

INFOWATCH

InfoWatch Traffic Monitor 7.9

Руководство по установке

14/01/2025

© 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 15

2.3 Требования к настройкам ОС и сети сервера 19

2.4 Настройка удаленной базы данных 20

2.4.1 Настройка СУБД 20

3 Установка Системы 26

3.1 Установка Data Storage 27

3.1.1 Подготовка сервера к установке Платформы 28

3.1.2 Установка Платформы 30

Чтобы установить Платформу в режиме central: 30

Чтобы установить Платформу в режиме office: 32

Установка Платформы в тихом режиме 33

3.2 Установка InfoWatch Traffic Monitor 35

3.2.1 Установка ТМ в режиме "Все-в-одном" 36

3.2.2 Распределенная установка ТМ 61

3.2.3 Установка в тихом режиме с файлом параметров 104

Файл параметров (option file) 109

Тихий режим установки 110

Полный состав файла параметров 111

3.3 Предустановленные серверные параметры 127

4 Обновление Системы 130

4.1 Обновление ТМ Все-в-одном (All-in-one) 135

4.1.1 Файл параметров (option file) 153

4.1.2 Тихий режим обновления 154

4.1.3 Полный состав файла параметров 155

4.2 Обновление ТМ при распределенной установке 161

4.2.1 Файл параметров (option file) 180

4.2.2 Тихий режим обновления 181

4.2.3 Полный состав файла параметров 182
4.3 Объединение конфигурационных файлов 191
4.3.1 Объединение конфигурационных файлов в Midnight Commander 192
4.3.2 Объединение конфигурационных файлов с помощью vimdiff 194
5 Удаление Системы 195
5.1 Удаление Data Storage 195
5.2 Удаление схемы базы данных 195
5.3 Удаление Traffic Monitor 197
6 Приложение A. Рекомендации по составлению имен и паролей 199
7 Приложение B. Лицензии на стороннее программное обеспечение 200

1 Введение

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

1.1 Аудитория

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

1.2 Комплект документов

В комплект документации по InfoWatch Traffic Monitor входят:

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

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

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

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

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

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

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

Содержит пояснения к часто используемым конфигурационным файлам.

1.3 Техническая поддержка пользователей

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

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

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

2 Подготовка к установке

В этой главе вы можете найти информацию о:

- схемах развертывания системы и возможных типах установки;
- программных и аппаратных требованиях;
- требованиях к настройкам ОС и сети сервера;
- настройке удаленной базы данных.

2.1 Схемы развертывания Системы и выбор типа установки

Система InfoWatch Traffic Monitor (далее также TM) может поставляться в нескольких вариантах. При этом имеет значение режим установки Системы и распределение компонентов.

В максимально развернутой конфигурации может выглядеть следующим образом:

- 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 и Агентов, распространяемых на рабочие станции компании.
- **Адаптеры**. Набор модулей перехвата для интеграции со сторонними системами.
- **Vision**. Модуль, предназначенный для визуализации расследования инцидентов на основе данных, полученных от InfoWatch Traffic Monitor.
- **Activity Monitor**. Модуль, предназначенный для контроля деятельности сотрудников.
- **Prediction**. Модуль предиктивной и поведенческой аналитики.
- **Data Discovery**. Модуль, предназначенный для поиска конфиденциальной информации на общих сетевых ресурсах, рабочих станциях, серверах и в хранилищах документов.
- **Data Analysis Service**. Сервис, предназначенный 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 вы можете использовать:

- Технологию анализа текстовых данных **Автолингвист**. Подробнее см. документ "*InfoWatch Traffic Monitor. Руководство пользователя*", раздел "Интерфейс Консоли управления Traffic Monitor" -> "Раздел "Технологии", статья "Автолингвист".
- **Data Explorer**. Программный продукт, позволяющий автоматизировать формирование политик DLP-системы с помощью выделения тематических кластеров документов в информационных потоках компании. Чтобы использовать Data Explorer, установите и настройте его. Подробнее см. документ " *InfoWatch Data Explorer. Руководство по установке, конфигурированию и администрированию*".

При развертывании Traffic Monitor вы можете:

- установить СУБД PostgreSQL поставляемую в дистрибутиве,
- либо подключиться к уже развернутой СУБД PostgreSQL.

В дополнение к базе данных может быть установлено внешнее хранилище бинарных данных Data Storage. Оно выполняет следующие функции:

- оптимизирует хранение данных;
- увеличивает производительность СУБД;
- ускоряет процесс обновления Traffic Monitor;
- существенно снижает нагрузку на БД при работе с большими объемами данных.

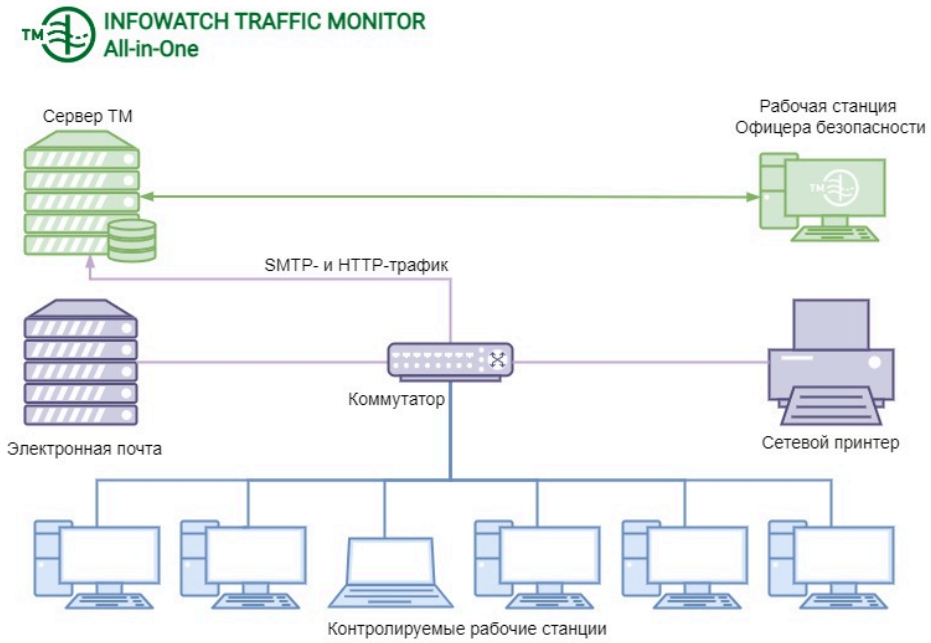
Data Storage может быть установлено как на один сервер с Traffic Monitor, так и на разные. Если количество рабочих станций в компании более 2000, рекомендуется устанавливать хранилище на отдельный сервер.

> **Важно!**
>
> Рекомендуется проверять функциональность Data Storage на тестовой группе рабочих станций и не устанавливать Data Storage в критической инфраструктуре.

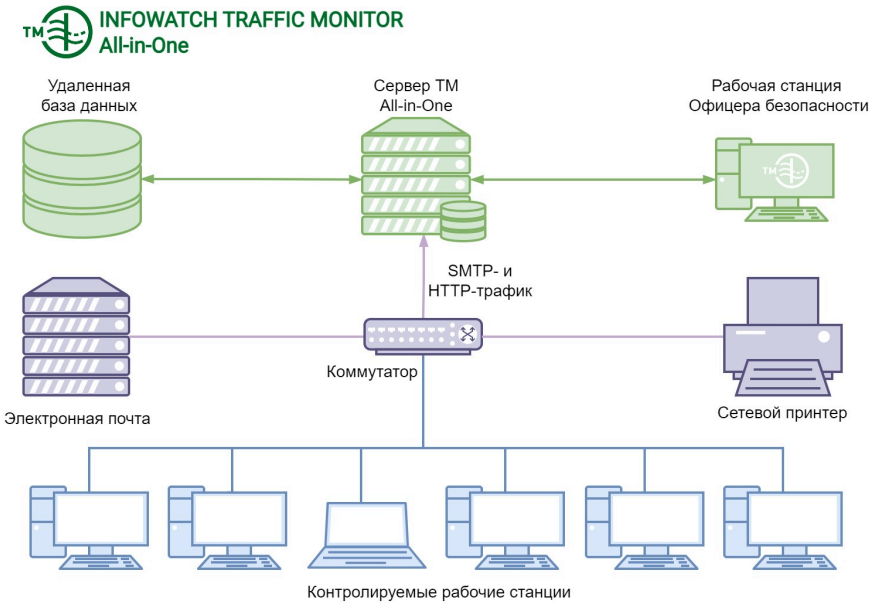
Типы установки Traffic Monitor

Traffic Monitor может быть установлен в одном из режимов:

- **All-in-One** (все-в-одном) – 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 представлен на схеме:

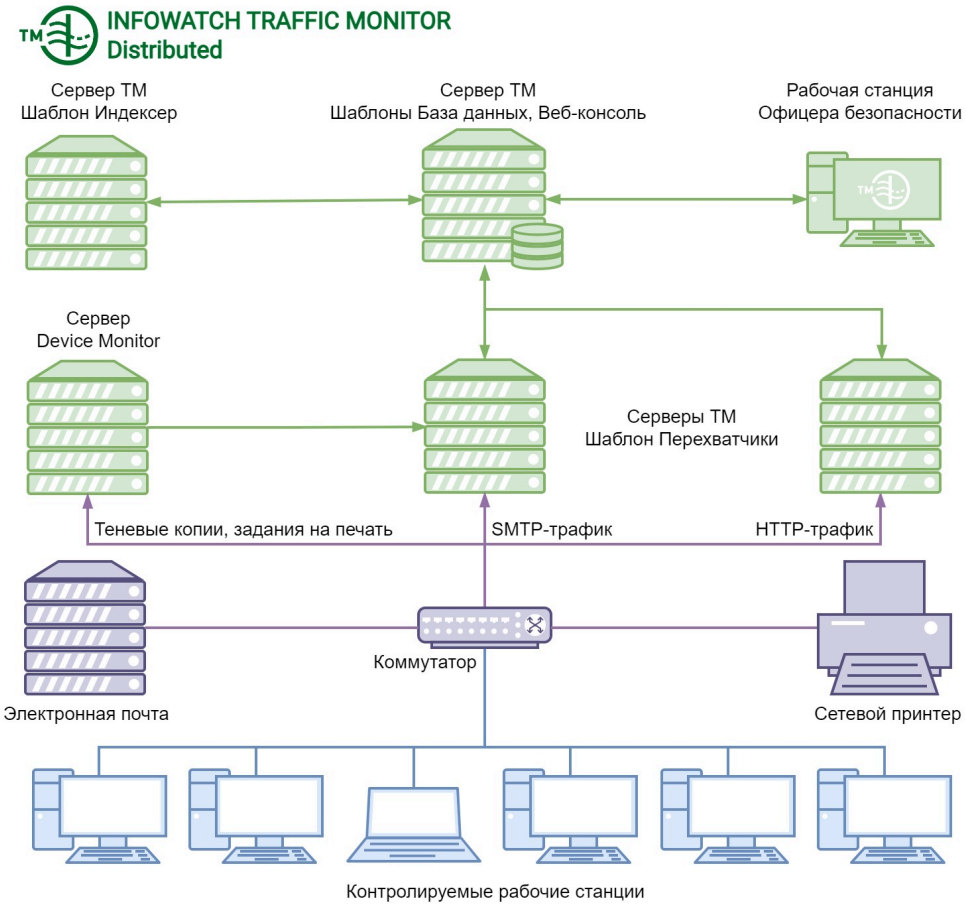


Пример развертывания Traffic Monitor All-in-One с подключением к удаленной базе данных:



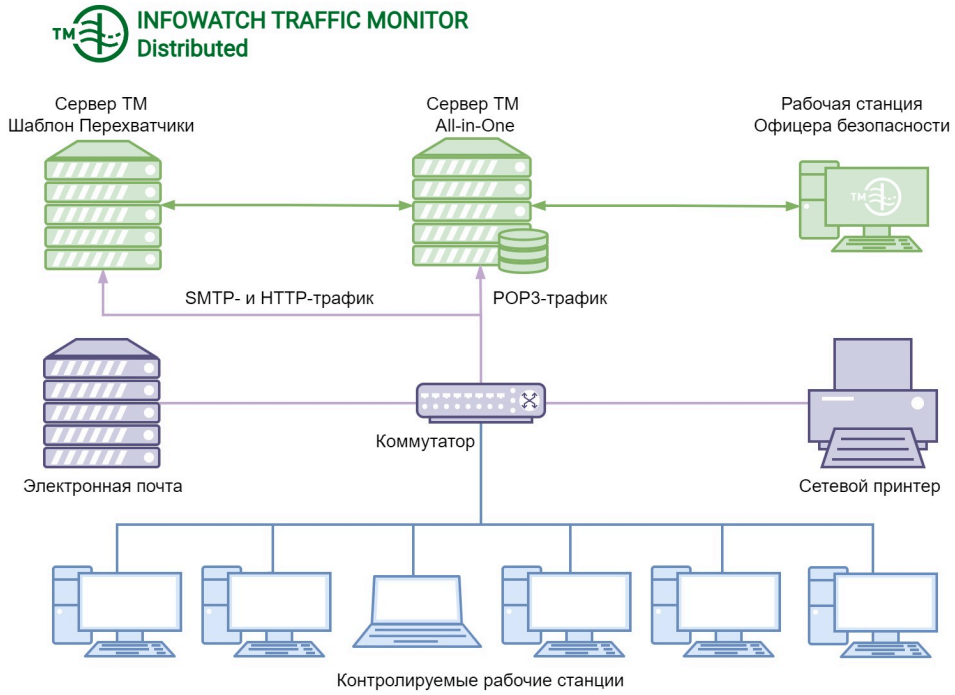
- **Distributed** (распределенная установка) – компоненты Traffic Monitor и СУБД устанавливаются на разные машины согласно их функциональным ролям. Распределенная установка позволяет увеличить производительность сервисов Traffic Monitor и СУБД путем их распределения по нескольким машинам с учетом предполагаемой нагрузки. Функциональные роли серверов определяются при помощи шаблонов. На схеме представлен пример развертывания Системы на нескольких

серверах:

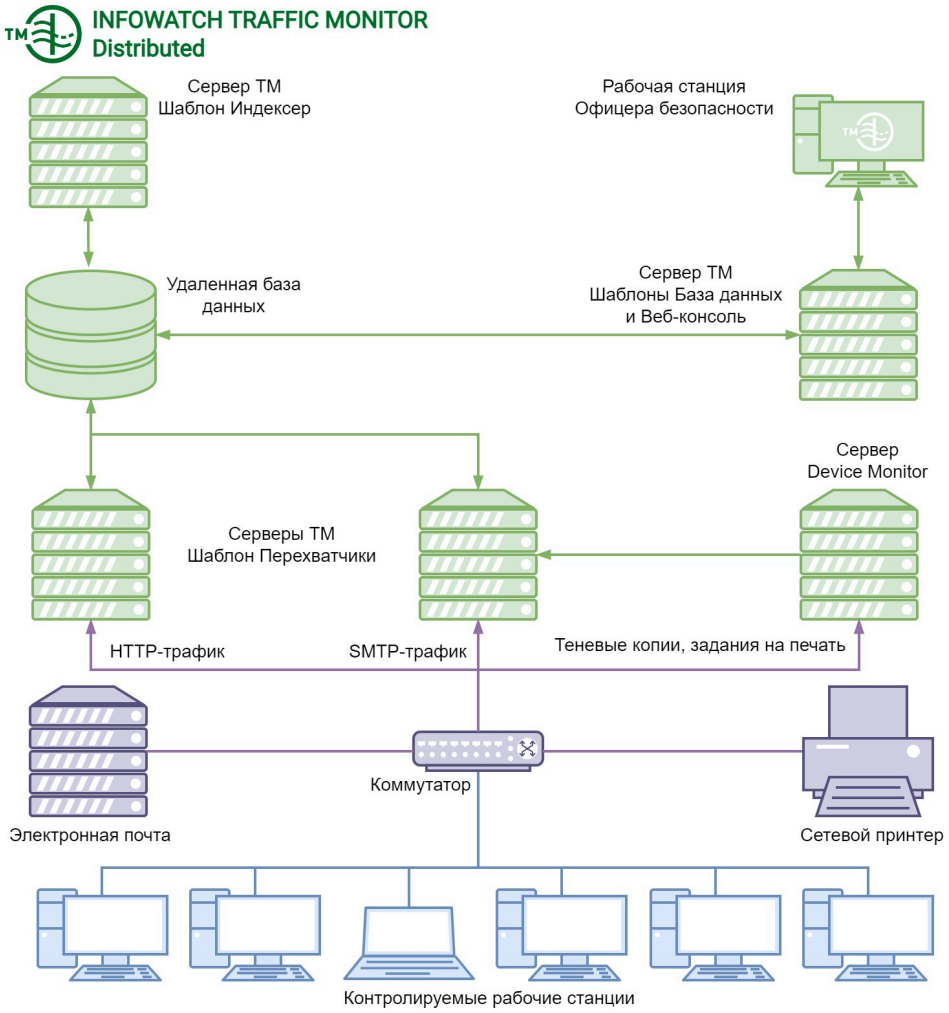


Сервер Traffic Monitor, установленный в режиме All-in-One, может использоваться при распределенной установке как один из компонентов Системы. Например, на схеме ниже сервер

All-in-One дополнен сервером перехвата:



Пример развертывания Traffic Monitor Distributed с подключением к удаленной базе данных:



Шаблоны установки

В инсталляторе Traffic Monitor реализована 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.

Независимо от выбранного шаблона, на сервер будут установлены все компоненты Traffic Monitor, шаблон же определяет набор активированных компонентов. При необходимости, после установки вы можете изменить набор активных компонентов на сервере.

На один сервер может быть установлено одновременно несколько шаблонов. Установка в режиме All-in-One является аналогом 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, который необходим для взаимодействия Системы с удаленной базой данных.

К шаблону База данных относятся следующие процессы:

Имя процесса	Краткое описание назначения
`iw_agent`	Требуется 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 событиях аудита. Модули шаблона позволяют выполнить 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`	Требуется для управления конфигурацией Системы
`iw_indexer`	Выполняет индексацию текста событий
`iw_is`	Выполняет индексацию метаданных
`iw_metainfo_fetcher`	Осуществляет выборку данных 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 осуществляется администрирование и управление Traffic Monitor: мониторинг сводной информации, создание политик и объектов защиты, добавление контактов, просмотр событий, выгрузка данных и формирование отчетов.

К шаблону Веб-консоль относятся следующие процессы:

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

Имя процесса	Краткое описание назначения
`iw_configerator`	Формирует конфигурацию для Агентов Device Monitor в части политик защиты данных на агентах
`iw_deliver`	Выполняет досылку писем из карантина по решению офицера безопасности при работе "в разрыв"
`iw_image_autoling`	Выполняет автоматическую классификацию графических объектов
`iw_kicker`	Компонент 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 отчётов.
`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, применение политик. Компоненты шаблона обеспечивают перехват трафика, передаваемого по протоколу SMTP, с поддержкой мандатных меток, и по протоколу ICAP.

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

В случае, когда показатель средней загрузки (load average) становится равным количеству ядер, рекомендуем горизонтально масштабировать серверы с ролью Перехватчики.

К шаблону Перехватчики относятся следующие процессы:

Имя процесса	Краткое описание назначения
`iw_agent`	Требуется для управления конфигурацией Системы
`iw_analysis`	Используется для проведения контентного анализа: • объектов от внешних 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_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_qmover_client`	Клиентская часть модуля для передачи объектов в удаленную базу данных. По умолчанию выключен
`iw_smtpd`	Принимает SMTP-письма. Поддерживается обработка мандатных меток на ОС Astra Linux Special Edition "Смоленск"
`iw_system_check`	Контролирует состояние Системы

Имя процесса	Краткое описание назначения
`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 внешних 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*», статья "Список процессов серверной части Traffic Monitor".

Важно!

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

2.2 Аппаратные и программные требования

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

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

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

- **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- и Linux-системах. *Требования см. в "InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию".*
- **Консоль управления** – автоматически устанавливается вместе с сервером Traffic Monitor и не предъявляет дополнительных программно-аппаратных требований к серверу. Для доступа к Консоли следует использовать браузер Google Chrome или Mozilla Firefox актуальной версии.
- **Внешнее хранилище бинарных данных Data Storage** – может быть установлено на одном сервере с Traffic Monitor или на разных. *Требования см. ниже.*

Для сервера Traffic Monitor аппаратно-программные требования варьируются в очень большом диапазоне.

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

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

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Сервер TM Enterprise, менее 10 GB трафика в день				
RAID-массив с fault tolerance: 600 GB	2CPU 8xC + Hyper-threading (Intel® Xeon® Processor E5-2640 v3 – частота 2,6 Hz)	24 GB	ОС Astra Linux Special Edition 1.7.5.9 уровней: • "Смоленск"; • "Воронеж"; • "Орел".	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков. Проверка цифровой подписи должна быть отключена.
Сервер TM Enterprise, от 10 до 50 GB трафика в день				
RAID-массив с fault tolerance	2SRVx2CPU 10xC	32-48 GB на каждый из серверов	ОС Astra Linux Special Edition	Сервер должен иметь сетевой интерфейс с

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			1.7.5.9 уровней: • "Смоленск"; • "Воронеж"; • "Орел".	назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков. Проверка цифровой подписи должна быть отключена.
Сервер TM Enterprise, более 50 GB трафика в день				
RAID-массив с fault tolerance	Рассчитывается по запросу	От 32GB на каждый из серверов	ОС Astra Linux Special Edition 1.7.5.9 уровней: • "Смоленск"; • "Воронеж"; • "Орел".	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков. Проверка цифровой подписи должна быть отключена.
Сервер БД PostgreSQL (Обеспечивает хранение трафика для 1-2 тыс. пользователей, сроком до 3 месяцев; в случае использования OCR и Device Monitor требования рассчитываются по запросу)				
RAID-массив с fault tolerance: 500 GB Для хранения логов действий (`xlog`) необходимо выделить директории `u01` дополнительное пространство, равное объему оперативной	2CPU от 6xC, 2,6 GHz	От 16GB и более в зависимости от объема данных, интенсивности вставки и обработки	ОС Astra Linux Special Edition 1.7.5.9 уровней: • "Смо	

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
памяти сервера БД. Если оперативной памяти меньше 20 GB, выделите под логи 20 GB.			• ленск"; • "Воронеж"; • "Орел".	
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 требуется 400 Гбайт. Тогда на сервере Traffic Monitor потребуется 60 Гбайт для базы данных. На сервере Data	–	–	ОС Astra Linux Special Edition 1.7.5.9 "Смоленск"	Для работы Data Storage должна быть установлена Платформа версии 2.0.0 и выше.

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Storage потребуется 340 Гбайт для хранения бинарных данных.				

Примечание:

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

2.3 Требования к настройкам ОС и сети сервера

Для успешной установки Системы сервер должен отвечать следующим требованиям:

- На сервере должна быть установлена ОС Astra Linux Special Edition (x64) 1.7.5.9;

  Важно!

  Не поддерживается работа с замкнутой программной средой (ЗПС). Для корректной работы не включайте данную опцию в ОС.

- Должен быть доступен базовый репозиторий `base`.
- Должны быть настроены репозитории ОС с возможностью установить пакеты:
  - `lsb-release`;
  - `lshw`;
  - `ntp`;
  - `ntpdate`;
  - `gsfonts`;
  - `libjemalloc2`
  - `libnewt0.52`;
  - `libwmf-bin`;
  - `libwmf0.2-7`;
  - `libxml2-utils`;
  - `liblzf1`
  - `python-newt;`
  - `redis-server`
  - `redis-tools`.

> **Примечание:**
>
> Если Traffic Monitor устанавливается на сервер без доступа в интернет, обеспечьте оффлайн-доступ к указанным репозиториям.
>
> Например, вы можете настроить локальные зеркала репозиториев.

- Минимальный объем Swap-пространства – 500MB (рекомендации приведены в статье "Рекомендации по разбиению дискового пространства серверов при установке в разных режимах").
- Просмотреть информацию о Swap-пространстве можно с помощью команды: `swapon -s`
- Опции точки монтирования не должны содержать `nosuid` и `noxattr` (можно проверить, открыв содержимое файла `/etc/fstab`);
- На сервере должны быть выполнены корректные сетевые настройки (в случае проблем с сетевыми параметрами обратитесь к системному администратору):
  - Внешний DNS-сервер должен преобразовывать ваше имя хоста (`hostname`) в тот же IP-адрес, который задан на одном из сетевых интерфейсов сервера;
  - IP-адрес должен принадлежать диапазонам частных IP-адресов:
    10.0.0.0 – 10.255.255.255 (RFC1918);
    172.16.0.0 – 172.31.255.255 (RFC1918);
    192.168.0.0 – 192.168.255.255 (RFC1918).
  - Должна выполняться команда:
    `ping -c 1 <hostname>`
    где `<hostname>` – ваше имя хоста.
    В результате выполнения команды должен быть успешно принят пакет.
  - Длина имени хоста (`hostname`) не должна превышать 15 символов;
- У пользователя должен быть необходимый для установки мандатный уровень доступа (63). Проверить мандатный уровень доступа пользователя можно командой `pdp-id -i`
- Антивирус на сервере должен быть настроен для совместной работы с Системой (см. статью базы знаний "Настройка антивируса на сервере Traffic Monitor").

2.4 Настройка удаленной базы данных

Если вы будете использовать уже развернутую базу данных PostgreSQL, перед установкой Системы обязательно выполните предварительную настройку.

> **Примечание:**
>
> На ОС Astra Linux поддерживается использование PostgreSQL 11.

2.4.1 Настройка СУБД

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

1. Установите дополнительные пакеты, выполнив команды:

```
dpkg -i postgresql-11-pathman_1.5.12-1.pgdg100+1_amd64.deb
apt-get install pgagent
apt-get install postgresql-contrib-11
```

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

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

3. Создайте директории для файлов и архивов, инициализируйте базу данных и смените директориям владельца и группу на `postgres` с помощью команд:

```
mkdir -p /u01/postgres
chown postgres:postgres /u01/postgres
locale -a | grep en_US.utf8 > /dev/null || echo "en_US.UTF-8 UTF-8" >> /etc/locale.gen
locale-gen
pg_dropcluster --stop 11 main
pg_createcluster -d /u01/postgres -p 5433 11 iwtm --locale=en_US.UTF-8 --encoding=UTF8
usermod -a -G shadow postgres
setfacl -d -m u:postgres:r /etc/parsec/macdb
setfacl -R -m u:postgres:r /etc/parsec/macdb
setfacl -m u:postgres:rx /etc/parsec/macdb
setfacl -d -m u:postgres:r /etc/parsec/capdb
setfacl -R -m u:postgres:r /etc/parsec/capdb
setfacl -m u:postgres:rx /etc/parsec/capdb
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
```

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

```
touch /etc/postgresql/11/iwtm/iwtm-postgres.conf
```

5. Добавьте в файл `/etc/postgresql/11/iwtm/iwtm-postgres.conf` следующее содержимое:

```
# -----------------------------
# 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,pg_pathman'
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 следующих параметров:

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

Выполните настройки перечисленных параметров в соответствии с официальной инструкцией (доступна на английском языке).

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

```
chown postgres:postgres /etc/postgresql/11/iwtm/iwtm-postgres.conf
```

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

```
echo "include = 'iwtm-postgres.conf'" >> /etc/postgresql/11/iwtm/postgresql.conf
```

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

```
echo "# Enable not local access" >> /etc/postgresql/11/iwtm/pg_hba.conf
echo "host    postgres        all             0.0.0.0/0               md5" >> /etc/
postgresql/11/iwtm/pg_hba.conf
```

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

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

10. Измените для администратора базы данных пароль по умолчанию:

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

11. Создайте требуемые 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 pg_pathman;
create extension if not exists pgagent;
```

12. Для выхода введите команды:

```
\q
exit
```

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

```
groupadd -f -r pgagent
useradd -g pgagent -r -s /bin/false -c "pgAgent Job Schedule" pgagent
mkdir -p /home/pgagent
chmod 0700 /home/pgagent
chown pgagent:pgagent /home/pgagent
touch /var/log/pgagent.log
chown pgagent:pgagent /var/log/pgagent.log
touch /home/pgagent/.pgpass
echo "localhost:5433:postgres:postgres:xxXX1234" > /home/pgagent/.pgpass
chmod 0600 /home/pgagent/.pgpass
chown pgagent:pgagent /home/pgagent/.pgpass
usermod -s /bin/bash pgagent
```

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

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

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

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

16. Для настройки сервиса `pgagent` создайте директорию и файл с помощью команд:

```
mkdir -p /usr/lib/systemd/system
touch /usr/lib/systemd/system/pgagent.service
```

17. Добавьте в файл `/usr/lib/systemd/system/pgagent.service` следующее содержимое:

```
[Unit]
Description=PgAgent for PostgreSQL
After=syslog.target
After=network.target
After=postgresql.service
After=postgresql@11-iwtm.service
BindsTo=postgresql.service
BindsTo=postgresql@11-iwtm.service
[Service]
Type=forking
User=pgagent
Group=pgagent
# Where to send early-startup messages from the server (before the logging
# options of pgagent.conf take effect)
# This is normally controlled by the global default set by systemd
```

```
# StandardOutput=syslog
# Disable OOM kill
OOMScoreAdjust=-1000
ExecStart=/usr/bin/pgagent -s /var/log/pgagent.log hostaddr=127.0.0.1 dbname=postgres
user=postgres port=5433
KillMode=mixed
KillSignal=SIGINT
# Give a reasonable amount of time for the server to start up/shut down
TimeoutSec=300
[Install]
WantedBy=multi-user.target
WantedBy=postgresql.service
WantedBy=postgresql@11-iwtm.service
```

18. Для применения изменений в конфигурации сервиса выполните команду::

```
systemctl daemon-reload
```

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

```
systemctl enable pgagent
systemctl start pgagent
systemctl status pgagent
```

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

3 Установка Системы

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

Инструкцию по установке внешнего хранилища бинарных данных Data Storage вы можете найти 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 в инсталляторе Traffic Monitor используются шаблоны. В зависимости от целевого назначения сервера, будет различаться набор активных компонентов.
О выборе типа установки и шаблонах см. "Схемы развертывания Системы и выбор типа установки".

Помимо установки из консоли сервера, доступен графический режим 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 параметры, запрашиваемые в процессе установки. Затем скопировать их вместе с дистрибутивами Traffic Monitor на серверы, где планируется развертывание Системы. После чего вы можете запустить на серверах установку в тихом режиме, указав соответствующие файлы параметров. В сочетании с системой шаблонов установки это позволяет также сократить участие пользователя в первичном развертывании Traffic Monitor.

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

- Установка InfoWatch Traffic Monitor
  - Установка TM в режиме "Все-в-одном"
  - Распределенная установка TM
  - 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:

- 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 требуется 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

Внешнее хранилище бинарных данных Data Storage является частью Платформы. Чтобы использовать Data Storage, необходимо установить Платформу. Это можно сделать одним из следующих способов:

- 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.
- Установить Платформу без продуктов. Данный тип установки описан ниже:
  1. Подготовка сервера к установке Платформы
  2. Установка Платформы

После установки Платформы:

- Вы можете приступить к установке Traffic Monitor, в ходе которой можно будет ввести параметры соединения с Data Storage.
  Одним из таких параметров является токен авторизации Data Storage.

> **Важно!**
>
> В целях повышения безопасности не рекомендуется 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, выполнив команду:
     `./setup.py tokens refresh DataStorageUser`
- В консоли управления продукта Платформы, 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.
  В этом случае токен можно обновить, нажав  .

- Если Платформа установлена на сервер, где уже установлен 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 Платформа установлена после Traffic Monitor, настройте соединение между Traffic Monitor и Data Storage. Подробнее см. "*InfoWatch Traffic Monitor. Руководство администратора* ", статья "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 Базы данных.

3.1.1 Подготовка сервера к установке Платформы

Перед установкой Платформы обязательно подготовьте сервер:

1. 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.
2. Настройте правила POD сети или отключите межсетевой экран (подробнее см. статьи Базы знаний "Конфликты при взаимодействии службы firewalld и Kubernetes", "Полное отключение межсетевого экрана"). В противном случае установка Платформы будет невозможна.
3. Для установки и корректной работы Платформы в ОС Astra Linux Special Edition убедитесь, что настройка безопасности *astra-nochmodx-lock* отключена.

Вы можете отключить эту настройку с помощью команды:
`astra-nochmodx-lock disable`

4. Если вы используете антивирус, настройте его для совместной работы с Платформой (см. статью Базы знаний "Настройка антивируса для продуктов Платформы").
5. 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 модуль не установлен, установите его с помощью команды:
   `apt-get install conntrack`
   Если пакет недоступен в репозитории, скачайте его, перейдите в директорию с пакетом и установите его вручную с помощью команды вида:
   `dpkg -i ./<имя_пакета>`
6. 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 PostrgeSQL, выполнив команды следующего вида:
```
systemctl stop pgagent
systemctl stop postgresql
```
c. Задайте нулевое значение параметру Huge Pages:
```
sysctl -w vm.nr_hugepages=0
```

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

d. Запустите СУБД PostgreSQL, выполнив команды следующего вида:
```
systemctl start pgagent
systemctl start postgresql
```
e. Запустите Систему:
```
iwtm start
```

3.1.2 Установка Платформы

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

Установка Платформы производится вручную, с помощью командной строки.

Для установки Платформы используется архив `iw_platform.tar.xz`. Архив входит в состав дистрибутива Traffic Monitor. Архив содержит полный набор бинарных модулей образов контейнеров, необходимых для развертывания Платформы без доступа к сети Интернет. Также архив содержит программу установки.

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

5. Запустите программу установки Платформы:

   ```
   ./setup.py install
   ```

   Если вы хотите хранить архивированные ежедневные табличные пространства на медленном диске сервера Data Storage, то запустите установку Платформы с параметром `--dsslowdatapath`:
   `./setup.py install --dsslowdatapath=/root/slowdisk`
   где `/root/slowdisk` – путь к медленному диску.
   Подробнее о табличных пространствах см.:
   - "*InfoWatch Traffic Monitor . Руководство администратора*", глава "Администрирование базы данных", статья "Архивирование ежедневных табличных пространств"
   - "*InfoWatch Traffic Monitor. Руководство пользователя*", статья "Управление табличными пространствами"
6. 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, предложенных по умолчанию, нажмите **Enter** без ввода значений.

7. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию: `80%`) и нажмите **Enter**.
8. Укажите путь для размещения данных Clickhouse (по умолчанию: `/mnt/chdata`) и нажмите **Enter**.
9. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/mnt/pgdata`) и нажмите **Enter**.
10. Укажите путь для размещения данных NATS (по умолчанию: `/mnt/natsdata`) и нажмите **Enter**.
11. Укажите путь для размещения бинарных данных (по умолчанию: `/mnt/dsdata`) и нажмите **Enter**.
12. Укажите порт подключения к веб-интерфейсу Платформы и нажмите **Enter**.

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

13. Дождитесь окончания процесса установки Платформы.
14. 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) Version: 2.0.0.1090
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
```

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

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

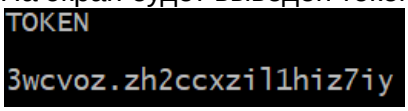
Установка в режиме office

Чтобы установить Платформу в режиме `office`:

1. Создайте новую директорию на диске (например, Platform):
   `mkdir Platform`
2. Скопируйте архив **`iw_platform.tar.xz`** в созданную директорию.
3. Перейдите в директорию, в которую был скопирован архив.
4. Распакуйте архив с дистрибутивом Платформы в эту директорию:
   `tar -xvf iw_platform.tar.xz`
5. Запустите программу установки Платформы:
   `./setup.py install --nodemode=office`

   Если вы хотите хранить архивированные ежедневные табличные пространства на медленном диске сервера Data Storage, то запустите установку Платформы с параметром `--dsslowdatapath`:
   `./setup.py install --nodemode=office --dsslowdatapath=/root/slowdisk`
   где `/root/slowdisk` – путь к медленному диску.
   Подробнее о табличных пространствах см.:
   - "*InfoWatch Traffic Monitor . Руководство администратора*", глава "Администрирование базы данных", статья "Архивирование ежедневных табличных пространств"
   - "*InfoWatch Traffic Monitor. Руководство пользователя*", статья "Управление табличными пространствами"
6. Укажите адрес центральной ноды кластера в формате IP-адреса или доменного имени (например: `192.0.2.0` или `host.example.com`).
7. 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`

8. 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.
9. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию: `80%`) и нажмите **Enter**.
10. Укажите путь для размещения данных Clickhouse (по умолчанию: `/mnt/chdata`) и нажмите **Enter**.
11. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/mnt/pgdata`) и нажмите **Enter**.
12. Укажите путь для размещения данных NATS (по умолчанию: `/mnt/natsdata`) и нажмите **Enter**.
13. Укажите путь для размещения бинарных данных (по умолчанию: `/mnt/dsdata`) и нажмите **Enter**.
14. Дождитесь окончания процесса установки Платформы.
15. Ознакомьтесь с отчетом об установке Платформы.

