, описанной в Шаге 3 данной инструкции.

4.5.3 Полный состав файла параметров

В таблице приведен полный список возможных параметров для обновления и их значения по умолчанию.

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`force_upgrade`	`0`	`0,1`	Принудительно переключает инсталлятор в режим обновления, даже если совпадают версии	
`fix_incorrect_file_owners`	`0`	`0,1`	Параметр определяет, должен ли инсталлятор по умолчанию исправить некорректного владельца файлов перед обновлением.	Если у обновляемых файлов будет некорректный владелец, инсталлятор прервет обновление.

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`cleanup_way`	`wait_stop`	`quick_stop`, `wait_stop`, `clean_fq`	Выбор режим остановки сервисов: • `quick_stop` - быстрая остановка без обработки событий; • `wait_stop` – перед остановкой дождаться завершения текущей обработки событий; • `clean_fq` – перед остановкой дождаться обработки всех событий и очистки файловых очередей.	Если компоненты Traffic Monitor функционируют на нескольких серверах, они должны быть остановлены в следующей последовательности: a. Перехватчики b. Индексер c. Веб-консоль d. База данных Режим обработки всех событий и очистки файловых очередей (`clean_fq`) доступен только на серверах, установленных при помощи шаблона Перехватчики. Если был указан этот режим, но на сервере отсутствуют компоненты перехвата, будет использован режим текущей обработки событий (`wait_stop`). Если компоненты перехвата и компоненты анализа (`iw_cas` , `iw_pas`) используются на разных серверах, остановка перехватчиков с очисткой файловых очередей может зависнуть. Рекомендуется использовать другие режимы или остановить компоненты вручную.

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`start_services_after_upgrade`	`1`	`0,1`	Параметр определяет, должен ли инсталлятор запустить ли сервисы после обновления.	Не запускайте сервисы Traffic Monitor до обновления и запуска сервера, установленного при помощи шаблона База данных. После обновления настройки системы мониторинга Nagios будут изменены на значения по умолчанию. Если до обновления конфигурационные файлы Nagios редактировались, в директории `/etc/infowatch/nagios/iwmon` будут созданы их копии с расширением `.saved`. Перед запуском сервисов Traffic Monitor перенесите настройки из файлов `.saved` в соответствующие новые конфигурационные файлы. После обновления для управления системой мониторинга используйте службу iwtm-nagios. Например, для просмотра статуса Nagios используйте команду: `systemctl status iwtm-nagios` Если в конфигурационном файле `luaengined.conf` указан параметр `SmtpTmBccList`, и при этом значение

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				параметра содержит угловые скобки (`<` и `>`) , перед запуском сервисов необходимо удалить скобки. В таком случае не следует включать запуск сервисов в файле параметров. Если компоненты Traffic Monitor функционируют на нескольких серверах, они должны быть запущены в следующей последовательности: a. База данных b. Веб-консоль c. Индексер d. Перехватчики
`eula`		`show`, `accept`	Вывести текст Лицензионного Соглашения, Принять Лицензионное Соглашение без предварительного просмотра	Если вы запускаете установку не в тихом режиме и параметр не указан, то будет выведен текст Лицензионного соглашения и будет предложено принять его. При установке в тихом режиме значение параметра игнорируется и Лицензионное Соглашение принимается по умолчанию.

13. Введите команду для поиска файлов с расширением **`.rpmnew`** за исключением резервных копий конфигурационных файлов:
`find / -name "*rpmnew*" -not -path "/opt/iw/tm5/etc_conf_backup*" -print`
Если такие файлы найдены, они будут выведены на экран консоли. В таком случае их необходимо корректно объединить с конфигурационными файлами (см. статью *Объединение конфигурационных файлов*).

> **Примечание:**
>
> Для успешного объединения конфигурационных файлов рекомендуется ознакомиться со статьями на официальном сайте (доступны на английском языке):
>
> - Файлы rpmnew и rpmsave;
> - Рекомендации по обработке файлов rpmnew и rpmsave после обновления системы Red Hat Enterprises Linux.

> **Важно!**
>
> В процессе обновления не вносите изменения в файлы **`database.conf`**, **`consul.json`**.
>
> На сервере, установленном при помощи шаблона Веб-консоль, после объединения в конфигурационном файле **`web.conf`** в блоке `search_meta` в параметре `hostname` укажите IP-адрес сервера СУБД.

14. На серверах, установленных при помощи шаблона Перехватчики, в директории `/opt/iw/tm5/etc/scripts/` должен быть файл **`iwssid.lua`**, его рекомендуется оставить без изменений, если до обновления он не редактировался.
    В противном случае его необходимо корректно объединить с конфигурационным файлом **`iwssid.lua.rpmnew`** (см. статью *Объединение конфигурационных файлов*).

    > **Примечание:**
    >
    > Все настройки для работы Системы "в разрыв" перенесены в конфигурационный файл `luaengined.conf`.

15. Traffic Monitor, начиная с версии 7.8.0, поддерживает OCR-экстрактор Content AI ContentReader Engine. После обновления режимы работы экстрактора будут настраиваться в новых файлах профилей `/opt/iw/tm5/etc/CRProfile.ini` и `/opt/iw/tm5/etc/CRProfile_fast.ini`.
    Если до обновления Системы вы использовали OCR-экстрактор ABBYY Finereader и вносили изменения в старые файлы профилей `FRProfile.ini` или `FRProfile_fast.ini`, для сохранения этих настроек перенесите их в новые файлы. При этом учитывайте возможные изменения названий и значений параметров в новой версии экстрактора.
16. Проверьте кластер службы Consul – описание смотрите ниже.

