

INFOWATCH

InfoWatch Traffic Monitor 7.5

Руководство по установке

27/06/2023

© 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

2.1.1 Шаблон База данных 5

2.1.2 Шаблон Индексер 6

2.1.3 Шаблон Веб-консоль 6

2.1.4 Шаблон Перехватчики 8

2.2 Аппаратные и программные требования 12

2.3 Требования к настройкам ОС и сети сервера 15

2.4 Настройка удаленной базы данных 17

3 Установка Системы 21

3.1 Установка InfoWatch Traffic Monitor 22

3.1.1 Установка ТМ в режиме "Все-в-одном" 23

3.1.2 Распределенная установка ТМ 41

3.1.3 Установка в тихом режиме с файлом параметров 77

Файл параметров (option file) 79

Тихий режим установки 79

Полный состав файла параметров 80

3.2 Предустановленные серверные параметры 94

4 Обновление Системы 96

4.1 Обновление ТМ Все-в-одном (All-in-one) 99

4.1.1 Файл параметров (option file) 115

4.1.2 Тихий режим обновления 116

4.1.3 Полный состав файла параметров 117

4.2 Обновление ТМ при распределенной установке 122

4.2.1 Файл параметров (option file) 139

4.2.2 Тихий режим обновления 140

4.2.3 Полный состав файла параметров 141

4.3 Объединение конфигурационных файлов 149

4.3.1 Объединение конфигурационных файлов в Midnight Commander 150

4.3.2 Объединение конфигурационных файлов с помощью vimdiff 151

5 Удаление Системы 153

5.1 Удаление схемы базы данных 153

5.2 Удаление Traffic Monitor 154

6 Приложение A. Рекомендации по составлению имен и паролей 156

7 Приложение B. Лицензии на стороннее программное обеспечение 157

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 может поставляться в нескольких вариантах. При этом имеет значение режим установки Системы и распределение компонентов.

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.
На один сервер может быть установлено одновременно несколько шаблонов.

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:

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

2.1.1 Шаблон База данных

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

К шаблону База данных относятся следующие процессы:

Имя процесса	Краткое описание назначения
`iw_agent`	Требуется для управления конфигурацией Системы
`iw_system_check`	Контроль состояния Системы

2.1.2 Шаблон Индексер

Шаблон содержит 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`	Используется для полнотекстового поиска по событиям
`iw_is`	Выполняет индексацию метаданных
`iw_metainfo_fetcher`	Осуществляет выборку данных для индексации из базы
`iw_system_check`	Контроль состояния Системы

Важно!

Следующие процессы в одном кластере должны быть в единственном экземпляре:

- `iw_indexer`;
- `iw_is`.

В противном случае возникнет несогласованность данных в Системе.

2.1.3 Шаблон Веб-консоль

Шаблон содержит 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
`iw_configerator`	Формирует конфигурацию для Device Monitor
`iw_deliver`	Выполняет досылку писем из карантина по решению офицера безопасности
`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`	Контроль состояния 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 текстовых данных из перехваченных объектов

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.

2.1.4 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.

Также компоненты шаблона могут взаимодействовать с подсистемой Device Monitor. Компоненты шаблона также могут взаимодействовать с внешними системами, для этого используются специальные адаптеры. В отличие от других шаблон Перехватчики может быть установлен несколько раз в одном кластере. Его использование упрощает процесс масштабирования Системы. Для обеспечения эффективной работы процессов, создающих высокую нагрузку на сервер, рекомендуется использовать несколько серверов Traffic Monitor с данным шаблоном.

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 контекстный анализ перехваченных данных

Имя процесса	Краткое описание назначения
`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.
`iw_system_check`	Контроль состояния Системы
`iw_updater`	Загружает конфигурацию из базы данных
`iw_warpd`	Управляет извлечением текстовых данных из перехваченных объектов
`iw_xapi_xapi`	Получает объекты от Infowatch Device Monitor
`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".

В максимально развернутой конфигурации может выглядеть следующим образом:

- **Отдельные серверы Traffic Monitor с шаблонами:**
  - **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.

Существуют следующие типы установки:

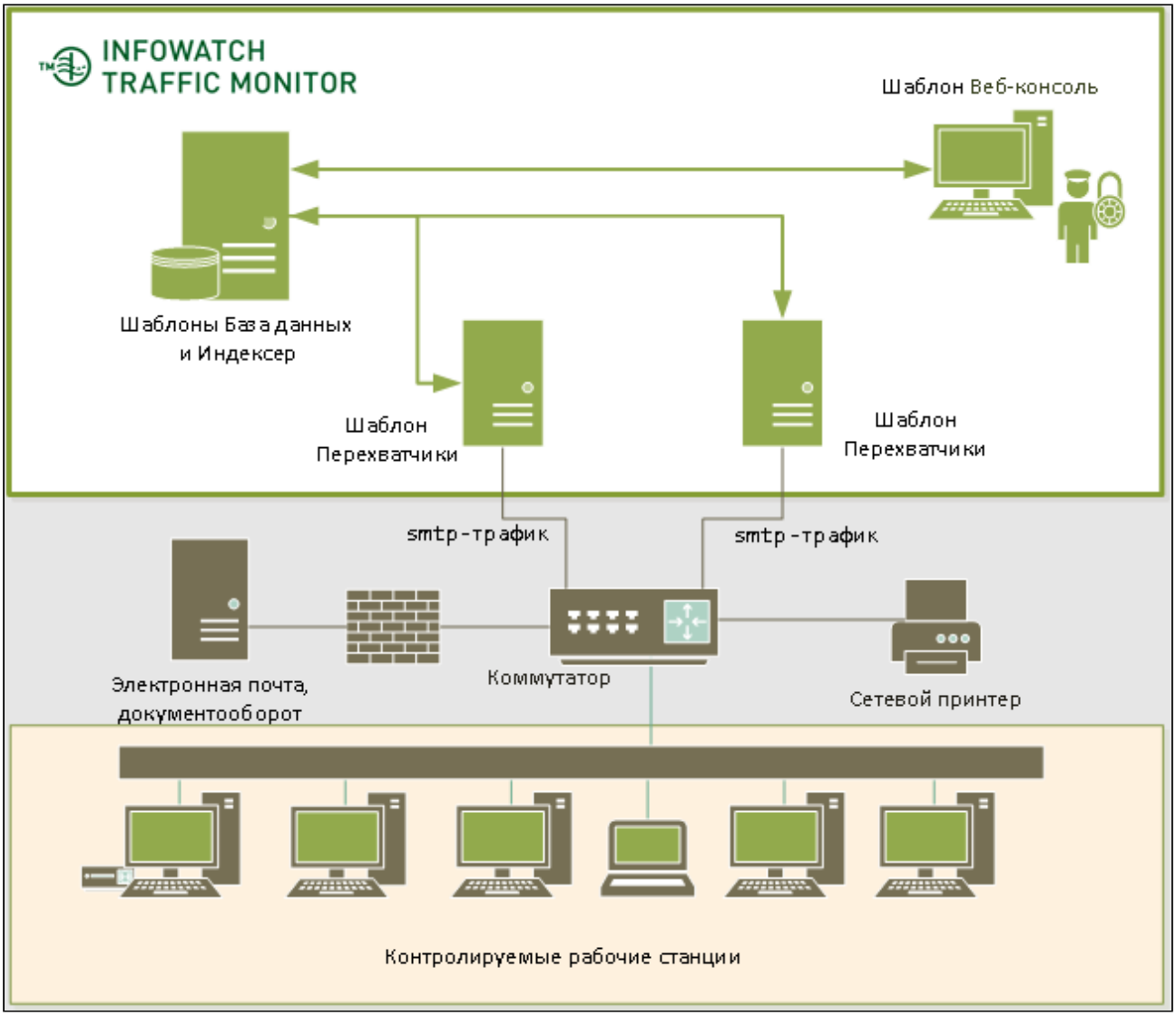
- *Все-в-одном* – все компоненты Системы (с СУБД PostgreSQL) устанавливаются на один сервер с возможностью подключения к удаленной базе данных. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor. Является аналогом установки всех шаблонов на один сервер.
- *Распределенная установка* – компоненты Traffic Monitor и СУБД PostgreSQL устанавливаются на разные машины с использованием представленных шаблонов. Такая установка используется, если с учетом предполагаемой нагрузки сервисы Traffic Monitor и СУБД не смогут производительно работать на одной машине.

Примеры развертывания Системы с использованием шаблонов установки Traffic Monitor:

Пример 1:

Система установлена на четырех серверах:

1. Сервер с шаблонами База данных и Индексер.
2. Сервер с шаблоном Веб-консоль.
3. Два сервера с шаблоном Перехватчики.

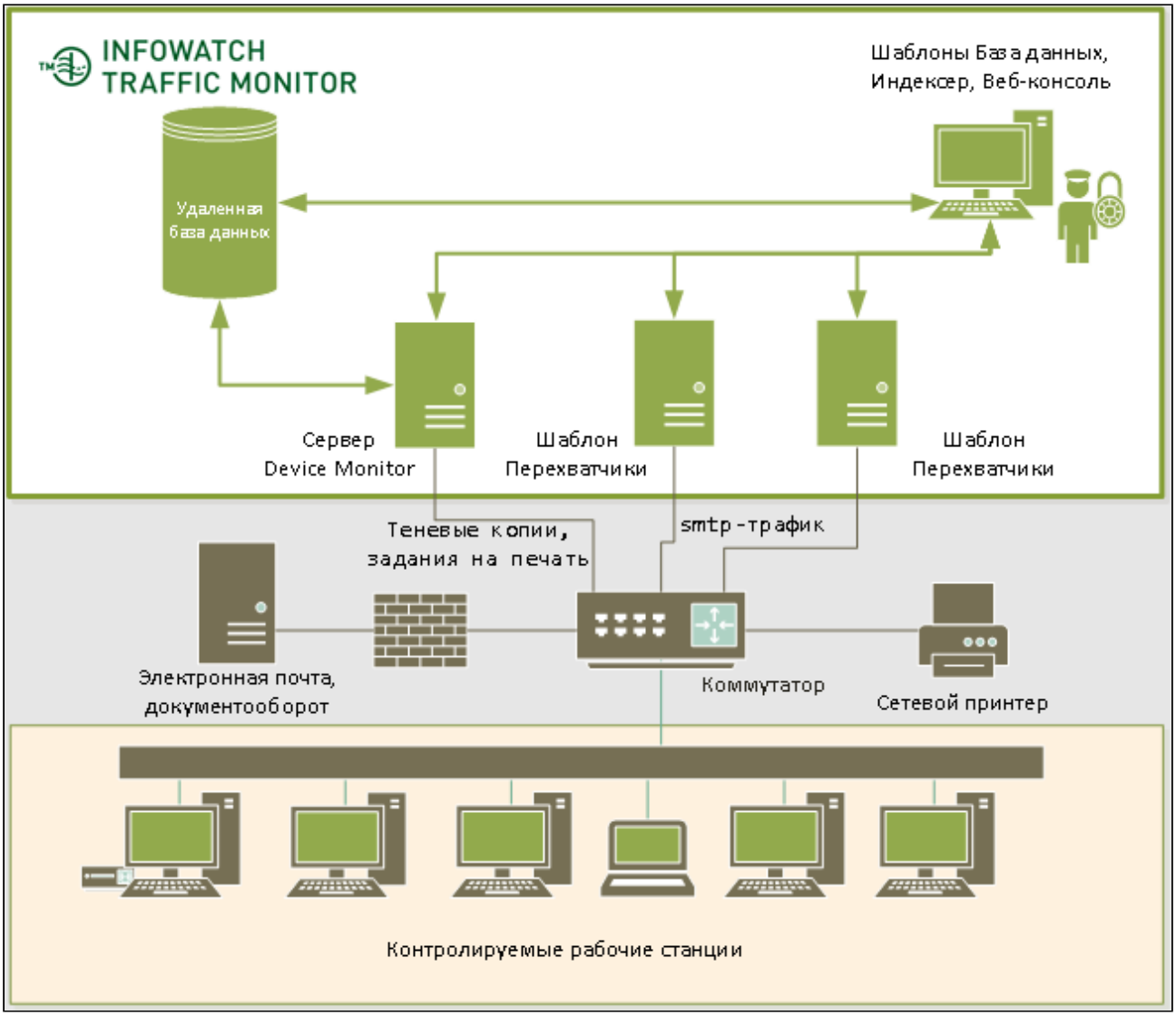


В данном примере для распределения нагрузки Перехватчики установлены на двух серверах. В зависимости от целей перехвата, на каждом из этих серверов могут быть дополнительно отключены неиспользуемые модули перехвата.

Пример 2:

Система установлена на четырех серверах:

1. Сервер с шаблонами База данных, Индексер и Веб-консоль. Шаблон База данных установлен с подключением к удаленной базе данных, на которую установлена схема базы данных Traffic Monitor.
2. Два сервера с шаблоном Перехватчики.
3. Сервер Device Monitor.