```
###Result###
Install product: Infowatch Platform(platform) Version: 2.0.0.1090
Install manifest section: office
Install node label: office
installed 15 components
updated   0 components
add ref   0 components
```

16. Чтобы вывести на экран информацию о Платформе, выполните команду:
`./setup.py showproducts`
17. 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 в тихом режиме

Установка Платформы в тихом режиме

Для минимизации участия в процессе установки Платформы, в инсталляторе предусмотрен тихий режим установки.

Чтобы запустить установку в тихом режиме:

1. Создайте новую директорию на диске (например, `Platform`):
`mkdir Platform`
2. Скопируйте архив с дистрибутивом Платформы **`iw_platform.tar.xz`** в созданную директорию.

3. Перейдите в директорию, в которую был скопирован архив.
4. Распакуйте архив в эту директорию:
   `tar -xvf iw_platform.tar.xz`
5. Выполните команду `./setup.py install`, указав параметры для установки.

Вы можете указать следующие параметры:

Параметр	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
`--advertise`	IP-адрес сетевого интерфейса для взаимодействия с кластером. Значение по умолчанию: `0.0.0.0` Не указывается в случае установки в режиме филиала.
`--chmemsize`	Объем оперативной памяти, используемой для данных ClickHouse. Значение по умолчанию: `80%`
`--chdbpath`	Путь для размещения данных ClickHouse. Значение по умолчанию: `/mnt/chdata`
`--pgdbpath`	Путь для размещения данных PostgreSQL. Значение по умолчанию: `/mnt/pgdata`
`--natspath`	Путь для размещения данных NATS. Значение по умолчанию: `/mnt/natsdata`
`--dsdatapath`	Путь для размещения бинарных данных. Значение по умолчанию: `/mnt/dsdata`
`--guiport`	Порт, по которому будет осуществляться подключение к веб-интерфейсу. Значение по умолчанию: `443.` Не указывается в случае установки в режиме филиала. **Важно!** При установке на один сервер с Traffic Monitor указывайте порт отличный от 443, так как по умолчанию порт 443 используется в качестве порта подключения к веб-интерфейсу Traffic Monitor.
`--cluster`	Адрес подключения к центральному офису. Указывается в случае установки в режиме филиала.

Параметр	Описание
`--clustertoken`	Токен подключения к центральному офису. Указывается в случае установки в режиме филиала. В центральном офисе можно: • получить токен, выполнив команду: `kubeadm token list` • создать токен с помощью команды: `kubeadm token create`
`--nodelabel`	Метка удаленного офиса. Указывается в случае установки в режиме филиала. В тексте метки можно использовать латинские буквы и цифры. Длина метки не должна превышать 32 символа.
`--dsslowdatapath`	Путь к медленному диску в случае, если вы планируете хранить на нем архивированные ежедневные табличные пространства. Пример: `--dsslowdatapath=/root/slowdisk`

Пример:

```
./setup.py install \
--advertise=0.0.0.0 \
--chmemsize=60% \
--chdbpath=/mnt/chdata \
--pgdbpath=/mnt/pgdata \
--natspath=/mnt/natsdata \
--dsdatapath=/mnt/dsdata \
--guiport=444
```

После установки 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 системы Traffic Monitor на операционную систему Astra Linux приведены в следующих разделах:

- Установка в режиме "Все-в-одном"
- Распределенная установка
- Установка в тихом режиме с файлом параметров

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

Важно!

Для установки InfoWatch Traffic Monitor на сервере должно быть установлено обновление ОС Astra Linux Special Edition 1.7.5.9.

Для установки Traffic Monitor потребуется репозиторий Astra Linux.
Вы можете использовать:

- локальный репозиторий с диска `base-1.7.5.9-16.10.23_16.58.iso`.
  О подключении локальных репозиториев вы можете прочитать в статье "Создание локальных и сетевых репозиториев" на официальном сайте компании-разработчика ОС Astra Linux.
- интернет-репозиторий `base`.
  О подключении интернет-репозиториев вы можете прочитать в статье "Интернет-репозитории Astra Linux Special Edition x.7" на официальном сайте компании-разработчика ОС Astra Linux. Убедитесь, что ОС Astra Linux использует загруженные сертификаты, способствующие подключению к репозиториям.

На сервере Traffic Monitor не будут задействованы перехватчики, работающие на шлюзе SNIFFER, поэтому следующие процессы окажутся выключенными:

- `iw_proxy_http`
- `iw_proxy_icq`
- `iw_proxy_smtp`
- `iw_sniffer`
- `iw_capstack`
- `iw_qmover_client`
- `iw_qmover_server`

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

Установка «все-в-одном» позволяет установить все компоненты Traffic Monitor на один компьютер. Данная установка аналогична установке всех шаблонов на один компьютер. Распаковка пакетов начнется непосредственно перед процессом установки, после указания всех параметров.

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

- текстовый в консоли сервера;
- графический.

Шаги установки и их последовательность аналогичны в обоих режимах.

Важно!

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

Если планируется использование удаленной базы данных, ее необходимо настроить.

Для установки InfoWatch Traffic Monitor на сервере должно быть установлено обновление ОС Astra Linux Special Edition 1.7.5.9.

Чтобы узнать версию установленной ОС, выполните команду:

```
cat /etc/astra_version
```

Для установки Traffic Monitor потребуется репозиторий Astra Linux.
Вы можете использовать:

- локальный репозиторий с диска `base-1.7.5.9-16.10.23_16.58.iso`.
  О подключении локальных репозиториев вы можете прочитать в статье

"Создание локальных и сетевых репозиториев" на официальном сайте компании-разработчика ОС Astra Linux.
- интернет-репозиторий `base`.
  О подключении интернет-репозиториев вы можете прочитать в статье "Интернет-репозитории Astra Linux Special Edition x.7" на официальном сайте компании-разработчика ОС Astra Linux. Убедитесь, что ОС Astra Linux использует загруженные сертификаты, способствующие подключению к репозиториям.
- локальный репозиторий с диска `base-1.7.5.9-16.10.23_16.58.iso` и несколько пакетов, которые необходимо установить дополнительно.
  Этот способ подходит для установки ТМ без доступа в интернет.

Независимо от выбранного режима работы инсталлятора выполните общие действия:

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

   Важно!

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

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

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

   Если вы устанавливаете Traffic Monitor с использованием установочного диска (без доступа в интернет):

   a. Переведите терминал в режим суперпользователя:
      `sudo su`
   b. Настройте сетевой интерфейс. Для этого:
      i. Откройте на редактирование файл `/etc/network/interfaces`.
      ii. В файле `interfaces` укажите значения параметров:

```
auto eth0
iface eth0 inet static
  address <IP-адрес интерфейса>
  netmask <маска подсети>
  gateway <IP-адрес шлюза>
  network <адрес сети>
  broadcast <канал сети>
```

> **Примечание:**
>
> Подробнее о параметрах см. статью "Настройка сетевых подключений в Astra Linux" в Справочном центре Astra Linux.

iii. Сохраните изменения и закройте файл.
iv. Включите сетевой интерфейс с помощью команды:
`ifup eth0`
v. Проверьте наличие файла `/etc/ resolv.conf` с настройками DNS. В случае его отсутствия создайте файл и укажите в нем имя домена и IP-адрес DNS-сервера. Используйте команду:
```
cat << EOF > /etc/resolv.conf
search <имя домена>
nameserver <IP-адрес DNS-сервера>
EOF
```

c. Подключите диск с дистрибутивом ОС Astra Linux к серверу.
d. Настройте репозиторий диска. Для этого:
i. Смонтируйте диск с помощью команды:
`mount /dev/cdrom /media/cdrom0`
ii. Откройте на редактирование файл `/etc/apt / sources.list`.
iii. В файле `sources.list` закомментируйте следующую строку, введя символ `#` в начало строки:
`deb cdrom:[OS Astra Linux 1.7.5 1.7_x86-64 devel]/ 1.7_x86-64 contrib main non-free`
iv. Внесите новую строку:
`deb file:///media/cdrom0 1.7_x86-64 contrib main non-free`
v. Сохраните изменения и закройте файл.
vi. Обновите пакеты с помощью команды:
`apt-get update`

> **Примечание:**
>
> В дальнейшей инструкции вы можете пропустить шаг 7, настраивающий репозитории в файле `sources.list`.

e. Измените IP-адрес в файле `hosts`. Для этого:
i. Откройте на редактирование файл `/etc/ hosts`.
ii. Во второй строке пропишите корректный IP-адрес вместо `127.0.1.1`.
iii. Сохраните изменения и закройте файл.

f. Установите следующие пакеты:
- `gsfonts_8.11+urwcyr1.0.7~pre44-4.4_all.deb`
- `libjemalloc2_5.1.0-3_amd64.deb`
- `liblzf1_3.6-3~bpo10+1_amd64.deb`
- `libnewt0.52_0.52.20-8_amd64.deb`
- `libwmf-bin_0.2.8.4-14_amd64.deb`
- `libwmf0.2-7_0.2.8.4-14_amd64.deb`

- `libxml2-utils_2.9.4+dfsg1-7+deb10u6+ci202308291455+astra2_amd64.deb`
- `python-newt_0.52.20-8_amd64.deb`
- `redis-server_7.0.13-1_amd64.deb`
- `redis-tools_7.0.13-1_amd64.deb`

Для этого:

i. Скачайте указанные пакеты из официальных репозиториев Astra Linux или Debian.
ii. Скопируйте их на сервер, куда будет установлен Traffic Monitor.
iii. Перейдите в каталог, куда были скопированы указанные пакеты.
iv. Выполните команду, которая установит пакеты:

```
dpkg -i python-newt_0.52.20-8_amd64.deb libnewt0.52_0.52.20-8_amd64.deb gsfonts_8.11+urwcyr1.0.7~pre44-4.4_all.deb libwmf-bin_0.2.8.4-14_amd64.deb libwmf0.2-7_0.2.8.4-14_amd64.deb libxml2-utils_2.9.4+dfsg1-7+deb10u6+ci202308291455+astra2_amd64.deb redis-server_7.0.13-1_amd64.deb redis-tools_7.0.13-1_amd64.deb libjemalloc2_5.1.0-3_amd64.deb liblzf1_3.6-3~bpo10+1_amd64.deb
```

> **Примечание:**
>
> Дополнительно вы можете установить утилиты `htop` и `screen` для работы с операционной системой, выполнив команду:
>
> ```
> apt install htop screen
> ```

g. Выйдите из режима суперпользователя:

```
exit
```

2. Чтобы включить службу SSH, выполните команды:

```
sudo systemctl enable ssh.service
sudo systemctl start ssh.service
```

3. Чтобы выставить уровень мандатного контроля целостности для пользователя `root`, в ОС Astra Linux Special Edition 1.7.5 уровня "Смоленск" выполните команду:

```
sudo pdpl-user -i 63 root
```

4. Чтобы изменения вступили в силу, заново войдите в вашу учетную запись:
   a. Введите команду для выхода:

```
exit
```

   b. Заново введите логин и пароль.

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

5. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой системы выполните следующую команду:

```
sudo mkdir /distr
```

6. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor:
   - **`iwtm-installer-x.x.x.xxx-astra-1.7`** (где `x.x.x.xxx` – номер сборки);
   - **`iwtm-postgresql-11.10-x.x.x.xxx-astra-1.7.tar.gz`**.

   В нашем примере:
   - **`iwtm-installer-7.9.0.150-astra-1.7`**;
   - **`iwtm-postgresql-11.10-7.9.0.150-astra-1.7.tar.gz`**.

   > **Примечание:**
   >
   > Инсталлятор и дальнейшие шаги установки подходят для ОС Astra Linux Special Edition 1.7.5.9 уровней "Смоленск", "Воронеж" и "Орел".

7. Проверьте содержимое файла `/etc/apt/`**`sources.list`**. В нем должны быть указаны локальные или внешние репозитории, требуемые для установки.

   > **Пример:**
   >
   > Если вы будете использовать локальные репозитории:
   >
   > a. Закомментируйте строки, описывающие подключение внешних репозиториев:
   > ```
   > #deb http://download.astralinux.ru/stable/1.7_x86-64/
   > repository-main/     1.7_x86-64 main contrib non-free
   > #deb http://download.astralinux.ru/stable/1.7_x86-64/
   > repository-update/   1.7_x86-64 main contrib non-free
   > #deb http://download.astralinux.ru/stable/1.7_x86-64/
   > repository-base/     1.7_x86-64 main contrib non-free
   > #deb http://download.astralinux.ru/stable/1.7_x86-64/
   > repository-extended/ 1.7_x86-64 main contrib non-free
   > ```
   > b. Убедитесь, что добавлено и не закомментировано описание подключения репозиториев с диска `base`.
   > В нашем примере строка вида:
   > ```
   > deb file:/mnt/ 1.7_x86-64 contrib main non-free
   > ```
   > В противном случае не должны быть закомментированы строки, описывающие подключение к внешним репозиториям.

   > **Важно!**
   >
   > Если ранее на сервере вы обновляли ОС, убедитесь, что в `/etc/apt/`**`sources.list`** указаны **только** репозитории ОС Astra Linux **1.7.5.9**. Если в файле указаны репозитории прошлых версий, отключите их.

8. Очистите кеш с помощью команды:
   ```
   sudo apt-get clean
   ```
9. Выполните следующую команду:
   ```
   sudo apt-get update
   ```
10. Проверьте наличие в системе сервисного файла `/etc/systemd/system/`**`rsyslog.service`**.

11. При наличии файла пропустите это действие.
    Если сервисного файла нет:
    a. Создайте его с нужным содержимым с помощью команды:

```
cat << EOF > /etc/systemd/system/rsyslog.service
[Service]
ExecStart=true
ExecStop=true

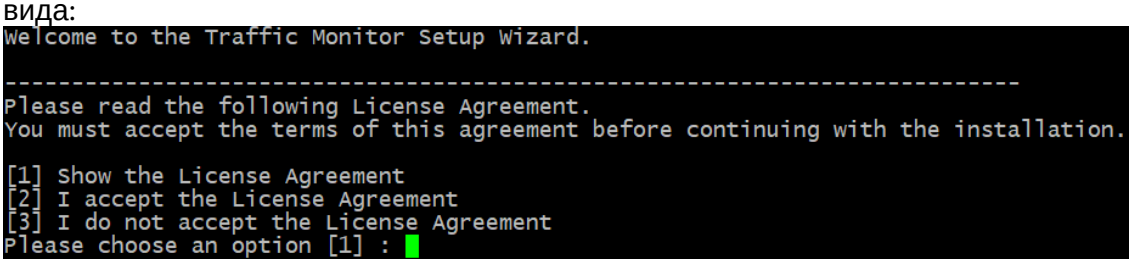
[Install]
WantedBy=multi-user.target
EOF
```

    b. Выполните команду:
    `systemctl daemon-reload`
12. Проверьте редакцию ОС, выполнив команду:
    `cat /etc/astra_license`
    Если используется ОС Astra Linux Special Edition 1.7.5.9 уровня "Орел", то дополнительно выполните команды:
    `sed -i 's/parsec.max_ilev=0/parsec.max_ilev=63/' /etc/default/grub`
    `update-grub`
    `reboot`
13. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
    В нашем примере:
    `cd /distr`
14. Перед запуском установки сделайте файл инсталлятора исполняемым. Для этого используйте команду вида:
    `sudo chmod +x ./iwtm-installer-x.x.x.xxx-astra-1.7`
    В нашем примере команда будет следующей:
    `sudo chmod +x ./iwtm-installer-7.9.0.150-astra-1.7`

Установка в текстовом режиме в консоли сервера

Чтобы установить Traffic Monitor в режиме «Все-в-одном» в консоли сервера, выполните следующие действия:

a. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
   `sudo ./iwtm-installer-x.x.x.xxx-astra-1.7`
   В нашем примере команда будет следующей:
   `sudo ./iwtm-installer-7.9.0.150-astra-1.7`
   Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов. По завершении на экране отобразится окно приветствия вида:



b. Для продолжения установки 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 установки.

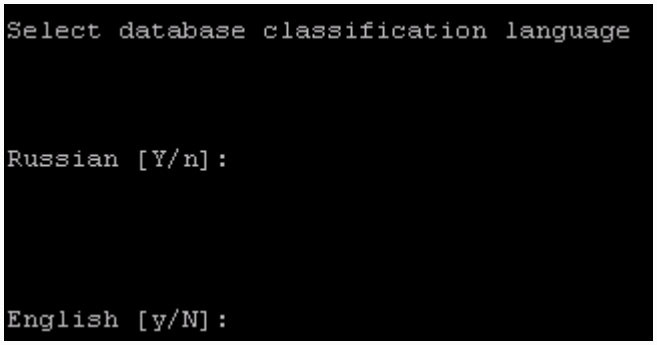
     > **Примечание:**
     >
     > При установке в консоли сервера перед полем ввода в квадратных скобках указано значение по умолчанию. Оно будет использовано, если оставить поле ввода пустым и нажать **Enter**.
     >
     > **Пример:**
     >
     > Если на изображении выше не вводить значение, а только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

c. На этапе выбора типа установки выберите `All in one`.
d. 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.
e. Выберите язык базы классификации. База классификации включает в себя предустановленные политики, элементы настройки технологий и объекты защиты. Вы можете выбрать одновременно несколько языков.
   Варианты будут предложены последовательно. Для использования предлагаемого варианта введите **Y**, для отказа от предложенного варианта введите **N**, 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:



Для выбора доступны:

- **`Russian`** – русский;
- **`English`** – английский;
- **`Malay`** – малайский.

Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.

f. 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.

g. Если выбрано использование удаленной базы данных, последовательно введите:
   i. IP-адрес или доменное имя сервера с базой данных.
   ii. Порт подключения.
   iii. Имя используемой базы данных, в которую будет добавлена схема.

h. 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 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.

i. 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.

j. 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 будет необходимо последовательно указать соответствующее число путей к ежедневным табличным пространствам.

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

k. 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.

l. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию – 90.
m. 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:
  i. Перейдите в директорию, куда был распакован дистрибутив Платформы;
  ii. 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 продукта Платформы, 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.

n. Укажите параметры подключения к службе Consul:
   i. `Network interface address` – выберите IP-адрес сетевого интерфейса.
   ii. `Datacenter name` – введите название дата-центра Consul.
o. 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 данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.
p. 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.

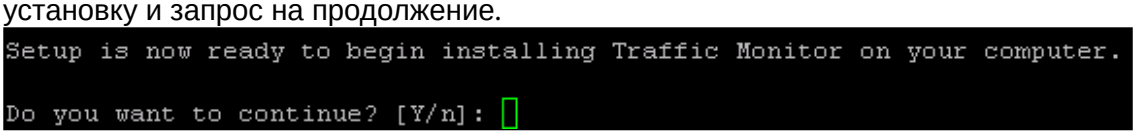
q. При необходимости вы можете изменить стандартные параметры работы службы Sphinx.
В этом случае будет предложено задать список языков с поддержкой морфологии. По этим языкам будет проводиться индексация.
Вы можете указать несколько языков, используя пробел в качестве разделителя.

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

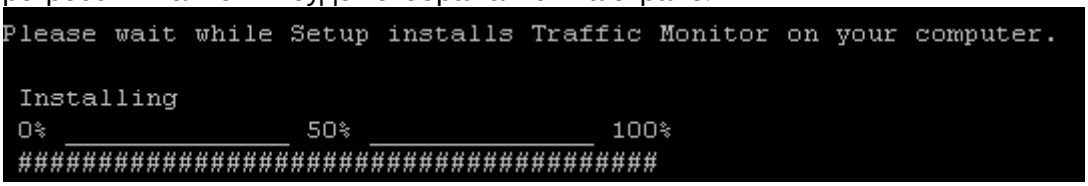
r. Вы можете включить использование технологии OCR.
В случае включения необходимо выбрать для использования одну из систем:
   - `ABBYY FineReader`;
   - `Tesseract`.

s. Если выбран OCR-экстрактор ABBYY Finereader:
   i. Выберите один из режимов распознавания:
      - `Quick` – быстрый режим;
      - `Quality` – тщательный режим, обеспечивающий более высокое качество распознавания.
   ii. Подтвердите наличие у вас активной лицензии на использование ABBYY Finereader.
   Если у вас отсутствует лицензия, введите **N** и нажмите **Enter**. В этом случае ABBYY Finereader будет установлен без лицензии. Для возможности работы ABBYY Finereader активную лицензию нужно будет добавить позже вручную. Подробнее смотрите в документе "*InfoWatch Traffic Monitor. Руководство администратора*" в статье "Настройка OCR-экстракторов".

t. 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.

u. 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:

```
\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:
`service iwtm-consul start`
Проверить статус службы можно командой:
`service iwtm-consul status`
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 при завершении работы, их нужно будет запустить вручную.

v. Для перехвата `smtp` с учетом мандатных меток на ОС Astra Linux Special Edition 1.7.5.9 "Смоленск":
i. Введите команду для вызова файлового менеджера:
`sudo mc`
ii. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
iii. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.
iv. Для выхода из файлового менеджера введите команду:
`exit`

w. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.

x. Если необходимо вывести список сервисов Traffic Monitor и их статусы, введите команду:
`iwtm status`

Примечание:

После установки Traffic Monitor не меняйте статус мандатных меток в ОС Astra Linux Special Edition 1.7.5.9 "Смоленск". Если до установки в ОС они были включены, не выключайте их, и наоборот.

В противном случае корректная работа Системы не гарантируется.

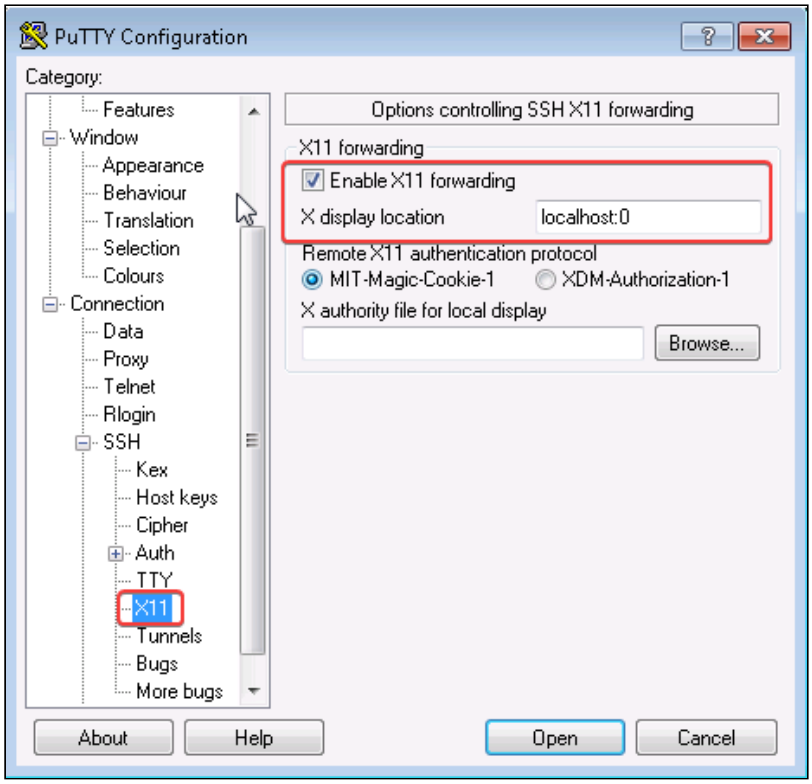
Установка с использованием графического режима инсталлятора

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. Данный режим реализуется с помощью SSH-подключения.

> **Примечание:**
>
> Если установка выполняется без удаленного подключения, непосредственно в графической среде сервера, достаточно просто запустить файл инсталлятора и перейти к установке шаблонов.

Чтобы установить Traffic Monitor в режиме «Все-в-одном» с использованием графического режима инсталлятора, выполните следующие действия:

a. На сервере, на котором планируется установка компонентов Traffic Monitor:
   i. Установите утилиту xauth с помощью команды:
   `sudo apt-get install xauth`
   ii. 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 `#`.
   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 серверу установки Traffic Monitor 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 установка компонентов Traffic Monitor, с помощью выбранного SSH-клиента.
   Пример окна настройки PuTTY при подключении



e. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:

```
sudo ./iwtm-installer-x.x.x.xxx-astra-1.7
```

В нашем примере команда будет следующей:

```
sudo ./iwtm-installer-7.9.0.150-astra-1.7
```

Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов. По завершении откроется окно приветствия вида:



Для перехода к следующему параметру используется кнопка **Вперед**, для

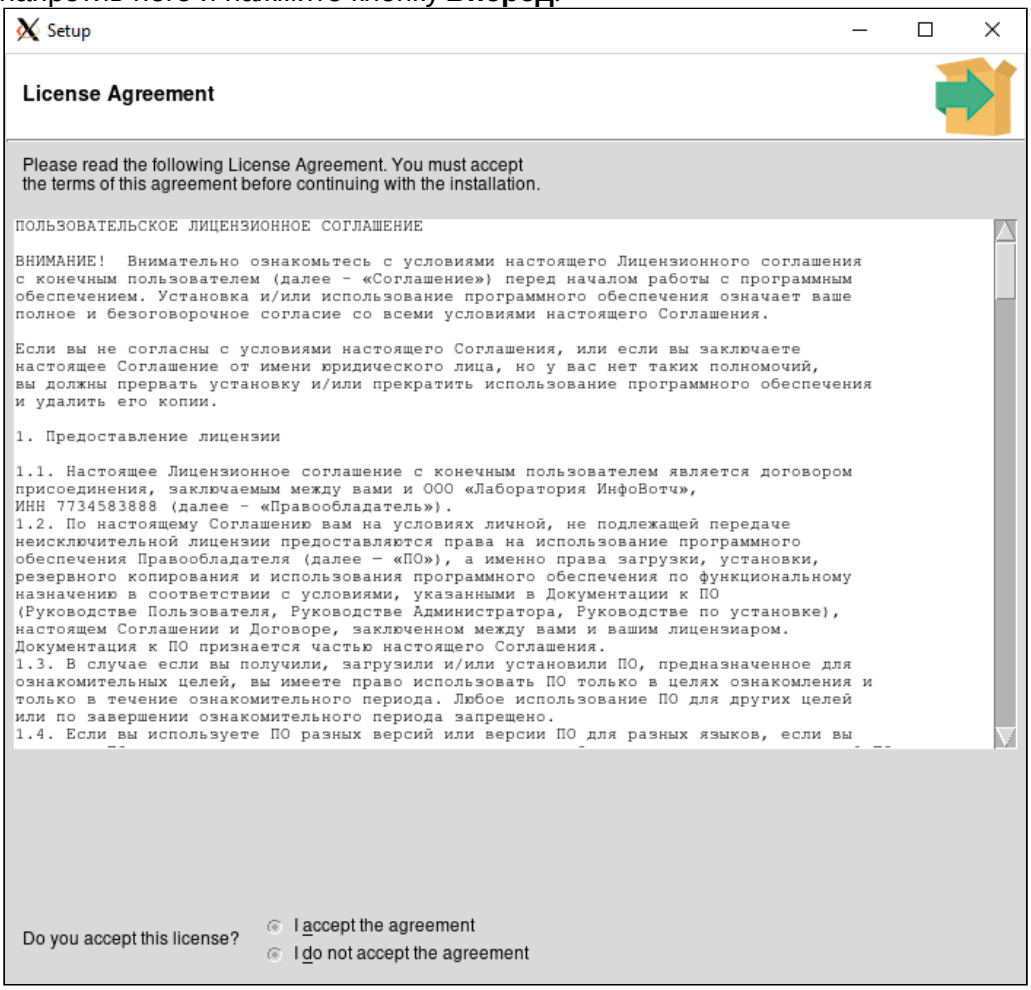
возврата к предыдущему – **Назад**. Для выхода из инсталлятора – кнопка **Отменить**.

f. Для продолжения установки 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 **Вперед**:



- `I accept the agreement` – чтобы принять Лицензионное соглашение и продолжить процесс установки;

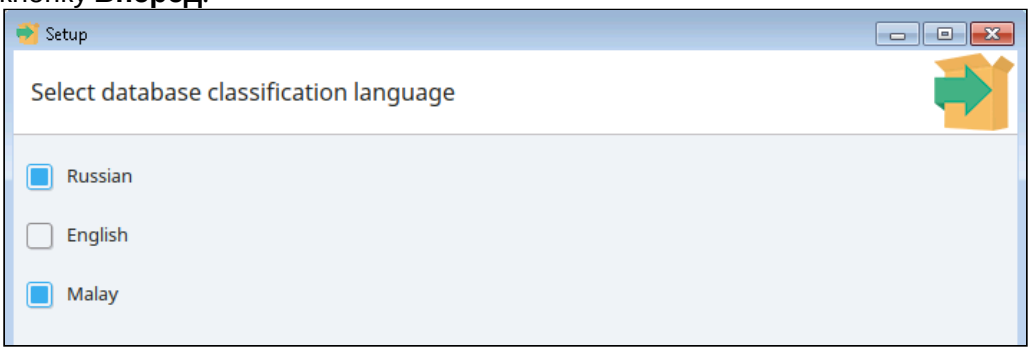
- `I do not accept the agreement` – чтобы не принимать Лицензионное соглашение и прервать процесс установки.

g. На этапе выбора типа установки выберите `All in one`.



h. 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.

i. Выберите язык базы классификации. База классификации включает в себя предустановленные политики, элементы настройки технологий и объекты защиты. Вы можете выбрать одновременно несколько языков.
Чтобы выбрать сразу несколько значений, отметьте их флажками и нажмите кнопку **Вперед**.



Для выбора доступны:
   - `Russian` – русский;
   - `English` – английский;
   - `Malay` – малайский.

Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.

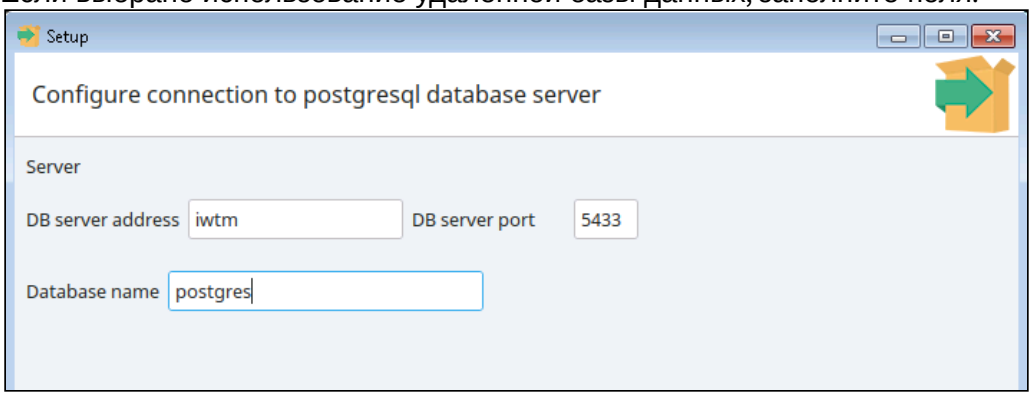
j. Выберите расположение базы данных:



   - `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.

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

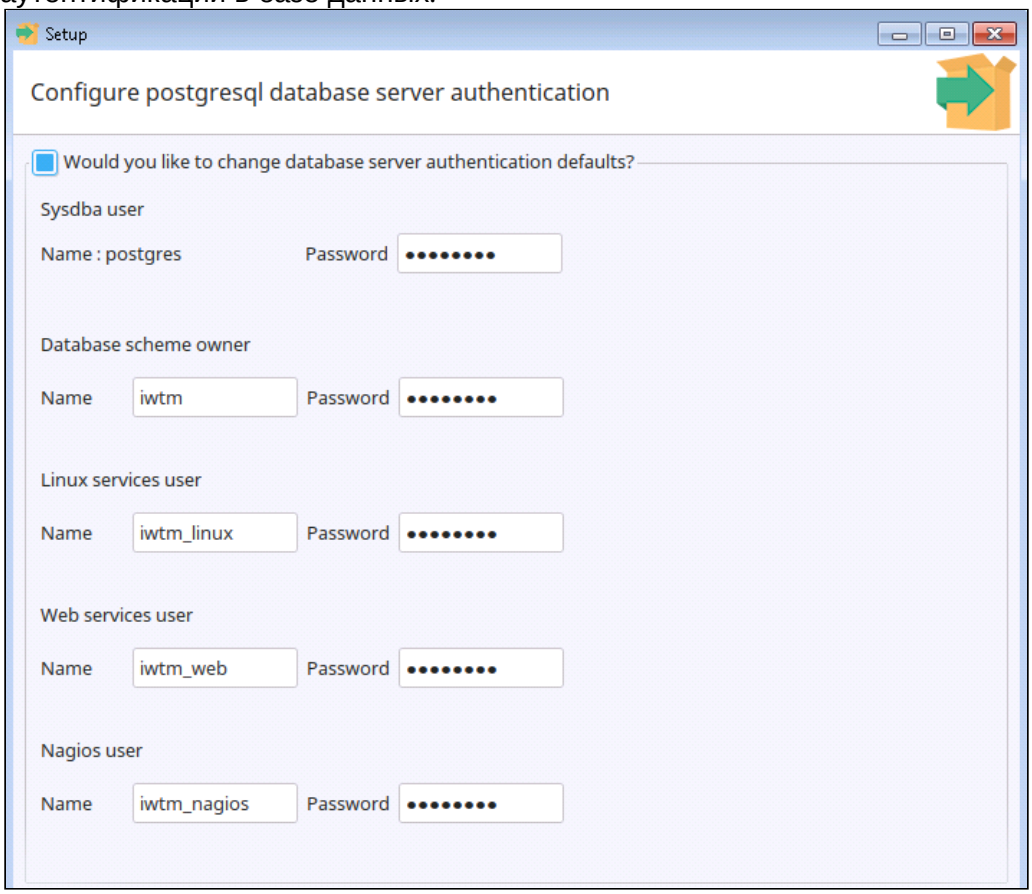


i. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.

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

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

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

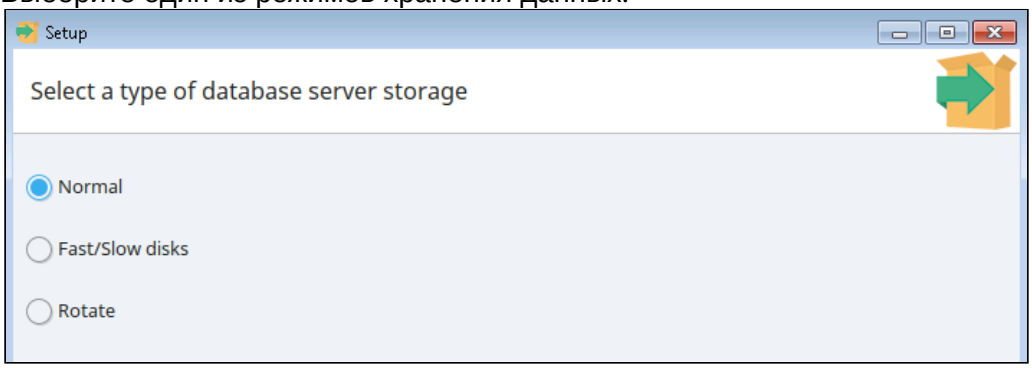


Чтобы отредактировать значения, установите флажок напротив поля с вопросом. Это сделает доступными для редактирования следующие разделы:

- **`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 кнопку **Вперед.** В этом случае поля останутся недоступны для редактирования, а инсталлятор использует значения по умолчанию.

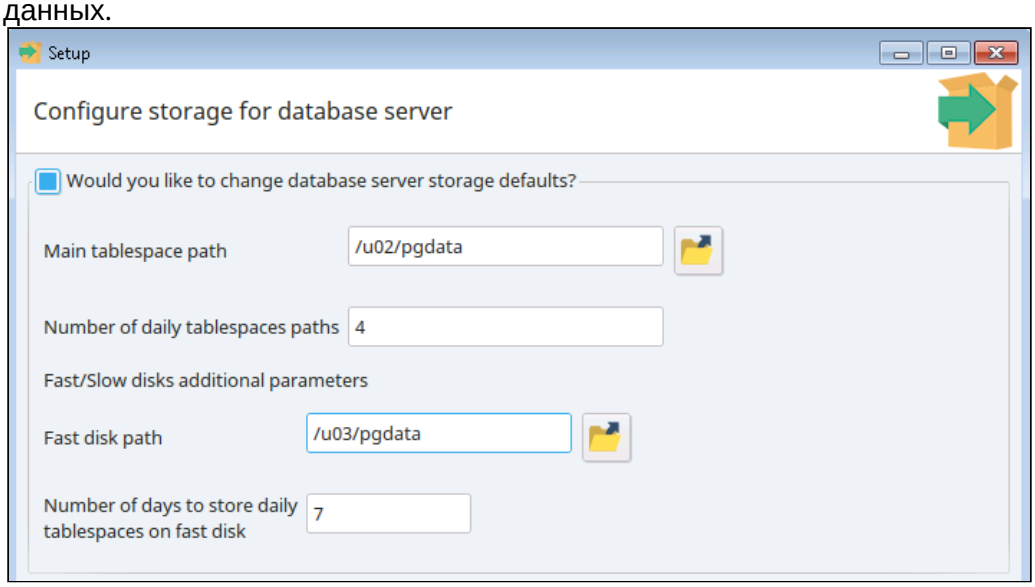
m. Выберите один из режимов хранения данных:



- **`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.