ШАГ 2. ПРОВЕРКА КЛАСТЕРА СЛУЖБЫ CONSUL

Для проверки кластера Consul выполните следующие действия:

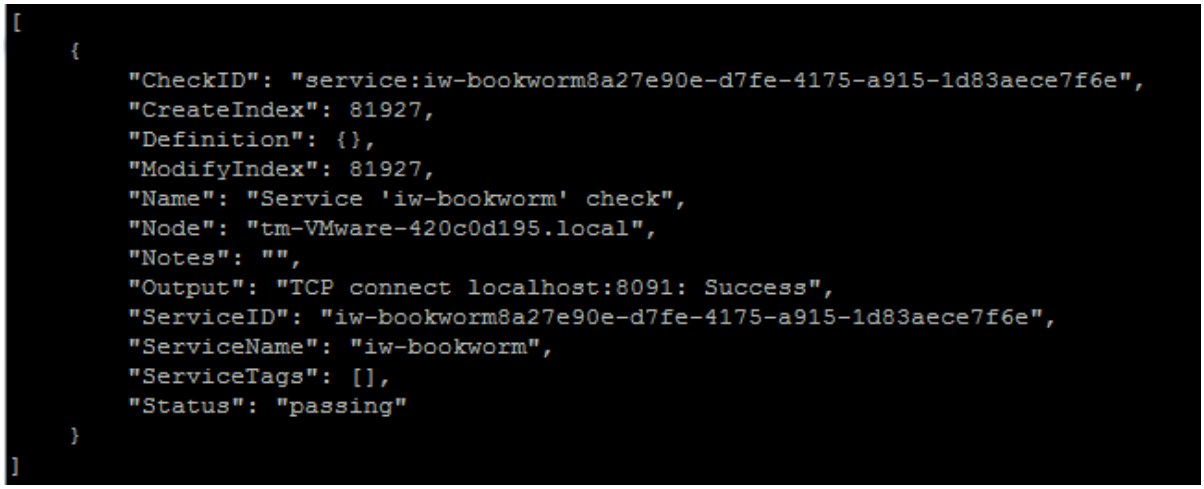
1. На всех обновляемых серверах запустите службу Consul, выполнив команду:
   `systemctl start iwtm-consul`
   Проверить статус службы можно командой:
   `systemctl status iwtm-consul`
2. Чтобы проверить службу Consul, на сервере, установленном при помощи шаблона База данных, выполните команды:

a. Для вывода IP-адреса основного сервера (лидера) кластера:
`curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
b. Для вывода информации о членах кластера:
`consul members`

3. Если не будет выведен IP-адрес лидера кластера, или не все серверы будут в списке членов кластера, выполните *конфигурирование кластера службы Consul*.
После настройки повторите проверку (действие 2).
4. Выполните проверку работоспособности внутренних сервисов Системы – описание смотрите ниже.

ШАГ 3. ПРОВЕРКА РАБОТОСПОСОБНОСТИ ВНУТРЕННИХ СЕРВИСОВ СИСТЕМЫ
На сервере, установленном при помощи шаблона Веб-консоль, запустите службы `iw_bookworm`, `iw_licensed`, `iw_updater`, `iw_kicker` и выполните проверку их работоспособности:

1. Выполните команду для запуска службы `iw_bookworm`:
`iwtm start bookworm`
2. Службе может потребоваться время на включение. Для проверки состояния службы введите команду:
`curl -s http://localhost:8500/v1/health/checks/iw-bookworm | python -mjson.tool`
В результате выполнения команды будет выведена информация об указанной службе:



3. Проверьте значения блоков "Node" и "Status":
a. В блоке "Node" должно быть указано имя ноды в кластере Consul, на которой установлена проверяемая служба;
b. В блоке "Status" должно быть указано "passing".
4. Служба **`iw_licensed`** должна быть запущена в единственном экземпляре на кластер. Выполните команду для запуска службы `iw_licensed`:
`iwtm start licensed`
5. Службе может потребоваться время на включение. Для проверки состояния службы `iw_licensed` введите команду:
`curl -s http://localhost:8500/v1/health/checks/iw-licensed | python -mjson.tool`
Выполните действие 3 текущего шага.

6. Выполните команду для запуска службы `iw_updater`:
   `iwtm start updater`
7. Службе может потребоваться время на включение. Для проверки состояния службы `iw_updater` введите команду:
   `curl -s http://localhost:8500/v1/health/checks/iw-updater | python -mjson.tool`
   Выполните действие 3 текущего шага.
8. Для проверки службы `iw_kicker` необходимо запустить службу `iw_blackboard`:
   `iwtm start blackboard`
9. Служба **`iw_kicker`** должна быть запущена в единственном экземпляре на кластер. Выполните команду для запуска службы `iw_kicker`:
   `iwtm start kicker`
10. Службе может потребоваться время на включение. Для проверки состояния службы `iw_kicker` необходимо проверить файл `/opt/iw/tm5/log/web-console-error.log` на наличие ошибок в процессе обновления. Введите команду:
    `grep -r 'error' /opt/iw/tm5/log/web-console-error.log || echo "All good"`
    Убедитесь, что адрес в команде указан верно. В случае отсутствия ошибок будет выведено сообщение `All good`.
11. Выполните команду для остановки служб:
    `iwtm stop`
12. Завершите обновление серверов – описание смотрите ниже.