Перехватчики так же разделены на два сервера, используется удаленная база данных, а на контролируемых рабочих станциях функционируют Агенты Device 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.*
- **Коннекторы** – требования к этим компонентам описаны в документации, поставляемой вместе с программным обеспечением коннекторов.
- **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.

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 "Смоленск" 1.7.0 Требуется 2 диска: • Astra-Linux-Smolensk	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.

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			• Astra-Linux-Smolensk-Devel	
Сервер ТМ Enterprise, от 10 до 50 GB трафика в день				
RAID-массив с fault tolerance	2SRVx2CPU 10xC	32-48 GB на каждый из серверов	ОС Astra Linux Special Edition "Смоленск" 1.7.0 Требуется 2 диска: • Astra-Linux-Smolensk • Astra-Linux-Smolensk-Devel	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков. Проверка цифровой подписи должна быть отключена.
Сервер ТМ Enterprise, более 50 GB трафика в день				
RAID-массив с fault tolerance	Рассчитывается по запросу	От 32GB на каждый из серверов	ОС Astra Linux Special Edition "Смоленск" 1.7.0 Требуется 2 диска: • Astra-Linux-	Сервер должен иметь сетевой интерфейс с назначенным IP-адресом. В случае использования на сервере перехватчиков требуется выполнить требования перехватчиков.

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			Smolensk • Astra-Linux-Smolensk-Devel	Проверка цифровой подписи должна быть отключена.
Сервер БД PostgreSQL (Обеспечивает хранение трафика для 1-2 тыс. пользователей, сроком до 3 месяцев; в случае использования OCR и Device Monitor требования рассчитываются по запросу)				
RAID-массив с fault tolerance: 500 GB Для хранения логов действий (xlog) необходимо выделить директории u01 дополнительное пространство, равное объему оперативной памяти сервера БД. Если оперативной памяти меньше 20 GB, выделите под логи 20 GB.	2CPU от 6xC, 2,6 GHz	От 16GB и более в зависимости от объема данных, интенсивности вставки и обработки	ОС Astra Linux Special Edition "Смоленск" 1.7.0 Требуется 2 диска: • Astra-Linux-Smolensk • Astra-Linux-Smolensk-Devel	

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 "Смоленск" (x64) 1.7.0;

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

- Должны быть настроены репозитории ОС с возможностью установить пакеты:
  - `lsb-release`;
  - `lshw`;
  - `ntp`;
  - `ntpdate`.

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

- Должны быть доступны следующие репозитории:
  - `os`;
  - `updates`;
  - `optional`.
- 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 планируется использовать уже развернутую базу данных, перед установкой Системы обязательно выполните предварительную настройку.**Настройка СУБД PostgreSQL**

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

1. Установите дополнительные пакеты, выполнив команды:
   ```
   dpkg -i postgresql-11-stat-kcache_2.1.3-1.pgdg100+1_amd64.deb
   dpkg -i postgresql-11-pathman_1.5.12-1.pgdg100+1_amd64.deb
   apt-get install pgagent
   ```
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_stat_kcache,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_stat_kcache;
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.

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 ТМ в режиме "Все-в-одном"
  - Распределенная установка ТМ
  - 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 с шаблоном установки Веб-консоль (где установлен пакет `web-gui`) – если компоненты Системы установлены на разные компьютеры.

3.1 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 должна быть установлена ОС Astra Linux Special Edition 1.7.0.

Для установки потребуются репозитории с 2-х дисков:

- Astra-Linux-Smolensk;
- Astra-Linux-Smolensk-Devel.

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

- iw_icap
- iw_icap_buf
- iw_proxy_http
- iw_proxy_icq
- iw_proxy_smtp
- iw_sniffer
- iw_capstack
- iw_qmover_client
- iw_qmover_server

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

Установка «все-в-одном» позволяет установить все компоненты 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 должна быть установлена ОС Astra Linux Special Edition 1.7.0.

Чтобы узнать версию установленной ОС, выполните команду:

```
cat /etc/astra_version
```

Не удаляйте репозитории, подключенные в процессе установки ОС Astra Linux Special Edition. Для установки потребуются репозитории с 2-х дисков:

- Astra-Linux-Smolensk;
- Astra-Linux-Smolensk-Devel.

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.

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

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

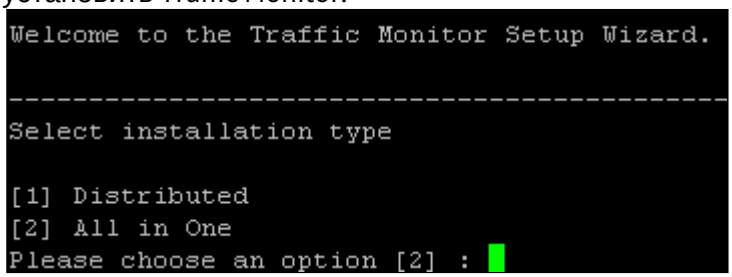
4. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой системы выполните следующую команду:
   `sudo mkdir /distr`
5. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch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

   В нашем примере:
   - **`iwtm-installer-7.5.0.120-astra-smolensk-1.7`**;
   - **`iwtm-postgresql-11.10-7.5.0.120-astra-smolensk-1.7.tar.gz`**.
6. Выполните следующую команду:
   `sudo apt-get update`
7. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
   `cd /distr`
8. Перед запуском установки сделайте файл инсталлятора исполняемым. Для этого используйте команду вида:
   `sudo chmod +x ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
   В нашем примере команда будет следующей:
   `sudo chmod +x ./iwtm-installer-7.5.0.120-astra-smolensk-1.7`

Установка в текстовом режиме в консоли сервера

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

1. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
   `sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
   В нашем примере команда будет следующей:
   `sudo ./iwtm-installer-7.5.0.120-astra-smolensk-1.7`
   Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов. По завершении на экране отобразится окно с приглашением установить Traffic Monitor:

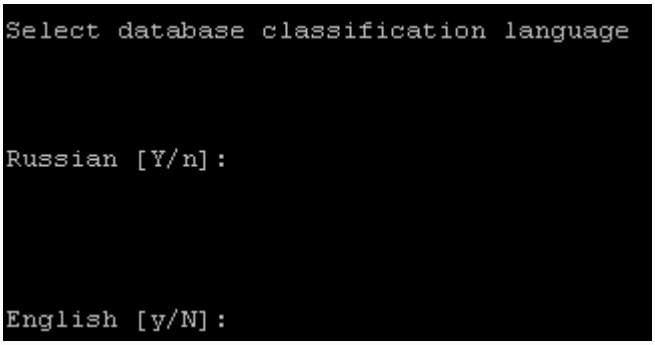


2. На этапе выбора типа установки выберите **`All in one`**.
   Для этого введите цифру, указанную напротив выбранного варианта, и нажмите **Enter**.

> **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 `[2] All in one`.

3. 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.
4. 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.

5. 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.
6. Если выбрано использование удаленной базы данных, последовательно введите:
   a. IP-адрес или доменное имя сервера с базой данных.
   b. Порт подключения.
   c. Имя используемой базы данных, в которую будет добавлена схема.
7. 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.
8. 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.
9. 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.

10. 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.

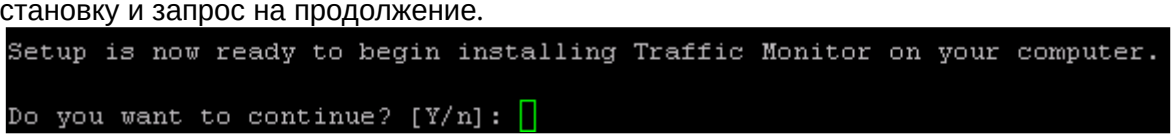
    Для каждого следующего параметра предварительно будет выведен запрос на использование:
    - `Archive non-violation events` - включить автоматическое архивирование событий, которые не являются нарушениям. В случае включения укажите число дней до архивирования, значение по умолчанию - 45.
    - `Archive 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.
11. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию - 90.
12. Укажите параметры подключения к службе Consul:
    a. `Network interface address` - выберите IP-адрес сетевого интерфейса.
    b. `Datacenter name` - введите название дата-центра Consul.
13. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:
    - `Use system NTP-server` - использовать системный NTP-сервер;
    - `Set manually` - указать NTP-сервер вручную. При выборе данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.
14. 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.

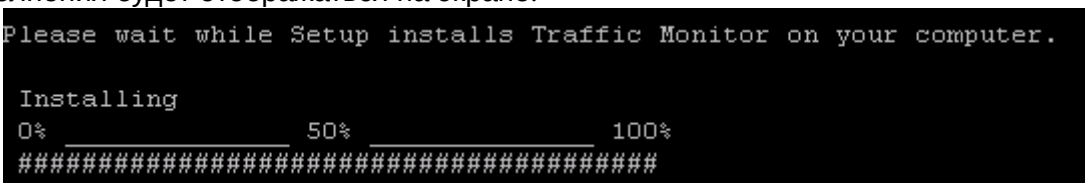
15. При необходимости вы можете изменить стандартные параметры работы службы Sphinx.
    В этом случае будет предложено задать список языков с поддержкой морфологии. По этим языкам будет проводиться индексация.
    Вы можете указать несколько языков, используя пробел в качестве разделителя.

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

16. Вы можете включить использование технологии OCR.
    В случае включения необходимо выбрать для использования одну из систем:
    - `ABBYY FineReader`;
    - `Tesseract`.
17. Если выбран OCR-экстрактор ABBYY Finereader:
    a. Выберите один из режимов распознавания:
       - `Quick` – быстрый режим;
       - `Quality` – тщательный режим, обеспечивающий более высокое качество распознавания.
    b. Подтвердите наличие у вас активной лицензии на использование 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".
18. 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.

19. 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**
>
> a. Запустите службу Consul, выполнив команду:
>   `service iwtm-consul start`
>   Проверить статус службы можно командой:
>   `service iwtm-consul status`
> b. Чтобы проверить службу Consul выполните команды:
>   i. Для вывода IP-адреса основного сервера (лидера) кластера:
>   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
>   ii. Для вывода информации о членах кластера:
>   `consul members`
> c. Если не будет выведен IP-адрес лидера кластера, выполните конфигурирование кластера службы Consul.
>   После настройки повторите проверку (действие ii).
>
> При данной ошибке инсталлятор не запустит сервисы Traffic Monitor при завершении работы, их нужно будет запустить вручную.

20. Для перехвата `smtp` с учетом мандатных меток:
    a. Введите команду для вызова файлового менеджера:
       `sudo mc`
    b. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
    c. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.
    d. Для выхода из файлового менеджера введите команду:
       `exit`
21. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.

22. 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. Если до установки в ОС они были включены, не выключайте их, и наоборот.
>
> В противном случае корректная работа Системы не гарантируется.

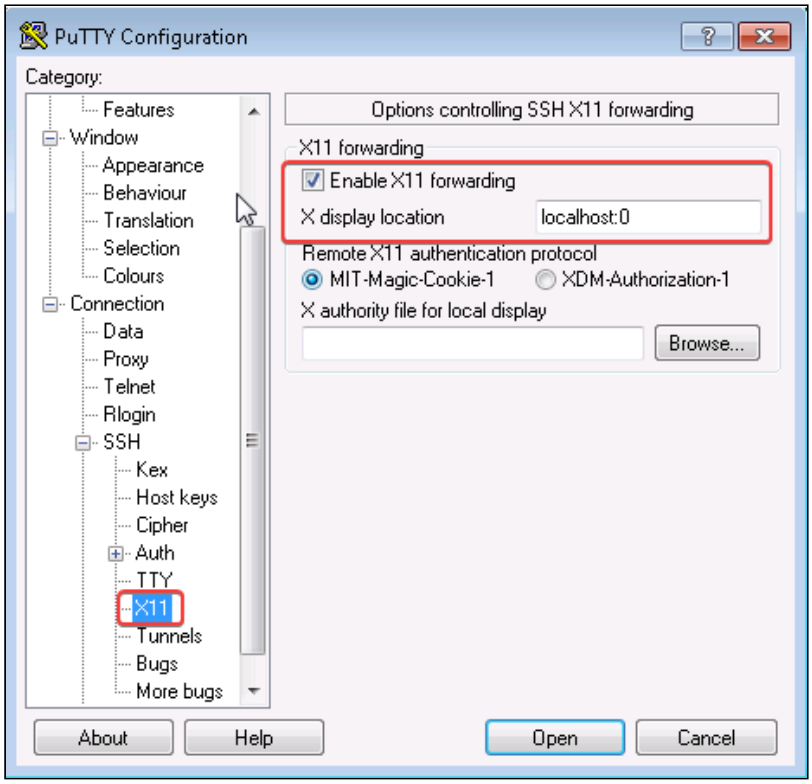
Установка с использованием графического режима инсталлятора

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:

1. На сервере, на котором планируется установка компонентов Traffic Monitor:
   a. Установите утилиту xauth с помощью команды:
   `sudo apt-get install xauth`
   b. В конфигурационном файле `/etc/ssh/sshd_config` раскомментируйте строку "`X11Forwarding yes`". Для этого удалите перед строкой символ `#`.
   c. Сохраните изменения в конфигурационном файле.
   d. Перезапустите службу SSH с помощью команды:
   `systemctl restart sshd`
2. На компьютере, на котором будет использован графический режим:
   a. Для подключения к серверу установки Traffic Monitor вам потребуется SSH-клиент с включенной опцией X11 Forwarding, например PuTTY.
   b. Для запуска инсталлятора в графическом режиме вам потребуется настроенное приложение-клиент для обращения к X Window System, например:
      - приложение Xming - для ОС семейства MS Windows;
      - оболочка Gnome 3 - для ОС семейства Linux.
3. Запустите настроенное приложение-клиент для обращения к X Window System.
4. Подключитесь к серверу, на котором планируется установка компонентов Traffic Monitor, с помощью выбранного SSH-клиента.
   Пример окна настройки PuTTY при подключении

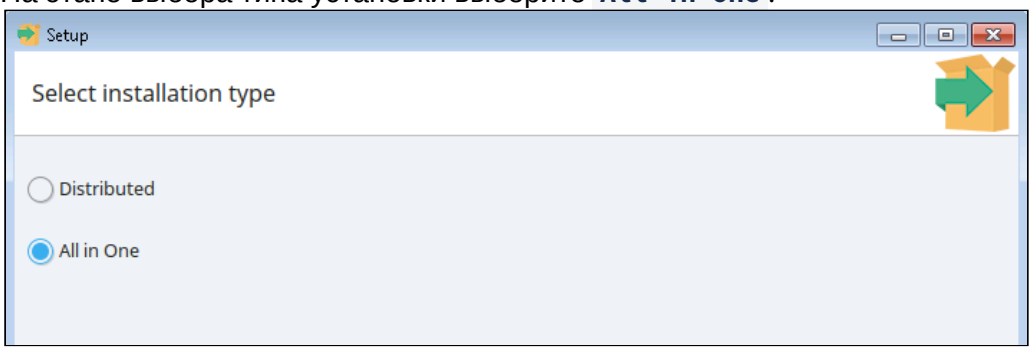


5. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
   `sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
   В нашем примере команда будет следующей:
   `sudo ./iwtm-installer-7.5.0.120-astra-smolensk-1.7`
   Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов. По завершении откроется окно с приглашением установить Traffic Monitor:



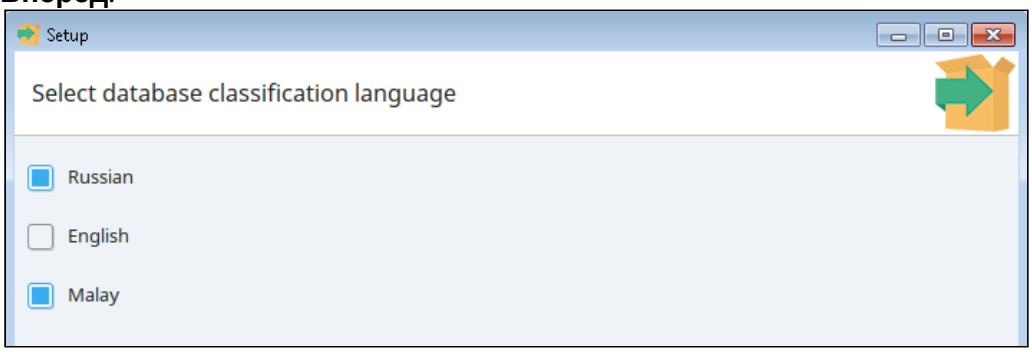
Для перехода к следующему параметру используется кнопка **Вперед**, для возврата к предыдущему - **Назад**. Для выхода из инсталлятора - кнопка **Отменить**.

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



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

7. 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.
8. 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.

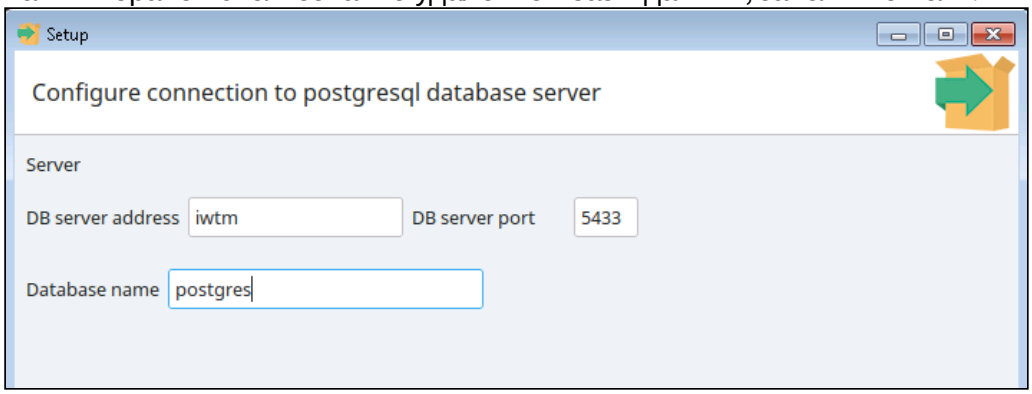
9. Выберите расположение базы данных:



   - `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.

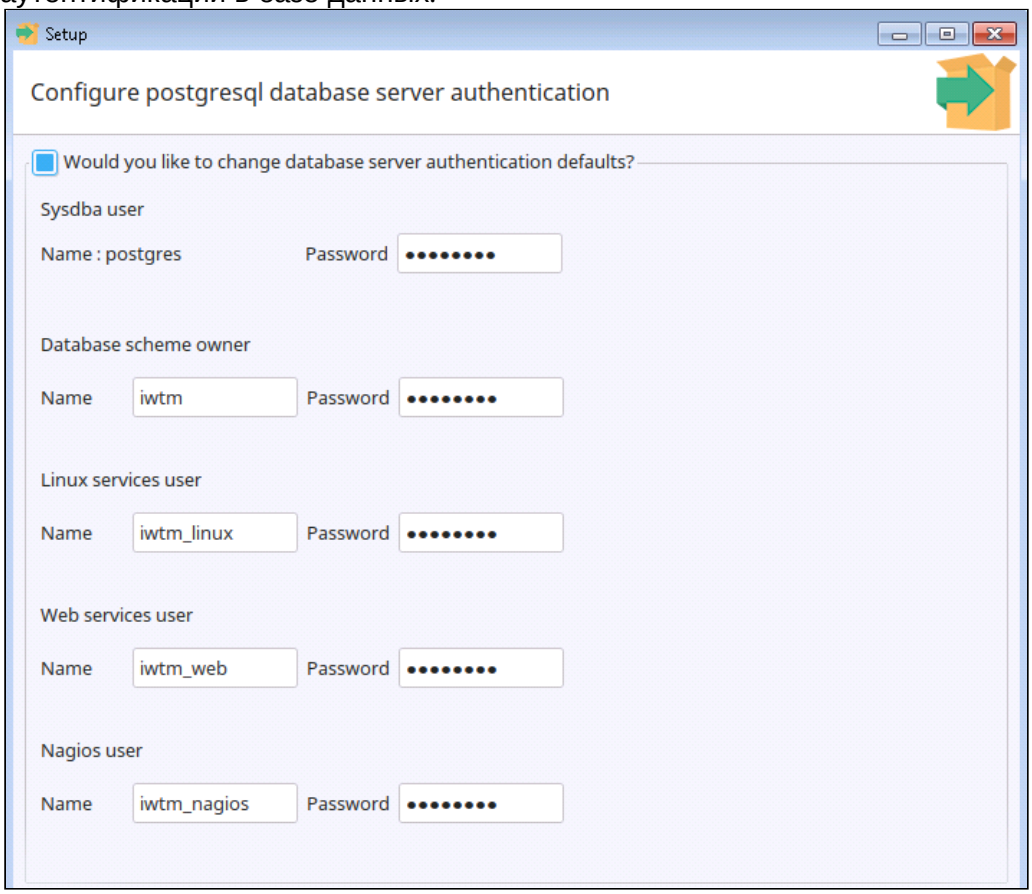
10. Если выбрано использование удаленной базы данных, заполните поля:



a. **`Address and Port`** - IP-адрес или доменное имя сервера с базой данных и порт подключения.
b. **`Database name`** - Имя используемой базы данных, в которую будет добавлена схема.

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

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

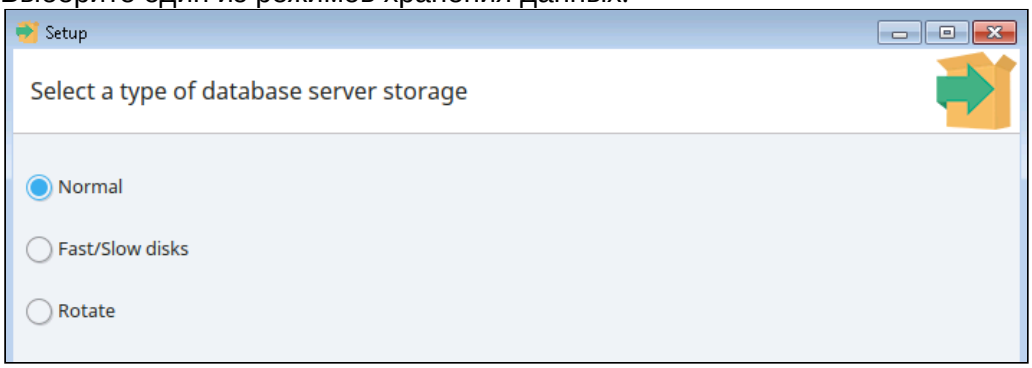


Чтобы отредактировать значения, установите флажок напротив поля с вопросом. Это сделает доступными для редактирования следующие разделы:

- **`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.

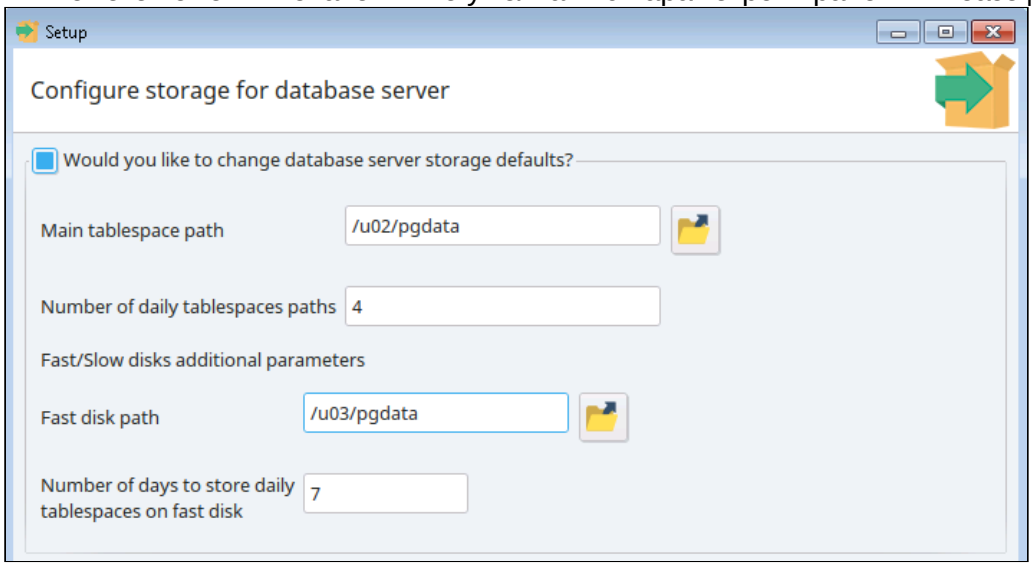
12. Выберите один из режимов хранения данных:



- **`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.

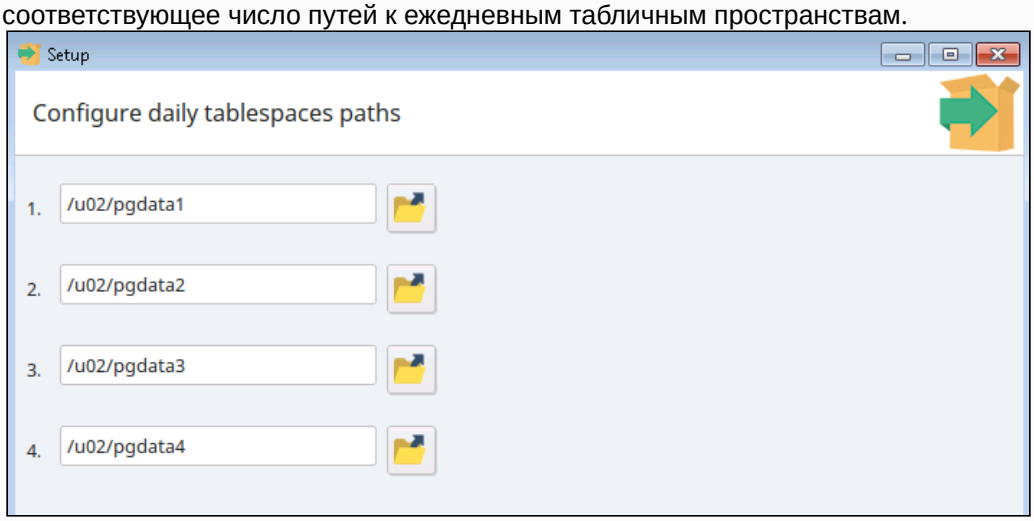
13. Вы можете изменить значения по умолчанию параметров хранения в базе данных.