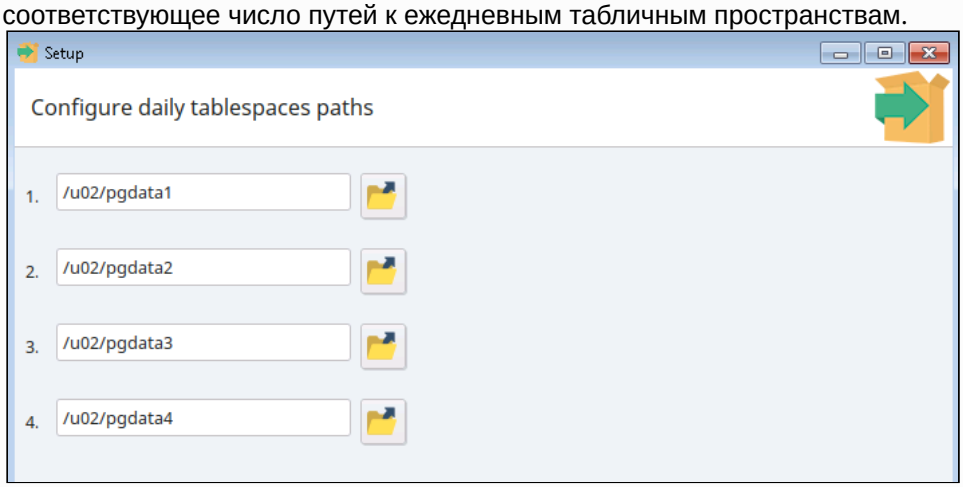
n. Вы можете изменить значения по умолчанию параметров хранения в базе данных.



- **`Main tablespaces path`** – путь к директории хранения данных основного табличного пространства;
  Вы можете вписать путь в поле или указать его в окне файлового менеджера, использовав кнопку .
- 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;

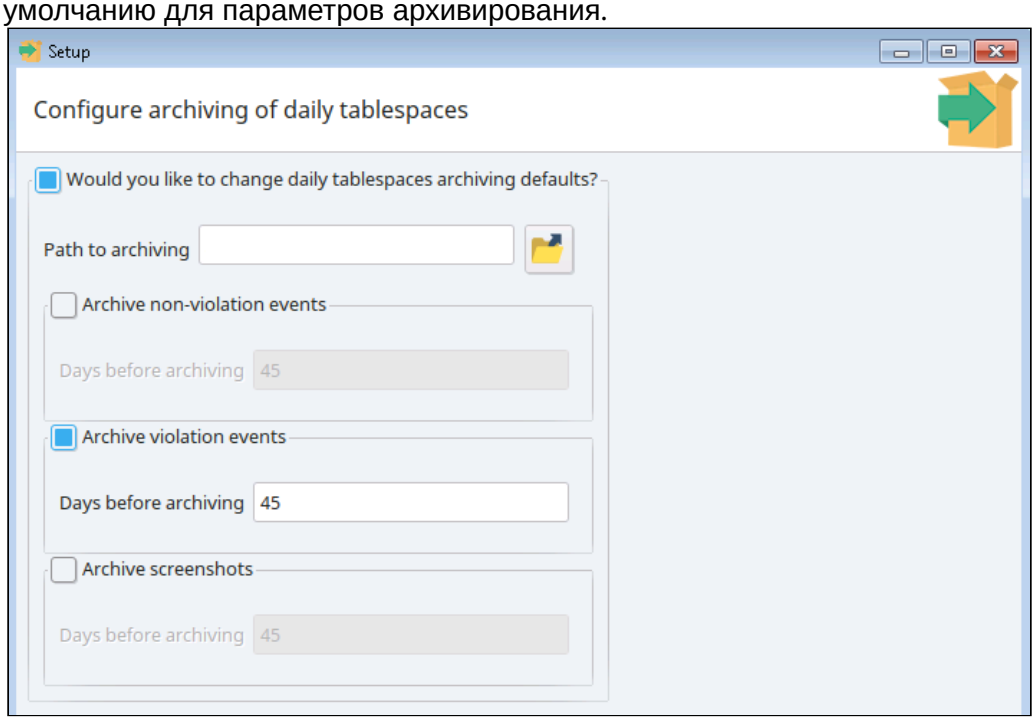
> **Примечание:**

Если указать значение больше 1, далее будет необходимо указать соответствующее число путей к ежедневным табличным пространствам.



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

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



- **`Path to archiving`** – путь к директории хранения файлов архивированных табличных пространств.

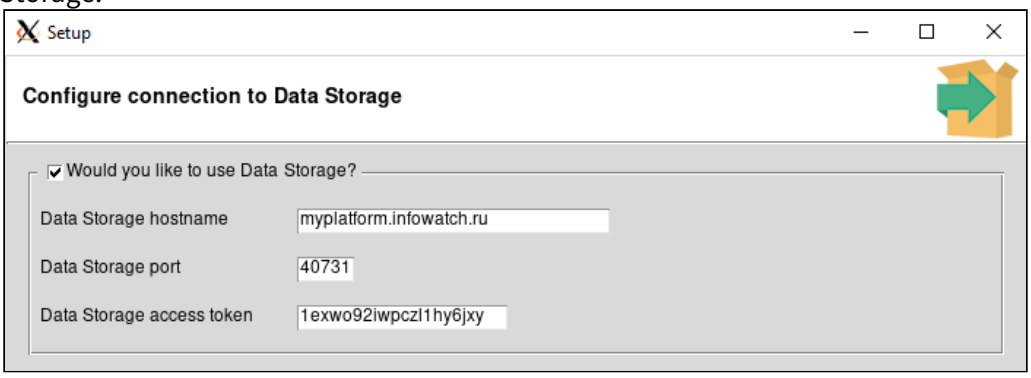
Использование каждого параметра включается отдельно:

- **`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.

p. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию – 90.

q. Вы можете включить использование внешнего хранилища бинарных данных Data Storage.



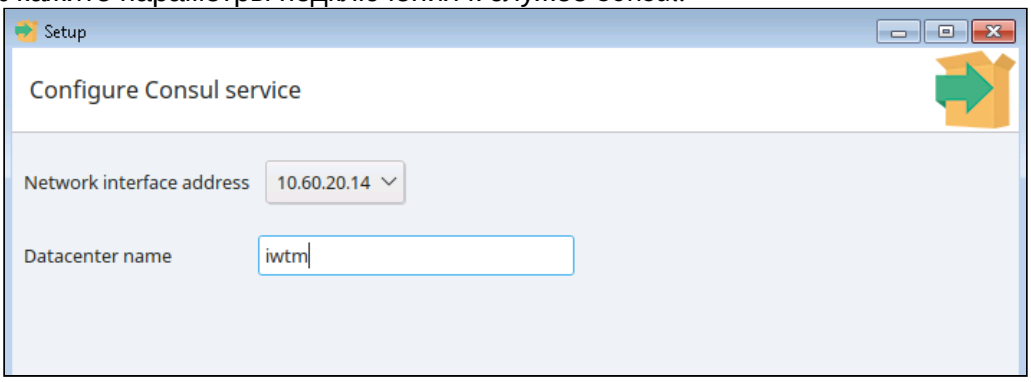
Для этого установите галочку напротив поля с вопросом и укажите параметры подключения к внешнему хранилищу:

- `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:
  i. Перейдите в директорию, куда был распакован дистрибутив Платформы;
  ii. 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 продукта Платформы, 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.

r. Укажите параметры подключения к службе Consul:

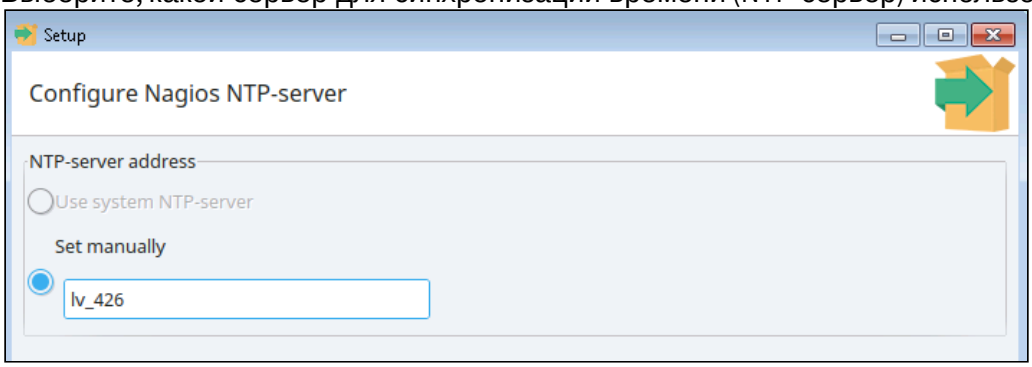


i. **`Network interface address`** – выберите IP-адрес сетевого интерфейса.

   Для выбора из списка параметров нажмите на кнопку  и в раскрывшемся списке выберите требуемое значение.

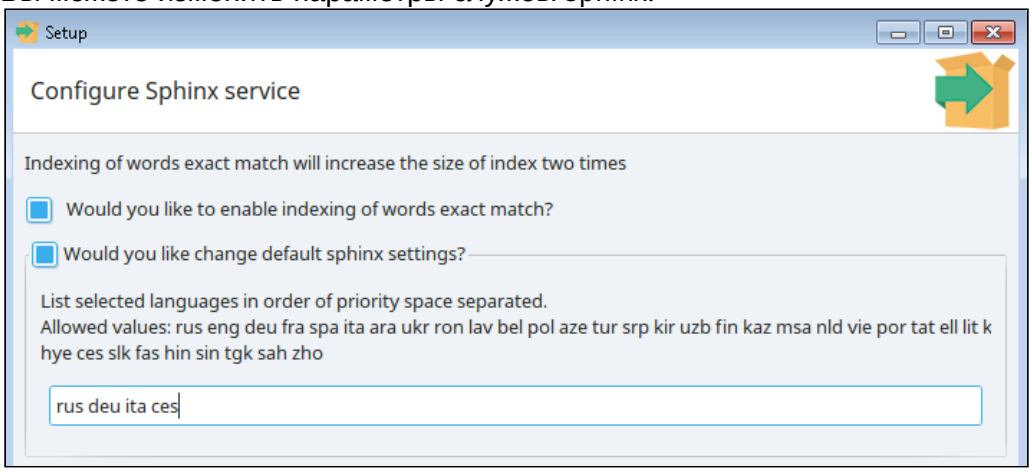
ii. **`Datacenter name`** – введите название дата-центра Consul.

s. 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 данного варианта укажите IP-адрес или имя доступного NTP-сервера.

t. Вы можете изменить параметры службы Sphinx:



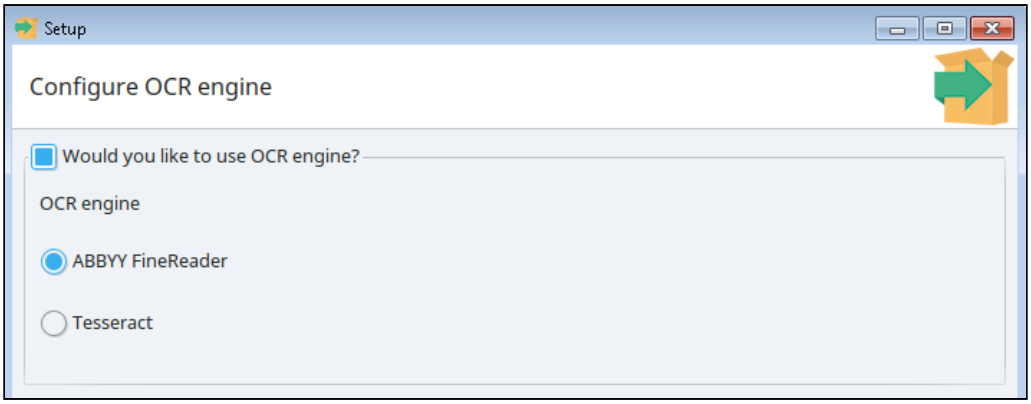
- **`Enable indexing of words exact match`** – включить индексацию на точное совпадение слов;

> **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, имеет самый высокий приоритет.

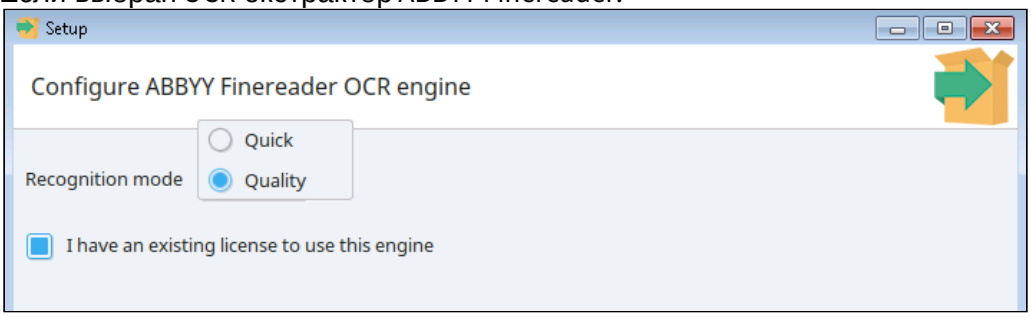
u. Вы можете включить использование технологии OCR.



В случае включения необходимо выбрать для использования одну из систем:

- **`ABBYY FineReader`**;
- **`Tesseract`**.

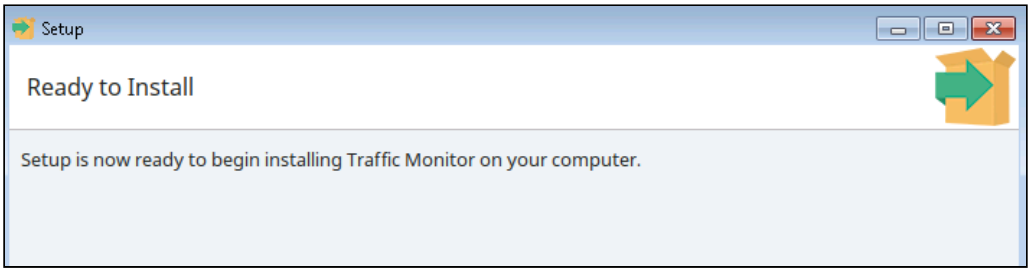
v. Если выбран OCR-экстрактор ABBYY Finereader:



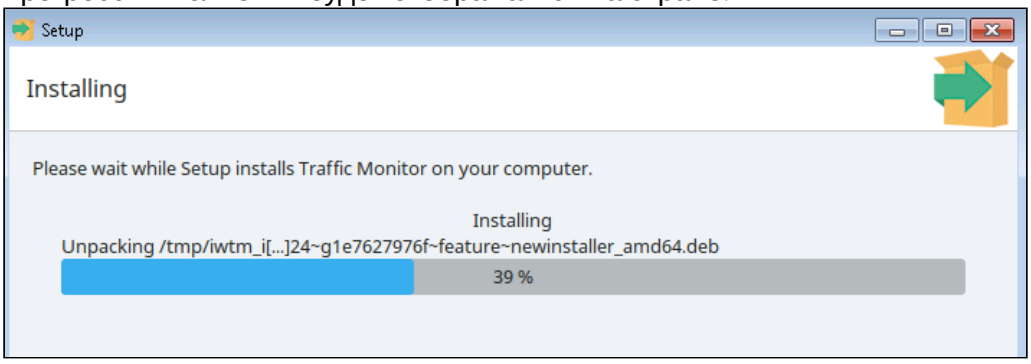
i. Выберите один из режимов распознавания (**`Recognition mode`**):
   - **`Quick`** – быстрый режим;
   - **`Quality`** – тщательный режим, обеспечивающий более высокое качество распознавания.

ii. Подтвердите наличие у вас активной лицензии на использование ABBYY Finereader.
   Если у вас отсутствует лицензия, не ставьте флажок в этом поле. В этом случае ABBYY Finereader будет установлен без лицензии. Для возможности работы ABBYY Finereader активную лицензию нужно будет добавить позже вручную. Подробнее смотрите в документе "*InfoWatch Traffic Monitor. Руководство администратора*" в статье "Настройка OCR-экстракторов".

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



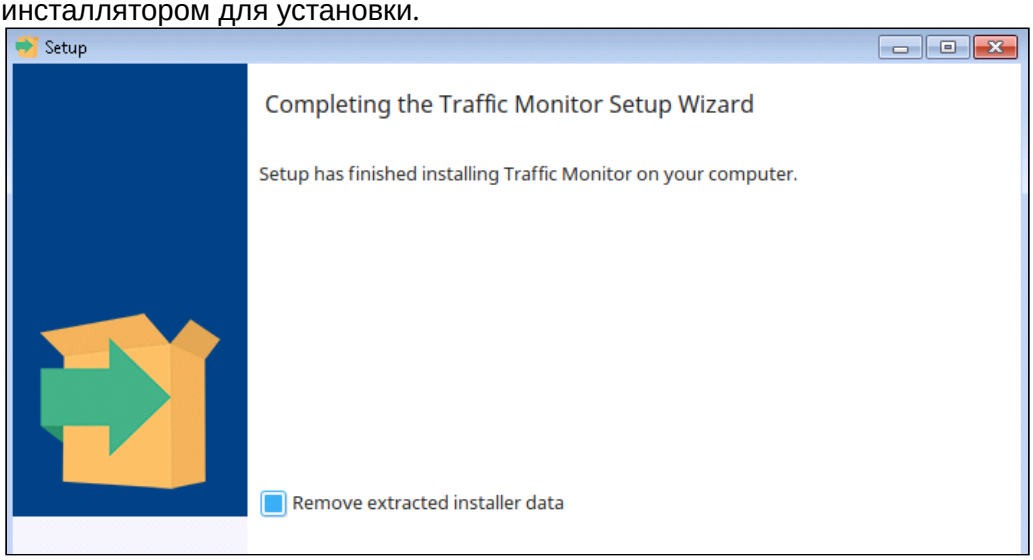
Для начала установки нажмите кнопку **Вперед**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor.
Прогресс выполнения будет отображаться на экране.



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.

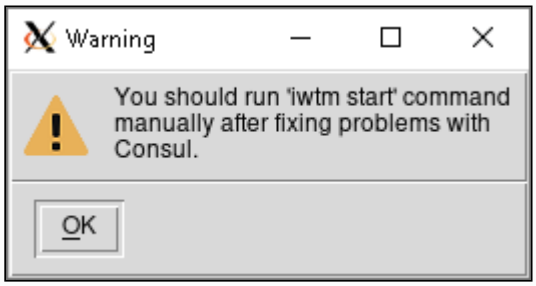
x. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.



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

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

i. Запустите службу Consul, выполнив команду:
`service iwtm-consul start`
Проверить статус службы можно командой:
`service iwtm-consul status`
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 при завершении работы, их нужно будет запустить вручную.

y. Для завершения нажмите кнопку **Finish**.
z. Для перехвата smtp с учетом мандатных меток на ОС Astra Linux Special Edition 1.7.5.9 "Смоленск":
i. Введите команду для вызова файлового менеджера:
`sudo mc`
ii. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
iii. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.
iv. Для выхода из файлового менеджера введите команду:
`exit`
aa. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
ab. Если необходимо вывести список сервисов Traffic Monitor и их статусы, в консоли сервера введите команду:
`iwtm status`

> **Примечание:**
>
> После установки Traffic Monitor не меняйте статус мандатных меток в ОС Astra Linux Special Edition 1.7.5.9 "Смоленск". Если до установки в ОС они были включены, не выключайте их, и наоборот.
>
> В противном случае корректная работа Системы не гарантируется.

15. Если ранее для установки вы создали файл `etc/systemd/system/rsyslog.service`:
    a. Вы можете удалить его с помощью команды:
    `rm /etc/systemd/system/rsyslog.service`
    b. В таком случае выполните команду:
    `systemctl daemon-reload`
16. Если используется ОС Astra Linux Special Edition 1.7.5.9 уровня "Орел", то выполните команды:
    `sed -i 's/parsec.max_ilev=63/parsec.max_ilev=0/' /etc/default/grub`
    `update-grub`
17. Перезагрузите сервер, выполнив команду:
    `reboot`

В результате установки в системе будут созданы учетные записи, приведенные в статье "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. документ «InfoWatch Traffic Monitor. Руководство администратора».

3.2.2 Распределенная установка ТМ

Traffic Monitor 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 производительно работать на одном сервере.

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 смотрите 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 может быть установлено одновременно 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 при установке с участием пользователя может работать в двух режимах:

- текстовый в консоли сервера;
- графический.

Шаги установки и их последовательность аналогичны в обоих режимах.

Важно!

Каждый сервер должен иметь уникальный корректный FQDN.

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

Если планируется использование удаленной базы данных, ее необходимо настроить.

Для установки InfoWatch Traffic Monitor на сервере должно быть установлено обновление ОС Astra Linux Special Edition 1.7.5.9.

Чтобы узнать версию установленной ОС, выполните команду:

```
cat /etc/astra_version
```

Для установки Traffic Monitor потребуется репозиторий Astra Linux.
Вы можете использовать:

- локальный репозиторий с диска `base-1.7.5.9-16.10.23_16.58.iso`.
  О подключении локальных репозиториев вы можете прочитать в статье "Создание локальных и сетевых репозиториев" на официальном сайте компании-разработчика ОС Astra Linux.
- интернет-репозиторий `base`.
  О подключении интернет-репозиториев вы можете прочитать в статье "Интернет-репозитории Astra Linux Special Edition x.7" на официальном сайте компании-разработчика ОС Astra Linux. Убедитесь, что ОС Astra Linux использует загруженные сертификаты, способствующие подключению к репозиториям.
- локальный репозиторий с установочного диска и несколько пакетов, которые необходимо установить дополнительно.
  Этот способ подходит для установки ТМ без доступа в интернет.

Независимо от выбранного режима работы инсталлятора выполните общие действия:

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

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

Если вы устанавливаете Traffic Monitor с использованием установочного диска (без доступа в интернет):

a. Переведите терминал в режим суперпользователя:
`sudo su`
b. Настройте сетевой интерфейс. Для этого:
   i. Откройте на редактирование файл `/etc/network/interfaces`.
   ii. В файле `interfaces` укажите значения параметров:
```
auto eth0
iface eth0 inet static
  address <IP-адрес интерфейса>
  netmask <маска подсети>
  gateway <IP-адрес шлюза>
  network <адрес сети>
  broadcast <канал сети>
```

> **Примечание:**
>
> Подробнее о параметрах см. статью "Настройка сетевых подключений в Astra Linux" в Справочном центре Astra Linux.

   iii. Сохраните изменения и закройте файл.
   iv. Включите сетевой интерфейс с помощью команды:
`ifup eth0`
   v. Проверьте наличие файла `/etc/ resolv.conf` с настройками DNS. В случае его отсутствия создайте файл и укажите в нем имя домена и IP-адрес DNS-сервера. Используйте команду:
```
cat << EOF > /etc/resolv.conf
search <имя домена>
nameserver <IP-адрес DNS-сервера>
EOF
```

c. Подключите диск с дистрибутивом ОС Astra Linux к серверу.
d. Настройте репозиторий диска. Для этого:
   i. Смонтируйте диск с помощью команды:
   `mount /dev/cdrom /media/cdrom0`
   ii. Откройте на редактирование файл `/etc/apt / sources.list`.
   iii. В файле `sources.list` закомментируйте следующую строку, введя символ `#` в начало строки:
   `deb cdrom:[OS Astra Linux 1.7.5 1.7_x86-64 devel ]/ 1.7_x86-64 contrib main non-free`
   iv. Внесите новую строку:
   `deb file:///media/cdrom0 1.7_x86-64 contrib main non-free`
   v. Сохраните изменения и закройте файл.
   vi. Обновите пакеты с помощью команды:
   `apt-get update`

> **Примечание:**
>
> В дальнейшей инструкции вы можете пропустить шаг 7, настраивающий репозитории в файле `sources.list`.

e. Измените IP-адрес в файле `hosts`. Для этого:
   i. Откройте на редактирование файл `/etc/ hosts`.
   ii. Во второй строке пропишите корректный IP-адрес вместо `127.0.1.1`.
   iii. Сохраните изменения и закройте файл.
f. Установите следующие пакеты:
   - `gsfonts_8.11+urwcyr1.0.7~pre44-4.4_all.deb`
   - `libjemalloc2_5.1.0-3_amd64.deb`
   - `liblzf1_3.6-3~bpo10+1_amd64.deb`
   - `libnewt0.52_0.52.20-8_amd64.deb`
   - `libwmf-bin_0.2.8.4-14_amd64.deb`
   - `libwmf0.2-7_0.2.8.4-14_amd64.deb`
   - `libxml2-utils_2.9.4+dfsg1-7+deb10u6+ci202308291455+astra2_amd64.deb`
   - `python-newt_0.52.20-8_amd64.deb`
   - `redis-server_7.0.13-1_amd64.deb`
   - `redis-tools_7.0.13-1_amd64.deb`

   Для этого:
   i. Скачайте указанные пакеты из официальных репозиториев Astra Linux или Debian.
   ii. Скопируйте их на сервер, куда будет установлен Traffic Monitor.
   iii. Перейдите в каталог, куда были скопированы указанные пакеты.
   iv. Выполните команду, которая установит пакеты:
   `dpkg -i python-newt_0.52.20-8_amd64.deb libnewt0.52_0.52.20-8_amd64.deb gsfonts_8.11+urwcyr1.0.7~pre44-4.4_all.deb libwmf-bin_0.2.8.4-14_amd64.deb libwmf0.2-7_0.2.8.4-14_amd64.deb libxml2-utils_2.9.4+dfsg1-7+deb10u6+ci202308291455+astra2_amd64.deb redis-server_7.0.13-1_amd64.deb redis-tools_7.0.13-1_amd64.deb libjemalloc2_5.1.0-3_amd64.deb liblzf1_3.6-3~bpo10+1_amd64.deb`

> **Примечание:**
>
> Дополнительно вы можете установить утилиты `htop` и `screen` для работы с операционной системой, выполнив команду:
>
> `apt install htop screen`

g. Выйдите из режима суперпользователя:
   `exit`

2. Чтобы включить службу SSH, выполните команды:
   `sudo systemctl enable ssh.service`
   `sudo systemctl start ssh.service`
3. Чтобы выставить уровень мандатного контроля целостности для пользователя `root`, в ОС Astra Linux Special Edition 1.7.5.9 уровня "Смоленск" выполните команду:
   `sudo pdpl-user -i 63 root`
4. Чтобы изменения вступили в силу, заново войдите в вашу учетную запись:
   a. Введите команду для выхода:
      `exit`
   b. Заново введите логин и пароль.

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

5. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой системы выполните следующую команду:
   `sudo mkdir /distr`
6. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor:
   - **`iwtm-installer-x.x.x.xxx-astra-1.7`** (где `x.x.x.xxx` – номер сборки);
   - **`iwtm-postgresql-11.10-x.x.x.xxx-astra-1.7.tar.gz`**.

   В нашем примере:
   - **`iwtm-installer-7.9.0.150-astra-1.7`**;
   - **`iwtm-postgresql-11.10-7.9.0.150-astra-1.7.tar.gz`**.

   > **Примечание:**
   >
   > Инсталлятор и дальнейшие шаги установки подходят для ОС Astra Linux Special Edition 1.7.5.9 уровней "Смоленск", "Воронеж" и "Орел".

7. Проверьте содержимое файла `/etc/apt/sources.list`. В нем должны быть указаны локальные или внешние репозитории, требуемые для установки.

   > **Пример:**

Если вы будете использовать локальные репозитории:

a. Закомментируйте строки, описывающие подключение внешних репозиториев:
```
#deb http://download.astralinux.ru/stable/1.7_x86-64/
repository-main/     1.7_x86-64 main contrib non-free
#deb http://download.astralinux.ru/stable/1.7_x86-64/
repository-update/   1.7_x86-64 main contrib non-free
#deb http://download.astralinux.ru/stable/1.7_x86-64/
repository-base/     1.7_x86-64 main contrib non-free
#deb http://download.astralinux.ru/stable/1.7_x86-64/
repository-extended/ 1.7_x86-64 main contrib non-free
```
b. Убедитесь, что добавлено и не закомментировано описание подключения репозиториев с диска `base`.
В нашем примере строка вида:
```
deb file:/mnt/ 1.7_x86-64 contrib main non-free
```

В противном случае не должны быть закомментированы строки, описывающие подключение к внешним репозиториям.

Важно!

Если ранее на сервере вы обновляли ОС, убедитесь, что в `/etc/apt/sources.list` указаны **только** репозитории ОС Astra Linux **1.7.5.9**. Если в файле указаны репозитории прошлых версий, отключите их.

8. Очистите кеш с помощью команды:
`sudo apt-get clean`
9. Выполните следующую команду:
`sudo apt-get update`
10. Проверьте наличие в системе сервисного файла `/etc/systemd/system/rsyslog.service`.
11. При наличии файла пропустите это действие.
Если сервисного файла нет:
    a. Создайте его с нужным содержимым с помощью команды:
    ```
    cat << EOF > /etc/systemd/system/rsyslog.service
    [Service]
    ExecStart=true
    ExecStop=true

    [Install]
    WantedBy=multi-user.target
    EOF
    ```
    b. Выполните команду:
    `systemctl daemon-reload`
12. Проверьте редакцию ОС, выполнив команду:
`cat /etc/astra_license`
Если используется ОС Astra Linux Special Edition 1.7.5.9 уровня "Орел", то дополнительно

выполните команды:

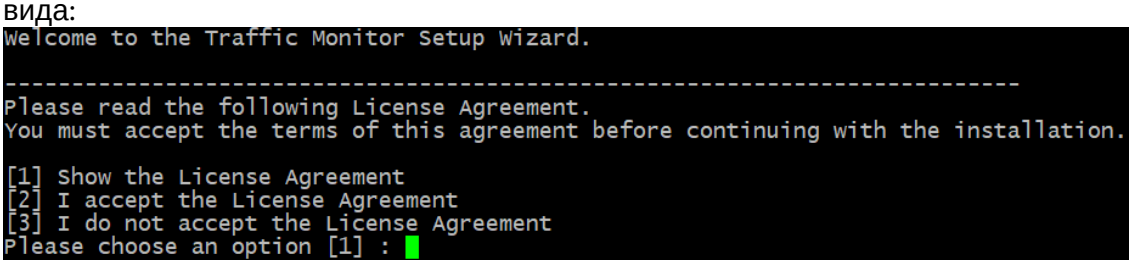
```
sed -i 's/parsec.max_ilev=0/parsec.max_ilev=63/' /etc/default/grub
update-grub
reboot
```

13. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
В нашем примере:
```
cd /distr
```
14. Перед запуском установки сделайте файл инсталлятора исполняемым. Для этого используйте команду вида:
```
sudo chmod +x ./iwtm-installer-x.x.x.xxx-astra-1.7
```
В нашем примере команда будет следующей:
```
sudo chmod +x ./iwtm-installer-7.9.0.150-astra-1.7
```

Установка в текстовом режиме в консоли сервера

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

a. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
```
sudo ./iwtm-installer-x.x.x.xxx-astra-1.7
```
В нашем примере команда будет следующей:
```
sudo ./iwtm-installer-7.9.0.150-astra-1.7
```
Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов. По завершении на экране отобразится окно приветствия вида:



b. Для продолжения установки 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;

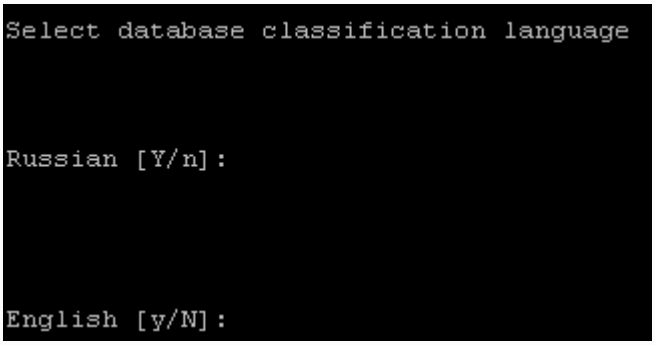
     При выборе этого варианта:

     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 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:**
>
> 
>

c. На этапе выбора типа установки укажите `Distributed`.
d. Далее с помощью выбора шаблонов вы можете последовательно указать, какие наборы компонентов необходимо 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 будет использована удаленная база данных, устанавливайте шаблон База данных вместе с ещё хотя 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

i. Запустите службу Consul, выполнив команду:
`service iwtm-consul start`
Проверить статус службы можно командой:
`service iwtm-consul status`
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 при 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`):

a. 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.

b. Выберите язык базы классификации. База классификации включает в себя предустановленные политики, элементы настройки технологий и объекты защиты. Вы можете выбрать одновременно несколько языков.
Варианты будут предложены последовательно. Для выбора доступны:
- **`Russian`** – русский;
- **`English`** – английский;
- **`Malay`** – малайский.

Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.

c. 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.

d. Если выбрано использование удаленной базы данных, последовательно введите:
i. IP-адрес или доменное имя сервера с базой данных.
ii. Порт подключения.
iii. Имя используемой базы данных, в которую будет добавлена схема.

e. 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 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.

f. 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.

g. 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 будет необходимо последовательно указать пути к соответствующему числу ежедневных табличных пространств.

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

h. 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.

i. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию – 90.

j. 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:
  i. Перейдите в директорию, куда был распакован дистрибутив Платформы;
  ii. 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 продукта Платформы, 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.

k. Укажите параметры подключения к службе Consul:
  i. `Network interface address` – выберите IP-адрес сетевого интерфейса.
  ii. Режим работы Consul. Доступны два режима:
    - `Server`
    - `Client`

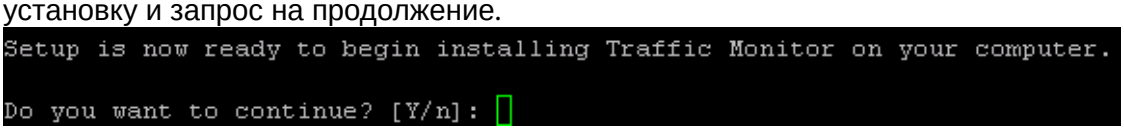
    > **Важно!**
    >
    > В одно кластере должно быть нечетное число серверов Consul, не больше 5.

  iii. `Datacenter name` – введите название дата-центра Consul. По умолчанию – `iwtm`.

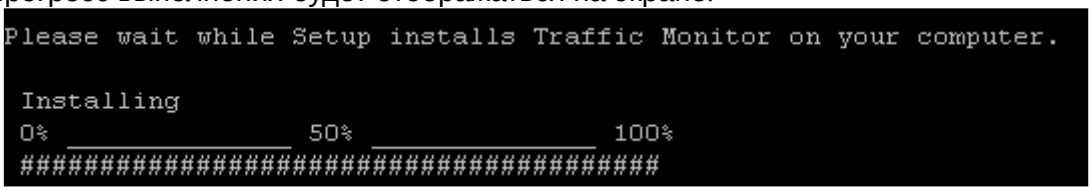
iv. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
v. **`Consul retryjoin servers`** – список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.
vi. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

l. 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 данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.

m. 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.

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

Установка шаблона Индексер

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

a. Последовательно укажите параметры подключения к базе данных:
i. IP-адрес или доменное имя сервера с базой данных.
ii. Порт подключения.
iii. Имя используемой базы данных.
b. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.

В случае утвердительного ответа будет предложено поменять следующие параметры:

- Имя пользователя сервисов Linux;
- Пароль пользователя сервисов Linux;
- Имя пользователя веб-сервисов;
- Пароль пользователя веб-сервисов;
- Имя пользователя nagios;
- Пароль пользователя nagios.

c. Укажите параметры подключения к службе Consul:
   i. `Network interface address` – выберите IP-адрес сетевого интерфейса.
   ii. Режим работы Consul. Доступны два режима:
      - `Server`
      - `Client`

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

   iii. `Datacenter name` – введите название дата-центра Consul. По умолчанию – `iwtm`.
   iv. `Node name` – имя сервера, на который устанавливаются компоненты Traffic Monitor.
   v. `Consul retryjoin servers` – список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.
   vi. `Consul retryjoin port` – порт подключения к указанным серверам Consul.

d. 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 данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.

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

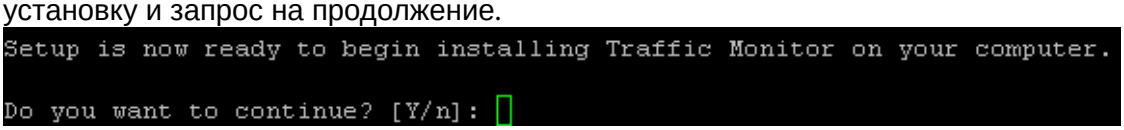
   > **Важно!**
   >
   > Включение индексации на точное совпадение, увеличит размер индекса минимум в 2 раза.

f. 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.

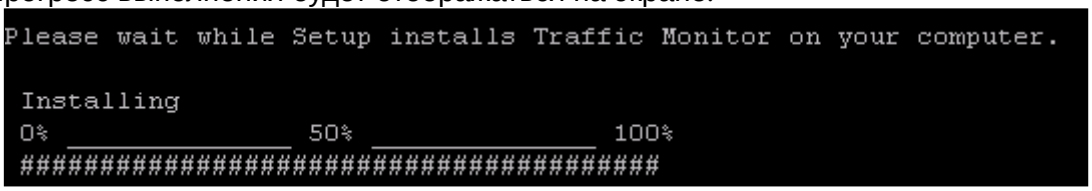
   > **Примечание:**

Приоритет языков соответствует последовательности их выбора. Английский язык будет добавлен по умолчанию, имеет самый высокий приоритет.

g. 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.

h. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
Если установка прошла успешно, данные рекомендуется удалить.
i. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
j. Если необходимо 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`):

a. Последовательно укажите параметры подключения к базе данных:
   i. IP-адрес или доменное имя сервера с базой данных.
   ii. Порт подключения.
   iii. Имя используемой базы данных.
b. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.
В случае утвердительного ответа будет предложено поменять следующие параметры:

- 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.

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

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

   iii. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.
   iv. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
   v. **`Consul retryjoin servers`** – список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.
   vi. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

d. 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 данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.