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

ШАГ 4. ЗАВЕРШЕНИЕ ОБНОВЛЕНИЯ СЕРВЕРОВ

Чтобы завершить обновление серверов, на каждом из них выполните следующие действия:

1. Если ранее работа инсталлятора не была завершена, выберите запуск сервисов и завершите обновление.
   Если ранее инсталлятор завершил работу без запуска сервисов, запустите их вручную или перезагрузите сервер для запуска всех остановленных сервисов.
   Команда для перезагрузки сервера:
   `reboot`

Важно!

Компоненты Traffic Monitor должны быть запущены в следующей последовательности:

a. База данных
b. Веб-консоль
c. Индексер
d. Перехватчики

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>
```

```
7   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.

2. В Traffic Monitor расширен список задач по умолчанию для автоматического удаления ненужных файлов.
   Задачи для планировщика `cron` теперь по умолчанию указаны в файле `/etc/cron.d/iwtm_cleanup` (о содержимом файла см. *Автоматическое удаление ненужных файлов в Traffic Monitor*).
   Для корректной работы новых задач:
   a. Удалите старые задачи, отредактировав файл конфигурации `cron`:
      `sudo crontab -e`
   b. Сохраните изменения и выйдите из редактора файла конфигурации.
   c. Перезапустите сервис:
      `systemctl reload crond`
3. Если до обновления вы не редактировали прошлый файл с задачами `/etc/cron.d/iwtm_error_queue`, пропустите данное действие.
   В противном случае `/etc/cron.d/iwtm_error_queue` будет удален, а его содержимое сохранено в файле `/etc/cron.d/iwtm_error_queue.rpmsave`.
   Чтобы задачи, добавленные вами ранее, снова работали, создайте файл для ваших задач в директории `/etc/cron.d/` и скопируйте в него нужные задачи из `/etc/cron.d/iwtm_error_queue.rpmsave`.

> **Примечание:**
>
> Вы можете добавить свои задачи в файл `/etc/cron.d/iwtm_cleanup`, но тогда при следующем обновлении он будет переименован в `/etc/cron.d/iwtm_cleanup.rpmnew` и заменен файлом с содержимым по умолчанию. После следующего обновления необходимо будет перенести добавленные вами задачи из `/etc/cron.d/iwtm_cleanup.rpmnew` в новый `/etc/cron.d/iwtm_cleanup`.
> Чтобы каждый раз не переносить ваши задачи, вы можете создать отдельный файл с вашими задачами в директории `/etc/cron.d/`.

4. Если используется система Prometheus и если сервер, установленный при помощи шаблона База данных, не был перезагружен, для запуска службы выполните на нем команду:
   `systemctl start iwtm-postgres_exporter` – для **СУБД PostgreSQL**
   `systemctl start iwtm-oracledb_exporter` – для **СУБД Oracle**
5. Если обновляемый сервер Traffic Monitor взаимодействует с Data Discovery 2.0 и более новыми, ранее вы остановили под (pod) `technologies`. Запустите под заново. Для этого:
   a. Подключитесь к ноде кластер Центра расследований.

b. Для запуска пода на ноде с лейблом `central` выполните команду:
`kubectl scale -n infowatch --replicas=1 deployment/technologies-central`
c. Подключитесь обратно к терминалу сервера с Traffic Monitor.

6. Если ранее вы остановили процессы адаптера Password Disclosure Adapter, запустите их. Подробнее см. документ *InfoWatch Password Disclosure Adapter. Руководство по установке и конфигурированию. Диагностика и удаление InfoWatch Password Disclosure Adapter*.
7. Введите команду для очистки кеша менеджера пакетов:
`yum clean all`
8. Введите команду для проверки статусов процессов:
`iwtm status`
На экране отобразится список процессов и их статусы.

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. 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.

Обновление Системы путем чистой установки и восстановления данных из резервной копии (для СУБД PostgreSQL)

Важно!

Крайне рекомендуется выполнить резервное копирование Системы, а также клонировать ее и провести обновление на этой тестовой машине.
Если вы планируете не копировать данные, а примонтировать диск или раздел с данными, все равно рекомендуется выполнить их резервное копирование.
После чистой установки Системы конфигурационные файлы Traffic Monitor необходимо будет настроить заново. Рекомендуется сохранить их для повторной настройки после обновления.

Если в конфигурационном файле `luaengined.conf` указан параметр `SmtpTmBccList`, и при этом значение параметра содержит угловые скобки (`<` и `>`), необходимо удалить скобки перед запуском сервисов.