- **`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;

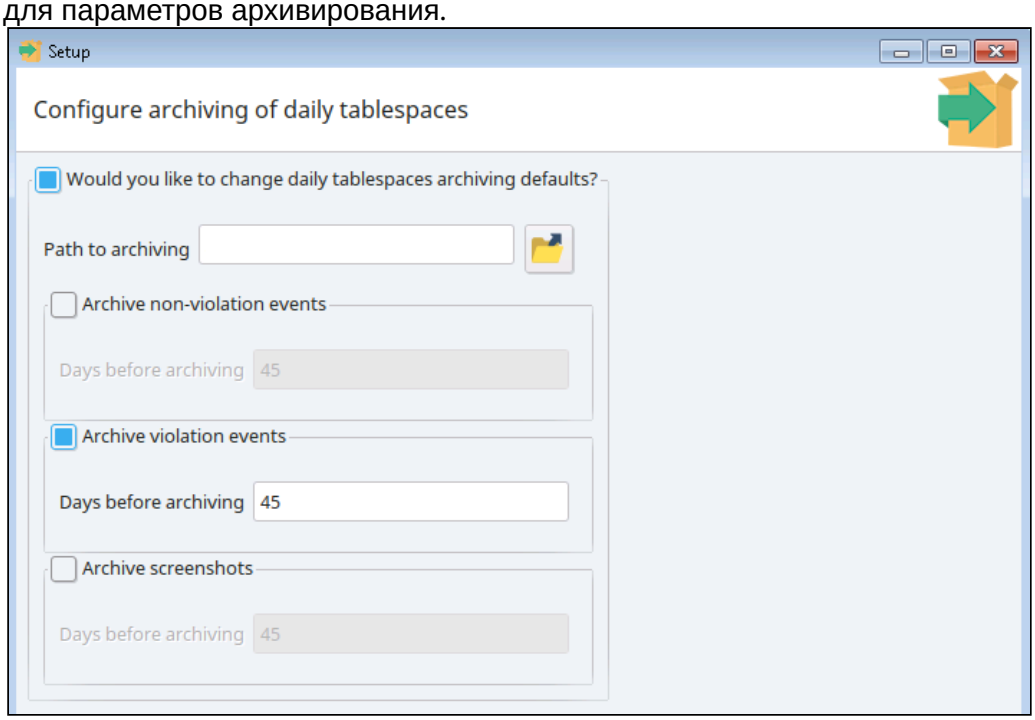
> **Примечание:**

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.

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



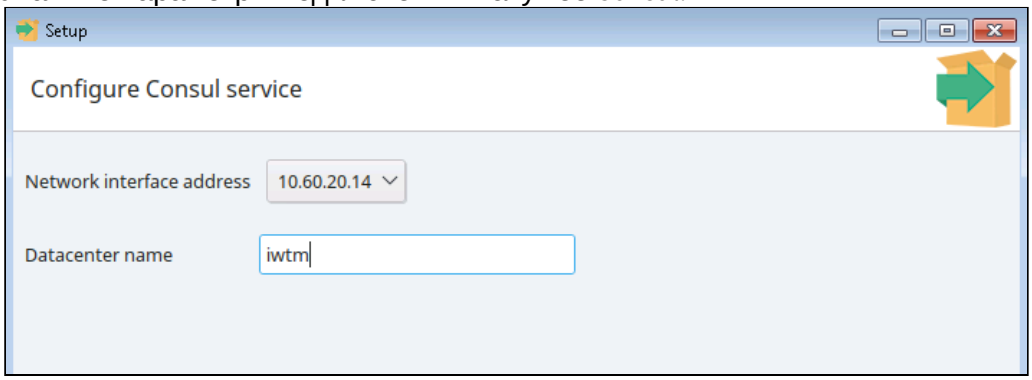
- **`Path to archiving`** - путь к директории хранения файлов архивированных табличных пространств.

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.

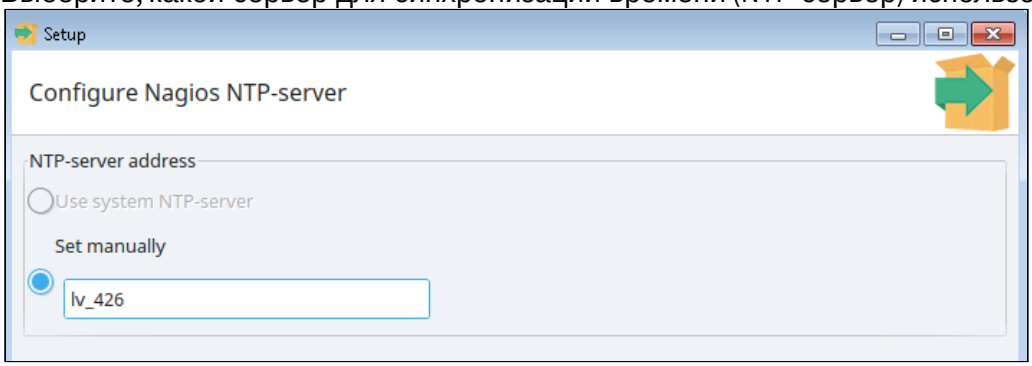
15. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию - 90.
16. Укажите параметры подключения к службе Consul:



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

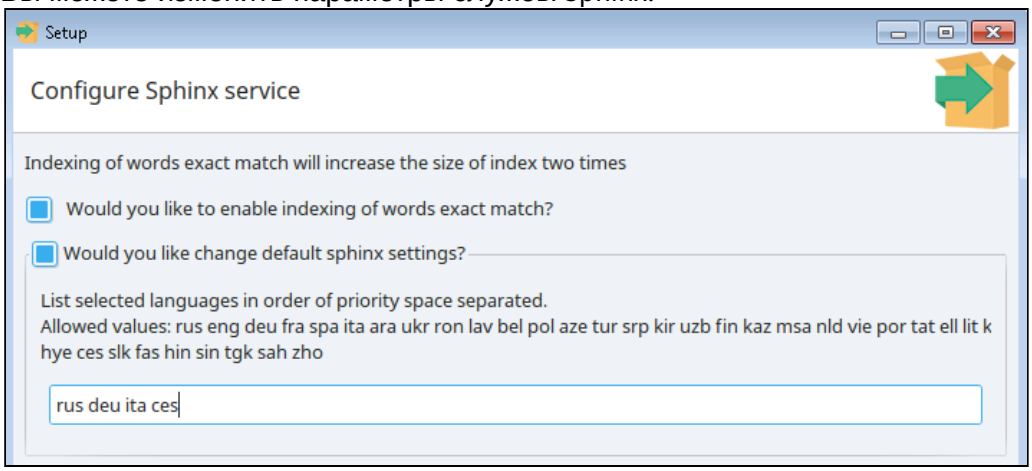
    Для выбора из списка параметров нажмите на кнопку  и в раскрывшемся списке выберите требуемое значение.

    b. **`Datacenter name`** - введите название дата-центра Consul.
17. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:



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

18. Вы можете изменить параметры службы Sphinx:



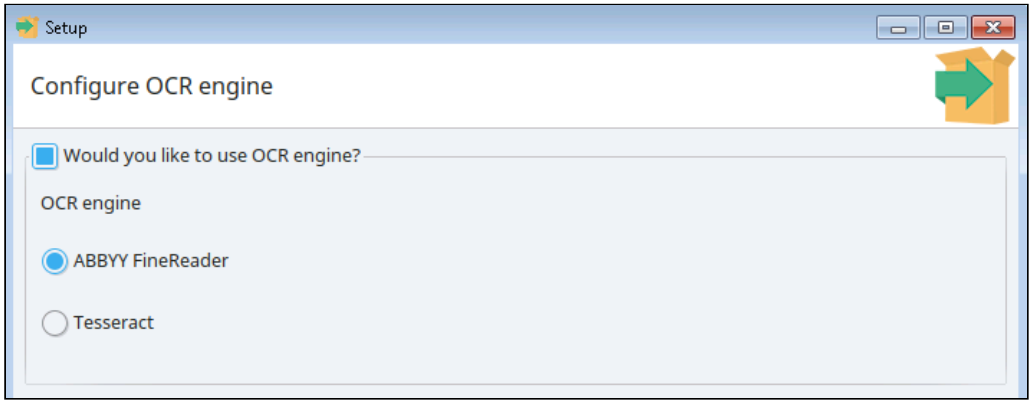
- `Enable indexing of words exact match` - включить индексацию на точное совпадение слов;

> **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.

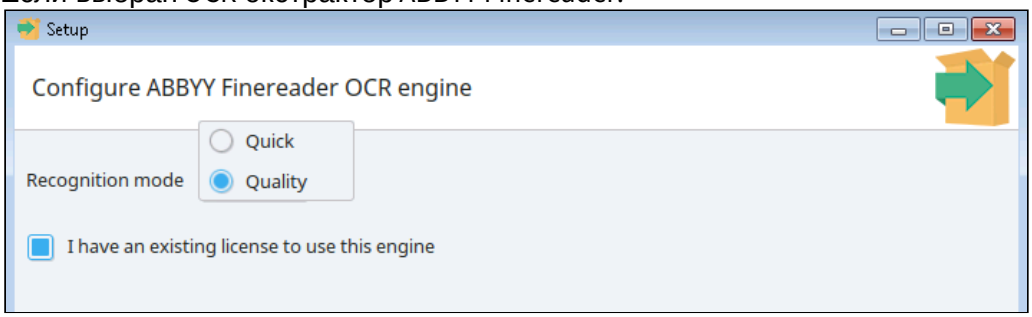
> **Примечание:**
>
> Приоритет языков соответствует последовательности их выбора. Английский язык будет добавлен по умолчанию, имеет самый высокий приоритет.

19. Вы можете включить использование технологии OCR.



В случае включения необходимо выбрать для использования одну из систем:
- `ABBYY FineReader` ;
- `Tesseract` .

20. Если выбран OCR-экстрактор ABBYY Finereader:

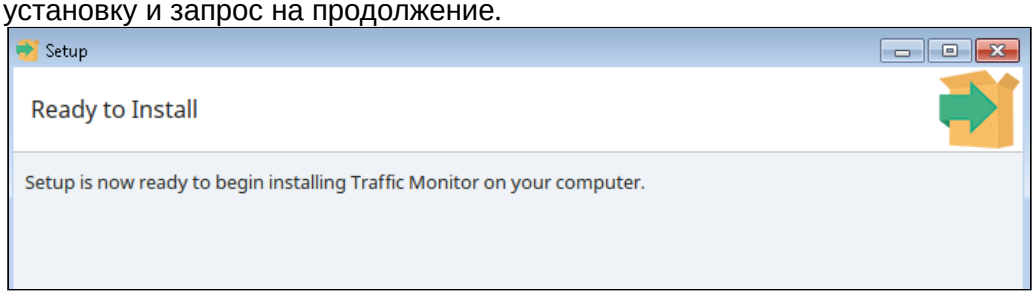


a. Выберите один из режимов распознавания (`Recognition mode`):
   - `Quick` – быстрый режим;
   - `Quality` – тщательный режим, обеспечивающий более высокое качество распознавания.

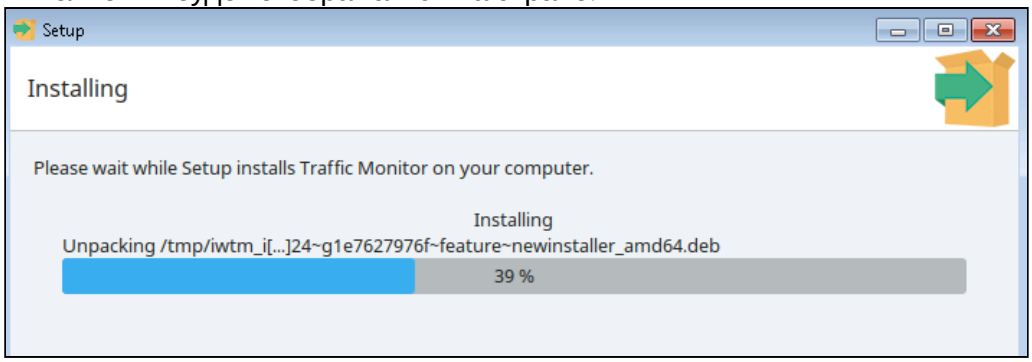
b. Подтвердите наличие у вас активной лицензии на использование ABBYY Finereader.