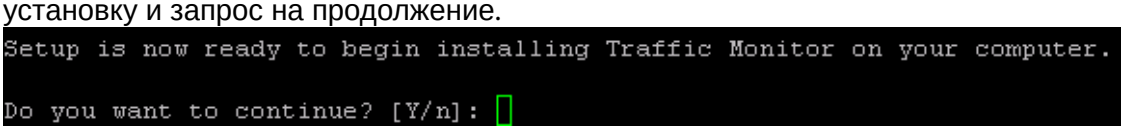
e. Укажите адрес сервера, на котором функционирует служба Sphinx (шаблон Индексер).

> **Примечание:**
>
> Если шаблоны Индексер и Веб-консоль устанавливаются на один сервер, данный параметр не будет запрошен инсталлятором.

f. Вы можете включить использование технологии OCR.

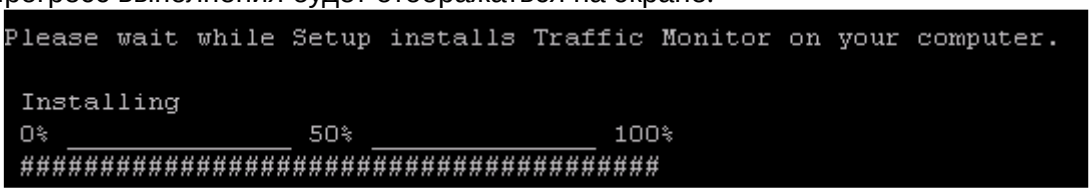
> **Примечание:**
>
> OCR-экстрактор выбирается при установке шаблона Перехватчики.

g. 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.

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

Установка шаблона Перехватчики

Если для установки выбран шаблон Перехватчики (Interceptors):

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

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

iii. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.
iv. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
v. **`Consul retryjoin servers`** – список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.
vi. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

d. 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 данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.

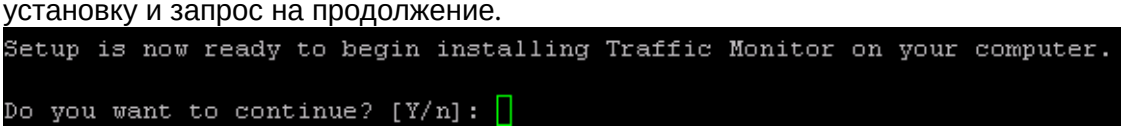
e. Вы можете включить использование технологии OCR.
В случае включения необходимо выбрать для использования одну из систем:
- **`ABBYY FineReader`**;
- **`Tesseract`**.

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

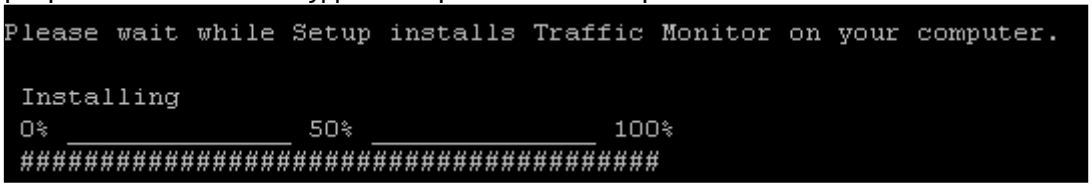
f. Если выбран OCR-экстрактор ABBYY Finereader:
i. Выберите один из режимов распознавания:
- **`Quick`** – быстрый режим;
- **`Quality`** – тщательный режим, обеспечивающий более высокое качество распознавания.

ii. Подтвердите наличие у вас активной лицензии на использование ABBYY Finereader.
Если у вас отсутствует лицензия, введите **N** и нажмите **Enter**. В этом случае ABBYY Finereader будет установлен без лицензии. Для возможности работы ABBYY Finereader активную лицензию нужно будет добавить позже вручную. Подробнее смотрите в документе "*InfoWatch Traffic Monitor. Руководство администратора*" в статье "Настройка OCR-экстракторов".

g. 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.

h. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
Если установка прошла успешно, данные рекомендуется удалить.
i. Для перехвата smtp с учетом мандатных меток на ОС Astra Linux Special Edition 1.7.5.9 "Смоленск":
   i. Введите команду для вызова файлового менеджера:
   `sudo mc`
   ii. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
   iii. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.
   iv. Для выхода из файлового менеджера введите команду:
   `exit`
j. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
k. Если необходимо вывести список сервисов Traffic Monitor и их статусы, введите команду:
`iwtm status`

> **Примечание:**
>
> После установки Traffic Monitor не меняйте статус мандатных меток в ОС Astra Linux Special Edition 1.7.5.9 "Смоленск". Если до установки в ОС они были включены, не выключайте их, и наоборот.
>
> В противном случае корректная работа Системы не гарантируется.

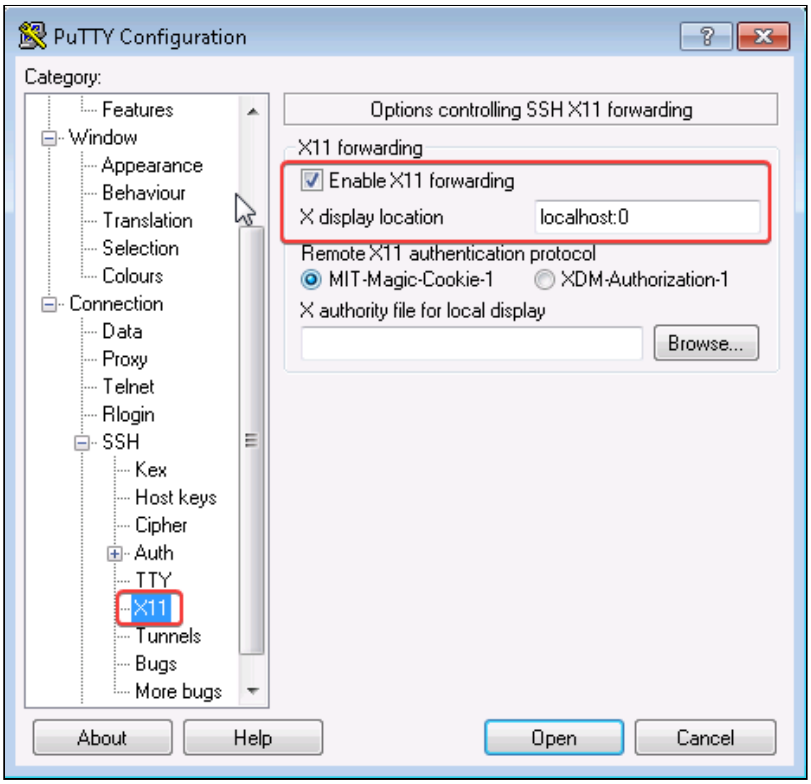
Установка с использованием графического режима инсталлятора

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. Данный режим реализуется с помощью SSH-подключения.

> **Примечание:**
>
> Если установка выполняется без удаленного подключения, непосредственно в графической среде сервера, достаточно просто запустить файл инсталлятора и перейти к установке шаблонов.

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

a. На сервере, на котором планируется установка компонентов Traffic Monitor:
   i. Установите утилиту xauth с помощью команды:
   `sudo apt-get install xauth`
   ii. 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 `#`.
   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 серверу установки Traffic Monitor 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 установка компонентов Traffic Monitor, с помощью выбранного SSH-клиента.
Пример окна настройки PuTTY при подключении



e. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
`sudo ./iwtm-installer-x.x.x.xxx-astra-1.7`
В нашем примере команда будет следующей:
`sudo ./iwtm-installer-7.9.0.150-astra-1.7`

Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов. По завершении откроется окно с приглашением установить Traffic Monitor:



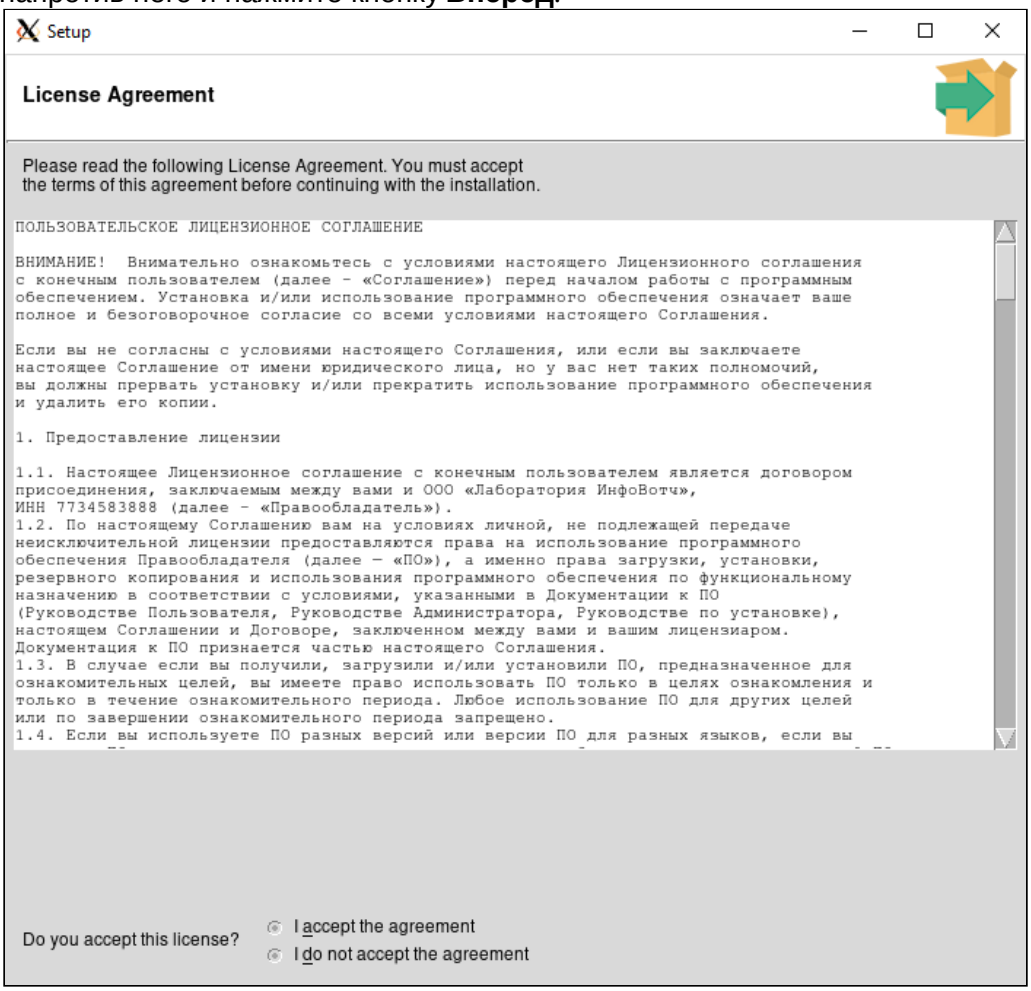
Для перехода к следующему параметру используется кнопка **Вперед**, для возврата к предыдущему – **Назад**. Для выхода из инсталлятора – кнопка **Отменить**.

f. Для продолжения установки необходимо принять условия Лицензионного соглашения. Для этого:
   i. Выберите язык, на котором будет выведен текст Лицензионного соглашения:



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

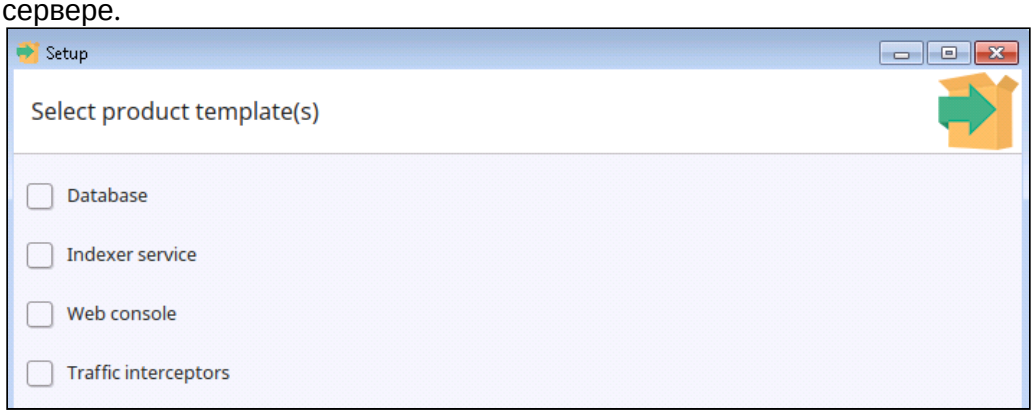
ii. Выберите один из предложенных вариантов. Для этого установите флажок напротив него и нажмите кнопку **Вперед**:



- **`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.

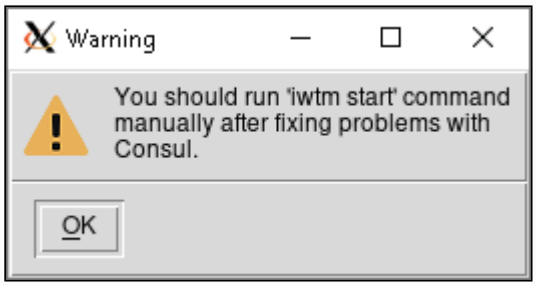
g. На этапе выбора типа установки выберите **`Distributed`**.

h. Далее с помощью выбора шаблонов вы можете указать, какие наборы компонентов необходимо будет использовать после установки на текущем сервере.



Чтобы выбрать сразу несколько значений, отметьте их флажками и нажмите кнопку **Вперед**.

> **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 одним другим шаблоном.

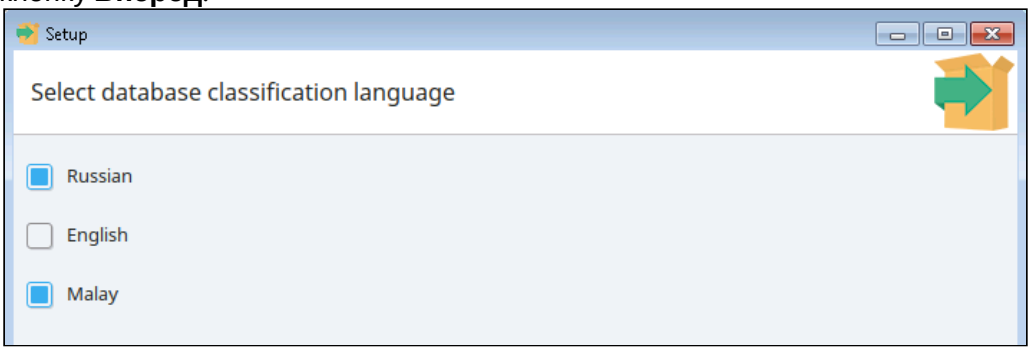
> **Примечание:**
>
> В случае некорректной настройки службы Consul по завершении установки в консоли будет выведено предупреждение:
>
> 
>
>
> Для завершения работы инсталлятора нажмите **Enter**.
>
> **Для корректной работы Системы выполните проверку и настройку кластера службы Consul**
>
> i. Запустите службу Consul, выполнив команду:
> `service iwtm-consul start`
> Проверить статус службы можно командой:
> `service iwtm-consul status`
> 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 при завершении работы, их нужно будет запустить вручную.

Ниже будет рассмотрена установка каждого шаблона на отдельный сервер.

Установка шаблона База данных

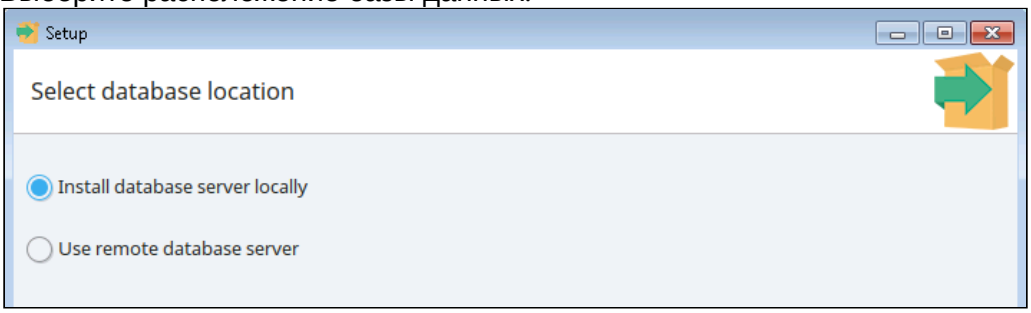
Если для установки выбран шаблон База данных (`Database`):

a. 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.
b. Выберите язык базы классификации. База классификации включает в себя предустановленные политики, элементы настройки технологий и объекты защиты. Вы можете выбрать одновременно несколько языков.
   Чтобы выбрать сразу несколько значений, отметьте их флажками и нажмите кнопку **Вперед**.



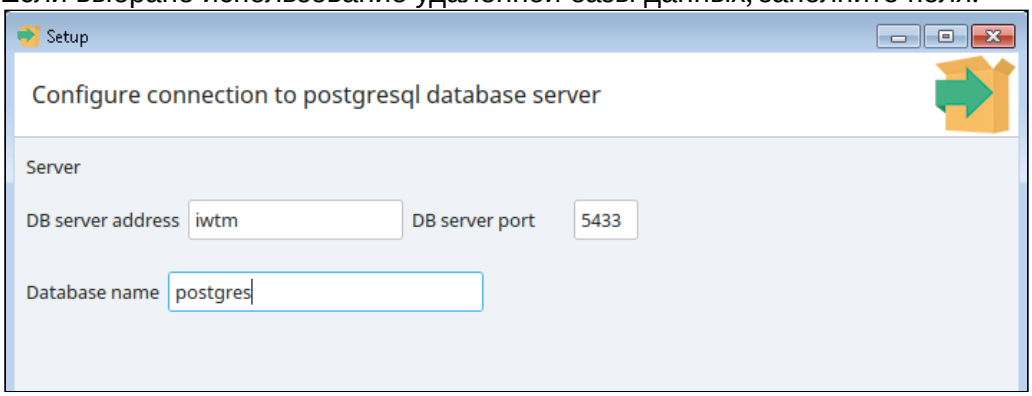
   Для выбора доступны:
   - `Russian` – русский;
   - `English` – английский;
   - `Malay` – малайский.

   Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.
c. 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.

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

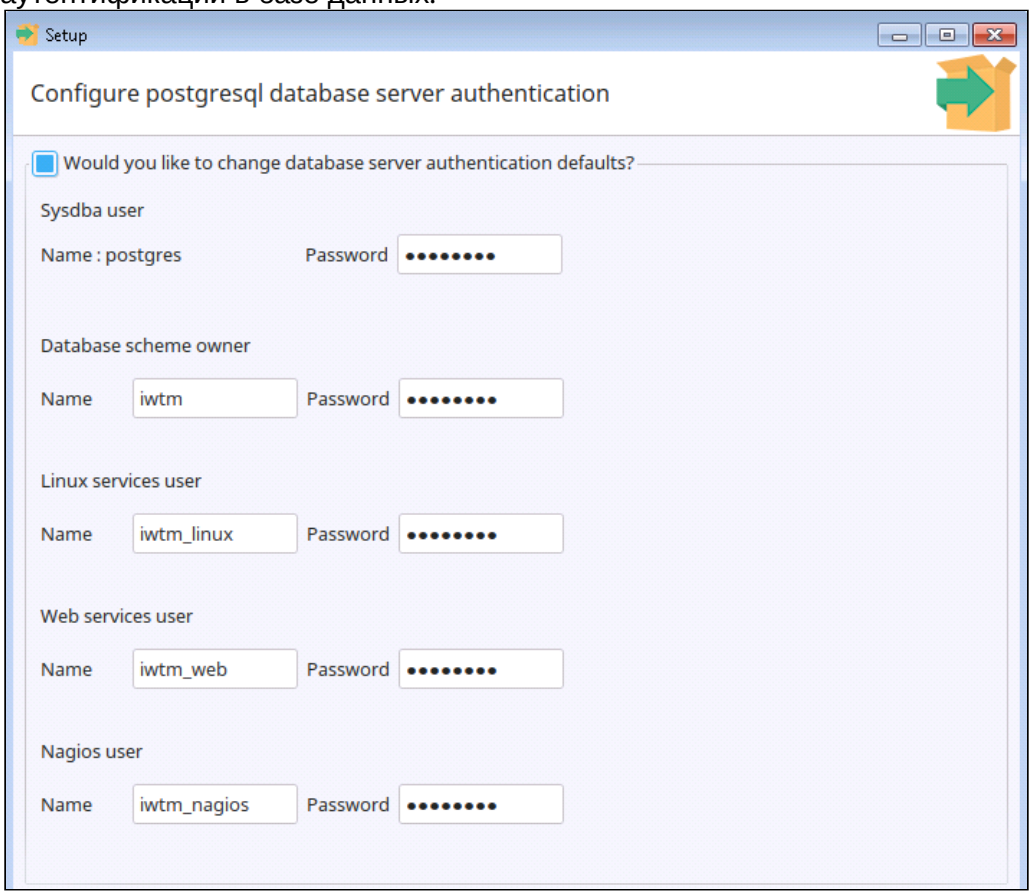


i. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.

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

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

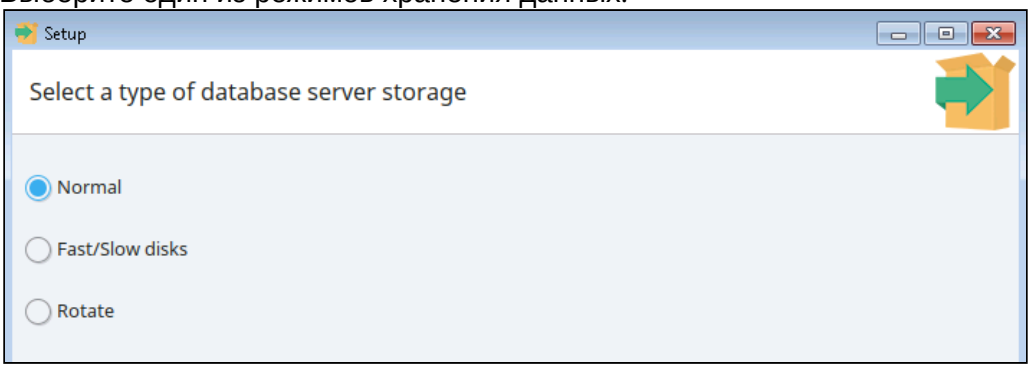
e. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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

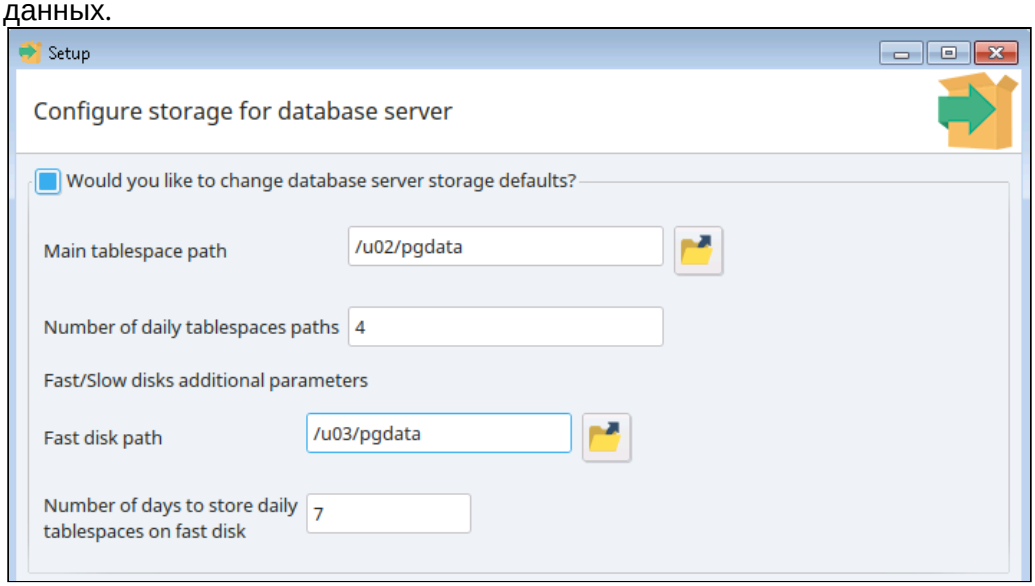
- **`Sysdba user`** – пароль пользователя с правами sysdba;
- **`Database scheme owner`** – Имя и пароль владельца схемы базы данных;
- **`Linux services user`** – Имя и пароль пользователя сервисов Linux;
- **`Web services user`** – Имя и пароль пользователя веб-сервисов;
- **`Nagios user`** – Имя и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

f. 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.

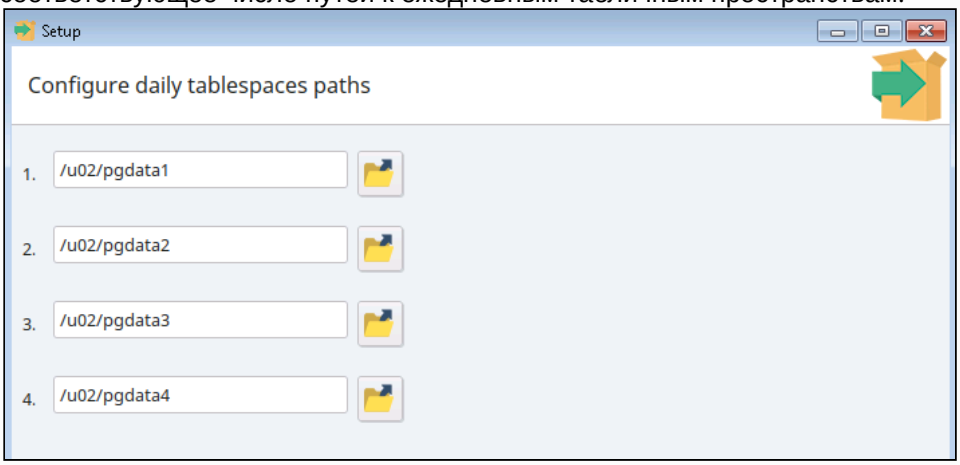
g. Вы можете изменить значения по умолчанию параметров хранения в базе данных.



- **`Main tablespaces path`** – путь к директории хранения данных основного табличного пространства;
  Вы можете вписать путь в поле или указать его в окне файлового менеджера, использовав кнопку .
- Если выбран режим **`Fast/Slow disks`**:

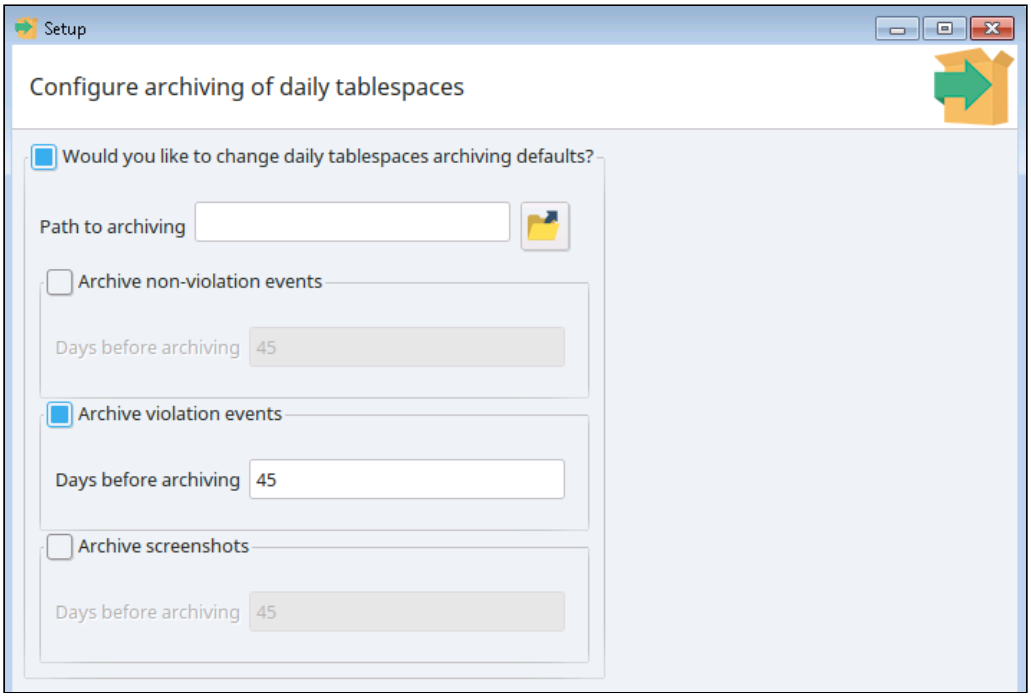
- **`Fast disk path`** – путь к директории хранения данных ежедневных табличных пространств в быстром разделе в режиме **`F ast/Slow disks`**;
- **`Number of days to store daily tablespaces on fast disk`** – период хранения данных ежедневных табличных пространств в быстром разделе в режиме **`F ast/Slow 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 будет необходимо указать соответствующее число путей к ежедневным табличным пространствам.
>
> 
>

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

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



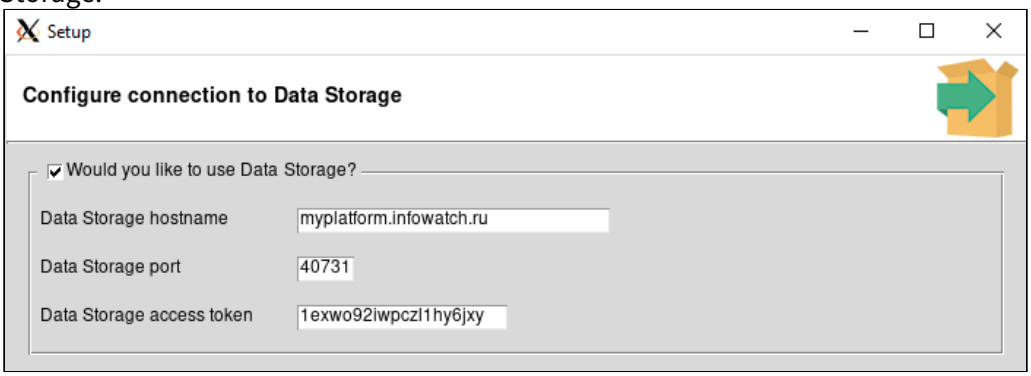
- **`Path to archiving`** – путь к директории хранения файлов архивированных табличных пространств.

Использование каждого параметра 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.

i. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию – 90.

j. Вы можете включить использование внешнего хранилища бинарных данных Data Storage.



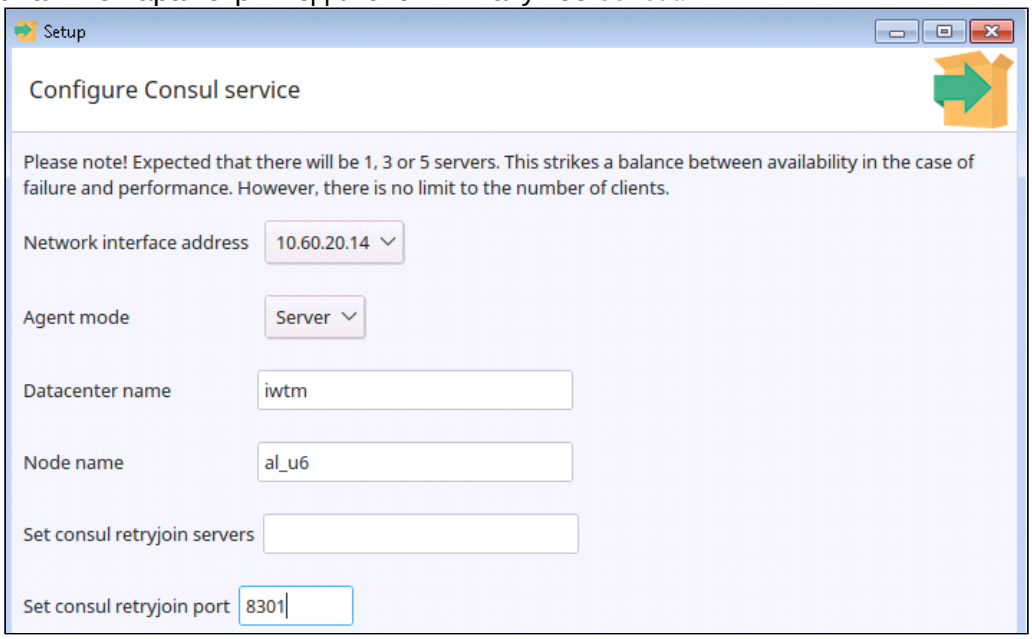
Для этого установите галочку напротив поля с вопросом и укажите параметры подключения к внешнему хранилищу:

- **`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:
  i. Перейдите в директорию, куда был распакован дистрибутив Платформы;
  ii. 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 продукта Платформы, 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.

k. Укажите параметры подключения к службе Consul:

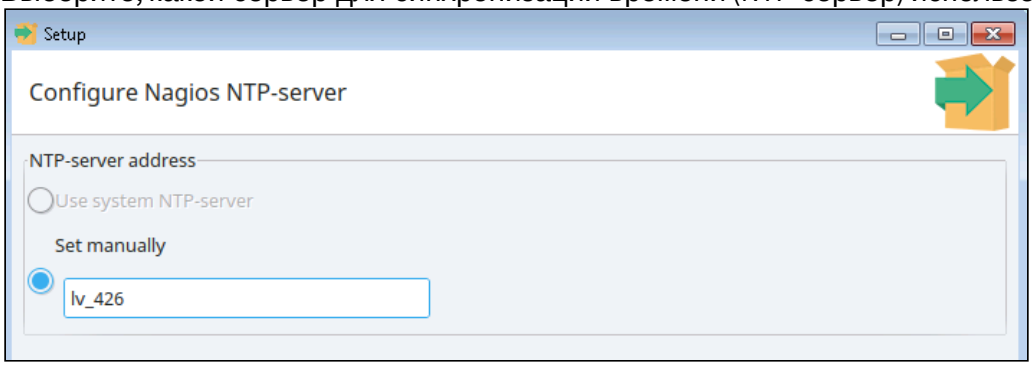


i. **`Network interface address`** – выберите IP-адрес сетевого интерфейса.
Для выбора из списка параметров нажмите на кнопку ⌄ и в раскрывшемся списке выберите требуемое значение.
ii. Режим работы Consul. Доступны два режима:
- **`Server`**
- **`Client`**

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

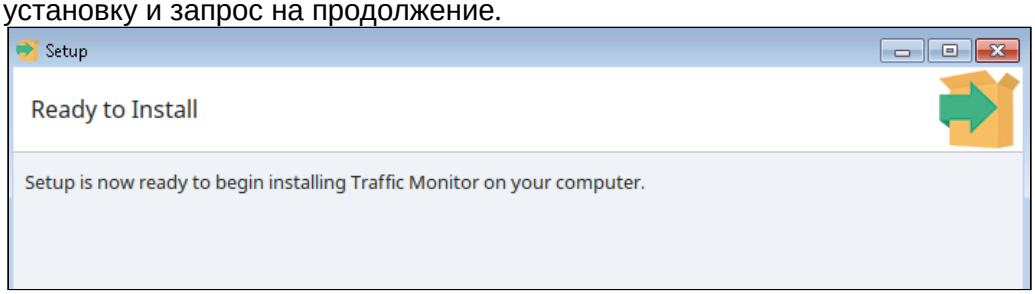
iii. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.
iv. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.
v. **`Consul retryjoin servers`** – список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.
vi. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

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

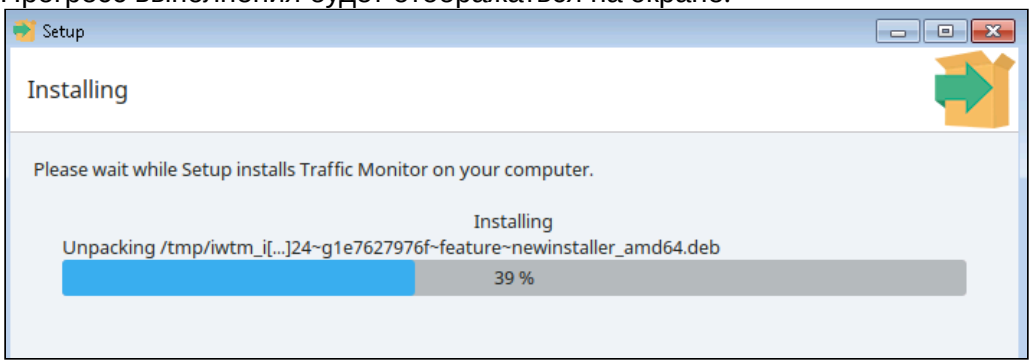


- **`Use system NTP-server`** – использовать системный NTP-сервер;
- **`Set manually`** – указать NTP-сервер вручную. При выборе данного варианта укажите IP-адрес или имя доступного NTP-сервера.

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



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

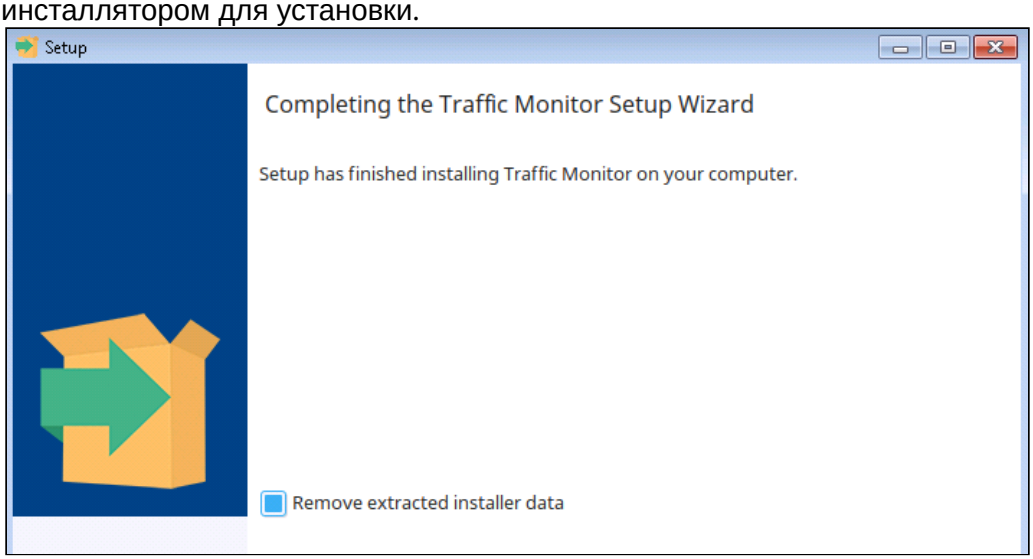


Процесс может занять некоторое время.