1. На всех серверах для остановки сервисов Traffic Monitor введите команду:
`iwtm stop`

2. На сервере, установленном при помощи шаблона База данных, проверьте количество содержащихся в БД событий. Для этого введите команду:
   `psql postgres iwtm -c "select count(1) from object;"`
3. Выполните *резервное копирование БД, индексов, конфигурации службы iw_adlibitum*.
4. Traffic Monitor, начиная с версии 7.8.0, поддерживает OCR-экстрактор Content AI ContentReader Engine.
   Если до обновления Системы вы использовали OCR-экстрактор ABBYY Finereader и на серверах с шаблоном Перехватчики вносили изменения в файлы профилей `FRProfile.ini` или `FRProfile_fast.ini`, сохраните эти кастомизации, чтобы восстановить их после установки новой версии Traffic Monitor.
5. Установите новую версию Traffic Monitor.

   Примечание:

   Если вы не планируете изменять серверы с шаблонами Индексер, Веб-консоль, Перехватчики (например, устанавливать новую ОС или переносить шаблоны на другие серверы), то их можно обновить *поверх установленных*. В таком случае пропустите шаги 8-10 данной инструкции.

   Важно!

   Если резервные копии Базы данных находятся на внешних хранилищах, не подключайте их в процессе установки. Это нужно будет сделать непосредственно перед восстановлением и обновлением Базы данных.

   По завершении установки не удаляйте пакеты созданные инсталлятором в процессе (пункт **Remove extracted installer data**).

   Последующие действия выполняйте на серверах с новой версией Traffic Monitor.
6. На всех серверах для остановки служб введите команду:
   `iwtm stop`
7. На сервере, установленном при помощи шаблона База данных:
   a. Введите команду для остановки службы:
      - для PostgreSQL 13:
        `systemctl stop postgresql-13`
      - для PostgreSQL 15:
        `systemctl stop postgresql-15`

        Примечание:

        Чтобы иметь возможность восстановить исходное состояние чистой установки, вы можете скопировать директории `u01` и `u02`.

   b. Для изменения прав доступа к директории введите команду:
      `chmod 777 /var/log/infowatch/update`
   c. Скопируйте резервную копию Базы данных таким образом, чтобы расположение и права соответствовали исходным.

d. Измените владельца директорий, выполнив команды:
```
chown -R postgres:postgres /u01/
chown -R postgres:postgres /u02/
```
e. Введите команду для перехода в директорию со скриптами:
```
cd /tmp/iwtm_installer/scripts
```
f. Находясь в директории, запустите скрипт обновления СУБД с помощью команды вида:
```
./install_postgres.sh --distrib_path=<директория_с_дистрибутивом_СУБД>
--tm_version=<версия_нового_Traffic_Monitor> --update
```
В нашем примере:
```
./install_postgres.sh --distrib_path=/root --tm_version=7.14.0.97 --
update
```

> **Примечание:**
>
> В примере дистрибутив `iwtm-postgresql-15.14-x.x.x.xxx-rhel7.tar.gz` расположен в директории `/root`.
> Чтобы узнать версию установленного Traffic Monitor, введите команду:
> `cat /opt/iw/tm5/version`

g. После успешного обновления выполните команду для проверки статус службы СУБД:
```
systemctl status postgresql-15
```
h. Запустите скрипт обновления схемы данных с помощью команды вида:
```
./install_dbschema.sh --tm_version=<версия_нового_Traffic_Monitor> --
db_type=postgres --update
```
В нашем примере:
```
./install_dbschema.sh --tm_version=7.14.0.97 --db_type=postgres --
update
```
i. Выполните действие 2 данной инструкции, чтобы сравнить количество событий в Базе данных до и после обновления.

8. На сервере с шаблоном Индексер:
   a. Скопируйте резервные копии индексов таким образом, чтобы расположение и права соответствовали исходным.
   Если исходное расположение индексов не являлось расположением по умолчанию, его необходимо будет указать в соответствующих разделах конфигурационных файлов (см. *инструкцию по созданию резервных копий*).
   b. Измените владельца директории, выполнив команду:
   ```
   chown -R iwtm:iwtm /var/lib/sphinx/
   ```
   В команде выше указано расположение по умолчанию.
9. На сервере с шаблоном Веб-консоль:
   a. Скопируйте резервную копию конфигурации службы `iw_adlibitum` таким образом, чтобы расположение и права соответствовали исходным.
   Если исходное расположение конфигурации службы `iw_adlibitum` не являлось расположением по умолчанию, его необходимо будет указать в соответствующих разделах конфигурационных файлов (см. *инструкцию по созданию резервных копий*).
   b. Измените владельца директории, выполнив команду:
   ```
   chown -R iwtm:iwtm /opt/iw/tm5/etc/adlibitum/
   ```
   В команде выше указано расположение по умолчанию.

c. Выполните команды
`sudo -u iwtm touch /opt/iw/tm5/www/backend/protected/runtime/first_run`
`iwtm restart kicker`

10. На серверах с шаблоном Перехватчики после обновления Системы режимы работы OCR-экстрактора Content AI ContentReader Engine будут настраиваться в новых файлах профилей `/opt/iw/tm5/etc/CRProfile.ini` и `/opt/iw/tm5/etc/CRProfile_fast.ini`. Если до обновления Системы вы использовали OCR-экстрактор ABBYY Finereader и вносили изменения в старые файлы профилей `FRProfile.ini` или `FRProfile_fast.ini`, для сохранения этих настроек перенесите их в новые файлы. При этом учитывайте возможные изменения названий и значений параметров в новой версии экстрактора.
11. Перезагрузите все серверы, выполнив на каждом из них команду:
`reboot`

> **Важно!**
>
> Компоненты Traffic Monitor должны быть запущены в следующей последовательности:
>
> a. База данных
> b. Веб-консоль
> c. Индексер
> d. Перехватчики

12. Проверьте статусы процессов на каждом сервере с помощью команды:
`iwtm status`
На экране отобразится список процессов и их статусы.