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".

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



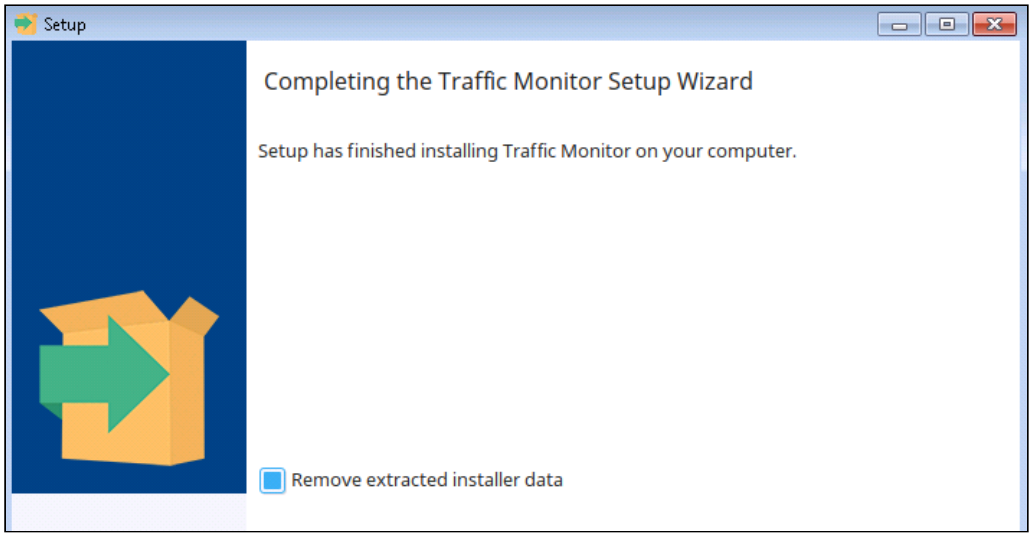
Для начала установки нажмите кнопку **Вперед**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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.

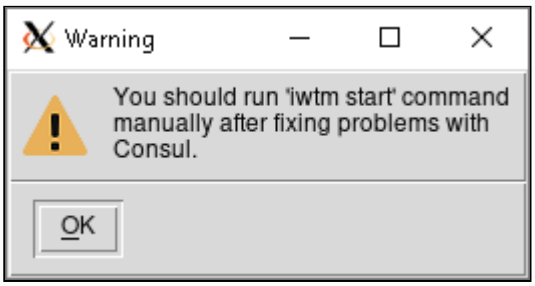
22. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.



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

a. Запустите службу Consul, выполнив команду:
`service iwtm-consul start`
Проверить статус службы можно командой:
`service iwtm-consul status`
b. Чтобы проверить службу Consul выполните команды:
   i. Для вывода IP-адреса основного сервера (лидера) кластера:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. Для вывода информации о членах кластера:
   `consul members`
c. Если не будет выведен IP-адрес лидера кластера, выполните конфигурирование кластера службы Consul.
После настройки повторите проверку (действие ii).

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

23. Для завершения нажмите кнопку **Finish**.
24. Для перехвата smtp с учетом мандатных меток:
    a. Введите команду для вызова файлового менеджера:
    `sudo mc`
    b. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл `smtpd.conf`.
    c. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.
    d. Для выхода из файлового менеджера введите команду:
    `exit`
25. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
26. 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. Если до установки в ОС они были включены, не выключайте их, и наоборот.

В противном случае корректная работа Системы не гарантируется.

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».

3.1.2 Распределенная установка ТМ

Traffic Monitor в редакции Enterprise позволяет развернуть Систему так, чтобы различные компоненты Traffic Monitor, например СУБД, модули или веб-консоль, были установлены на разные серверы. Такая установка используется, если с учетом предполагаемой нагрузки все компоненты Traffic Monitor, включая СУБД, не смогут 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 должна быть установлена ОС Astra Linux Special Edition 1.7.0.

Чтобы узнать версию установленной ОС, выполните команду:

```
cat /etc/astra_version
```

Не удаляйте репозитории, подключенные в процессе установки ОС Astra Linux Special Edition. Для установки потребуются репозитории с 2-х дисков:

- Astra-Linux-Smolensk;
- Astra-Linux-Smolensk-Devel.

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.

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

Примечание:

Если используется подключение по SSH, выполните повторное подключение.

4. 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`
5. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor:
   - **`iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`** (где x.x.x.xxx - номер сборки);
   - **`iwtm-postgresql-11.10-x.x.x.xxx-astra-smolensk-1.7.tar.gz`**.

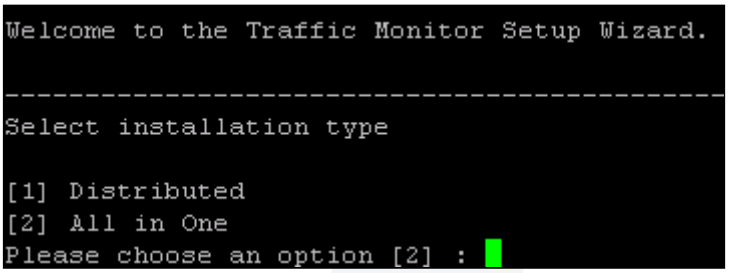
   В нашем примере:
   - **`iwtm-installer-7.5.0.120-astra-smolensk-1.7`**;
   - **`iwtm-postgresql-11.10-7.5.0.120-astra-smolensk-1.7.tar.gz`**.
6. Выполните следующую команду:
   `sudo apt-get update`
7. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
   `cd /distr`
8. Перед запуском установки сделайте файл инсталлятора исполняемым. Для этого используйте команду вида:

`sudo chmod +x ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
В нашем примере команда будет следующей:
`sudo chmod +x ./iwtm-installer-7.5.0.120-astra-smolensk-1.7`

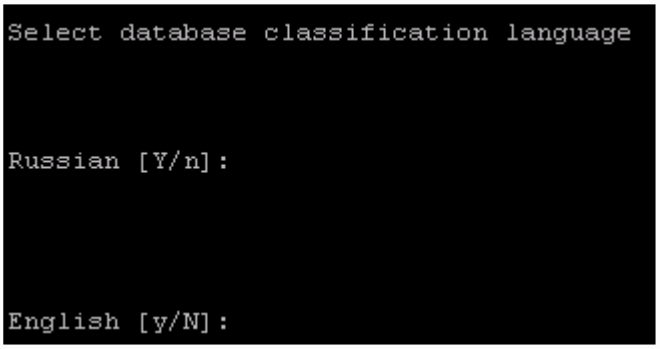
Установка в текстовом режиме в консоли сервера

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

1. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
`sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
В нашем примере команда будет следующей:
`sudo ./iwtm-installer-7.5.0.120-astra-smolensk-1.7`
Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов. По завершении на экране отобразится окно с приглашением установить Traffic Monitor:



2. На этапе выбора типа установки укажите **`Distributed`**.
Для этого введите цифру, указанную напротив выбранного варианта, и нажмите **Enter**.

> **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 `[2]All in one`.
>
> Также значение по умолчанию в квадратных скобках может быть указано заглавной буквой.
>
> **Пример**
>
> 
>

3. 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:
>
> ```
> \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:
> `service iwtm-consul start`
> Проверить статус службы можно командой:
> `service iwtm-consul status`
> b. Чтобы проверить службу Consul выполните команды:
> i. Для вывода IP-адреса основного сервера (лидера) кластера:
> `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
> ii. Для вывода информации о членах кластера:
> `consul members`
> c. Если не будет выведен IP-адрес лидера кластера, выполните конфигурирование кластера службы Consul.
> После настройки повторите проверку (действие ii).
>
> При данной ошибке инсталлятор не запустит сервисы Traffic Monitor 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`):

1. Выберите основной язык пользовательского интерфейса консоли управления, а также формат отображения даты, времени и язык предустановленных настроек:
   - **`Russian`** – для русскоязычного интерфейса;
   - **`English`** – для англоязычного интерфейса.

2. Выберите язык базы классификации. База классификации включает в себя предустановленные политики, элементы настройки технологий и объекты защиты. 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.
3. Выберите расположение базы данных:
   - **`Install database server locally`** - для локальной установки на текущем сервере;
   - **`Use remote database server`** - для использования уже развернутой удаленной базы данных. В этом случае в удаленную базу данных будет добавлена схема Traffic Monitor.
4. Если выбрано использование удаленной базы данных, последовательно введите:
   a. IP-адрес или доменное имя сервера с базой данных.
   b. Порт подключения.
   c. Имя используемой базы данных, в которую будет добавлена схема.
5. 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.
6. 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.
7. 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.

8. 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.

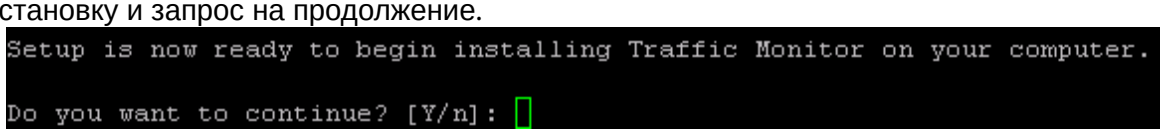
   Для каждого следующего параметра предварительно будет выведен запрос на использование:
   - **`Archive non-violation events`** - включить автоматическое архивирование событий, которые не являются нарушениям. В случае включения укажите число дней до архивирования, значение по умолчанию - 45.
   - **`Archive 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.
9. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию - 90.
10. Укажите параметры подключения к службе Consul:
    a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса.
    b. Режим работы Consul. Доступны два режима:
       - **`Server`**
       - **`Client`**

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

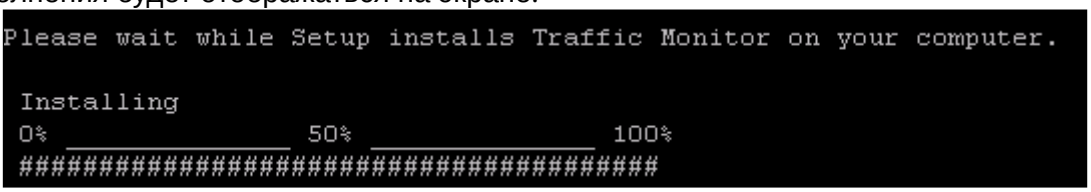
    c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
    d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
    e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.
    f. **`Consul retryjoin port`** - порт подключения к указанным серверам Consul.
11. 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.

12. 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.

13. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
    Если установка прошла успешно, данные рекомендуется удалить.
14. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
15. 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`):

1. Последовательно укажите параметры подключения к базе данных:
   a. IP-адрес или доменное имя сервера с базой данных.
   b. Порт подключения.
   c. Имя используемой базы данных.
2. 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.
3. Укажите параметры подключения к службе Consul:

a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса.
b. Режим работы Consul. Доступны два режима:
   - **`Server`**
   - **`Client`**

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

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

4. 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.
5. 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.

6. 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.

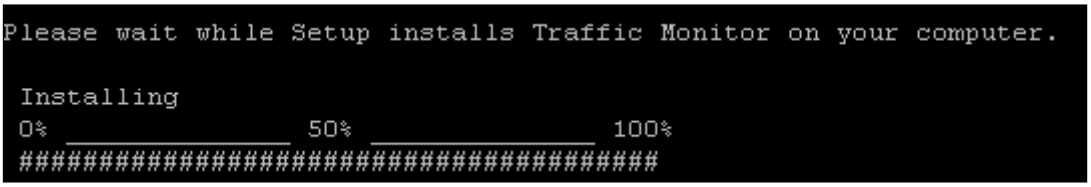
> **Примечание:**
>
> Приоритет языков соответствует последовательности их выбора. Английский язык будет добавлен по умолчанию, имеет самый высокий приоритет.

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

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

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

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



Процесс может занять некоторое время.

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

8. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
   Если установка прошла успешно, данные рекомендуется удалить.
9. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
10. 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`):

1. Последовательно укажите параметры подключения к базе данных:
   a. IP-адрес или доменное имя сервера с базой данных.
   b. Порт подключения.
   c. Имя используемой базы данных.
2. 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.
3. Укажите параметры подключения к службе Consul:
   a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса.
   b. Режим работы Consul. Доступны два режима:
      - **`Server`**
      - **`Client`**

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

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

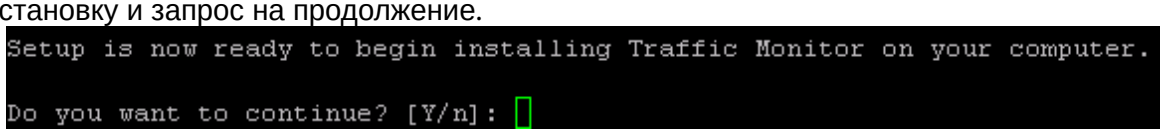
4. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:
   - **`Use system NTP-server`** - использовать системный NTP-сервер;
   - **`Set manually`** - указать NTP-сервер вручную. При выборе данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.
5. Укажите 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.