> **Примечание:**

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

n. 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 exctracted installer data`**.

o. Для завершения нажмите кнопку **Finish**.

p. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.

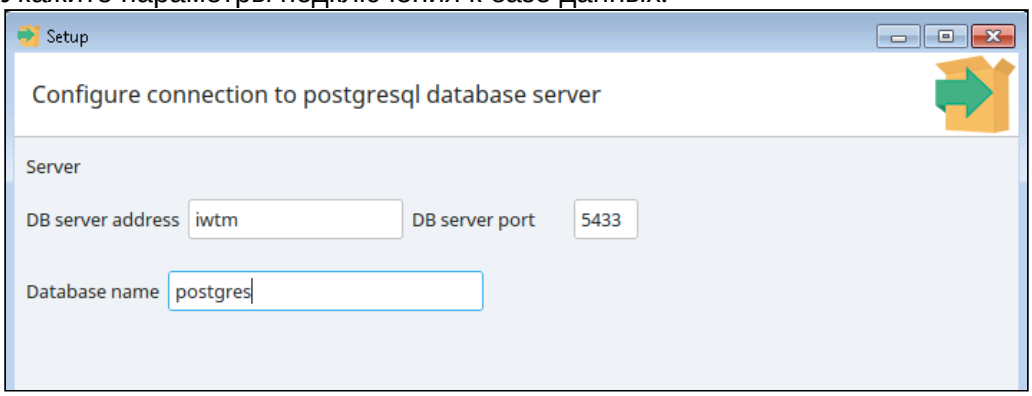
q. Если необходимо вывести список сервисов Traffic Monitor и их статусы, введите команду:

```
iwtm status
```

Установка шаблона Индексер

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

a. Укажите параметры подключения к базе данных:

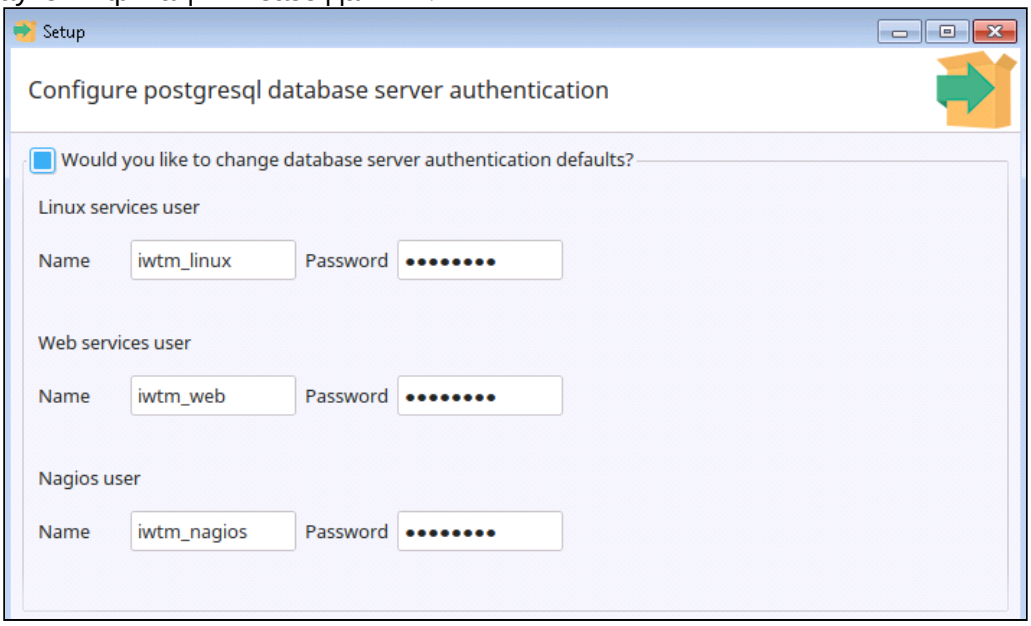


i. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.

ii. **`Database name`** – Имя используемой базы данных.

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

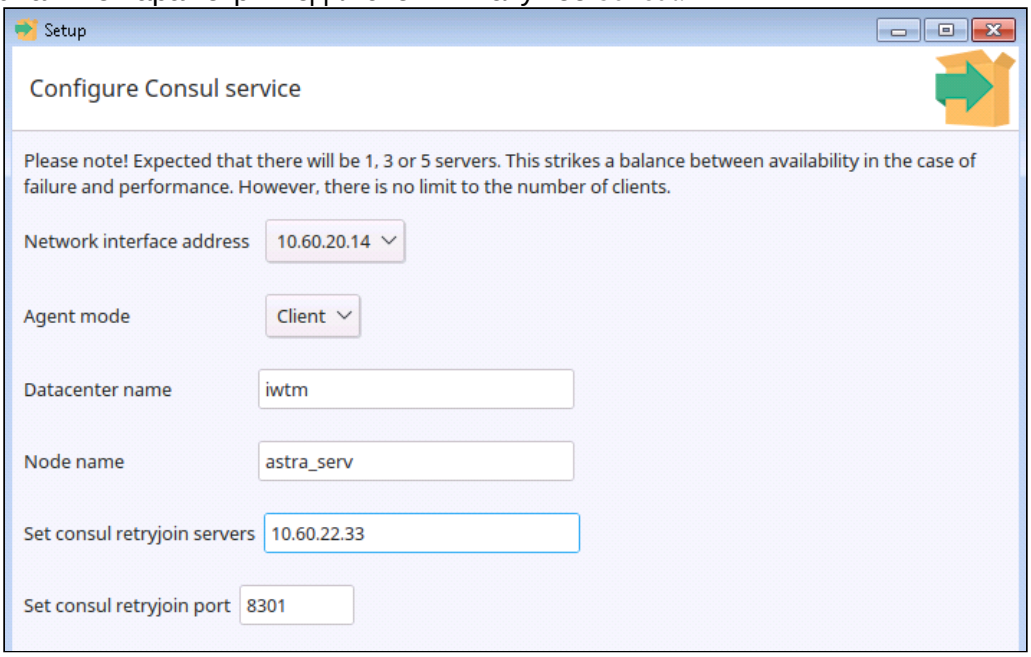
b. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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

- **`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.

c. Укажите параметры подключения к службе Consul:



i. **`Network interface address`** – выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите на кнопку ▼ и в раскрывшемся списке выберите требуемое значение.

ii. Режим работы Consul. Доступны два режима:
   - **`Server`**
   - **`Client`**

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

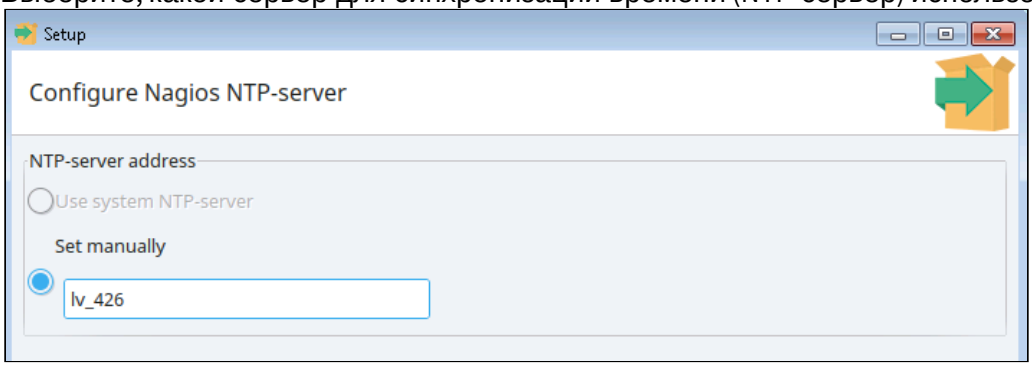
iii. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.

iv. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.

v. **`Consul retryjoin servers`** – список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.

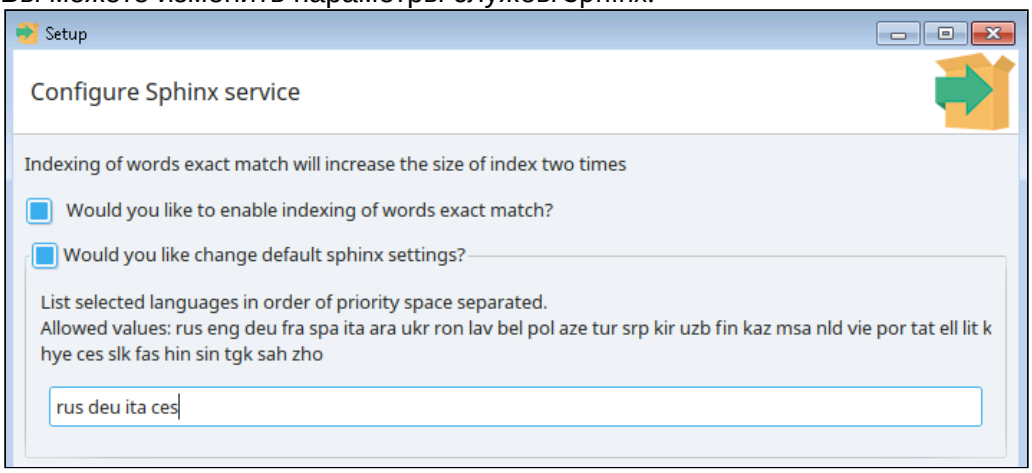
vi. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

d. 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 данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.

e. Вы можете изменить параметры службы Sphinx:



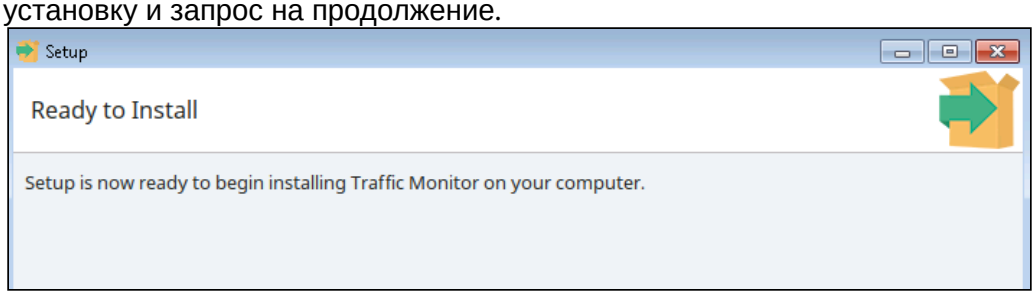
- `Enable indexing of words exact match` – включить индексацию на точное совпадение слов;

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

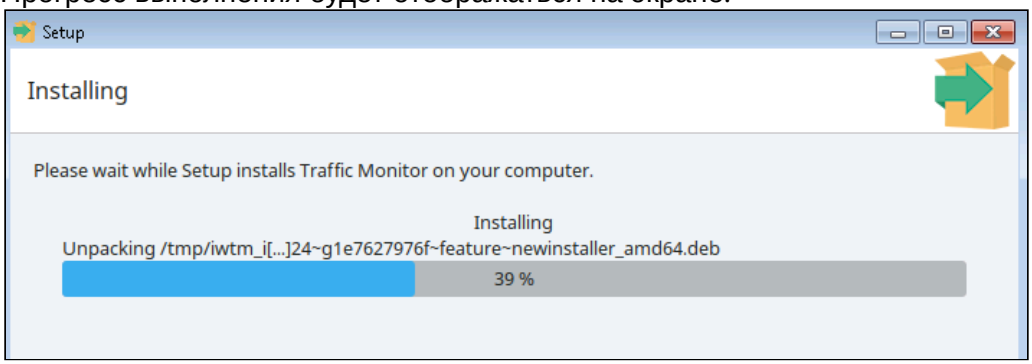
- При необходимости вы можете изменить стандартные параметры работы службы Sphinx (`default sphinx settings`). В этом случае укажите список языков с поддержкой морфологии. По этим языкам будет проводиться индексация. Вы можете указать несколько языков, используя пробел в качестве разделителя.

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

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



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

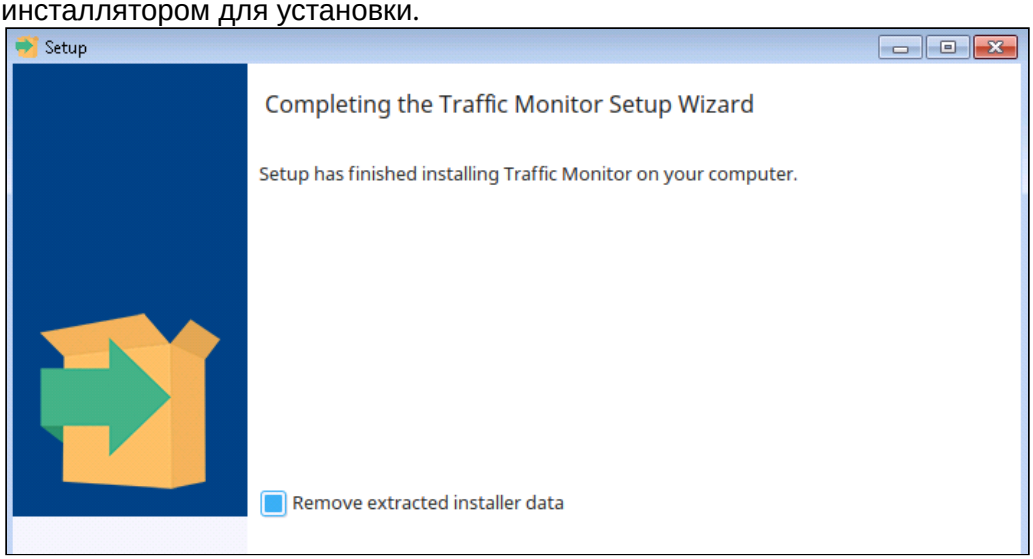


Процесс может занять некоторое время.

> **Примечание:**

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

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



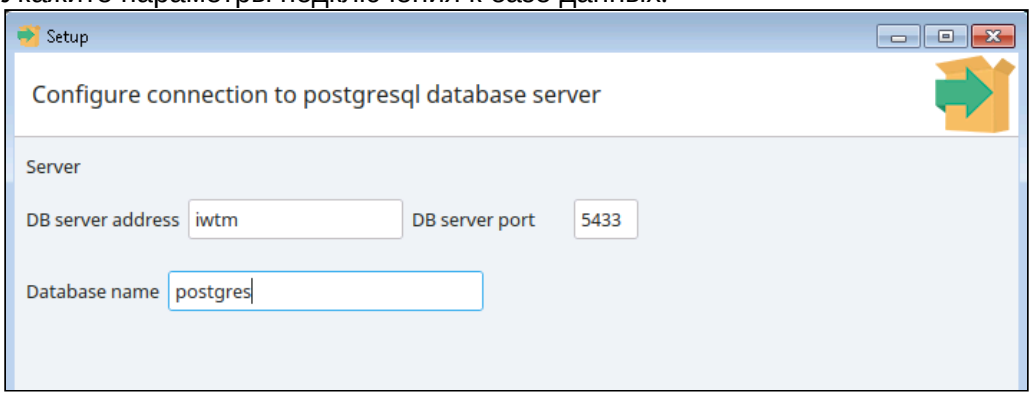
Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove exctracted installer data`**.

h. Для завершения нажмите кнопку **Finish**.
i. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
j. Если необходимо 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`):

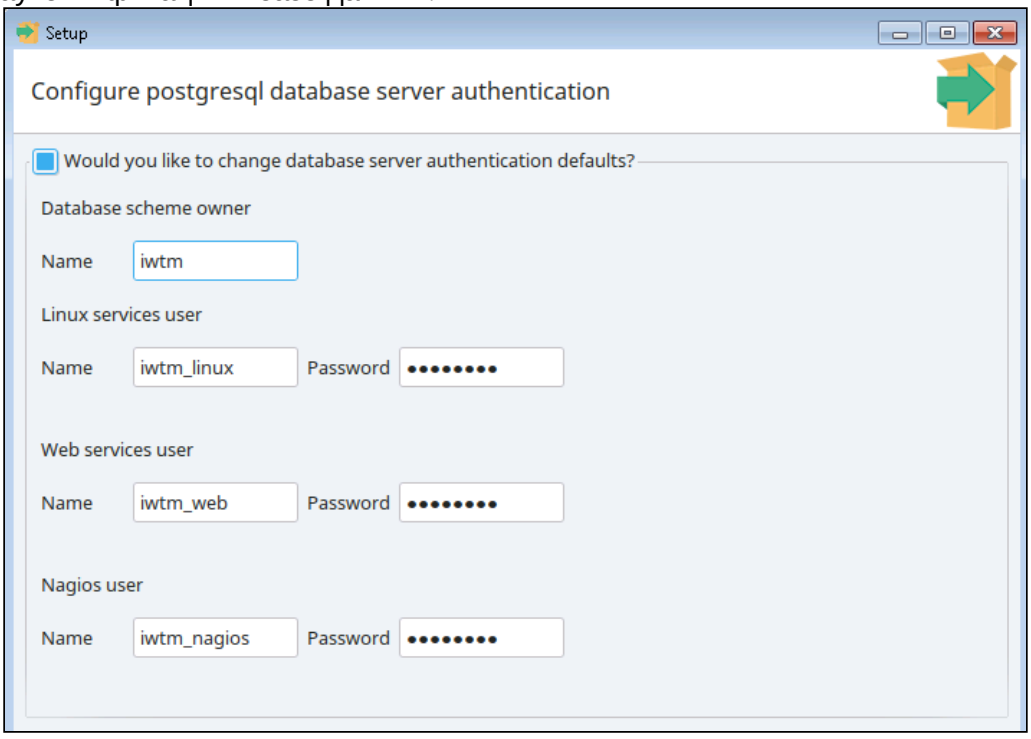
a. Укажите параметры подключения к базе данных:



i. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.
ii. **`Database name`** – Имя используемой базы данных.

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

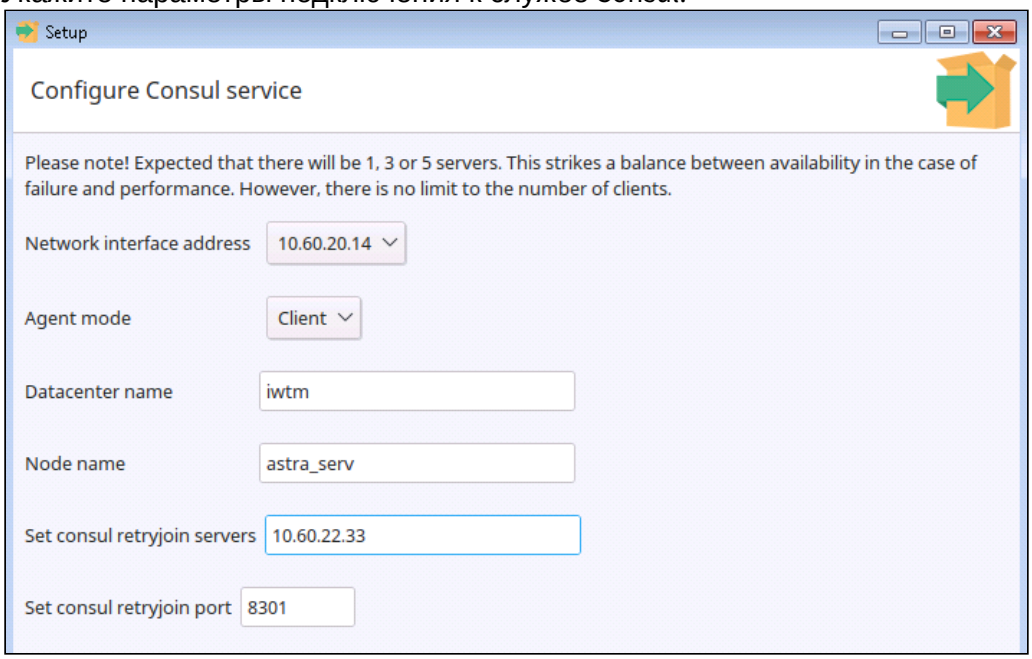
b. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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

- **`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.

c. Укажите параметры подключения к службе Consul:



i. **`Network interface address`** – выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите на кнопку и в раскрывшемся списке выберите требуемое значение.

ii. Режим работы Consul. Доступны два режима:
   - **`Server`**
   - **`Client`**

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

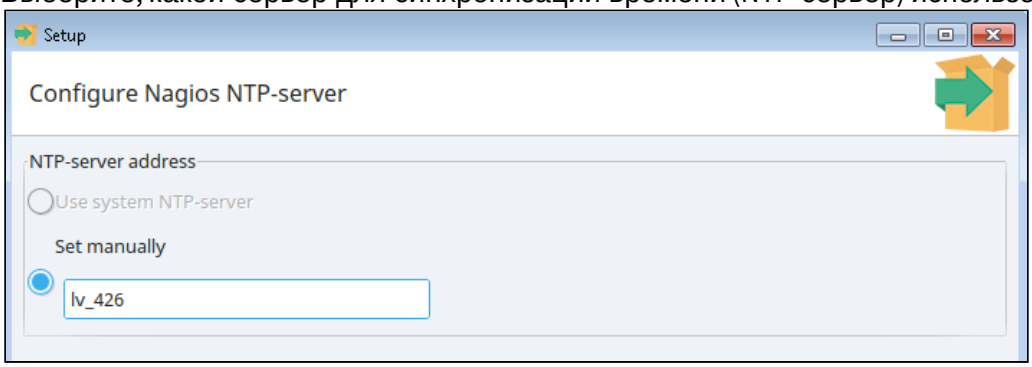
iii. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.

iv. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.

v. **`Consul retryjoin servers`** – список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.

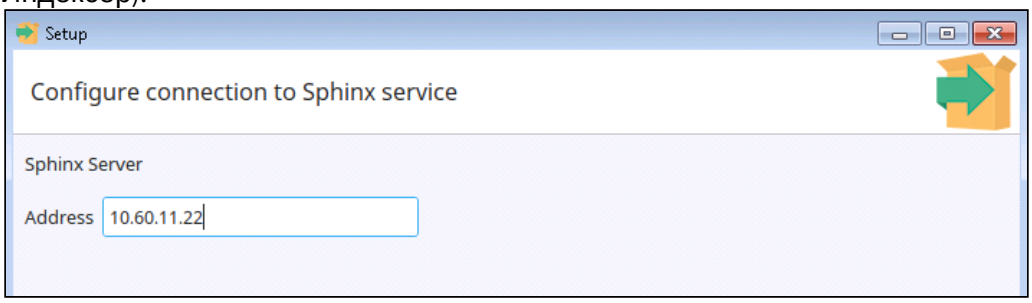
vi. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

d. 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 данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.

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



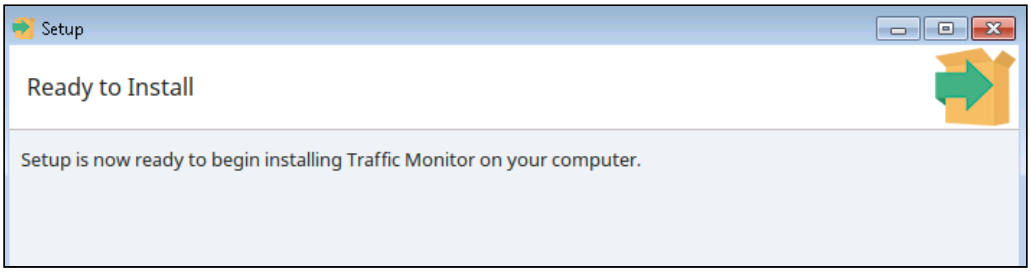
> **Примечание:**
>
> Если шаблоны Индексер и Веб-консоль устанавливаются на один сервер, данный параметр не будет запрошен инсталлятором.

f. Вы можете включить использование технологии OCR.

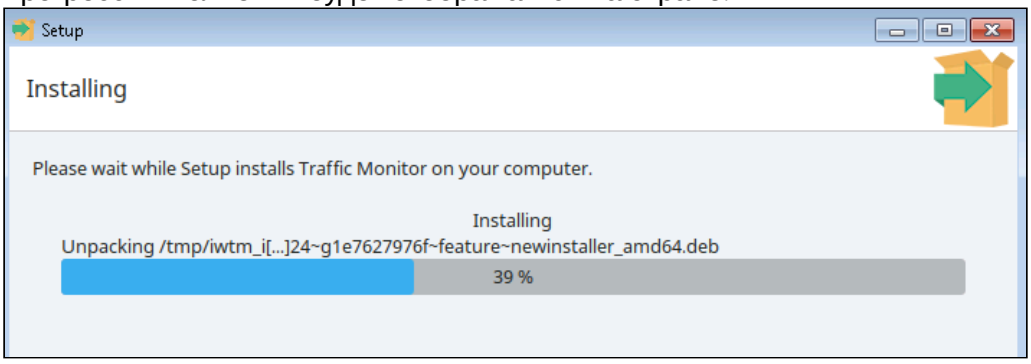


> **Примечание:**
>
> OCR-экстрактор выбирается при установке шаблона Перехватчики.

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



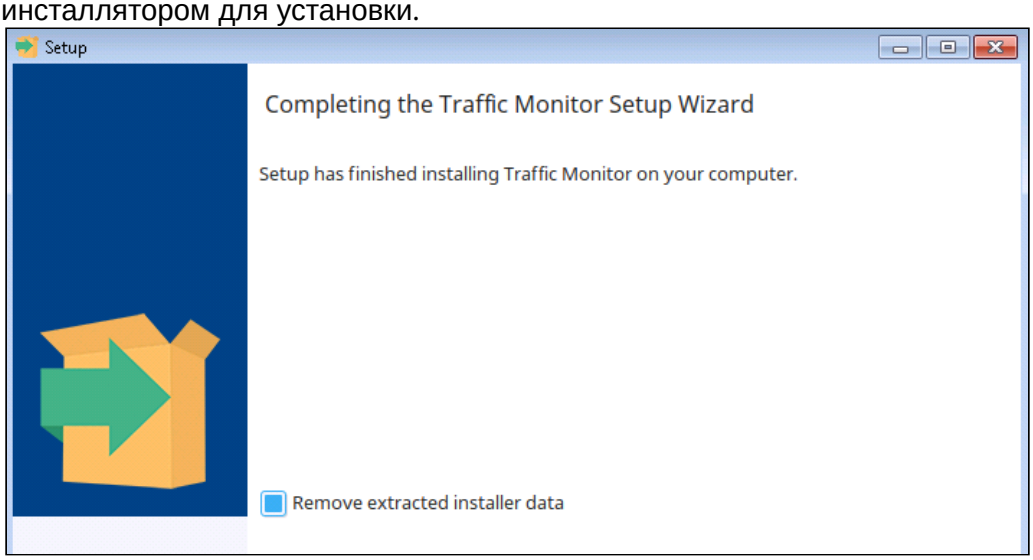
Для начала установки нажмите кнопку **Вперед**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor.
Прогресс выполнения будет отображаться на экране.



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.

h. 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 exctracted installer data`.

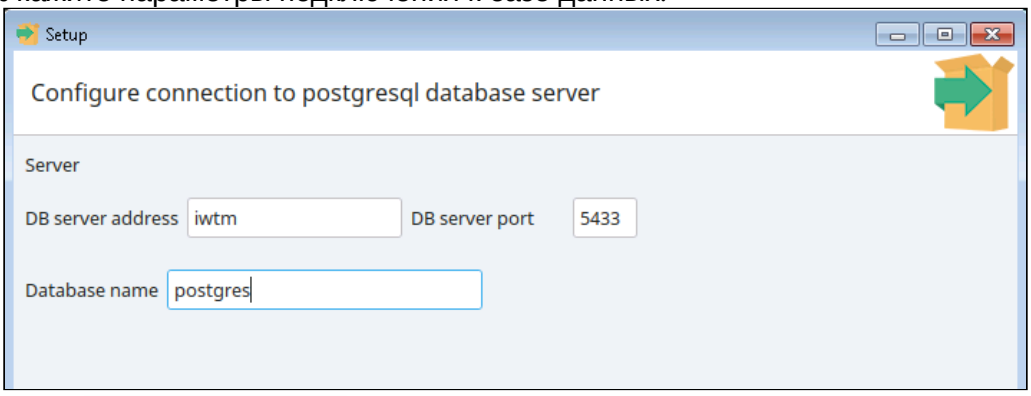
i. Для завершения нажмите кнопку **Finish**.

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

Установка шаблона Перехватчики

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

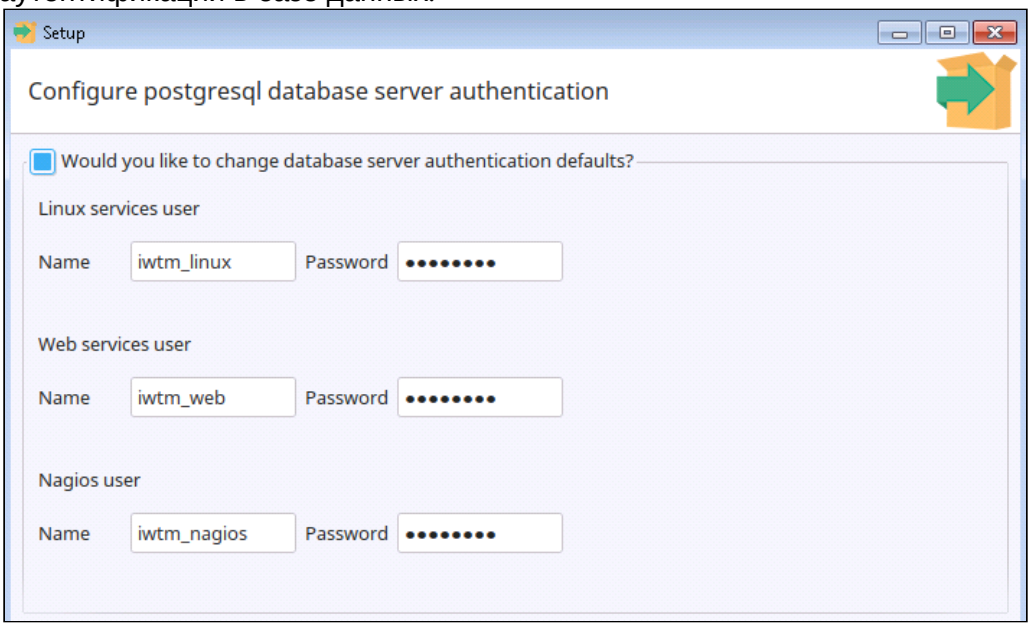
a. Укажите параметры подключения к базе данных:



i. **`Address and Port`** – IP-адрес или доменное имя сервера с базой данных и порт подключения.
ii. **`Database name`** – Имя используемой базы данных.

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

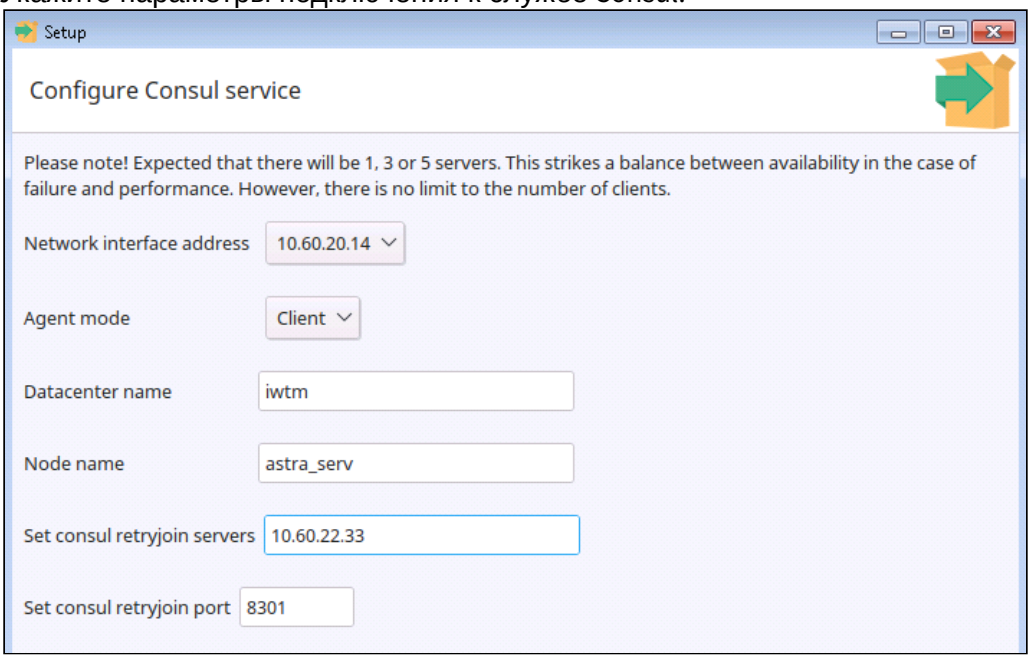
b. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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

- **`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.

c. Укажите параметры подключения к службе Consul:



i. **`Network interface address`** – выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите на кнопку и в раскрывшемся списке выберите требуемое значение.

ii. Режим работы Consul. Доступны два режима:
   - **`Server`**
   - **`Client`**

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

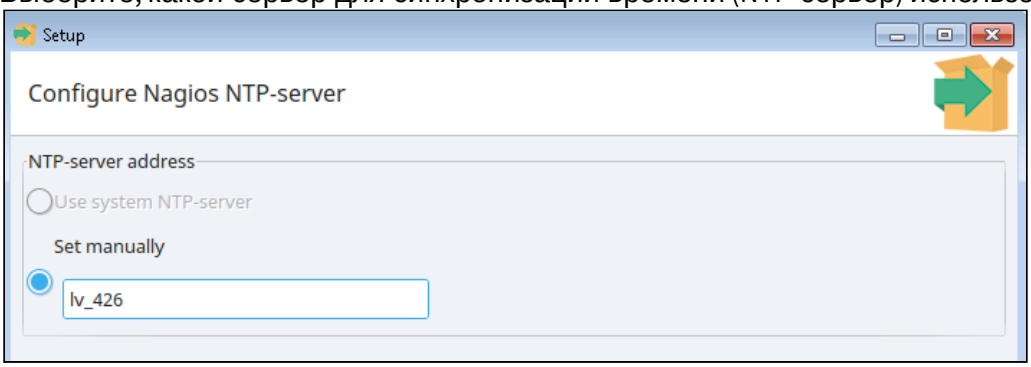
iii. **`Datacenter name`** – введите название дата-центра Consul. По умолчанию – `iwtm`.

iv. **`Node name`** – имя сервера, на который устанавливаются компоненты Traffic Monitor.

v. **`Consul retryjoin servers`** – список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.

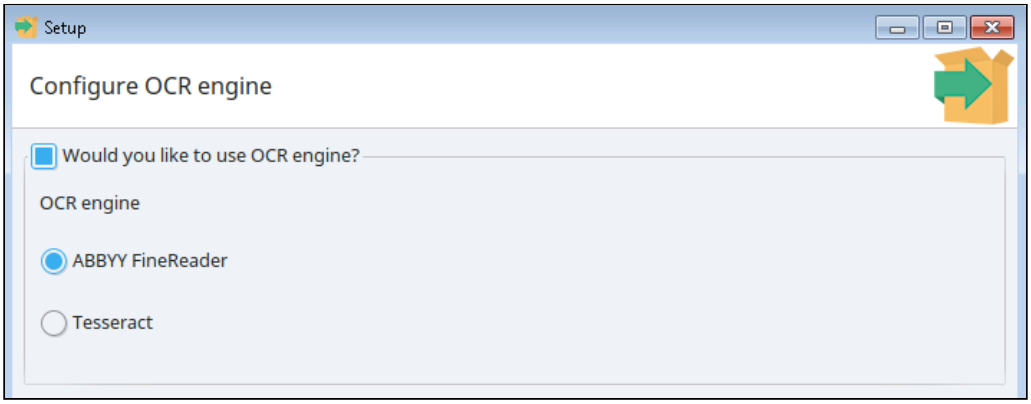
vi. **`Consul retryjoin port`** – порт подключения к указанным серверам Consul.

d. 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 данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.

e. Вы можете включить использование технологии OCR.

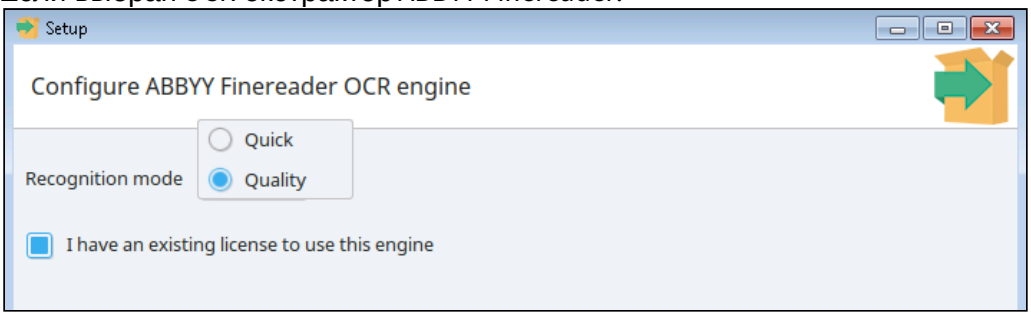


В случае включения необходимо выбрать для использования одну из систем:

- **`ABBYY FineReader`**;
- **`Tesseract`**.