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

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

Если вы обновили компоненты Traffic Monitor на ОС Oracle Linux 8, AlmaLinux 8 или Rocky Linux 8, восстановите исходный файл выпуска ОС.

Для этого:

1. Выполните команду в зависимости от ОС:
   - в ОС Oracle Linux 8:
     `mv /etc/release.bak /etc/oracle-release`
   - в ОС AlmaLinux 8 или Rocky Linux 8:
     `mv /etc/release.bak /etc/redhat-release`

2. Подтвердите перезапись файла. Для этого введите " `yes` " и нажмите **Enter**.
3. Убедитесь, что исходный файл выпуска успешно восстановлен. Для этого выполните команду:

   ```
   lsb_release -a
   ```

   В результате должна быть выведена информация о вашей операционной системе. Например, для ОС AlmaLinux 8 будет выведено:

   ```
   Distributor ID: AlmaLinux
   Description:    AlmaLinux release 8.10 (Cerulean Leopard)
   Release:        8.10
   Codename:       CeruleanLeopard
   ```

Важно!

В Traffic Monitor 7.14 обновили поставляемые сертификаты и публичный ключ, которые используются для SSL-соединения с сервисом XAPI. По умолчанию сертификаты и ключ расположены в папке `/opt/iw/tm5/etc/cert`.

Если вы обновляете Traffic Monitor с версии 7.13 или более ранней и в вашем контуре Data Discovery, Device Monitor, адаптеры или другие сторонние сервисы взаимодействуют с Traffic Monitor с помощью сервиса XAPI, учтите замену сертификатов и публичного ключа.

Если ранее вы:

- **Использовали собственные** сертификаты и ключ **с названиями отличными** от имен файлов по умолчанию, **обновление не повлияет** на взаимодействие сервисов, так как добавленные вами файлы не будут удалены.
- **Удалили файлы**, **поставляемые** с продуктом, и **использовали собственные** сертификаты и ключ **с аналогичными названиями**, после обновления **замените сертификаты в Traffic Monitor на сгенерированные вами**.
- **Копировали** в папки других продуктов, адаптеров или сервисов сертификаты и ключ, **поставляемые** с Traffic Monitor, после обновления **скопируйте их заново** из папки `/opt/iw/tm5/etc/cert`.

Об установке или замене сертификатов:

- в **Device Monitor Windows** см. *InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию. Настройка проверки сертификатов удаленных серверов*;
- в **Device Monitor Linux** см. *InfoWatch Device Monitor for Linux. Руководство по установке. Настройка проверки сертификатов удаленных серверов*;
- в **Data Discovery** см. *InfoWatch Data Discovery*. *Руководство администратора. Зоны и серверы*.

4.6 Объединение конфигурационных файлов

Во время обновления сервера Traffic Monitor конфигурационные файлы (например, с расширениями **.conf**, **.cfg** и **.lua**), которые были изменены во время использования предыдущей версии, не перезаписываются новыми. В тех же директориях создаются новые файлы с теми же названиями, но с расширением **.rpmnew**. Это сделано для того, чтобы поддержать возможность изменения структуры

файлов новых версий. Для корректной работы Системы потребуется объединить файлы старой и новой версий.

> **Важно!**
>
> В процессе обновления не вносите изменения в файлы `web.conf`, `database.conf`, `consul.json`.

Используйте любой из приведенных ниже способов объединения файлов.

4.6.1 Объединение конфигурационных файлов в Midnight Commander

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

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

Файл **postgresql.conf** имеет вид:

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

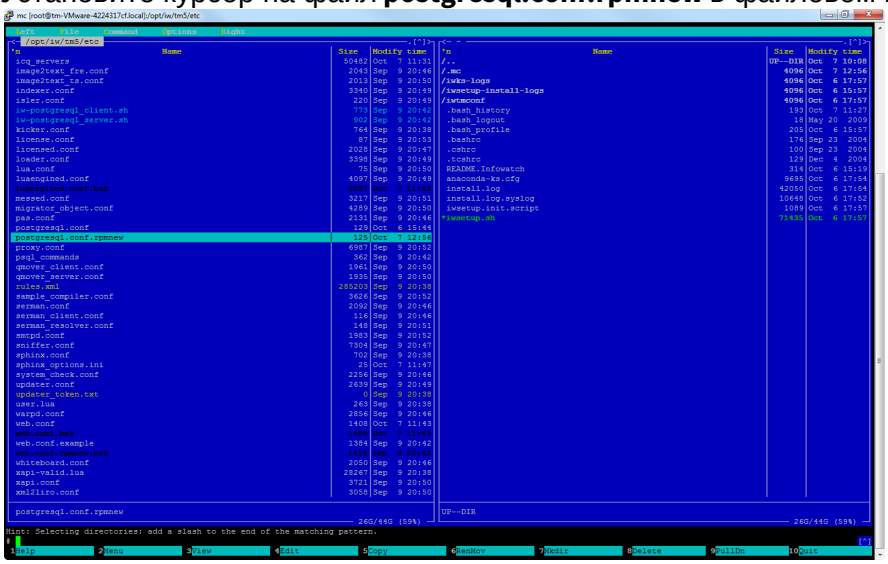
Файл **postgresql.conf.rpmnew** имеет вид:

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

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

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

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



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

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

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

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

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

4.6.2 Объединение конфигурационных файлов с помощью vimdiff

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

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

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

Важно!