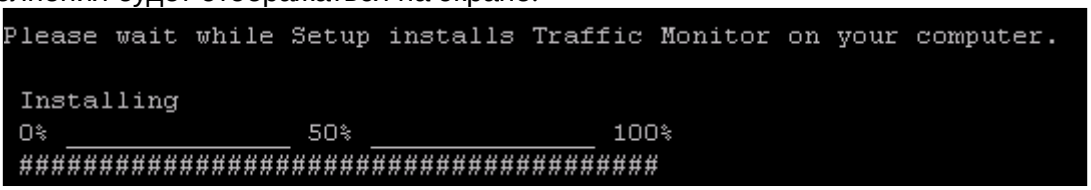
6. Вы можете включить использование технологии OCR.

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

7. 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.

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

Установка шаблона Перехватчики

Если для установки выбран шаблон Перехватчики (Interceptors):

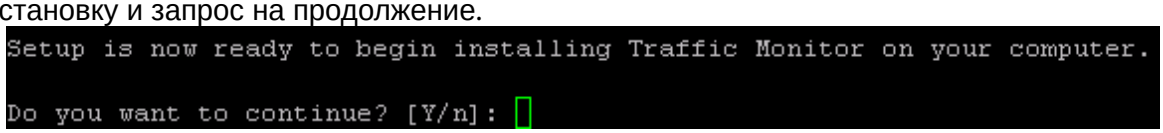
1. Последовательно укажите параметры подключения к базе данных:
   a. IP-адрес или доменное имя сервера с базой данных.
   b. Порт подключения.
   c. Имя используемой базы данных.
2. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.
   В случае утвердительного 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.
3. Укажите параметры подключения к службе Consul:
   a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса.
   b. Режим работы Consul. Доступны два режима:
      - **`Server`**
      - **`Client`**

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

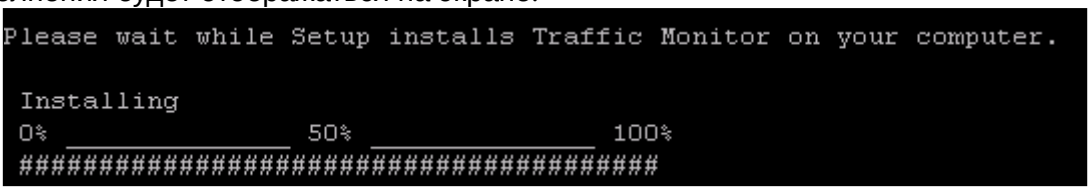
   c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
   d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
   e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если в кластере один сервер Consul на текущей машине, оставьте поле пустым.
   f. **`Consul retryjoin port`** - порт подключения к указанным серверам Consul.
4. 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.
5. 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.

6. Если выбран OCR-экстрактор ABBYY Finereader:
   a. Выберите один из режимов распознавания:
      - **`Quick`** – быстрый режим;
      - **`Quality`** – тщательный режим, обеспечивающий более высокое качество распознавания.
   b. Подтвердите наличие у вас активной лицензии на использование 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".
7. 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.

8. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.
   Если установка прошла успешно, данные рекомендуется удалить.
9. Для перехвата `smtp` с учетом мандатных меток:
   a. Введите команду для вызова файлового менеджера:
      `sudo mc`
   b. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
   c. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.

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

10. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
11. 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. Если до установки в ОС они были включены, не выключайте их, и наоборот.
>
> В противном случае корректная работа Системы не гарантируется.

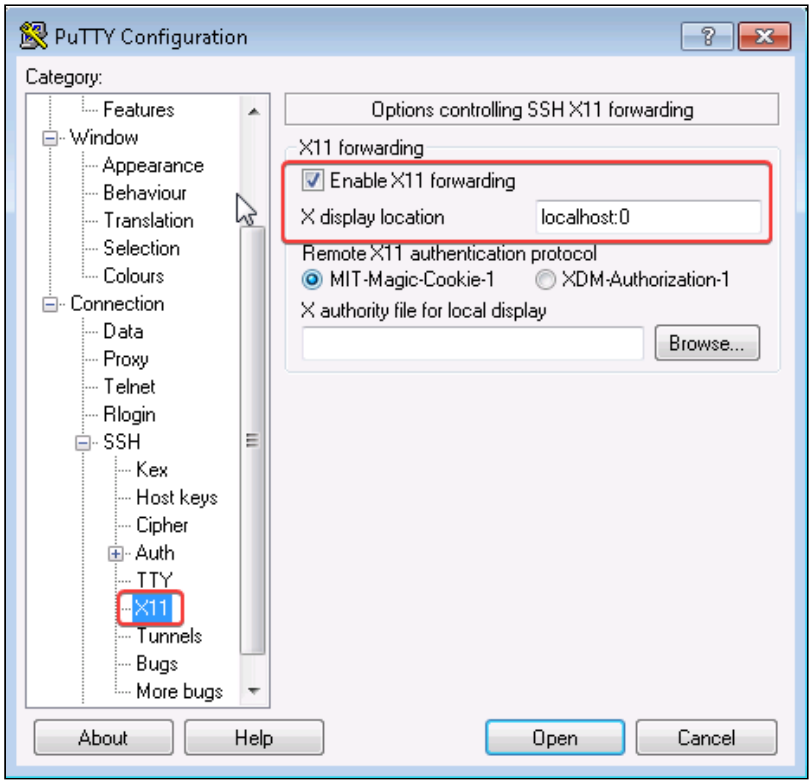
Установка с использованием графического режима инсталлятора

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:

1. На сервере, на котором планируется установка компонентов Traffic Monitor:
   a. Установите утилиту xauth с помощью команды:
   `sudo apt-get install xauth`
   b. В конфигурационном файле `/etc/ssh/sshd_config` раскомментируйте строку "`X11Forwarding yes`". Для этого удалите перед строкой символ `#`.
   c. Сохраните изменения в конфигурационном файле.
   d. Перезапустите службу SSH с помощью команды:
   `systemctl restart sshd`
2. На компьютере, на котором будет использован графический режим:
   a. Для подключения к серверу установки Traffic Monitor вам потребуется SSH-клиент с включенной опцией X11 Forwarding, например PuTTY.
   b. Для запуска инсталлятора в графическом режиме вам потребуется настроенное приложение-клиент для обращения к X Window System, например:
      - приложение Xming - для ОС семейства MS Windows;
      - оболочка Gnome 3 - для ОС семейства Linux.
3. Запустите настроенное приложение-клиент для обращения к X Window System.
4. Подключитесь к серверу, на котором планируется установка компонентов Traffic Monitor, с помощью выбранного SSH-клиента.
   Пример окна настройки PuTTY при подключении

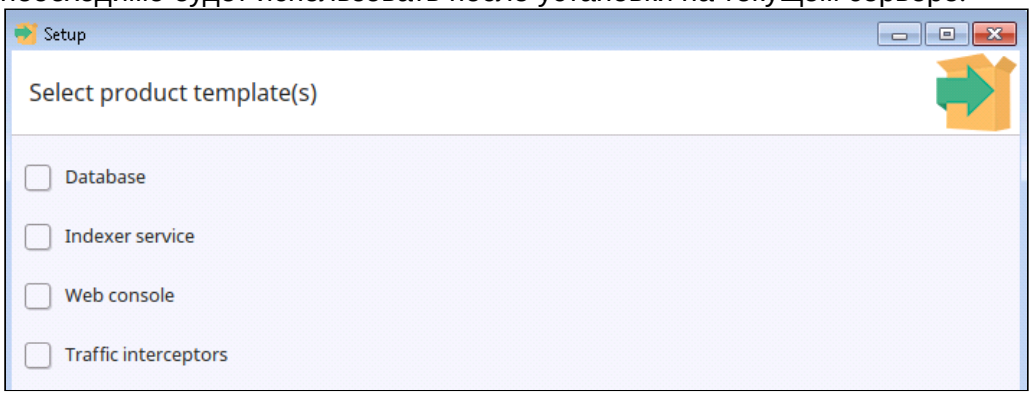


5. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
   `sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
   В нашем примере команда будет следующей:
   `sudo ./iwtm-installer-7.5.0.120-astra-smolensk-1.7`
   Начнется подготовка к запуску инсталлятора. На данном этапе 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**.

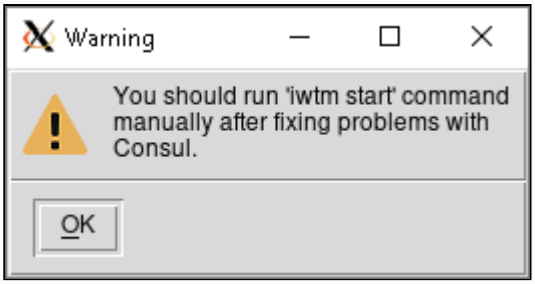
6. На этапе выбора типа установки выберите `Distributed`.
   Для выбора установите флажок напротив соответствующего значения и нажмите кнопку **Вперед**.
7. Далее с помощью выбора шаблонов вы можете указать, какие наборы компонентов необходимо будет использовать после установки на текущем сервере.



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

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

b. Чтобы проверить службу Consul выполните команды:
   i. Для вывода IP-адреса основного сервера (лидера) кластера:
   `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
   ii. Для вывода информации о членах кластера:
   `consul members`
c. Если не будет выведен IP-адрес лидера кластера, выполните конфигурирование кластера службы Consul.
   После настройки повторите проверку (действие ii).

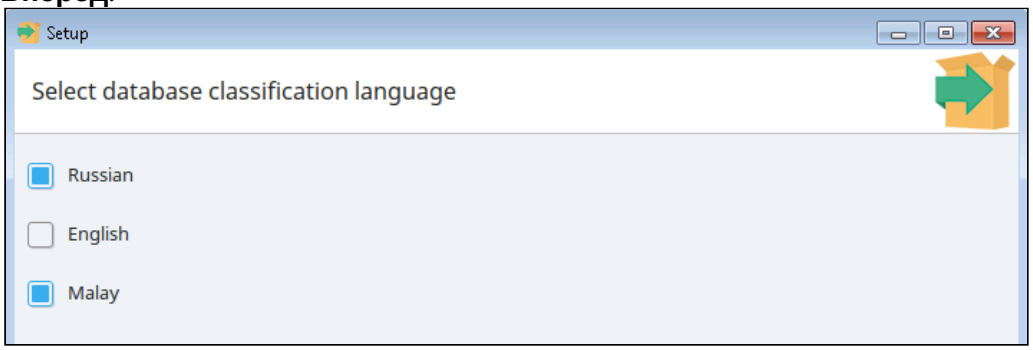
При данной ошибке инсталлятор не запустит сервисы Traffic Monitor при завершении работы, их нужно будет запустить вручную.

Ниже будет рассмотрена установка каждого шаблона на отдельный сервер.

Установка шаблона База данных

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

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

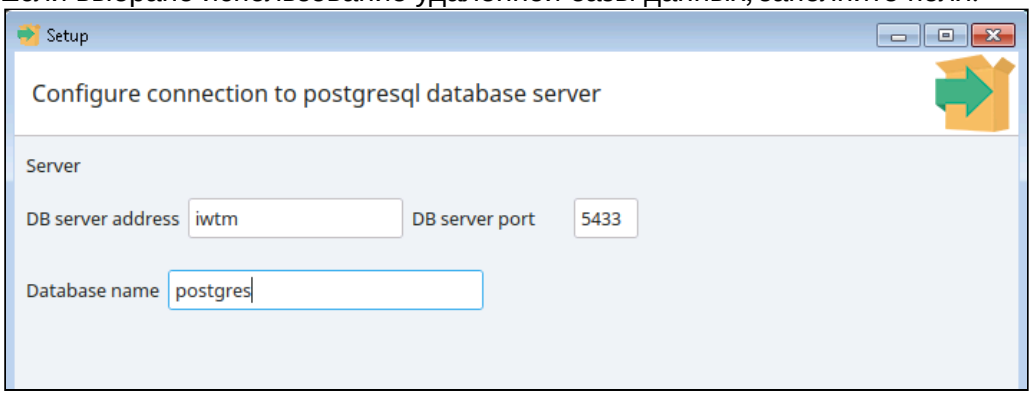
Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.