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

f. Если выбран OCR-экстрактор ABBYY Finereader:



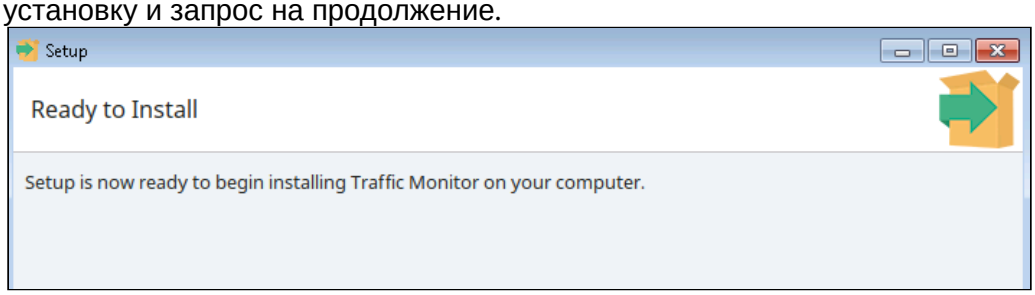
i. Выберите один из режимов распознавания (**`Recognition mode`**):

- **`Quick`** – быстрый режим;

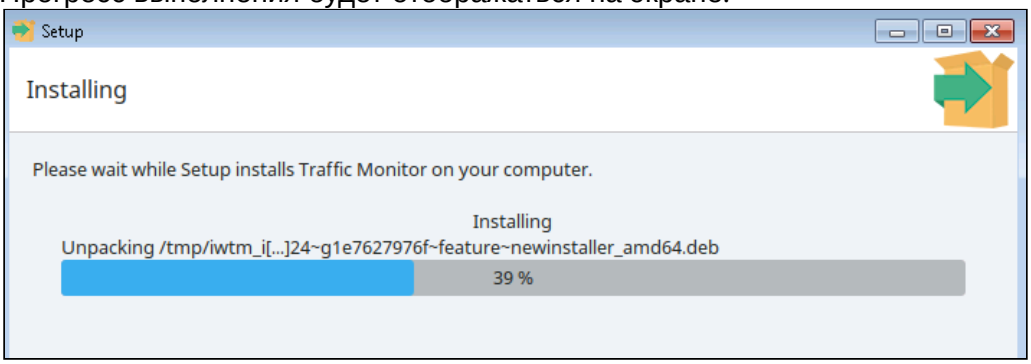
- `Quality` – тщательный режим, обеспечивающий более высокое качество распознавания.

ii. Подтвердите наличие у вас активной лицензии на использование ABBYY Finereader.
Если у вас отсутствует лицензия, не ставьте флажок в этом поле. В этом случае ABBYY Finereader будет установлен без лицензии. Для возможности работы ABBYY Finereader активную лицензию нужно будет добавить позже вручную. Подробнее смотрите в документе "*InfoWatch Traffic Monitor. Руководство администратора*" в статье "Настройка OCR-экстракторов".

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



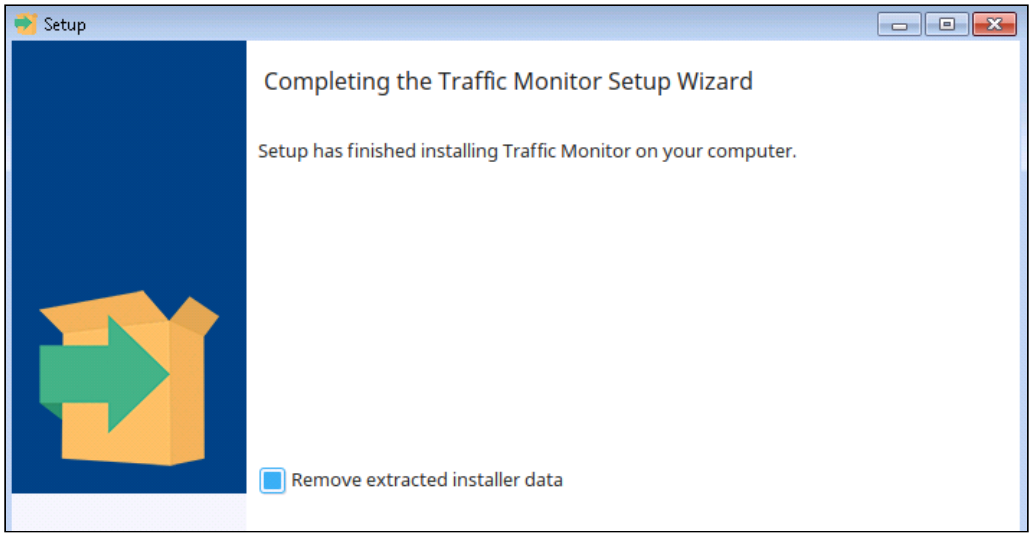
Для начала установки нажмите кнопку **Next**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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.

h. 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 exctracted installer data`**.

i. Для завершения нажмите кнопку **Finish**.

j. Для перехвата smtp с учетом мандатных меток на ОС Astra Linux Special Edition 1.7.5.9 "Смоленск":

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

   ii. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.

   iii. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.

   iv. Для выхода из файлового менеджера введите команду:
   `exit`

k. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.

l. Если необходимо вывести список сервисов Traffic Monitor и их статусы, введите команду:
`iwtm status`

> **Примечание:**
>
> После установки Traffic Monitor не меняйте статус мандатных меток в ОС Astra Linux Special Edition 1.7.5.9 "Смоленск". Если до установки в ОС они были включены, не выключайте их, и наоборот.
>
> В противном случае корректная работа Системы не гарантируется.

15. Если используется ОС Astra Linux Special Edition 1.7.5.9 уровня "Орел", то выполните команды:
```
sed -i 's/parsec.max_ilev=63/parsec.max_ilev=0/' /etc/default/grub
update-grub
```
16. Если ранее для установки вы создали файл `etc/systemd/system/`**`rsyslog.service`**:
    a. Вы можете удалить его с помощью команды:
    `rm /etc/systemd/system/rsyslog.service`

b. В таком случае выполните команду:
`systemctl daemon-reload`

17. Перезагрузите сервер, выполнив команду:
`reboot`

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

После окончания установки работа в консоли управления доступна 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. документ «*InfoWatch Traffic Monitor. Руководство администратора*».

> **Примечание:**
>
> Если после установки будет принято решение о расширении Системы и добавлении дополнительных серверов, их необходимо будет зарегистрировать в кластере Consul. Смотрите подробнее в документе "*InfoWatch Traffic Monitor. Руководство администратора*" в разделе "Настройка межсервисного взаимодействия (служба Consul)" в статье "Распределенная установка".

Список процессов, которые должны быть запущены только на одном из серверов, приведен в документе "*InfoWatch Traffic Monitor. Руководство администратора*" в статье "Проверка автозапуска процессов". О том, как включить и выключить автозапуск процессов, смотрите в том же документе, статья "Включение и выключение автозапуска процессов". С описанием процессов можно ознакомиться также в документе "*InfoWatch Traffic Monitor. Руководство администратора*" в статье "Список процессов серверной части Traffic Monitor".

3.2.3 Установка в тихом режиме с файлом параметров

Чтобы минимизировать участие в процессе установки Системы, в инсталляторе предусмотрен тихий режим установки. В этом режиме инсталлятор может установить 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.

Таким образом, использование тихого режима и подготовленного файла параметров позволяет установить Traffic Monitor практически без участия пользователя.

> **Важно!**
>
> Перед началом установки убедитесь, что сервер соответствует требованиям к настройкам ОС и сети сервера.
>
> Если планируется использование удаленной базы данных, ее необходимо настроить.
>
> Для установки InfoWatch Traffic Monitor на сервере должно быть установлено обновление ОС Astra Linux Special Edition 1.7.5.9.
>
> Чтобы узнать версию установленной ОС, выполните команду:
>
> `cat /etc/astra_version`

Для установки Traffic Monitor потребуется репозиторий Astra Linux.
Вы можете использовать:

- локальный репозиторий с диска `base-1.7.5.9-16.10.23_16.58.iso`.
  О подключении локальных репозиториев вы можете прочитать в статье "Создание локальных и сетевых репозиториев" на официальном сайте компании-разработчика ОС Astra Linux.
- интернет-репозиторий `base`.
  О подключении интернет-репозиториев вы можете прочитать в статье "Интернет-репозитории Astra Linux Special Edition x.7" на официальном сайте компании-разработчика ОС Astra Linux. Убедитесь, что ОС Astra Linux использует загруженные сертификаты, способствующие подключению к репозиториям.
- локальный репозиторий с диска и несколько пакетов, которые необходимо установить дополнительно.
  Этот способ подходит для установки ТМ без доступа в интернет.

Перед установкой выполните общие действия:

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

   Важно!

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

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

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

   Если вы устанавливаете Traffic Monitor с использованием установочного диска (без доступа в интернет):

   a. Переведите терминал в режим суперпользователя:
      `sudo su`
   b. Настройте сетевой интерфейс. Для этого:
      i. Откройте на редактирование файл `/etc/network/interfaces`.
      ii. В файле `interfaces` укажите значения параметров:

```
auto eth0
iface eth0 inet static
  address <IP-адрес интерфейса>
  netmask <маска подсети>
  gateway <IP-адрес шлюза>
```

```
network <адрес сети>
broadcast <канал сети>
```

> **Примечание:**
>
> Подробнее о параметрах см. статью "Настройка сетевых подключений в Astra Linux" в Справочном центре Astra Linux.

iii. Сохраните изменения и закройте файл.
iv. Включите сетевой интерфейс с помощью команды:
`ifup eth0`
v. Проверьте наличие файла `/etc/ resolv.conf` с настройками DNS. В случае его отсутствия создайте файл и укажите в нем имя домена и IP-адрес DNS-сервера. Используйте команду:
```
cat << EOF > /etc/resolv.conf
search <имя домена>
nameserver <IP-адрес DNS-сервера>
EOF
```

c. Подключите диск с дистрибутивом ОС Astra Linux к серверу.
d. Настройте репозиторий диска. Для этого:
i. Смонтируйте диск с помощью команды:
`mount /dev/cdrom /media/cdrom0`
ii. Откройте на редактирование файл `/etc/apt / sources.list`.
iii. В файле `sources.list` закомментируйте следующую строку, введя символ `#` в начало строки:
`deb cdrom:[OS Astra Linux 1.7.5 1.7_x86-64 devel ]/ 1.7_x86-64 contrib main non-free`
iv. Внесите новую строку:
`deb file:///media/cdrom0 1.7_x86-64 contrib main non-free`
v. Сохраните изменения и закройте файл.
vi. Обновите пакеты с помощью команды:
`apt-get update`

> **Примечание:**
>
> В дальнейшей инструкции вы можете пропустить шаг 7, настраивающий репозитории в файле `sources.list`.

e. Измените IP-адрес в файле `hosts`. Для этого:
i. Откройте на редактирование файл `/etc/ hosts`.
ii. Во второй строке пропишите корректный IP-адрес вместо `127.0.1.1`.
iii. Сохраните изменения и закройте файл.
f. Установите следующие пакеты:
- `gsfonts_8.11+urwcyr1.0.7~pre44-4.4_all.deb`
- `libjemalloc2_5.1.0-3_amd64.deb`
- `liblzf1_3.6-3~bpo10+1_amd64.deb`
- `libnewt0.52_0.52.20-8_amd64.deb`
- `libwmf-bin_0.2.8.4-14_amd64.deb`
- `libwmf0.2-7_0.2.8.4-14_amd64.deb`

- `libxml2-utils_2.9.4+dfsg1-7+deb10u6+ci202308291455+astra2_amd64.deb`
- `python-newt_0.52.20-8_amd64.deb`
- `redis-server_7.0.13-1_amd64.deb`
- `redis-tools_7.0.13-1_amd64.deb`

Для этого:

i. Скачайте указанные пакеты из официальных репозиториев Astra Linux или Debian.
ii. Скопируйте их на сервер, куда будет установлен Traffic Monitor.
iii. Перейдите в каталог, куда были скопированы указанные пакеты.
iv. Выполните команду, которая установит пакеты:

```
dpkg -i python-newt_0.52.20-8_amd64.deb libnewt0.52_0.52.20-8_amd64.deb gsfonts_8.11+urwcyr1.0.7~pre44-4.4_all.deb libwmf-bin_0.2.8.4-14_amd64.deb libwmf0.2-7_0.2.8.4-14_amd64.deb libxml2-utils_2.9.4+dfsg1-7+deb10u6+ci202308291455+astra2_amd64.deb redis-server_7.0.13-1_amd64.deb redis-tools_7.0.13-1_amd64.deb libjemalloc2_5.1.0-3_amd64.deb liblzf1_3.6-3~bpo10+1_amd64.deb
```

> **Примечание:**
>
> Дополнительно вы можете установить утилиты `htop` и `screen` для работы с операционной системой, выполнив команду:
>
> ```
> apt install htop screen
> ```

g. Выйдите из режима суперпользователя:

```
exit
```

2. Чтобы включить службу SSH, выполните команды:

```
sudo systemctl enable ssh.service
sudo systemctl start ssh.service
```

3. Чтобы выставить уровень мандатного контроля целостности для пользователя `root`, в ОС Astra Linux Special Edition 1.7.5.9 уровня "Смоленск" выполните команду:

```
sudo pdpl-user -i 63 root
```

4. Чтобы изменения вступили в силу, заново войдите в вашу учетную запись:
   a. Введите команду для выхода:

```
exit
```

   b. Заново введите логин и пароль.

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

5. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой системы выполните следующую команду:

```
sudo mkdir /distr
```

6. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor:
   - **`iwtm-installer-x.x.x.xxx-astra-1.7`** (где `x.x.x.xxx` – номер сборки);
   - **`iwtm-postgresql-11.10-x.x.x.xxx-astra-1.7.tar.gz`**.

   В нашем примере:
   - **`iwtm-installer-7.9.0.150-astra-1.7`**;
   - **`iwtm-postgresql-11.10-7.9.0.150-astra-1.7.tar.gz`**.

   > **Примечание:**
   >
   > Инсталлятор и дальнейшие шаги установки подходят для ОС Astra Linux Special Edition 1.7.5.9 уровней "Смоленск", "Воронеж" и "Орел".

7. Проверьте содержимое файла `/etc/apt/sources.list`. В нем должны быть указаны локальные или внешние репозитории, требуемые для установки.

   > **Пример:**
   >
   > Если вы будете использовать локальные репозитории:
   >
   > a. Закомментируйте строки, описывающие подключение внешних репозиториев:
   > ```
   > #deb http://download.astralinux.ru/stable/1.7_x86-64/
   > repository-main/     1.7_x86-64 main contrib non-free
   > #deb http://download.astralinux.ru/stable/1.7_x86-64/
   > repository-update/   1.7_x86-64 main contrib non-free
   > #deb http://download.astralinux.ru/stable/1.7_x86-64/
   > repository-base/     1.7_x86-64 main contrib non-free
   > #deb http://download.astralinux.ru/stable/1.7_x86-64/
   > repository-extended/ 1.7_x86-64 main contrib non-free
   > ```
   > b. Убедитесь, что добавлено и не закомментировано описание подключения репозиториев с диска `base`.
   > В нашем примере строка вида:
   > ```
   > deb file:/mnt/ 1.7_x86-64 contrib main non-free
   > ```
   >
   > В противном случае не должны быть закомментированы строки, описывающие подключение к внешним репозиториям.

   > **Важно!**
   >
   > Если ранее на сервере вы обновляли ОС, убедитесь, что в `/etc/apt/sources.list` указаны **только** репозитории ОС Astra Linux **1.7.5.9**. Если в файле указаны репозитории прошлых версий, отключите их.

8. Очистите кеш с помощью команды:
   ```
   sudo apt-get clean
   ```
9. Выполните следующую команду:
   ```
   sudo apt-get update
   ```

10. Проверьте наличие в системе сервисного файла `/etc/systemd/system/rsyslog.service`.
11. При наличии файла пропустите это действие.
    Если сервисного файла нет:
    a. Создайте его с нужным содержимым с помощью команды:

```
cat << EOF > /etc/systemd/system/rsyslog.service
[Service]
ExecStart=true
ExecStop=true

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

    b. Выполните команду:
    systemctl `daemon-reload`
12. Проверьте редакцию ОС, выполнив команду:
    `cat /etc/astra_license`
    Если используется ОС Astra Linux Special Edition 1.7.5.9 уровня "Орел", дополнительно выполните команды:
    `sed -i 's/parsec.max_ilev=0/parsec.max_ilev=63/' /etc/default/grub`
    `update-grub`
    `reboot`

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
installation_type=distributed
template_database=1
template_indexer=1
template_web=1
template_interceptors=0
product_language=rus
```

В данном примере указаны параметры:

- тип установки – распределенная;
- для установки на сервер выбраны шаблоны:
  - База данных;
  - Индексер;
  - Веб-консоль.
- основной язык продукта – русский.

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:

```
sudo ./iwtm-installer-7.9.0.150-astra-1.7 --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.

Тихий режим установки

Для установки в тихом режиме используйте опцию `--mode unattended`.

Уровень взаимодействия с пользователем задается параметром `--unattendedmodeui`, которые имеет следующие значения:

- `none` – в процессе установки инсталлятор не выводит на экран никакую информацию и не требует взаимодействия с пользователем;
- `minimal` – в процессе отображает ход выполнения установки, не требует взаимодействия с пользователем;
- `minimalWithDialogs` – отображает ход выполнения установки, 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:

```
sudo ./iwtm-installer-7.9.0.150-astra-1.7 --optionfile /some_directory/option-file-example --mode
unattended --unattendedmodeui minimal
```

Примечание:

Если процесс завершится без ошибок, инсталлятор удалит пакеты, созданные для установки.

Для перехвата `smtp` с учетом мандатных меток на ОС Astra Linux Special Edition 1.7.5.9 "Смоленск":

1. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
2. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.

Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.

Примечание:

После установки Traffic Monitor не меняйте статус мандатных меток в ОС Astra Linux Special Edition 1.7.5.9 "Смоленск". Если до установки в ОС они были включены, не выключайте их, и наоборот.

В противном случае корректная работа Системы не гарантируется.

После установки Traffic Monitor:

1. Если ранее для установки вы создали файл `etc/systemd/system/rsyslog.service`:
   a. Вы можете удалить его с помощью команды:
      `rm /etc/systemd/system/rsyslog.service`
   b. В таком случае выполните команду:
      `systemctl daemon-reload`
2. Если используется ОС Astra Linux Special Edition 1.7.5.9 уровня "Орел", выполните команды:
   `sed -i 's/parsec.max_ilev=63/parsec.max_ilev=0/' /etc/default/grub`
   `update-grub`
3. Перезагрузите сервер, выполнив команду:
   `reboot`

Полный состав файла параметров

В таблице приведен полный список возможных параметров и их значения по умолчанию.

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`use_debug`	`0`	`0, 1`	Включение режима отладки для скриптов, входящих в состав инсталлятора	
`skip_check_swap`	`0`	`0, 1`	Отключение проверки объема Swap-пространства	
`skip_check_space`	`0`	`0, 1`	Отключение проверки объема свободного пространства на диске	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`skip_check_ram`	`0`	`0, 1`	Отключение проверки объема оперативной памяти (RAM)	
`skip_check_network`	`0`	`0, 1`	Отключение проверки доступности сети	
`skip_check_tmp`	`0`	`0, 1`	Отключение проверки временной директории	
`skip_check_home`	`0`	`0, 1`	Отключение проверки домашней директории	
`setup_cron_jobs`	`1`	`0, 1`	Установить задания для планировщика cron	
`log_dir`	`/var/log/infowatch/install`		Путь к директории для лог-файлов	
`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

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				Соглашение принимается по умолчанию.
`product_language`	`rus`	`rus`, `eng`	Основной язык продукта	
`installation_type`	`all_in_one`	`distributed`, `all_in_one`	Тип установки	
`template_database`	`0`	`0`, `1`	Установить шаблон База данных	Если выбрана распределенная установка (`installation_type=distributed`)
`template_indexer`	`0`	`0`, `1`	Установить шаблон Индексер	
`template_web`	`0`	`0`, `1`	Установить шаблон Веб-консоль	
`template_interceptors`	`0`	`0`, `1`	Установить шаблон Перехватчики	
`db_classification_lang_ru`	`1`	`0`, `1`	Установить русский язык для базы классификации	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`)
`db_classification_lang_en`	`0`	`0`, `1`	Установить английский язык для базы классификации	
`db_classification_lang_ma`	`0`	`0`, `1`	Установить малайский язык для базы классификации	
`db_installation_type`	`local`	`local`, `remote`	Расположение базы данных	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`db_server_address`	`iwtm`		Адрес сервера с шаблоном База данных или адрес сервера удаленной базой данных	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_server_port`			Порт сервера с базой данных	
`db_name`	`postgres`		Имя базы данных	
`db_sysdba_password`	`xxXX1234`		Пароль пользователя с правами SYSDBA	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`)
`db_scheme_owner_name`	`iwtm`		Имя владельца схемы базы данных	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`)

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`db_scheme_owner_password`	`xxXX1234`		Пароль владельца схемы базы данных	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`)
`db_linux_user_name`	`iwtm_linux`		Имя пользователя сервисов Linux	
`db_linux_user_password`	`xxXX1234`		Пароль пользователя сервисов Linux	
`db_web_user_name`	`iwtm_web`		Имя пользователя веб-сервисов	
`db_web_user_password`	`xxXX1234`		Пароль пользователя веб-сервисов	
`db_nagios_user`	`iwtm_nagios`		Имя пользователя nagios	
`db_nagios_password`	`xxXX1234`		Пароль пользователя nagios	
`db_auth_change_defaults`	`0`	`0, 1`	Изменить параметры подключения к базе данных по умолчанию	
`db_storage_type`	`normal`	`normal, fast_slow, rotate`	Режим хранения данных	
`db_storage_main_tbs_path`	`/u02/pgdata`		Путь к основному	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
			табличному пространству	
`db_storage_dtbs_paths_number`	`1`	`1` - `10`	Количество путей к ежедневным табличным пространствам	
`db_storage_fast_disk_path`	`/u03/pgdata`		Путь к директории хранения данных ежедневных табличных пространств в быстром разделе	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`)
`db_storage_dtbs_days_on_fast_disk`	`7`		Период хранения данных ежедневных табличных пространств в быстром раздел, в днях	
`db_storage_change_defaults`	`0`	`0, 1`	Изменить параметры хранения в базе данных	
`db_storage_dtbs_path_1`	`/u02/pgdata1`		Путь к ежедневному табличному пространству №1	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`), также зависит от значения параметра `db_storage_d`

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`db_storage_dtbs_path_2`	`/u02/pgdata2`		Путь к ежедневному табличному пространству №2	`tbs_paths_number`
`db_storage_dtbs_path_3`	`/u02/pgdata3`		Путь к ежедневному табличному пространству №3	
`db_storage_dtbs_path_4`	`/u02/pgdata4`		Путь к ежедневному табличному пространству №4	
`db_storage_dtbs_path_5`	`/u02/pgdata5`		Путь к ежедневному табличному пространству №5	
`db_storage_dtbs_path_6`	`/u02/pgdata6`		Путь к ежедневному табличному пространству №6	
`db_storage_dtbs_path_7`	`/u02/pgdata7`		Путь к ежедневному табличному пространству №7	
`db_storage_dtbs_path_8`	`/u02/pgdata8`		Путь к ежедневному табличному пространству №8	
`db_storage_dtbs_path_9`	`/u02/pgdata9`		Путь к ежедневному табличному пространству №9	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`db_storage_dtbs_path_10`	`/u02/pgdata10`		Путь к ежедневному табличному пространству №10	
`db_archiving_dtbs_path`	`/u02/arch`		Путь к директории хранения архивированных табличных пространств	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`)
`db_days_before_archiving_nonviolations`	`45`		Сколько дней хранить события без нарушений до архивирования	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`
`db_archive_nonviolations`	`0`	`0, 1`	Архивировать события без нарушений	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`)

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`db_days_before_archiving_violations`	`45`		Сколько дней хранить события с нарушением до архивирования	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`
`db_archive_violations`	`0`	`0, 1`	Архивировать события с нарушениями	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`)
`db_days_before_archiving_screenshots`	`45`		Сколько дней хранить события скриншотов до архивирования	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`
`db_archive_screenshots`	`0`	`0, 1`	Архивировать события скриншотов	Если выбран тип установки all-in-one (`installation`

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				`_type=all_in_one`) или шаблон База данных (`template_database=1`)
`db_archiving_dtbs_change_defaults`	`0`	`0, 1`	Изменить параметры архивирования по умолчанию	
`db_days_before_removing_nonviolations`	`90`		Сколько дней хранить события без нарушений до удаления	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`
`db_remove_nonviolations`	`0`	`0, 1`	Удалять события без нарушений	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`)
`db_days_before_removing_violations`	`90`		Сколько дней хранить события с нарушением до удаления	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				данных (`template_database=1`), а также `db_remove_violations=1`
`db_remove_violations`	`0`	`0, 1`	Удалять события с нарушением	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`)
`db_days_before_removing_screenshots`	`90`		Сколько дней хранить события скриншотов до удаления	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`
`db_remove_screenshots`	`0`	`0, 1`	Удалять события скриншотов	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`)

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`db_removing_dtbs_change_defaults`	`0`	`0, 1`	Изменить параметры удаления по умолчанию	
`use_data_storage`	`0`	`0, 1`	Использовать внешнее хранилище бинарных данных Data Storage	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон База данных (`template_database=1`). 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

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`ds_set_uri`	`myplatform.infowatch.ru`		Имя хоста или IP-адрес сервера, на котором установлено хранилище Data Storage	подключения к Платформе. Актуальный токен авторизации Data Storage будет указан напротив сущности *DataStorage User*. • В консоли управления продукта Платформы, 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.
`ds_set_port`	`40731`		Порт подключения к Data Storage	
`ds_set_token`	`1exwo92iwpczl1hy6jxy`		Токен авторизации Data Storage	
`consul_bind_addr`	`<список_ip_адресов>`		Адрес сетевого интерфейса Consul	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`consul_mode`	`server` – для шаблона База данных и установки All in one `client` – для остальных шаблонов	`server`, `client`	Режим работы Consul, сервер или клиент	
`consul_datacenter_name`	`iwtm`		Имя дата-центра Consul	
`consul_node_name`	`<hostname>`		Имя ноды	
`consul_retryjoin_manual`			Список агентов Consul	
`consul_retryjoin_port`	`8301`		Порт для подключения агентов Consul	
`ntp_manual_addr`			Адрес NTP сервера	Если выбрано указание NTP-сервера вручную (`ntp_mode=ntp_manual_addr`)
`ntp_mode`	`ntp_use_system`	`ntp_use_system`, `ntp_manual_addr`	Тип NTP сервера: • `ntp_use_system` – использовать системный NTP-сервер; • `ntp_manual_addr` – указать NTP-сервер вручную.	
`sphinx_server_address`			Адрес sphinx-сервера	Если выбран шаблон Веб-консоль

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				(`template_web=1`) и не выбран шаблон Индексер (`template_indexer=0`)
`sphinx_exact_match_words`	`0`	`0, 1`	Включить индексацию на точное совпадение слов	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон Индексер (`template_indexer=1`)
`sphinx_change_language_settings`	`0`	`0,1`	Изменить список языков sphinx	
`sphinx_langs`	`rus`	`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`	Список языков sphinx	Последовательность языков определяет их приоритет
`ocr_enabled`	`1`	`0, 1`	Включить использование OCR	Если выбран тип установки all-in-one (`installation_type=all_in_`

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				`one`), шаблон Перехватчики (`template_interceptors=1`) или шаблон Веб-консоль (`template_web=1`)
`ocr_type`	`ts`	`fre`, `ts`	Выбор OCR-экстрактора: • `fre` – ABBYY FineReader; • `ts` – Tesseract.	Если выбран тип установки all-in-one (`installation_type=all_in_one`) или шаблон Перехватчики (`template_interceptors=1`)
`ocr_finereader_mode`	`quality`	`quick, quality`	Режим работы OCR ABBYY FineReader	Если выбран OCR ABBYYFineReader (`ocr_type=fre`)
`ocr_finereader_have_license`	`1`	`0, 1`	Наличие лицензии на OCR ABBYY FineReader	
`db_unpack_dir`	`/tmp/iwtm_installer/database`	Строка – путь к директории	В директорию будет распакован архив БД	Директория будет создана автоматически. Допускается указать существующую директорию. Если установка завершится без ошибок, директория будет автоматически удалена.

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`packages_unpack_dir`	`/tmp/iwtm_installer/packages`	Строка – путь к директории	В директорию будут распакованы установочные пакеты Traffic Monitor	Директория будет создана автоматически. Допускается указать существующую директорию. Если установка завершится без ошибок, директория будет автоматически удалена.

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

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

Параметры базы данных Traffic Monitor:

`oinstall` – группа владельца инсталляции клиента СУБД, в состав которой включены пользователи `iwtm` и `root`.

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 PostgreSQL	`postgres`	Не задан*

Учетные записи баз данных:

> **Примечание:**
>
> Учетные записи доступны после запуска `psql` .

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

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 TM, бинарных файлов и индексов Sphinx. Редактирование учетной записи недоступно.
- Список групп, в которые входит пользователь `postgres`, ограничен группами этого пользователя.

Учетные записи Веб-консоли управления:

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

4 Обновление Системы

Важно!

Обновление до версии 7.9.X поддерживается с версий 7.7.x и 7.8.x. Порядок выпуска версий Системы указан в статье "Документация InfoWatch Traffic Monitor".

Примечание:

Обновление Системы происходит с использованием подключаемого репозитория.

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

Примечание:

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

Важно!

Перед тем, как приступить к обновлению Системы до версии 7.9.X, запустите скрипт, позволяющий определить наличие дубликатов графических объектов и инициирующий их удаление. Для этого в используемой консоли СУБД PostgreSQL выполните следующий 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 их отсутствии и вы сможете приступить к процедуре обновления.

После завершения работы скрипта осуществите выход пользователя из базы данных.

Важно!

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

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

Примечание:

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

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

Важно!

На сервере под управлением ОС Astra Linux 1.7.0 перед обновлением Traffic Monitor на версию 7.9.X:

1. Обновите ОС до версии 1.7.5.9.
2. Отредактируйте региональные настройки:
   a. В файле `/etc/locale.gen` включите русскую и английскую настройки. Для этого вставьте следующие строки или раскомментируйте их, удалив знак `#`:

```
ru_RU.UTF-8 UTF-8
en_US.UTF-8 UTF-8
```

b. Актуализируйте настройки с помощью команды:
```
locale-gen
```

Перед обновлением убедитесь в наличии:

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

Также до начала обновления требуется выяснить:

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

Важно!

Если в Системе установлен и запущен адаптер Password Disclosure Adapter, перед обновлением ТМ остановите процессы PDA. Подробнее см. документ "InfoWatch Password Disclosure Adapter. Руководство по установке и конфигурированию", статья "Диагностика, обновление и удаление InfoWatch Password Disclosure Adapter".

До начала обновления выполните следующие действия:

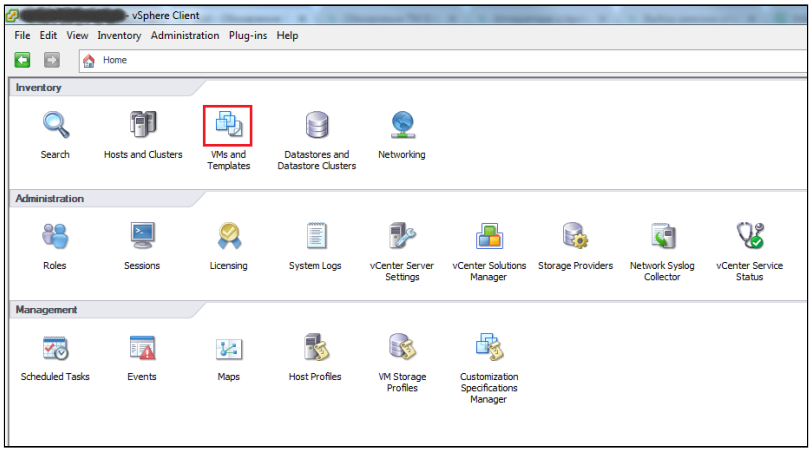
1. Включите (если он был выключен) каждый сервер, предназначенный для обновления:
   - в случае физического сервера – нажмите кнопку включения, расположенную на корпусе сервера (подробнее см. в инструкции к серверу);
   - в случае виртуального сервера – выполните команду **Power On** (см. пример ниже).

   Примечание:

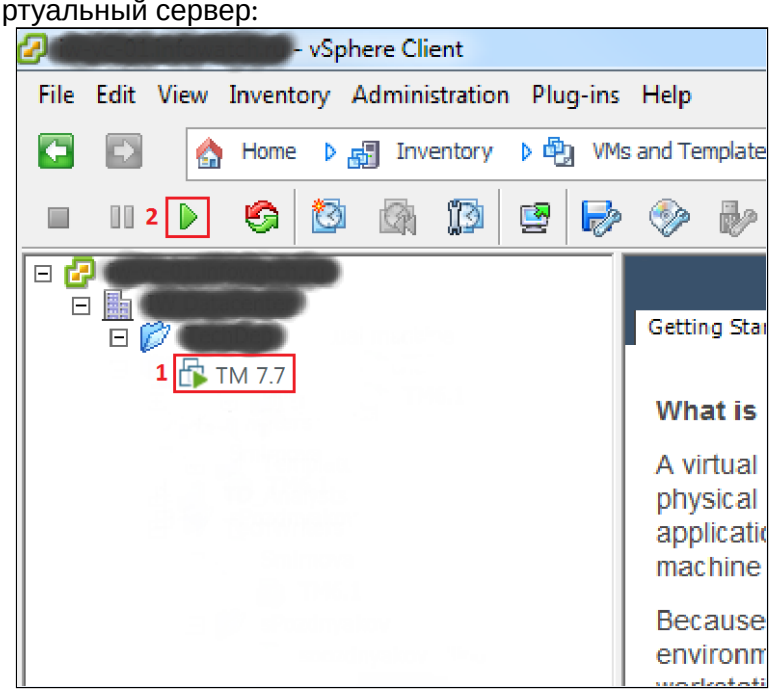
   В настоящей инструкции приводятся примеры по работе с виртуальным сервером в клиентском приложении одной из наиболее часто используемых сред виртуализации – VMware vSphere (VMware vSphere Client).

   Рамками на рисунках выделены области интерфейса, которые нужно последовательно выделять щелчком мыши для достижения требуемых результатов.

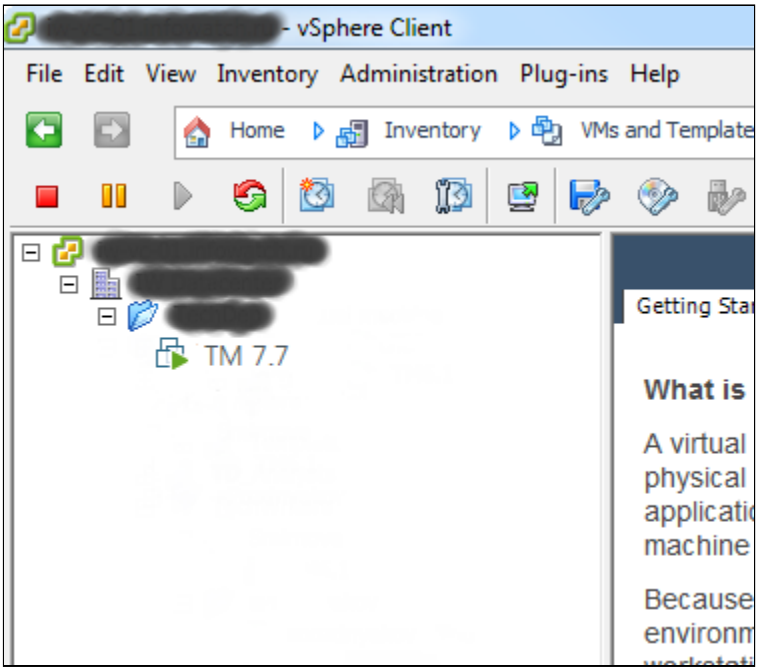
   Запустите клиентское приложение VMware vSphere Client от имени администратора (щелкните правой кнопкой мыши на иконке приложения и выберите **Запуск от имени администратора**). Войдите в приложение, используя логин и пароль, выданные администратором вашей информационной сети. Перейдите в раздел с виртуальными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



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



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



2. Подключите дистрибутив InfoWatch Traffic Monitor к серверам, предназначенным для обновления, используя средства вашей ОС или системы виртуализации.

Обновите серверы согласно следующим инструкциям:

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

Примечание:

Сведения по обновлению подсистемы Device Monitor смотрите в документе *"InfoWatch Device Monitor. Руководство по установке, конфигурированию и администрированию"*.

Примечание:

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

Примечание:

При наличии выгрузок из БД, требуется ожидание до 7 минут после обновления Системы для корректной работы технологии анализа. Если ожидание невозможно, добавьте любой элемент технологии выгрузок из БД и примените конфигурацию. После чего добавленный элемент может быть удален.

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

Важно!

Перед обновлением Traffic Monitor обновите сервер Device Monitor.

Поддерживается обновление с версий **7.7.x** и **7.8.x**.

Для обновления Traffic Monitor потребуется репозиторий Astra Linux.
Вы можете использовать:

- локальный репозиторий с диска `base-1.7.5.9-16.10.23_16.58.iso`.
  О подключении локальных репозиториев вы можете прочитать в статье "Создание локальных и сетевых репозиториев" на официальном сайте компании-разработчика ОС Astra Linux.
- интернет-репозиторий `base`.
  О подключении интернет-репозиториев вы можете прочитать в статье "Интернет-репозитории Astra Linux Special Edition x.7" на официальном сайте компании-разработчика ОС Astra Linux. Убедитесь, что ОС Astra Linux использует загруженные сертификаты, способствующие подключению к репозиториям.

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

- текстовый в консоли сервера;
- графический.

Шаги обновления 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.
2. Введите имя пользователя, от имени которого планируется обновление, и нажмите **Enter**.
3. Введите пароль и нажмите **Enter**.
4. Вызовите командную строку (например, терминал *Fly*).

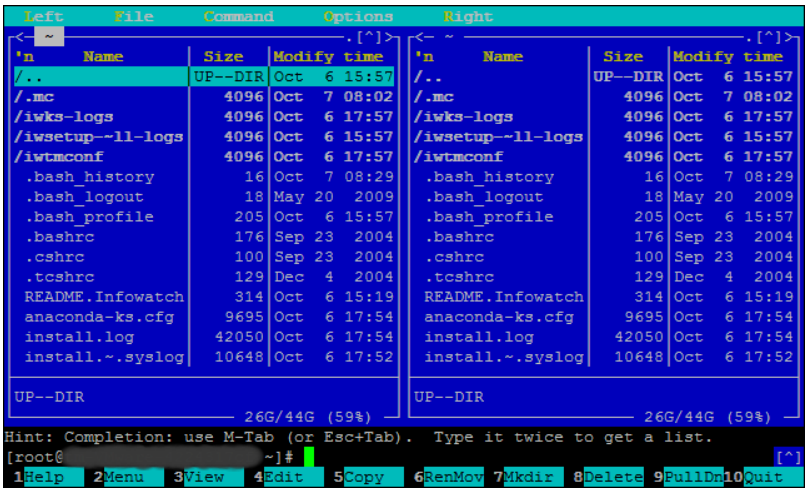
Важно!

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

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

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

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



   На экране отобразится окно файлового менеджера *Midnight Commander*, в котором удобно просматривать файлы.
6. Проверьте версию и тип установки обновляемого сервера. Версия и тип установки указаны в файле `/opt/iw/tm5/install_mode`.

Пример содержимого