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

Важно!

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

1. /etc/rc.d/init.d/postgresql-13.rpmnew
2. /etc/sgml/docbook/xmlcatalog.rpmnew

4.7 Обновление Data Storage

Внешнее хранилище бинарных данных Data Storage является частью Платформы. Чтобы обновить Data Storage, необходимо обновить Платформу. Это можно сделать одним из следующих способов:

- Обновить платформенный продукт, если он установлен на сервере Data Storage. В этом случае Платформа будет обновлена автоматически.
  Описание обновления можно найти в документации на этот продукт.

- Обновить Платформу, установленную без продуктов. Данный тип обновления описан ниже.

Обновление Платформы

В комплект Traffic Monitor 7.14.0 входит Data Storage на базе Платформы 2.5.0.

Платформа 2.5.0 поддерживает:

- прямое стандартное обновление с версий 2.3.X и 2.4.X;
- обновление с помощью сброса текущей установки и переустановки на старые данные.

Дистрибутив представляет собой архив **`iw_platform.tar.xz`**. Этот архив содержит полный набор бинарных модулей образов контейнеров, необходимых для развертывания Платформы без доступа к Интернету (офлайн-установка). Кроме этого, данный архив содержит программу обновления.

Для обновления Платформы используйте командную строку.

> **Примечание:**
>
> Чтобы узнать версию устанавливаемой Платформы:
>
> 1. Распакуйте архив с дистрибутивом Платформы (см. *Обновление Платформы с помощью сброса установки (reset)*, шаг 5). В нашем примере, в директорию `platform`.
> 2. Выполните команду:
> `cat platform/setup.yaml | grep version`

4.7.1 Прямое обновление Платформы

Чтобы обновить Платформу:

1. Выполните шаги по подготовке сервера к обновлению Платформы (см. *Подготовка сервера*).

   > **Примечание:**
   >
   > В ходе обновления инсталлятор проверит наличие:
   >
   > - не менее 100 ГБ на диске для директорий размещения данных ClickHouse, PostgreSQL, NATS и бинарных данных. Если директории для хранения данных находятся на разных дисках, то проверяется наличие 100 ГБ свободного места на каждом из них;
   > - не менее 20 ГБ на диске для директорий с образами;
   > - не менее 8 ГБ ОЗУ;
   > - не менее 2 ядер процессора;
   > - поддержки инструкции SSE 4.2;
   > - установленного пакета **`conntrack.`**

2. Создайте папку для дистрибутива новой версии Платформы и перейдите в нее:

```
mkdir new_platform
```

```
cd new_platform
```

3. Скопируйте в папку архив с дистрибутивом.
4. Распакуйте архив с помощью команды:

```
tar -xvf iw_platform.tar.xz
```

5. Убедитесь, что в разделе с директорией `/var/lib/containerd` доступно не менее 50 ГБ дискового пространства.
Чтобы проверить доступное дисковое пространство, используйте команду:

```
df -h /var/lib/containerd
```

> **Примечание:**
>
> Чтобы освободить дисковое пространство, вы можете удалить неиспользуемые образы контейнеров прошлых версий. **Не удаляйте контейнеры текущей установленной версии**.
>
> **Чтобы удалить все версии контейнеров, кроме указанной:**
>
> a. Создайте или дополните файл `/etc/crictl.yaml` следующим содержимым:
>
> ```
> runtime-endpoint: unix:///run/containerd/containerd.sock
> image-endpoint: unix:///run/containerd/containerd.sock
> timeout: 2
> pull-image-on-create: false
> disable-pull-on-run: false
> ```
>
> b. Выполните команды:
>
> i. Для удаления контейнеров Платформы (где x.x.x.x - **текущая установленная** версия Платформы):
>
> ```
> crictl rmi $(crictl image | awk '($2 !~ /x.x.x.x|latest/ && $1 ~ /
> docker.infowatch.ru\/platform-core-release/ && $1 !~ /flannel/) {print
> $3}')
> ```
>
> ii. Для удаления контейнеров Docker:
>
> ```
> rm -rf /var/lib/docker
> ```

6. Запустите процесс обновления Платформы:

```
/setup.py update
```

7. Укажите путь для временного размещения событий Traffic Monitor перед их загрузкой в Платформу (по умолчанию: `/opt/factsldrtmdata`) и нажмите **Enter**.
8. Дождитесь окончания процесса обновления Платформы.
9. Убедитесь, что все сервисы запущены. Для этого выполните команду:

   ```
   kubectl get pods -n infowatch
   ```

   Команда выведет список сервисов. Каждый сервис должен иметь статус `Running`.
10. Если после обновления вам необходимо освободить место на диске, вы можете удалить неиспользуемые контейнеры аналогично п.5.