```
{
  "product_type": "tme",
  "version": "7.7.2.136",
  "all_in_one": true,
  "templates": {
    "db": {
      "local": true
    },
    "indexer": {},
```

```
    "web": {},
    "interceptors": {}
  },
  "upgrade": {
    "previous_version": "7.6.0.122",
    "state": "done"
  }
}
```


Запись из примера соответствует серверу с типом установки *Traffic Monitor Enterprise All-in-One* и версией *7.7.2.136*.

7. Обновите ОС на сервере, если ее версия отсутствует в списке поддерживаемых версий ОС в статье "Аппаратные и программные требования".
8. Проверьте содержимое файла `/etc/apt/sources.list`. В нем должны быть указаны локальные или внешние репозитории, требуемые для установки.

> **Пример:**
>
> Если вы будете использовать локальные репозитории:
>
> a. Закомментируйте строки, описывающие подключение внешних репозиториев:
> ```
> #deb http://download.astralinux.ru/stable/1.7_x86-64/repository-main/     1.7_x86-64 main contrib non-free
> #deb http://download.astralinux.ru/stable/1.7_x86-64/repository-update/   1.7_x86-64 main contrib non-free
> #deb http://download.astralinux.ru/stable/1.7_x86-64/repository-base/     1.7_x86-64 main contrib non-free
> #deb http://download.astralinux.ru/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main contrib non-free
> ```
> b. Убедитесь, что добавлено и не закомментировано описание подключения репозитория с диска `base`.
> В нашем примере строка вида:
> ```
> deb file:/mnt/ 1.7_x86-64 contrib main non-free
> ```
> В противном случае не должны быть закомментированы строки, описывающие подключение к внешним репозиториям.

> **Важно!**
>
> Если ранее на сервере вы обновляли ОС, убедитесь, что в `/etc/apt/sources.list` указаны **только** репозитории ОС Astra Linux **1.7.5.9**. Если в файле указаны репозитории прошлых версий, отключите их.

9. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
   `exit`
10. Очистите кеш с помощью команды:
    `sudo apt-get clean`

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 будет необходимо 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. Введите команду для остановки Базы данных:
      `systemctl stop 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.

      Примечание:

      Для уточнения директорий, содержащих Базу данных, проверьте также содержимое файла `/opt/iw/tm5/csw/postgres/database.conf`.

      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:

   - `/etc/default/iwtm`
   - `/etc/profile.d/iw-postgresql-env.sh`
   - `/etc/profile.d/iw-postgresql-client-env.sh`
   - `/etc/sudoers.d/iw-pgagent`
   - `/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.

> **Важно!**
>
> Крайне рекомендуется выполнить резервное копирование Системы, а также клонировать ее и провести обновление на этой тестовой машине.

Чтобы обновить Систему выполните следующие действия:

1. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой

системы выполните следующую команду:
`sudo mkdir /distr`

2. Скопируйте в директорию `/root` файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor:
   - **`iwtm-installer-x.x.x.xxx-astra-1.7`** (где `x.x.x.xxx` – номер сборки);
   - **`iwtm-postgresql-11.10-x.x.x.xxx-astra-1.7.tar.gz`**.

   В нашем примере:
   - **`iwtm-installer-7.9.0.150-astra-1.7`**;
   - **`iwtm-postgresql-11.10-7.9.0.150-astra-1.7.tar.gz`**.

   > **Примечание:**
   >
   > Инсталлятор и дальнейшие шаги инструкции подходят для ОС Astra Linux Special Edition 1.7.5.9 уровней "Смоленск", "Воронеж" и "Орел".

3. Чтобы сделать файл **`iwtm-installer-x.x.x.xxx-astra-1.7`** исполняемым, введите команду:
   `sudo chmod u+x /root/iwtm-installer-x.x.x.xxx-astra-1.7`
   В нашем примере команда будет следующей:
   `sudo chmod u+x /root/iwtm-installer-7.9.0.150-astra-1.7`
4. Для обновления пакетов введите команду:
   `sudo apt-get update`
5. Если у вас установлена система Prometheus, для остановки службы отправки данных выполните команду:
   `systemctl stop iwtm-postgres_exporter`
6. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
   `cd /distr`
7. В инсталляторе реализован механизм автоматического объединения конфигурационных файлов Traffic Monitor старой и новой версии.

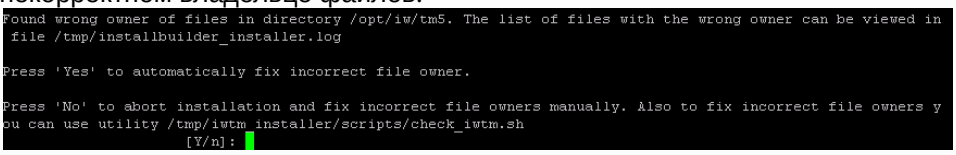
   > **Важно!**
   >
   > Автоматическое объединение затрагивает только конфигурационные файлы Traffic Monitor с расширением **`.conf`**, расположенные в директории `/opt/iw/tm5/etc`.
   > Перед объединением в директории `/opt/iw/tm5/etc_conf_backup_<дата_время>` будут созданы резервные копии исходных конфигурационных файлов. Пример названия директории: `/opt/iw/tm5/etc_conf_backup_05.05.2023_09:26:33`.
   > После успешного объединения файлы с расширением **`.dpkg-dist`**, 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-7.9.0.150-2023-09-10_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.

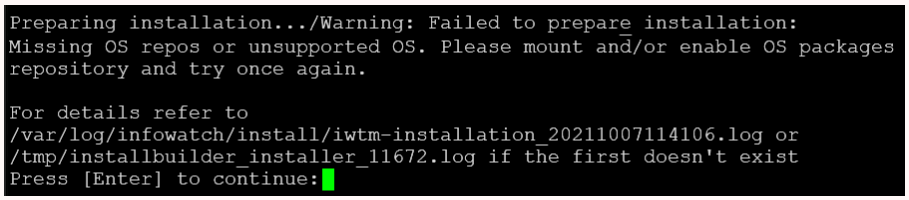
Запустите инсталлятор в одном из режимов:

- **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:
  `sudo ./iwtm-installer-x.x.x.xxx-astra-1.7`
  В нашем примере команда будет следующей:
  `sudo ./iwtm-installer-7.9.0.150-astra-1.7`
  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 репозитории с дисков Astra-Linux и Astra-Linux-Devel 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:

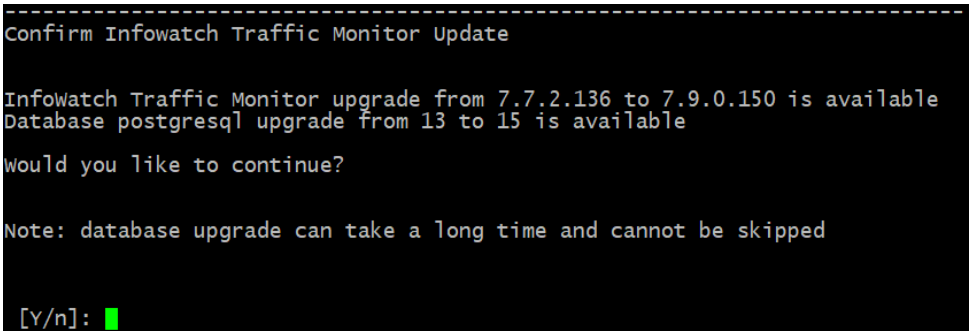
  i. Выберите язык, на котором будет выведен текст Лицензионного соглашения:
  - `English` – английский;
  - `Russian` – русский;

  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:



В окне 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.

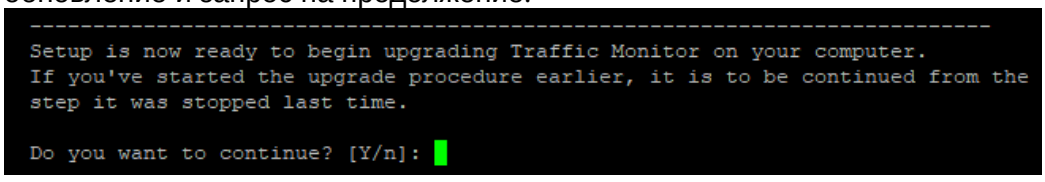
e. Выберите режим остановки Traffic Monitor:
   - `Quick stop` – быстрая остановка без обработки событий;
   - `Waiting for stop` – перед остановкой дождаться завершения текущей обработки событий;
   - `Waiting for emptying file queues` – перед остановкой дождаться обработки всех событий и очистки файловых очередей.

   Для выбора введите цифру, указанную напротив выбранного варианта, и нажмите **Enter**.

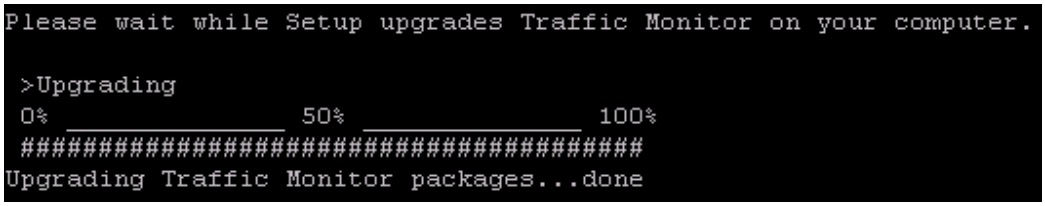
> **Примечание:**
>
> Если выбран `Quick stop`, остановленные сервисы до запуска будут иметь статус `failed (failed)`.

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`

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:
>
> 
>
>
> 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 при завершении работы, их нужно будет запустить вручную.

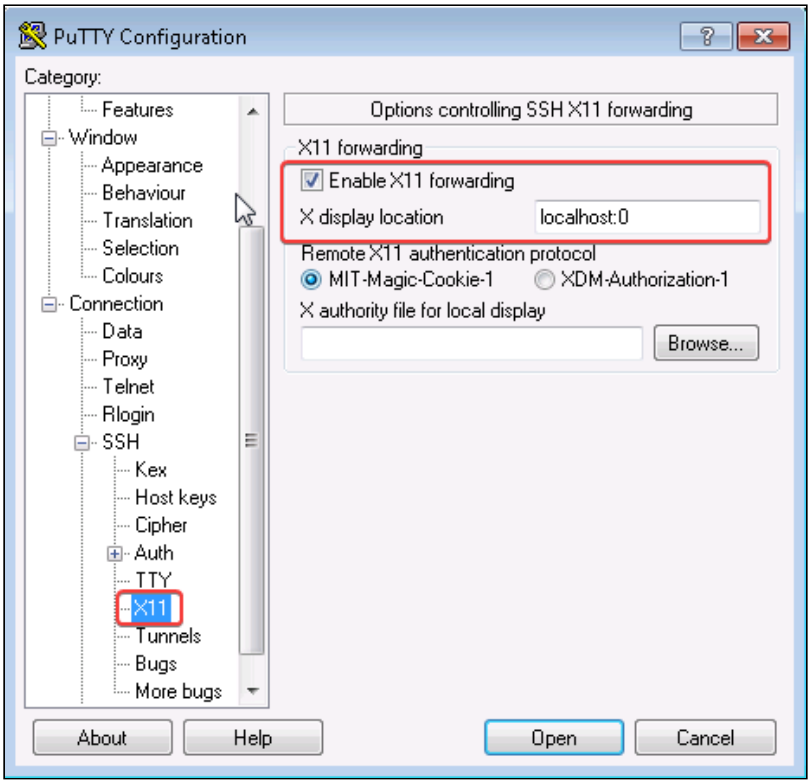
i. Перед завершением работы инсталлятор предложит удалить пакеты, созданные для обновления.
   Если обновление прошло успешно, данные рекомендуется удалить.
j. Дождитесь завершения работы инсталлятора.

- **обновление с использованием графического режима инсталлятора**

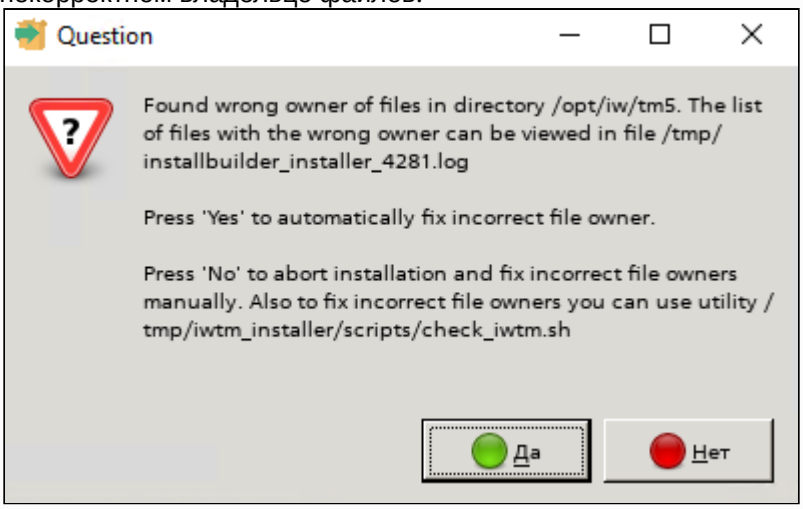
  В ОС оконная система X Window System использует клиент-серверную модель. Для запуска инсталлятора в графическом режиме используется перенаправление графического вывода удаленной подсистемы (**X11 Forwarding**). Это позволит работать напрямую с графическими приложениями среды Linux на компьютере, с которого 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:
        `sudo apt-get 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



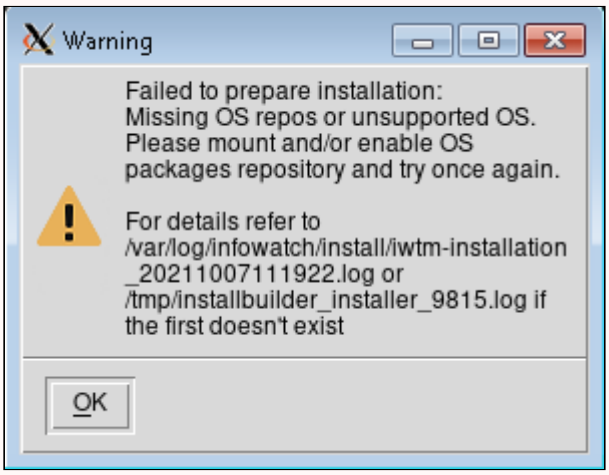
e. Запустите инсталлятор, выполнив следующую команду:
`sudo ./iwtm-installer-x.x.x.xxx-astra-1.7`
В нашем примере команда будет следующей:
`sudo ./iwtm-installer-7.9.0.150-astra-1.7`
Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

> **Примечание:**
>
> Перед запуском инсталлятора может быть выведено предупреждение о некорректном владельце файлов.
>
> 
>
>
> Нажмите кнопку **Да**, чтобы инсталлятор исправил владельца файлов и продолжил запуск.

В противном случае нажмите кнопку **Нет**, исправьте несоответствие вручную или с помощью скрипта `/tmp/iwtm_installer/scripts/check_iwtm.sh` и повторно запустите инсталлятор.

Важно!

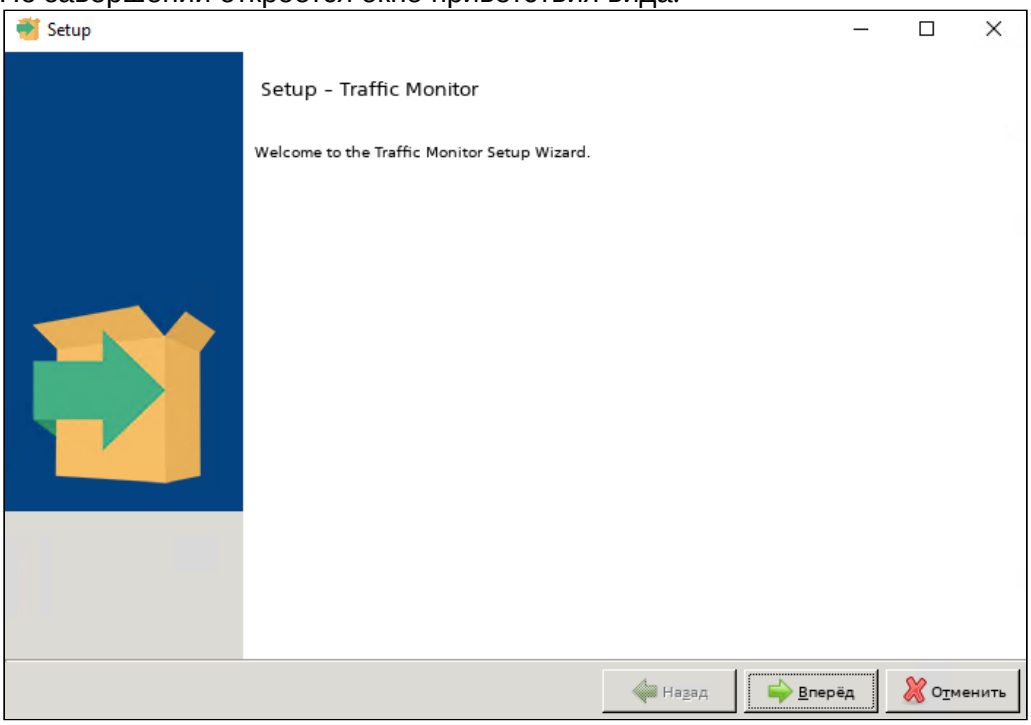
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите **Enter** для завершения работы инсталлятора, затем подключите репозитории с дисков Astra-Linux и Astra-Linux-Devel и повторно запустите инсталлятор.

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

По завершении откроется окно приветствия вида:



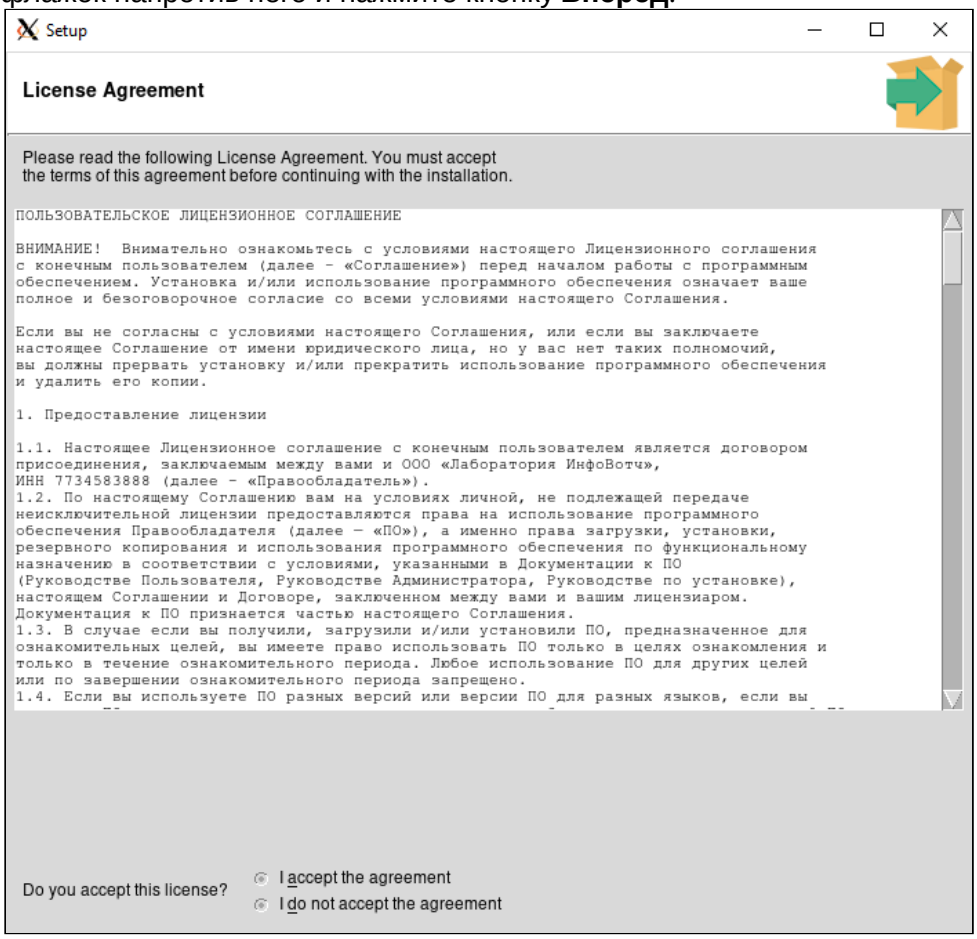
Для перехода к следующему окну используется кнопка **Вперед**, для возврата к предыдущему – **Назад**. Для выхода из инсталлятора – кнопка **Отменить**.

f. Для продолжения обновления необходимо принять условия Лицензионного соглашения. Для этого:
   i. Выберите язык, на котором будет выведен текст Лицензионного соглашения:



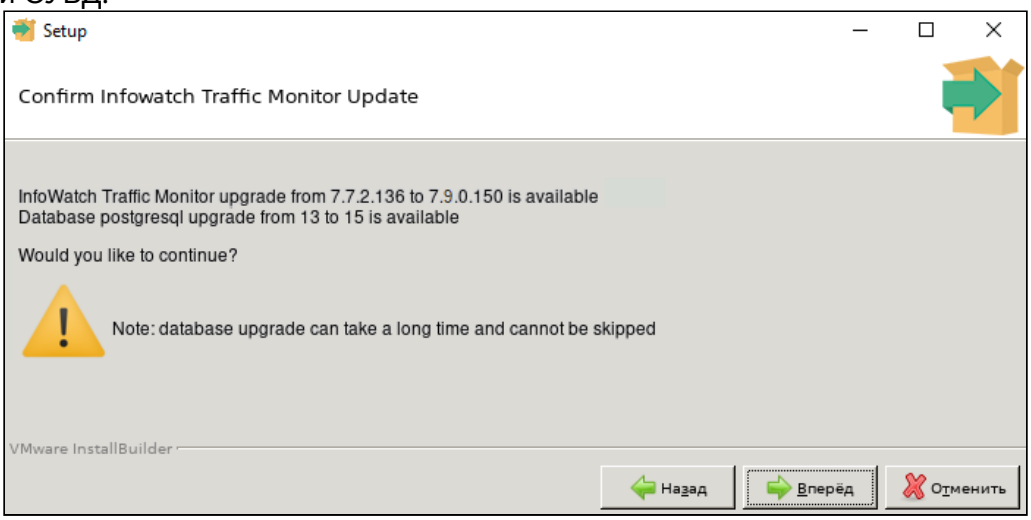
- `English` – английский;
- `Russian` – русский;

ii. Выберите один из предложенных вариантов. Для этого установите флажок напротив него и нажмите кнопку **Вперед**:



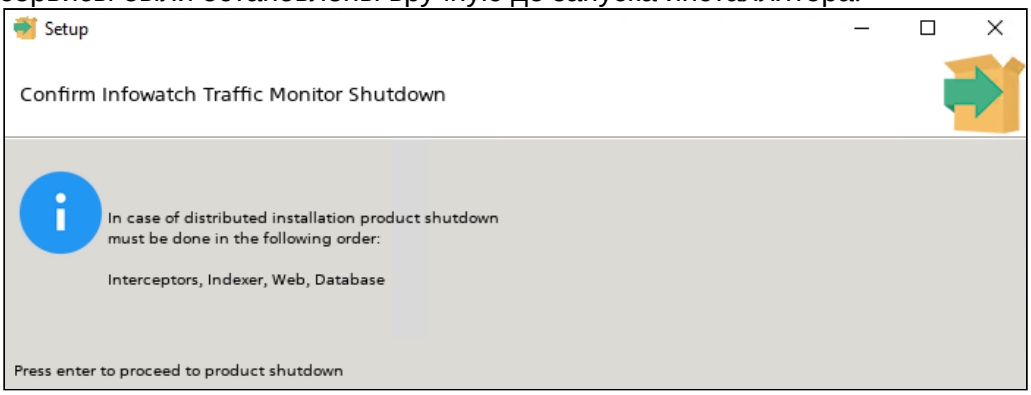
- **`I accept the agreement`** – чтобы принять Лицензионное соглашение и продолжить процесс обновления;
- **`I do not accept the agreement`** – чтобы не принимать Лицензионное соглашение и прервать процесс обновления.

g. В следующем окне будут указаны доступные обновления для Traffic Monitor и СУБД.

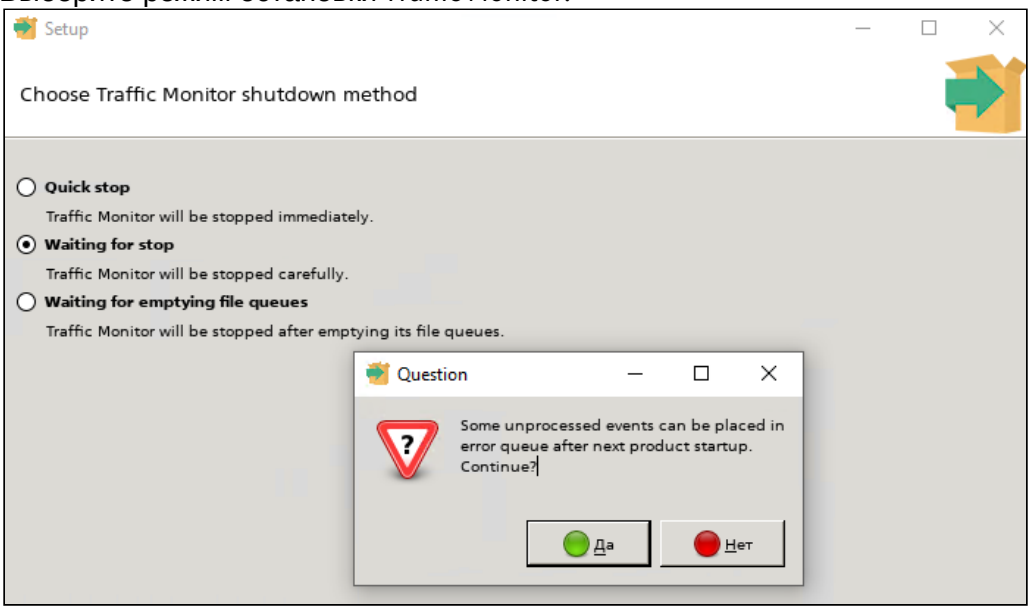


Для продолжения нажмите **Вперед**.

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.

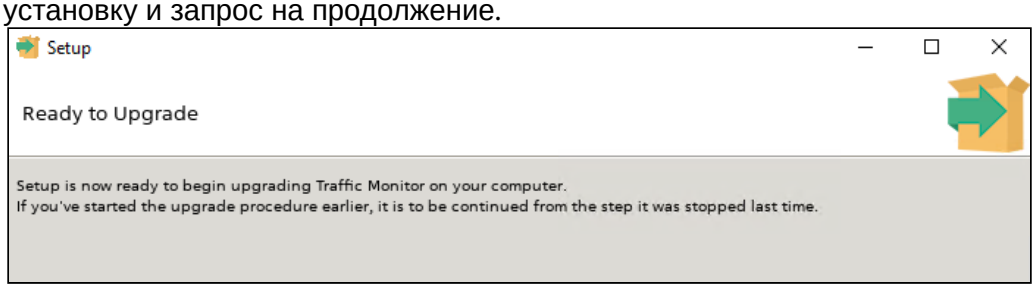
Для выбора установите флажок напротив соответствующего значения и нажмите кнопку **Вперед**.

> **Примечание:**
>
> Если выбран `Quick stop`, остановленные сервисы до запуска будут иметь статус `failed (failed)`.

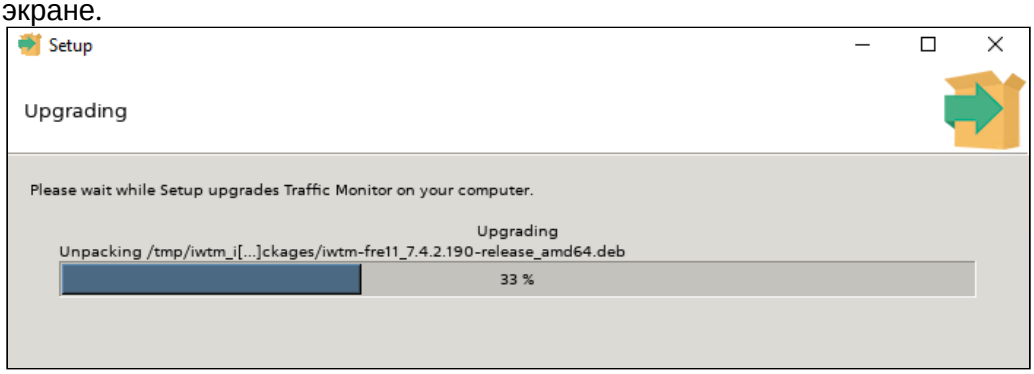
j. Если выбран `Quick stop` или `Waiting for stop`, после возобновления работы Traffic Monitor необработанные события могут попасть в очередь ошибок обработки.
Для продолжения нажмите кнопку **Да**.

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.



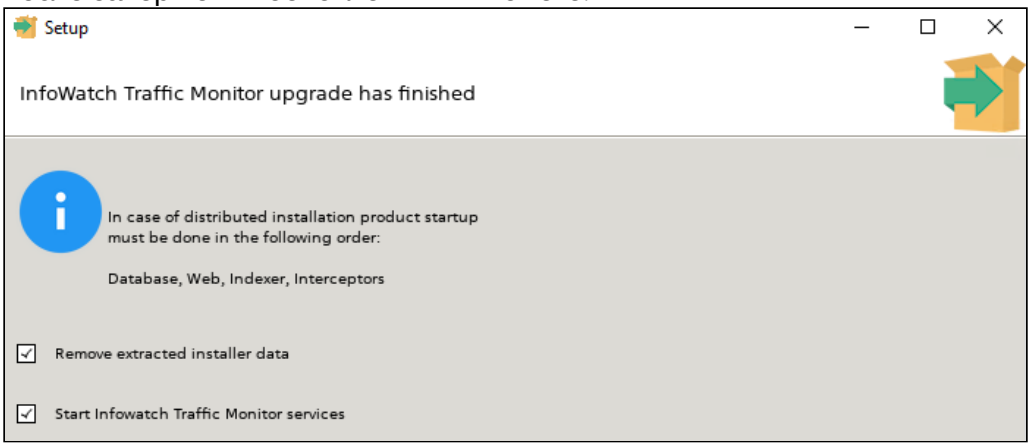
Для начала обновления нажмите кнопку **Вперед**.
Начнется распаковка пакетов, обновление имеющихся и установка новых компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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:

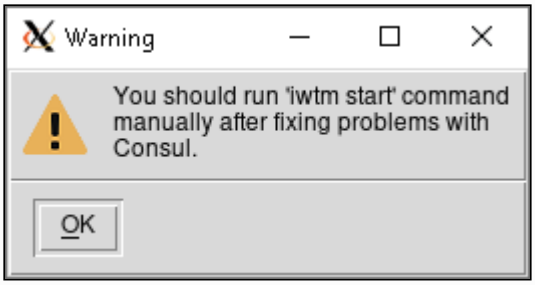


- `Remove exctracted installer data` – удалить пакеты, созданные инсталлятором для установки. Если установка прошла успешно, данные рекомендуется удалить;

- `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`

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**.
>
> **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 при завершении работы, их нужно будет запустить вручную.

m. Для завершения работы инсталлятора нажмите кнопку **Finish**.

- **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.

4.1.1 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-7.9.0.150-astra-1.7 --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.

4.1.2 Тихий режим обновления

Для обновления в тихом режиме используйте опцию `--mode unattended`.

Уровень взаимодействия с пользователем задается параметром `--unattendedmodeui`, который имеет следующие значения:

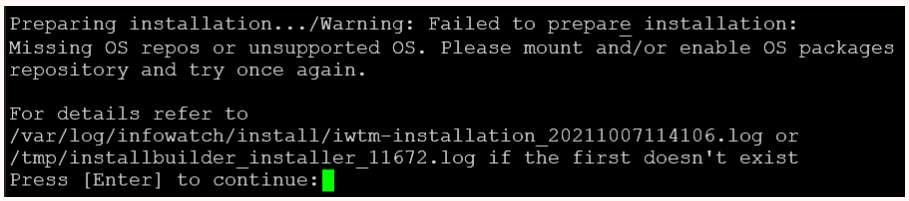
- `none` – в процессе работы инсталлятор не выводит на экран никакую информацию и не требует взаимодействия с пользователем;
- `minimal` – отображает прогресс обновления, не требует взаимодействия с пользователем;
- `minimalWithDialogs` – отображает прогресс обновления, также в процессе могут появляться всплывающие окна, может потребоваться взаимодействие с пользователем.

Пример команды запуска инсталлятора в тихом режиме без участия пользователя и с файлом параметров:

```
./iwtm-installer-7.9.0.150-astra-1.7 --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 репозитории с дисков Astra-Linux-Smolensk и Astra-Linux-Smolensk-Devel 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:

```
\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

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 при завершении работы, их нужно будет запустить вручную.

4.1.3 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	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
			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.
`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	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	Значение по умолчанию	Допустимые значения	Описание	Примечание
			обработки всех событий и очистки файловых очередей.	
`start services after_upgrade`	`1`	`0,1`	Параметр определяет, должен ли инсталлятор запустить ли сервисы после обновления.	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`

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`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.

8. Введите команду для поиска файлов с расширением **`.dpkg-dist`** за исключением резервных копий конфигурационных файлов:
   `sudo find / -name "*.dpkg-dist*" -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").
9. 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.dpkg-dist`** (см. статью "Объединение конфигурационных файлов").
10. Traffic Monitor, начиная с версии 7.8.0, поддерживает OCR-экстрактор ABBYY Finereader 12. 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.
11. 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
Diagnostic information.
/sandbox/src/cas3/handler.cpp(682): Throw in function
 cas::Handler::LoadedConfigData
cas::Handler::GetLoadedConfigData(const prop::Property&, const Ptr&)
Dynamic exception type:
boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
std::exception::what: Cannot open xml file with cas configuration:
etc/config/cas/cas_config.xml
```

После успешной загрузки файла конфигурации `cas_config.xml` Система прекратит запись сообщений об ошибках и заработает в штатном режиме.

Если в течение длительного времени Система продолжает запись об ошибках, проверьте соединение с базой данных.

12. 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`

13. 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/`.

14. Если у вас установлена система Prometheus и если сервер не был перезагружен, для запуска службы выполните команду:
`systemctl start iwtm-postgres_exporter`
15. Введите команду для очистки кеша:
`redis-cli flushall`
16. Введите команду для проверки статусов процессов:
`iwtm status`
На экране отобразится список процессов и их статусы.

> **Примечание:**
>
> После обновления Traffic Monitor не меняйте статус мандатных меток в ОС Astra Linux Special Edition 1.7.5.9 "Смоленск". Если до обновления в ОС они были включены, не выключайте их, и наоборот.
>
> В противном случае корректная работа Системы не гарантируется.

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

Важно!

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

Примечание:

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

4.2 Обновление TM при распределенной установке

Важно!

Перед обновлением Traffic Monitor обновите сервер Device Monitor.

Поддерживается обновление с версий **7.7.x** и **7.8.x**.

Для обновления Traffic Monitor потребуется репозиторий Astra Linux.
Вы можете использовать:

- локальный репозиторий с диска `base-1.7.5.9-16.10.23_16.58.iso`.
  О подключении локальных репозиториев вы можете прочитать в статье "Создание локальных и сетевых репозиториев" на официальном сайте компании-разработчика ОС Astra Linux.
- интернет-репозиторий `base`.
  О подключении интернет-репозиториев вы можете прочитать в статье "Интернет-репозитории Astra Linux Special Edition x.7" на официальном сайте компании-разработчика ОС Astra Linux. Убедитесь, что ОС Astra Linux использует загруженные сертификаты, способствующие подключению к репозиториям.

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

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

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



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

6. Проверьте версию и тип установки обновляемого сервера. Версия и тип установки указаны в файле `/opt/iw/tm5/install_mode`.

Пример содержимого

```
{
  "product_type": "tme",
  "version": "7.7.2.136",
  "all_in_one": false,
  "templates": {
    "db": {
      "local": true
    },
    "indexer": {},
  }
}
```

Запись из примера соответствует серверу с *распределенной* установкой *Traffic Monitor Enterprise* версии *7.7.2.136*. На сервере из примера активированы шаблоны *База данных* и *Индексер*. Используется *локальная* база данных.

7. Обновите ОС на сервере, если ее версия отсутствует в списке поддерживаемых версий ОС в статье "Аппаратные и программные требования".
8. Проверьте содержимое файла `/etc/apt/sources.list`. В нем должны быть указаны локальные или внешние репозитории, требуемые для установки.

Пример:

Если вы будете использовать локальные репозитории:

a. Закомментируйте строки, описывающие подключение внешних репозиториев:

```
#deb http://download.astralinux.ru/stable/1.7_x86-64/
repository-main/     1.7_x86-64 main contrib non-free
```

```
#deb http://download.astralinux.ru/stable/1.7_x86-64/
repository-update/   1.7_x86-64 main contrib non-free
#deb http://download.astralinux.ru/stable/1.7_x86-64/
repository-base/     1.7_x86-64 main contrib non-free
#deb http://download.astralinux.ru/stable/1.7_x86-64/
repository-extended/ 1.7_x86-64 main contrib non-free
```

b. Убедитесь, что добавлено и не закомментировано описание подключения репозитория с диска `base`.
В нашем примере строка вида:
`deb file:/mnt/ 1.7_x86-64 contrib main non-free`

В противном случае не должны быть закомментированы строки, описывающие подключение к внешним репозиториям.

Важно!

Если ранее на сервере вы обновляли ОС, убедитесь, что в `/etc/apt/sources.list` указаны **только** репозитории ОС Astra Linux **1.7.5.9**. Если в файле указаны репозитории прошлых версий, отключите их.

9. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
`exit`
10. Очистите кеш с помощью команды:
`sudo apt-get clean`

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. Введите команду для остановки Базы данных:
    `systemctl stop postgresql-13`

    > **Примечание:**
    >
    > Для уточнения директорий, содержащих Базу данных, проверьте также содержимое файла `/opt/iw/tm5/csw/postgres/database.conf`.

    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:

   - `/etc/default/iwtm`
   - `/etc/profile.d/iw-postgresql-env.sh`
   - `/etc/profile.d/iw-postgresql-client-env.sh`
   - `/etc/sudoers.d/iw-pgagent`
   - `/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.

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, при помощи которых были установлены серверы:

1. Перехватчики
2. Индексер
3. Веб-консоль
4. База данных

Процесс обновления серверов инсталлятором аналогичен для всех шаблонов. Если действие относится только к серверу, установленному с помощью конкретного шаблона, это будет указано. Остальные действия относятся ко всем серверам.

Порядок обновления следующий:

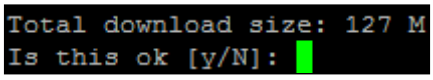
Шаг 1. Обновление всех серверов.
Шаг 2. Проверка кластера службы Consul.
Шаг 3. Проверка работоспособности внутренних сервисов Системы.
Шаг 4. Завершение обновления серверов.

ШАГ 1. ОБНОВЛЕНИЕ ВСЕХ СЕРВЕРОВ

Чтобы обновить серверы, на каждом из них выполните следующие действия:

1. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой системы выполните следующую команду:
   `sudo mkdir /distr`
2. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor:
   - **`iwtm-installer-x.x.x.xxx-astra-1.7`** (где x.x.x.xxx – номер сборки);
   - **`iwtm-postgresql-11.10-x.x.x.xxx-astra-1.7.tar.gz`**.

   В нашем примере:
   - **`iwtm-installer-7.9.0.150-astra-1.7`**;
   - **`iwtm-postgresql-11.10-7.9.0.150-astra-1.7.tar.gz`**.
3. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
   `cd /distr`
4. Чтобы сделать файл **`iwtm-installer-x.x.x.xxx-astra-1.7`** исполняемым, введите команду:
   `sudo chmod u+x ./iwtm-installer-x.x.x.xxx-astra-1.7`
   В нашем примере команда будет следующей:
   `sudo chmod u+x ./iwtm-installer-7.9.0.150-astra-1.7`
5. Для обновления пакетов введите команду:
   `sudo apt-get update`
   Будет выведен запрос вида:

   Для продолжения наберите **Y** на клавиатуре и нажмите **Enter**.
6. Если у вас установлена система Prometheus, на сервере, установленном при помощи шаблона База данных, для остановки службы выполните команду:
   `systemctl stop iwtm-postgres_exporter`
7. На сервере, установленном при помощи шаблона База данных, перед запуском инсталлятора рекомендуется запустить сервис базы данных, если ранее он был остановлен:
   `service postgresql start`
8. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor:
   `cd /root`
9. 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_05.06.2023_09:26:33`.
   После успешного объединения файлы с расширением **`.dpkg-dist`**, которые относятся к затрагиваемым конфигурационным файлам, будут удалены.
   Все выполненные действия будут отражены в лог-файле `/var/log/infowatch/iwtm-`

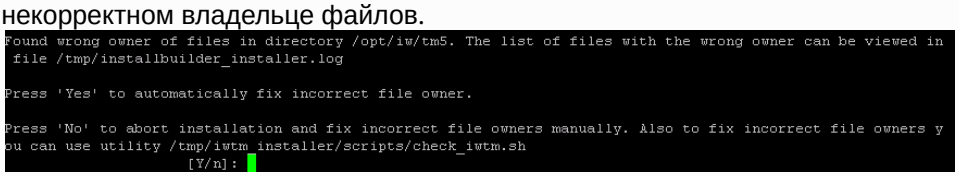
`install-<версия>-<дата>_<время>.log`. Пример названия лог-файла: `/var/log/iwtm-install-7.9.0.150-2023-09-10_09-56-25.log`.
Также информацию о процессе можно найти в директории `/var/log/infowatch/config_merge/`.
Если во время действий с конфигурационным файлом будут обнаружены ошибки, процесс будет остановлен до исправления ошибок пользователем. После исправления ошибок повторно запустите обновление.

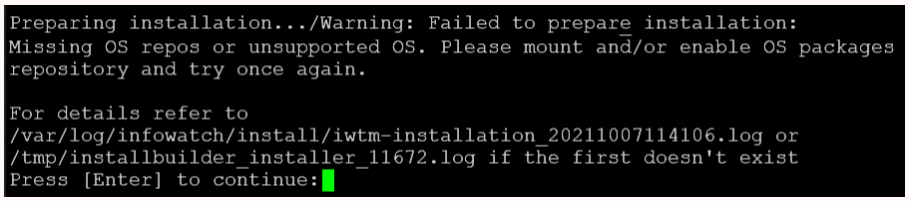
Запустите инсталлятор в одном из режимов:

- **обновление в текстовом режиме в консоли сервера**

  Чтобы обновить Traffic Monitor в консоли сервера, выполните следующие действия:

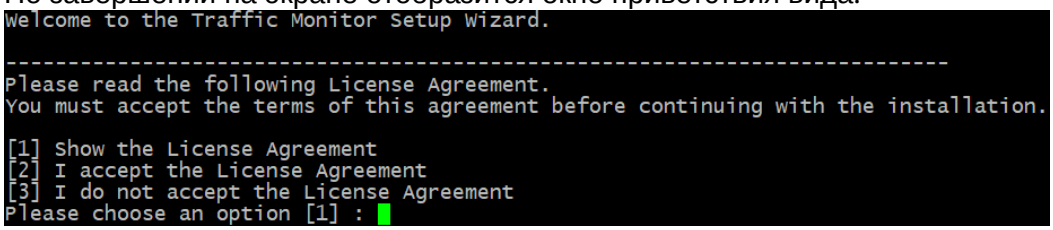
  a. Для обновления Traffic Monitor запустите инсталлятор, выполнив следующую команду:
  `sudo ./iwtm-installer-x.x.x.xxx-astra-1.7`
  В нашем примере команда будет следующей:
  `sudo ./iwtm-installer-7.9.0.150-astra-1.7`
  Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка 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 репозитории с дисков Astra-Linux и Astra-Linux-Devel 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:

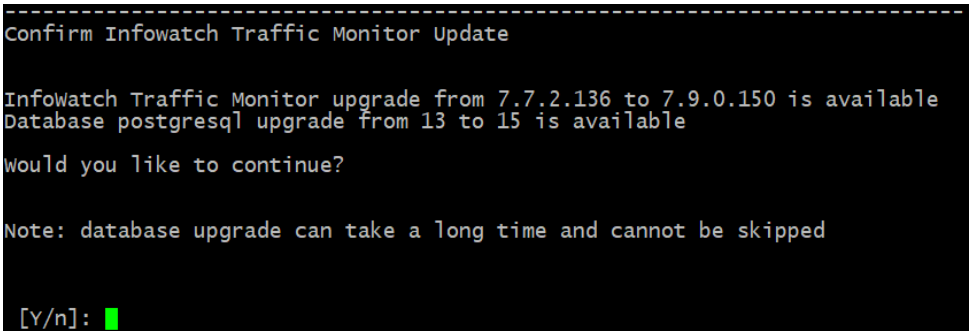


b. Для продолжения обновления необходимо принять условия Лицензионного соглашения. Выберите один из предложенных вариантов. Для этого введите цифру, указанную напротив него, и нажмите **Enter**:

- `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.

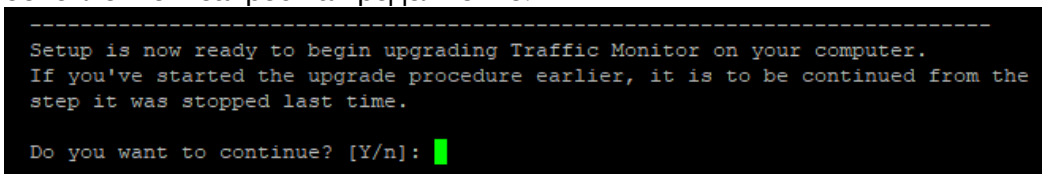
Для выбора введите цифру, указанную напротив выбранного варианта, и нажмите **Enter**.

> **Примечание:**

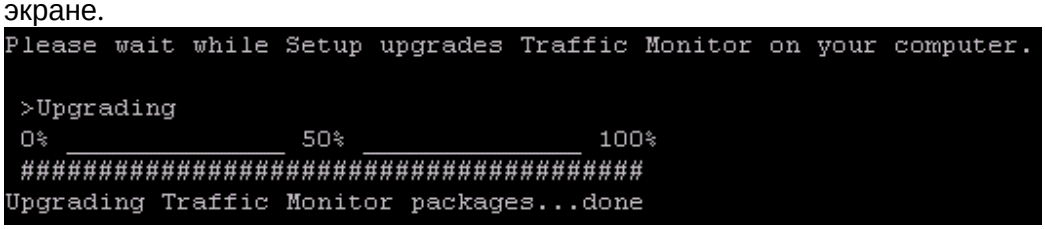
Если выбран `Quick stop`, остановленные сервисы до запуска будут иметь статус `failed (failed)`.

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 с активированным шаблоном 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`

- **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:

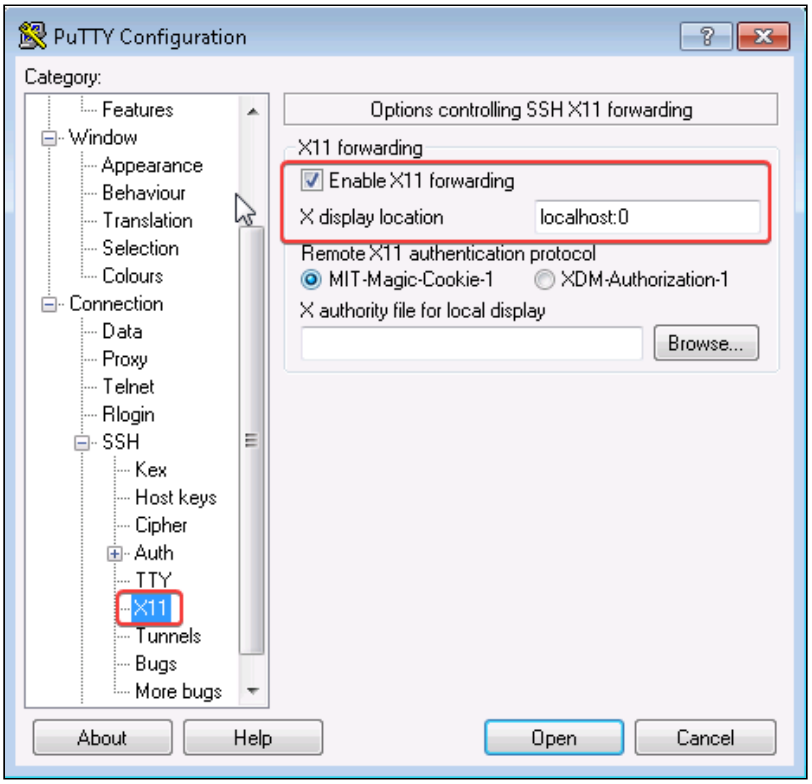
  a. На обновляемом сервере:
     i. Установите утилиту `xauth` с помощью команды:
     `sudo apt-get install xauth`
     ii. В конфигурационном файле `/etc/ssh/sshd_config` раскомментируйте строку "`X11Forwarding yes`". Для этого удалите перед строкой символ `#`.
     iii. Сохраните изменения в конфигурационном 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. Для обновления Traffic Monitor запустите инсталлятор, выполнив следующую команду:

```
sudo ./iwtm-installer-x.x.x.xxx-astra-1.7
```

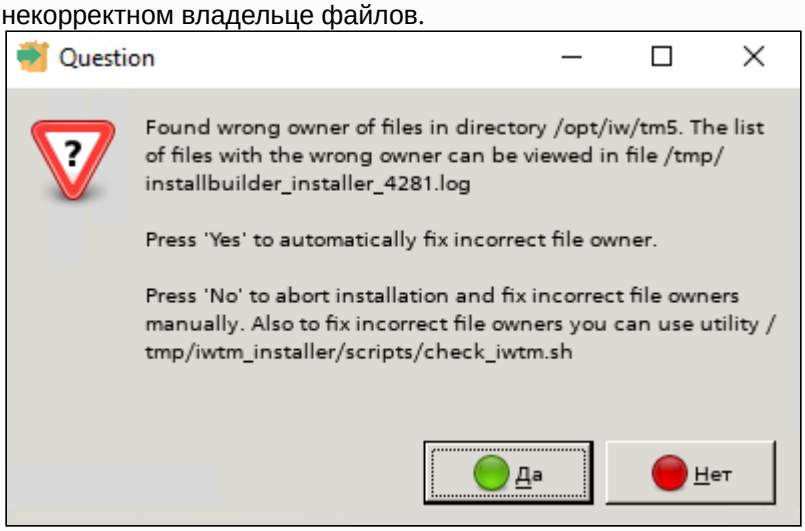
В нашем примере команда будет следующей:

```
sudo ./iwtm-installer-7.9.0.150-astra-1.7
```

Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

> **Примечание:**

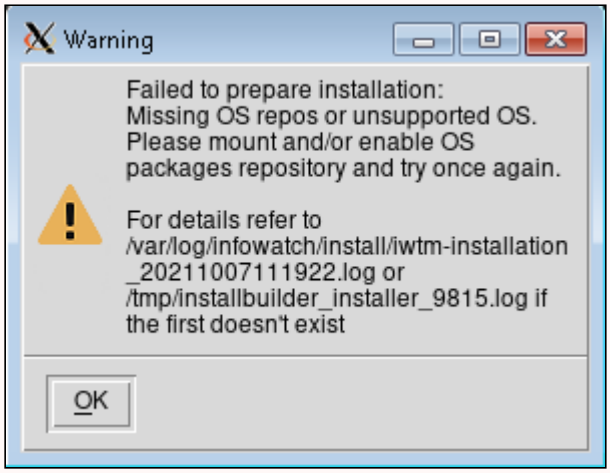
Перед запуском инсталлятора может быть выведено предупреждение о некорректном владельце файлов.



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!

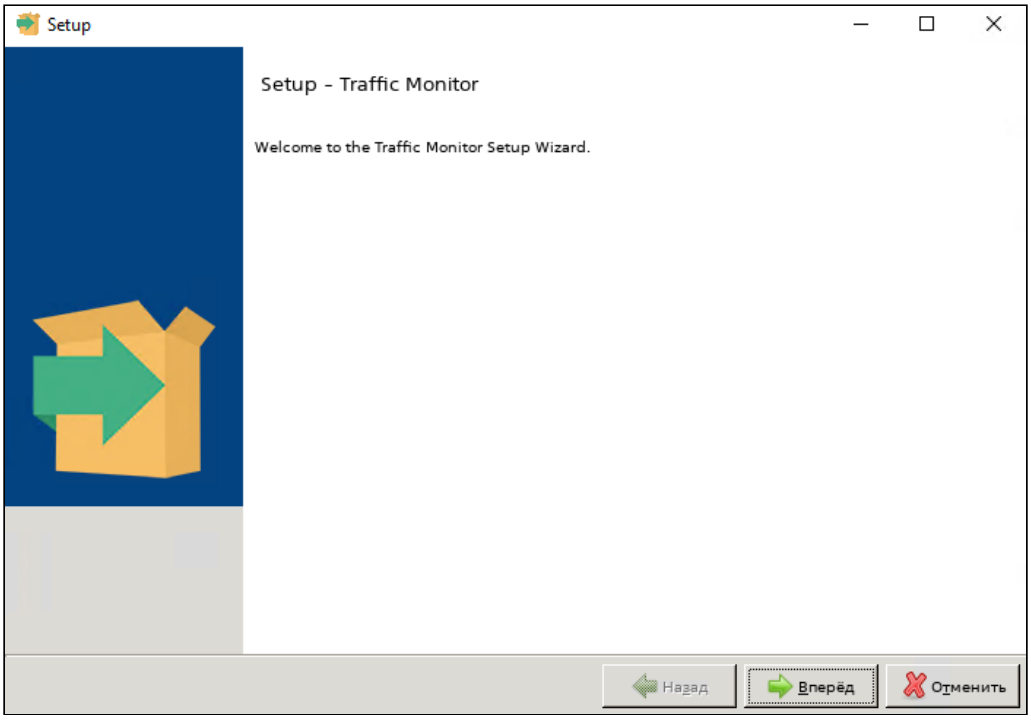
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите **Enter** для завершения работы инсталлятора, затем подключите репозитории с дисков Astra-Linux и Astra-Linux-Devel и повторно запустите инсталлятор.

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

По завершении откроется окно приветствия вида:



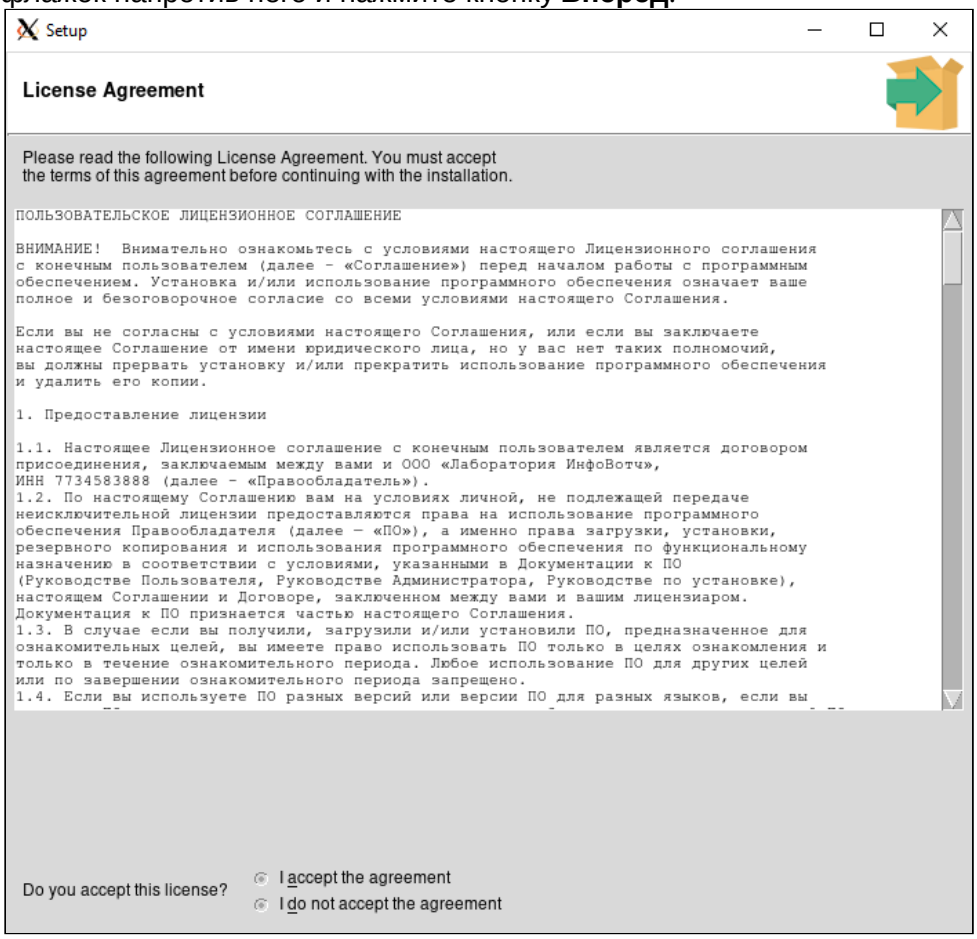
Для перехода к следующему окну используется кнопка **Вперед**, для возврата к предыдущему – **Назад**. Для выхода из инсталлятора – кнопка **Отменить**.

f. Для продолжения обновления необходимо принять условия Лицензионного соглашения. Для этого:
   i. Выберите язык, на котором будет выведен текст Лицензионного соглашения:



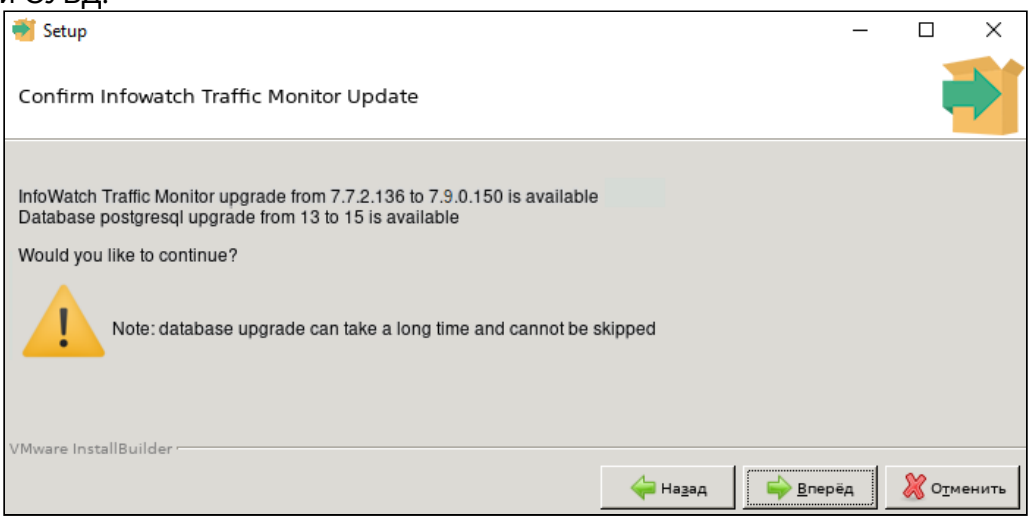
- `English` – английский;
- `Russian` – русский;

ii. Выберите один из предложенных вариантов. Для этого установите флажок напротив него и нажмите кнопку **Вперед**:



- `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.



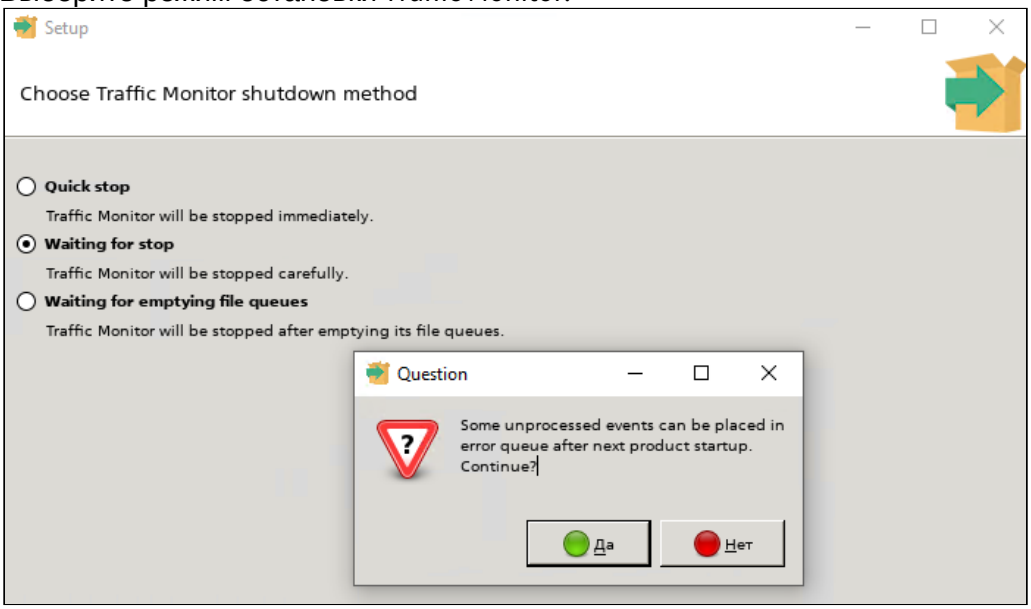
Для продолжения нажмите **Вперед**.

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.

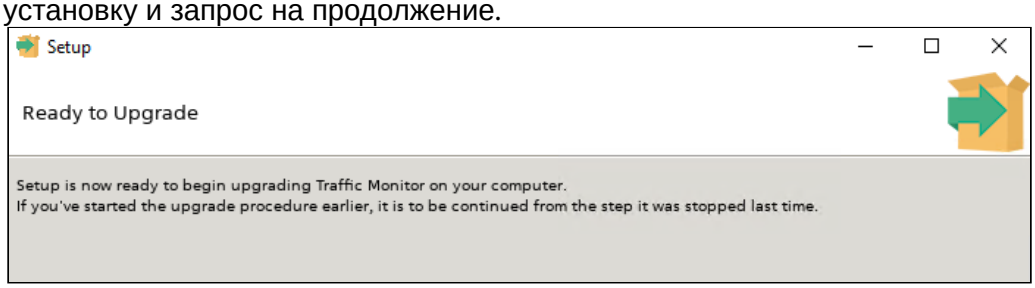
> **Важно!**
>
> Если компоненты перехвата и компоненты анализа (`iw_cas` , `iw_pas`) используются на разных серверах, остановка перехватчиков с очисткой файловых очередей может зависнуть. Рекомендуется использовать другие режимы или остановить компоненты вручную.

Для выбора установите флажок напротив соответствующего значения и нажмите кнопку **Вперед**

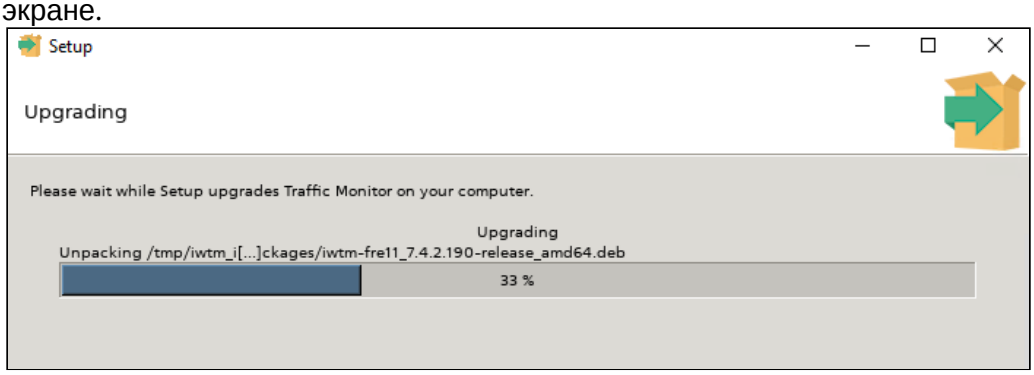
> **Примечание:**
>
> Если выбран `Quick stop` , остановленные сервисы до запуска будут иметь статус `failed (failed)` .

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 **Да**.
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 **Вперед**.
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:

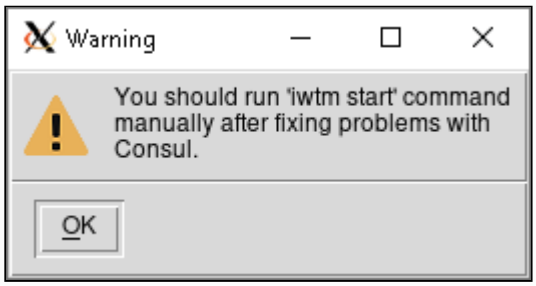


- `Remove exctracted installer data` – удалить пакеты, созданные инсталлятором для установки. Если установка прошла успешно, данные рекомендуется удалить;
- `Start Infowatch Traffic Monitor services` – запустить остановленные сервисы.

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 с активированным шаблоном 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`

m. Для завершения работы инсталлятора нажмите кнопку **Finish** 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.

4.2.1 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-7.9.0.150-astra--1.7 --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.

4.2.2 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-7.9.0.150-astra-1.7 --optionfile /some_directory/option-file-example --mode unattended --unattendedmodeui minimal
```

> **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, затем подключите репозитории с дисков Astra-Linux и Astra-Linux-Devel 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:

```
\Warning: You should run 'iwtm start' command manually after fixing problems with
Consul.
Press [Enter] to continue:
```

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.

4.2.3 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	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
			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 с помощью 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.	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 компоненты Traffic Monitor функционируют на нескольких серверах, они должны быть запущены в следующей последовательности: a. База данных b. Веб-консоль c. Индексер d. Перехватчики

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`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.

10. Введите команду для поиска файлов с расширением **`.dpkg-dist`** за исключением резервных копий конфигурационных файлов:
    `sudo find / -name "*.dpkg-dist*" -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").
11. 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`.

12. Traffic Monitor, начиная с версии 7.8.0, поддерживает OCR-экстрактор ABBYY Finereader 12. 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.
13. Проверьте кластер службы Consul – описание смотрите ниже.

ШАГ 2. ПРОВЕРКА КЛАСТЕРА СЛУЖБЫ CONSUL

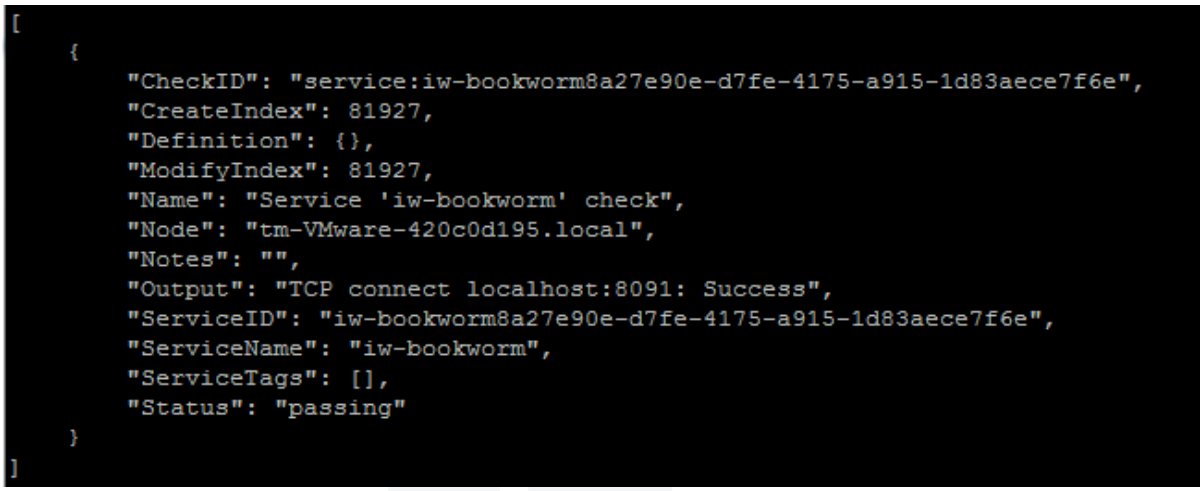
Для проверки кластера Consul выполните следующие действия:

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 с помощью 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.
```

```
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.

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 у вас установлена 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`
5. На сервере, установленном с помощью шаблона Веб-консоль, введите команду для очистки кеша:
   `redis-cli flushall`

6. Введите команду для проверки статусов процессов:
   `iwtm status`
   На экране отобразится список процессов и их статусы.

Примечание:

После обновления Traffic Monitor не меняйте статус мандатных меток в ОС Astra Linux Special Edition 1.7.5.9 "Смоленск". Если до обновления в ОС они были включены, не выключайте их, и наоборот.

В противном случае корректная работа Системы не гарантируется.

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

Важно!

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

Примечание:

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

4.3 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`.

Важно!

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

Используйте любой из приведенных ниже способов объединения файлов.

4.3.1 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"
}
```

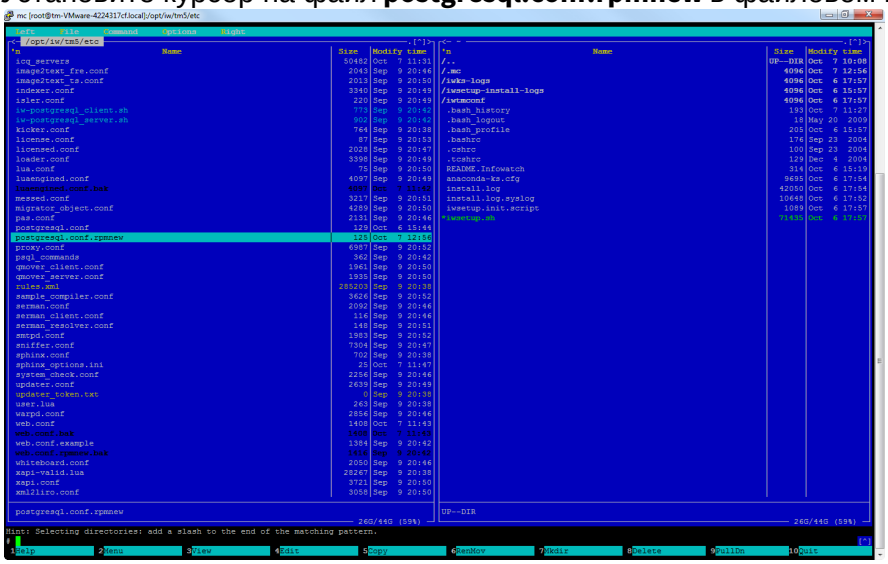
Файл **postgresql.conf.rpmnew** имеет вид:

```
{
    "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"
}
```

4.3.2 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

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. Руководство по установке, конфигурированию и администрированию"*.

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.

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/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*", статья "Предустановленные политики");
- запросы и отчеты (см. "*InfoWatch Traffic Monitor. Руководство пользователя*", разделы "Запросы" и "Отчеты");
- плагины и токены (см. "*InfoWatch Traffic Monitor. Руководство пользователя*", статья "Плагины").

Для восстановления плагина Device Monitor, предустановленных запросов и отчетов, а также для повторного распространения предустановленных политик после повторной установки БД выполните следующие действия:

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

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

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*", раздел Администрирование базы данных > PostgreSQL > Резервное копирование базы данных, статья "Создание резервной копии базы данных").
Также рекомендуется создать резервные копии конфигурации и настроек.

Процесс удаления Traffic Monitor запускается в консоли сервера. Удаление 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, созданного при установке).
2. Остановите процессы Traffic Monitor с помощью команды:
   `iwtm stop`
3. Для удаления пакетов Traffc Monitor и символических ссылок последовательно выполните команды:

```
sudo dpkg-query -f '${Package}\n' -W | grep -E "iwtm" | sudo xargs apt-get -y purge 2>/dev/null || true
sudo apt-get -y autoremove --purge
sudo update-rc.d pgagent remove
sudo rm -f /etc/init.d/pgagent
sudo apt-get clean
sudo rm -f /etc/apt/sources.list.d/tm-*.list
```

   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 **.dpkg-dist** - например, **web.conf.dpkg-dist**; файлы, которые не изменялись, будут удалены);
- очередь объектов (о порядке удаления файлов из директории временных файлов операционной системы и данных из директорий файловых очередей Traffic Monitor см.

«*InfoWatch Traffic Monitor. Руководство администратора*», статья "Удаление временных файлов");
- 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:

```
sudo rm -Rvf /opt/iw
```

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 «'».

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.

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