4.7.2 Обновление Платформы с помощью сброса установки (reset)

Обновление с помощью сброса установки состоит из следующих шагов:

1. Сброс установки **с помощью нового инсталлятора**. При сбросе данные Системы не будут удалены.
2. Установка новой версии Платформы с указанием уже имеющихся папок с данными.

> **Примечание:**
>
> Если вы используете удаленное подключение по протоколу SSH, чтобы избежать проблем в случае разрыва соединения с сервером, рекомендуем использовать утилиту Screen. При отключении от утилиты запущенные в ней процессы не прервутся, что позволит безопасно продолжить обновление.

Чтобы обновить Платформу:

1. Выполните шаги по подготовке сервера к обновлению (см. *Подготовка сервера*).

   > **Примечание:**
   >
   > В ходе обновления инсталлятор проверит наличие:
   >
   > - не менее 100 ГБ на диске для директорий размещения данных ClickHouse, PostgreSQL, NATS и бинарных данных. Если директории для хранения данных находятся на разных дисках, то проверяется наличие 100 ГБ свободного места на каждом из них;
   > - не менее 20 ГБ на диске для директорий с образами;
   > - не менее 8 ГБ ОЗУ;
   > - не менее 2 ядер процессора;
   > - поддержки инструкции SSE 4.2;
   > - установленного пакета **`conntrack.`**

2. Создайте новую директорию на диске (например, `platform`):

   ```
   mkdir platform
   ```

3. Скопируйте архив **`iw_platform.tar.xz`** в созданную директорию.
4. Перейдите в директорию, в которую был скопирован архив.

5. Распакуйте архив с дистрибутивом в эту директорию:

```
tar -xvf iw_platform.tar.xz
```

6. До сброса установки запомните или сохраните пути к текущим директориям хранения данных. Получить список директорий можно, выполнив команду:

```
cat /var/lib/iwplatform/data/volumes.txt
```

7. Выполните сброс текущей установки **с помощью инсталлятора новой версии**:

```
./setup.py reset
```

8. Дождитесь окончания процесса сброса установки Платформы.
9. Перезагрузите сервер с помощью команды:

```
reboot
```

10. Если вы обновляетесь с переходом на другой сервер или на новую ОС, скопируйте на другой раздел или на новый сервер директории с данными, которые были указаны при установке.

> **Примечание:**
>
> В **Платформе 2.1 и более ранних** директории по умолчанию расположены по пути `/mnt`.
> В **Платформе 2.2 и более новых** - по умолчанию по пути `/opt`.
> Обязательно копируйте директории с сохранением прав и владельцев. Для копирования используйте стандартные средства, например утилиту `rsync`.

11. Чтобы освободить дисковое пространство, вы можете удалить директорию с образами контейнеров прошлых версий `/var/lib/containerd`. Для этого выполните команду:

```
rm -rf /var/lib/containerd
```

12. Установите новую версию Платформы (см. *Установка Платформы*).

> **Важно!**
>
> Когда инсталлятор потребует указать директории для размещения данных, указывайте директории с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?»

Если вы обновляетесь **с версии 2.1 и более ранних**, учитывайте, что с версии 2.2 пути установки по умолчанию изменились. Если ранее вы использовали пути по умолчанию, при установке Платформы 2.2 и более новых по умолчанию инсталлятор не обнаружит данные прошлой версии и создаст директории по пути `/opt`. Поэтому переместите данные в `/opt` или укажите старые директории при установке новой версии.

13. Если после обновления вам необходимо освободить место на диске, вы можете удалить неиспользуемые контейнеры docker или containerd. Подробнее, см. в статье *Как удалить неиспользуемые контейнеры Docker и Containerd?*.

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 внешнего хранилища Data Storage см. *Удаление Data Storage*.
- О порядке удаления схемы БД см. *Удаление схемы базы данных*.
- О порядке удаления Traffic Monitor (все установленные на сервере компоненты: веб-консоль, модули перехвата и другие) см. *Удаление Traffic Monitor*.
- О порядке удаления Device Monitor (серверная и клиентская часть) см. *InfoWatch Device Monitor for Windows. Руководство по установке, конфигурированию и администрированию* или *InfoWatch Device Monitor for Linux. Руководство по установке*.

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 Data Storage

Data Storage удаляется с помощью командной строки.

Чтобы удалить Data Storage:

1. Разорвите соединение Traffic Monitor с Data Storage. Для этого на сервере Traffic Monitor выполните команду:
   `platform_conf_ctl --ds-remove`
2. На сервере Data Storage перейдите в директорию, в которой распакован дистрибутив последней версии Платформы.
3. Удалите Платформу, выполнив команду:
   `./setup.py remove`
4. Дождитесь завершения процесса.

> **Примечание:**
>
> Инсталлятор удалит сервисы и компоненты Платформы. После удаления на сервере останутся результаты работы Платформы. Данные останутся в директориях, которые были указаны при установке Платформы.

5.2 Удаление схемы базы данных

> **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.

Удаление схемы запускается на сервере, установленном при помощи шаблона База данных, в том числе при использовании удаленной базы данных.

Если вы используете СУБД Oracle, убедитесь, что:

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

Для удаления схемы базы данных выполните следующие шаги:

1. **Остановка Traffic Monitor**
   a. Остановите все процессы Traffic Monitor:
   `iwtm stop`
   b. Закройте все экземпляры Консоли управления;
   c. Остановите сервис:
   `service iwtm-php-fpm stop`
   d. Прекратите все соединения с удаляемой схемой базы данных, осуществляемые из других программ.
2. **Запуск удаления схемы**
   a. Перейдите в директорию `/opt/iw/tm5/csw/oracle` или `/opt/iw/tm5/csw/postgres`
   b. Выполните скрипт:
   `./uninstall.sh`
3. **Удаление старых версий конфигурации**
   a. Удалите содержимое директории с помощью команды:
   `rm -rf /opt/iw/tm5/etc/configerator/*`

Важно!

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

- политики, в том числе предустановленные (см. *InfoWatch Traffic Monitor. Руководство пользователя. Предустановленные политики*);
- запросы и отчеты (см. *InfoWatch Traffic Monitor. Руководство пользователя. Раздел "Отчеты"*);
- плагины и токены (см. *InfoWatch Traffic Monitor. Руководство пользователя. 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. Добавление плагина*) и создать необходимые политики (см. статьи "*InfoWatch Traffic Monitor. Руководство пользователя. Создание политики защиты данных* и *Создание политики контроля персон*).

Примечание:

При необходимости вы можете удалить содержимое самой базы данных и индексы. Удаляйте их, только если уверены, что данные больше не понадобятся.
Для этого:

1. Удалите директории `u01` и `u02` с помощью команды:
   `rm -Rvf /u01 /u02`
2. Удалите индексы с помощью команды:
   `rm -Rvf /var/lib/sphinx`

5.3 Удаление Traffic Monitor

Важно!

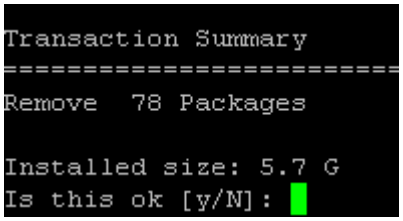
Если база данных находится на сервере, на котором будет запущен процесс удаления, сначала *удалите схему базы данных*.

Удаление затронет **только** тот сервер, на котором будет выполнена команда удаления.
Для возможности восстановления событий в случае переустановки Traffic Monitor рекомендуем перед удалением создать резервную копию базы данных (см. *InfoWatch Traffic Monitor. Руководство администратора*. *Создание резервной копии базы данных* в разделе *PostgreSQL* или *Oracle*).
Также рекомендуется создать резервные копии конфигурации и настроек.

Процесс удаления Traffic Monitor запускается в консоли сервера. Удаление выполняется средствами ОС.

Чтобы удалить Traffic Monitor выполните следующие действия:

1. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя **root** с использованием пароля, созданного при установке).
2. Остановите процессы Traffic Monitor с помощью команды:
   `iwtm stop`
3. Для удаления пакетов Traffc Monitor выполните следующую команду:
   - На сервере под управлением ОС Red Hat Enterprise Linux, РЕД ОС, Oracle Linux, AlmaLinux и Rocky Linux:
     `yum remove `rpm -qa | grep iwtm``
   - На сервере под управлением ОС Альт Сервер:
     `apt-get remove `rpm -qa | grep iwtm``
     Начнется подготовка к удалению.
4. После подготовки в консоли сервера будет выведен список удаляемых пакетов и запрос подтверждения вида:



Для продолжения введите "**Y**" и нажмите **Enter**.
Начнется удаление пакетов Traffic Monitor.
Дождитесь завершения процесса удаления.

В результате буду удалены все службы Traffic Monitor. После удаления на компьютере останутся:

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

Для удаления оставшихся файлов вы можете удалить директорию `/opt/iw` со всем содержимым, используя средства ОС.

> **Важно!**
>
> Перед удалением убедитесь, что в директориях не содержится важная информация.

Для удаления директории вы можете использовать команду:

```
rm -Rvf /opt/iw
```

Для возможности корректной повторной установки:

1. Удалите файл с информацией о репозитории, созданном для продукта, с помощью команды вида:
   `rm -f /etc/yum.repos.d/tm-x.x.x.xxx-release.repo`
   В нашем примере:
   `rm -f /etc/yum.repos.d/tm-7.14.0.97-release.repo`
2. Если использовалась СУБД PostgreSQL, для удаления оставшихся компонентов выполните команду:
   - На сервере под управлением ОС Red Hat Enterprise Linux, РЕД ОС, Oracle Linux, AlmaLinux и Rocky Linux:
     `yum remove phantomjs pgagent_15 redis postgresql15 postgresql15-libs postgresql15-server postgresql15-contrib`
   - На сервере под управлением ОС Альт Сервер:
     `apt-get remove pgagent redis postgresql15 postgresql15-server postgresql15-contrib`

Примечание:

В случае распределенной установки для удаления Traffic Monitor выполните действия данной инструкции на каждом сервере.

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 «'».
- Пароль не должен быть вида «**%**<другие_символы>**%**», т.е. одновременно начинаться с символа «%» и заканчиваться им.

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/*
  - libcole.so – *arturo@directmail.org*; *andy.scriven@research.natpower.co.uk*
  - libhtmltree.so – *pauljlucas@mac.com*