3. Выберите расположение базы данных:



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

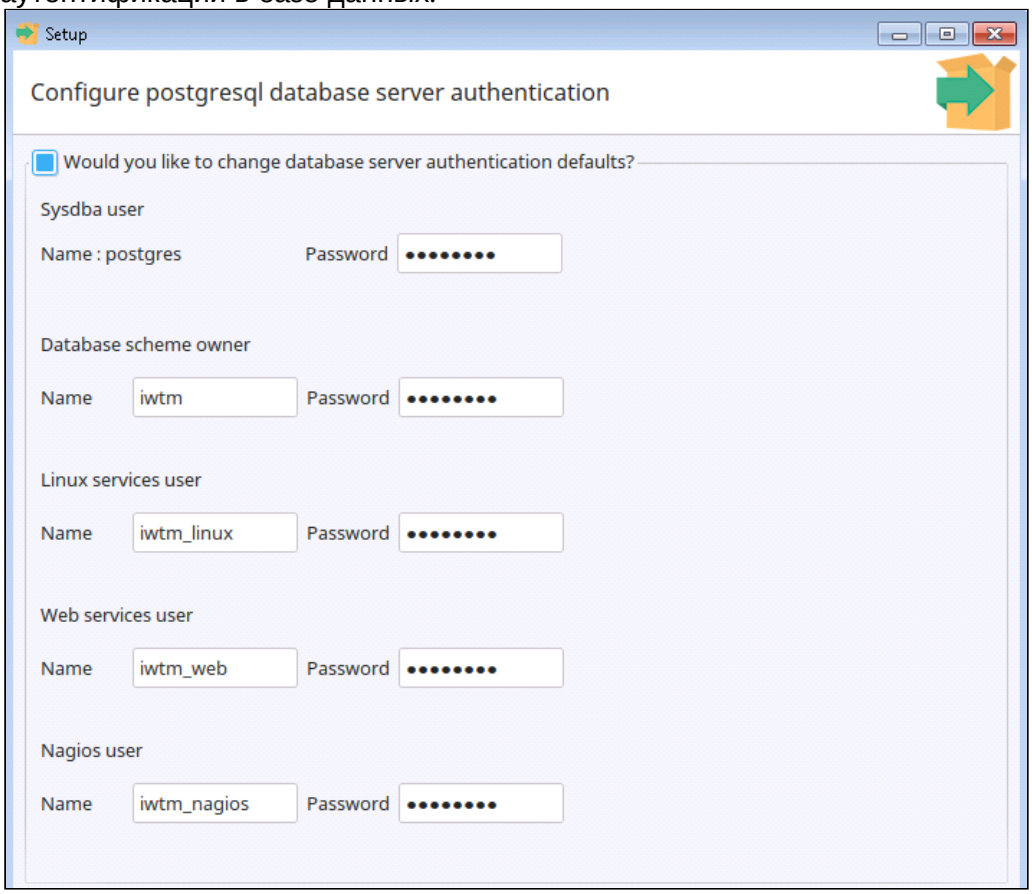
4. Если выбрано использование удаленной базы данных, заполните поля:



a. **`Address and Port`** - IP-адрес или доменное имя сервера с базой данных и порт подключения.
b. **`Database name`** - Имя используемой базы данных, в которую будет добавлена схема.

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

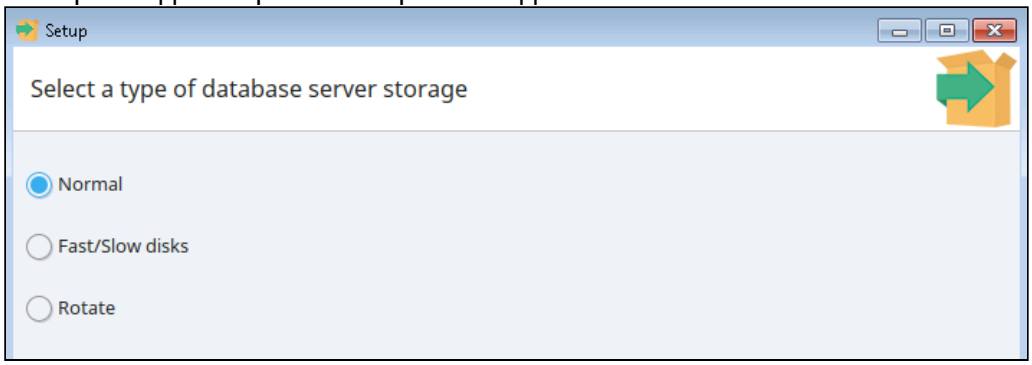
5. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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.

6. Выберите один из режимов хранения данных:

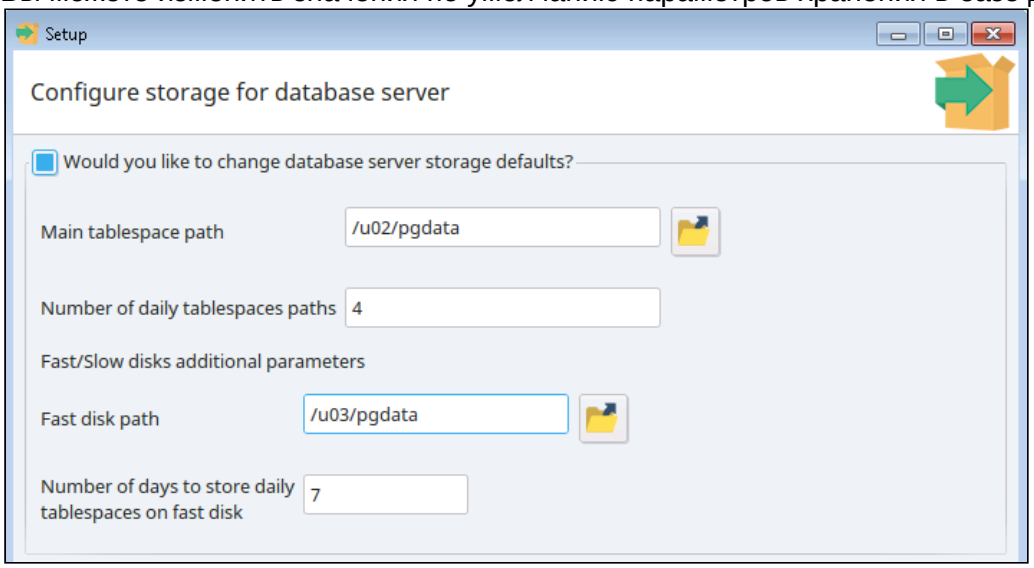


- **`Norma`** l - (обычный) - переключение на следующий раздел, если он указан, происходит при переполнении предыдущего.
- **`Fast/Slow disks`** - разделение пулов на быстрый и медленный. Новые данные сохраняются в быстром разделе и через указанное количество дней

перемещаются на медленные разделы. Медленный пул работает при этом в режиме `normal`.

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

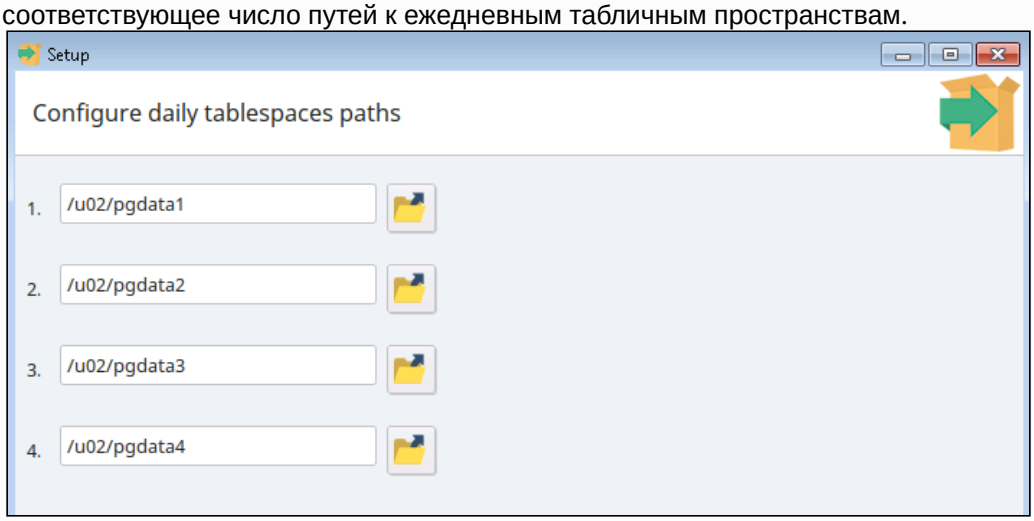
7. Вы можете изменить значения по умолчанию параметров хранения в базе данных.



- **`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;

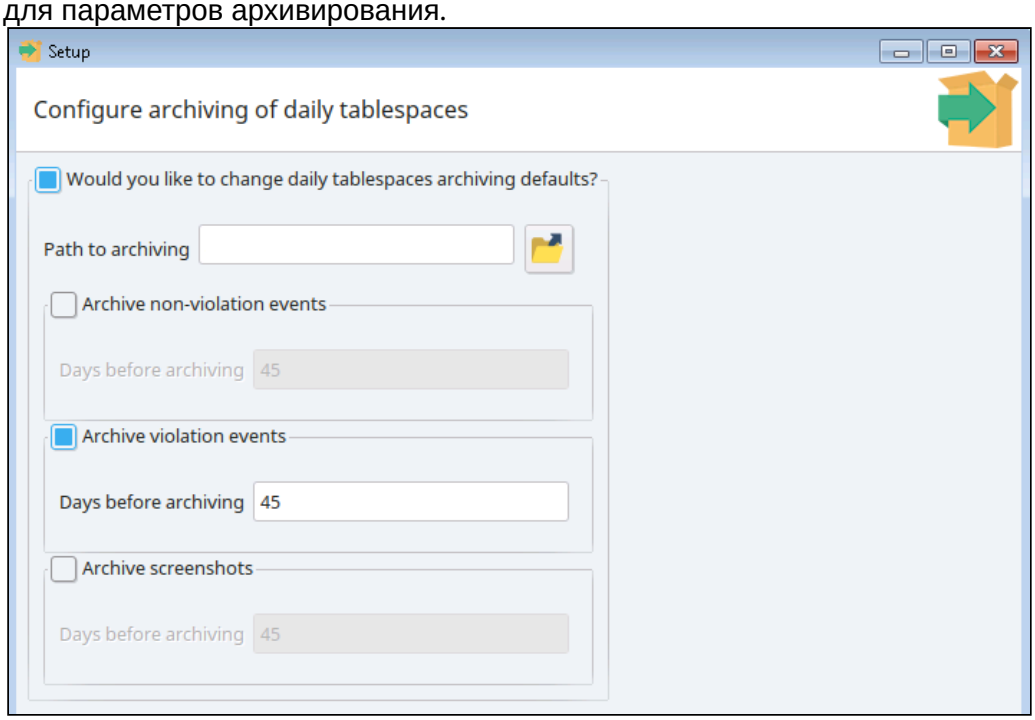
> **Примечание:**

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.

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



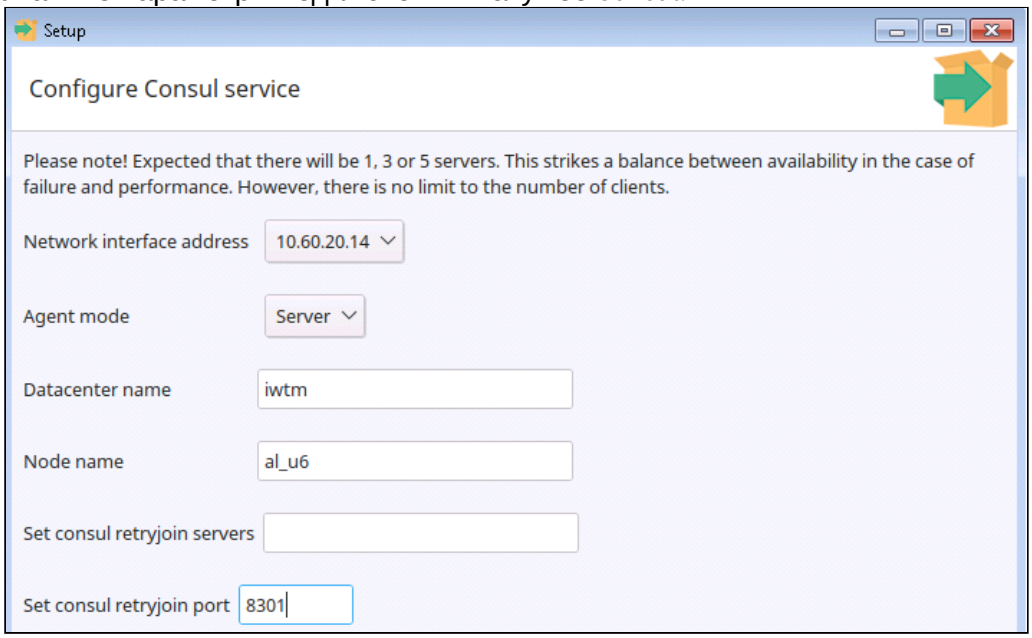
- **`Path to archiving`** - путь к директории хранения файлов архивированных табличных пространств.

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.

9. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию - 90.
10. Укажите параметры подключения к службе Consul:



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

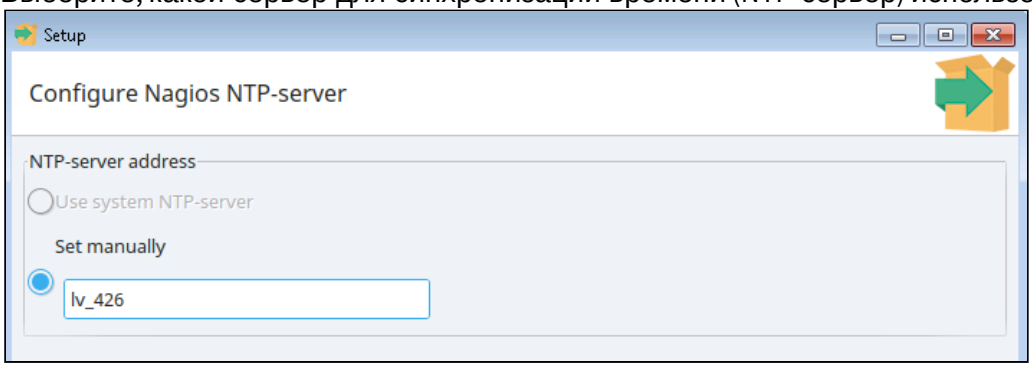
   Для выбора из списка параметров нажмите на кнопку  и в раскрывшемся списке выберите требуемое значение.

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

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

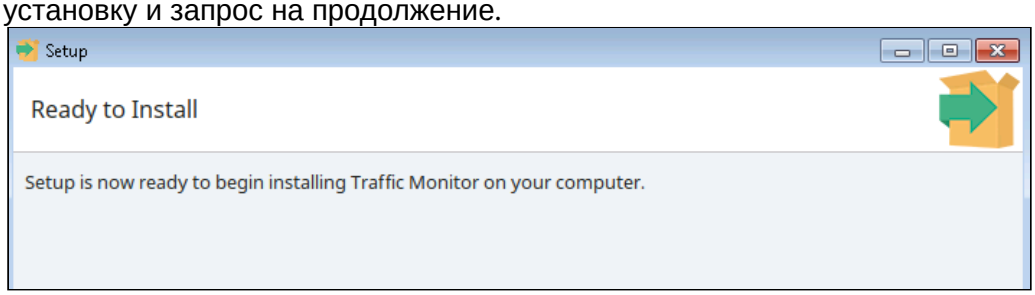
c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую.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

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

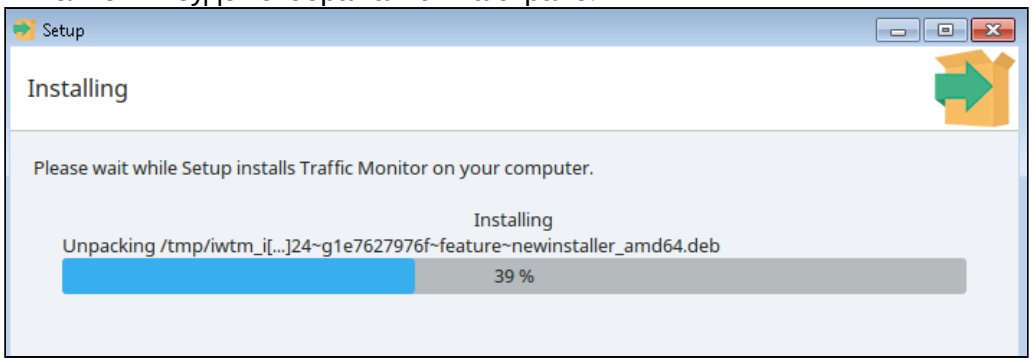


- `Use system NTP-server` - использовать системный NTP-сервер;
- `Set manually` - указать NTP-сервер вручную. При выборе данного варианта укажите IP-адрес или имя доступного NTP-сервера.

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



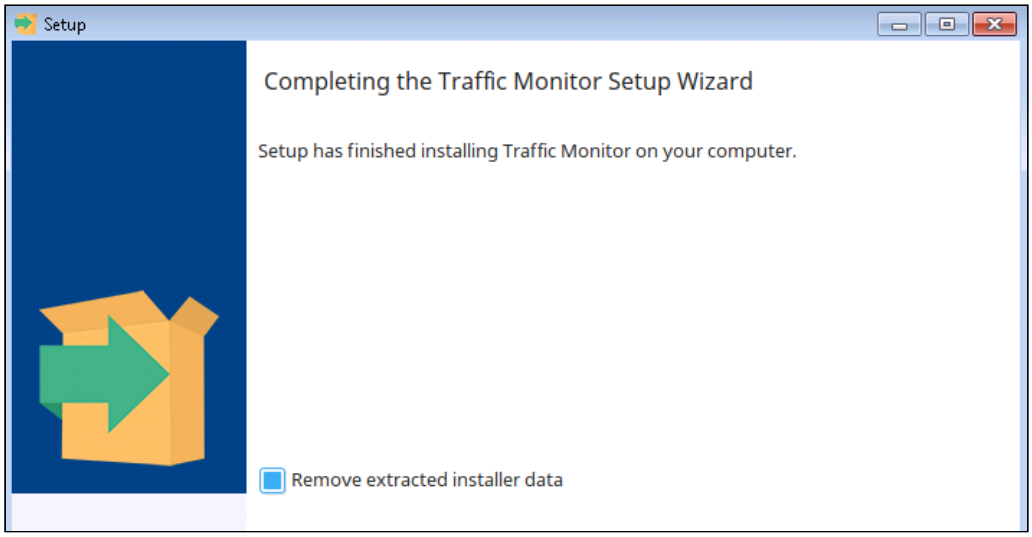
Для начала установки нажмите кнопку **Next**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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.

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



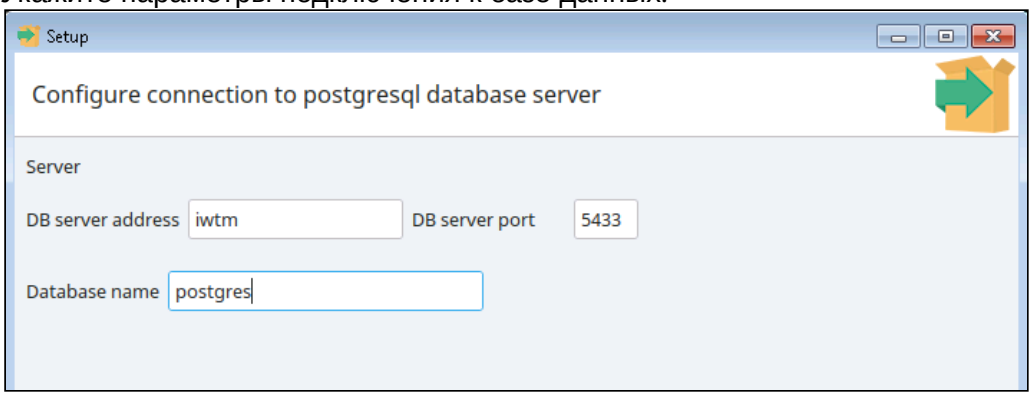
Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove exctracted installer data`**.

14. Для завершения нажмите кнопку **Finish**.
15. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
16. 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`):

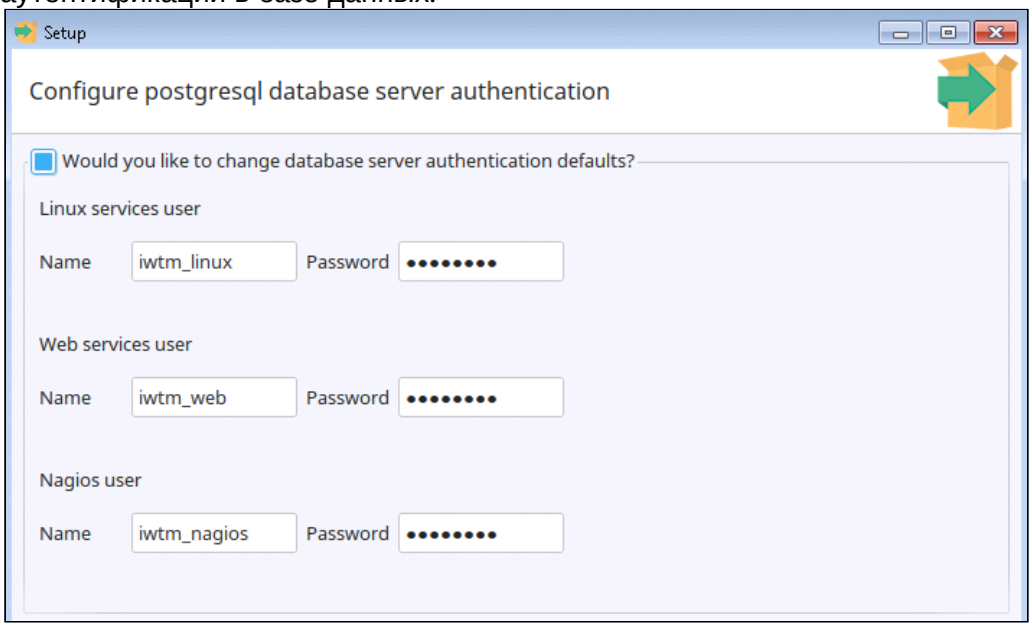
1. Укажите параметры подключения к базе данных:



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

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

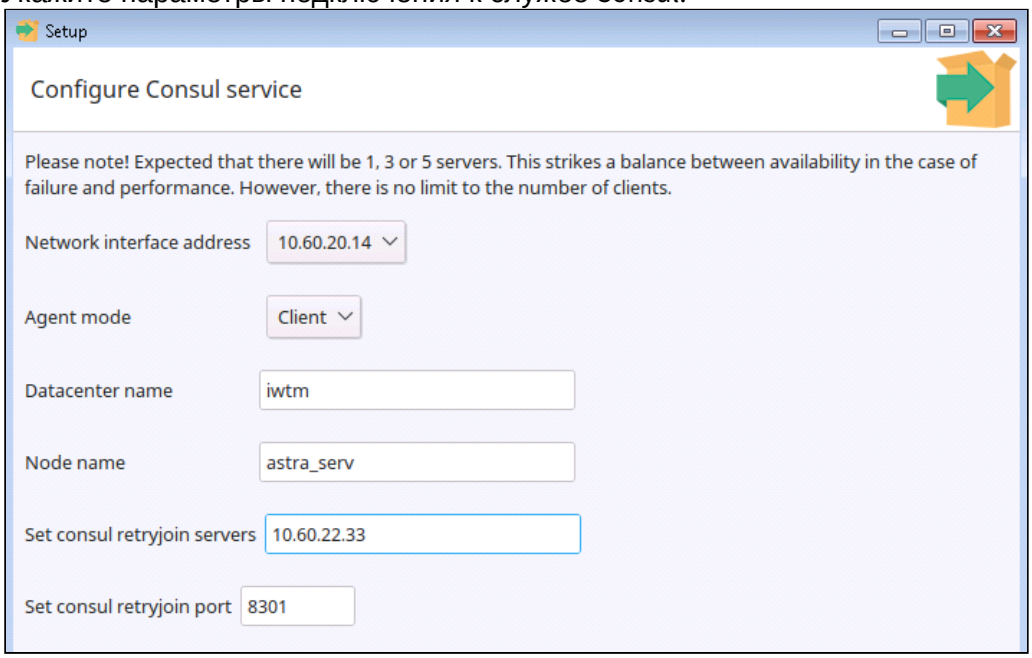
2. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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.

3. Укажите параметры подключения к службе Consul:

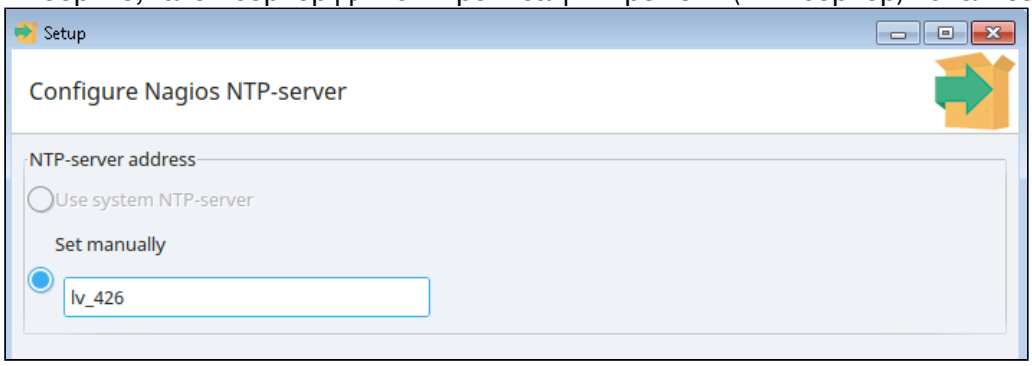


a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите на кнопку и в раскрывшемся списке выберите требуемое значение.
b. Режим работы Consul. Доступны два режима:
   - **`Server`**
   - **`Client`**

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

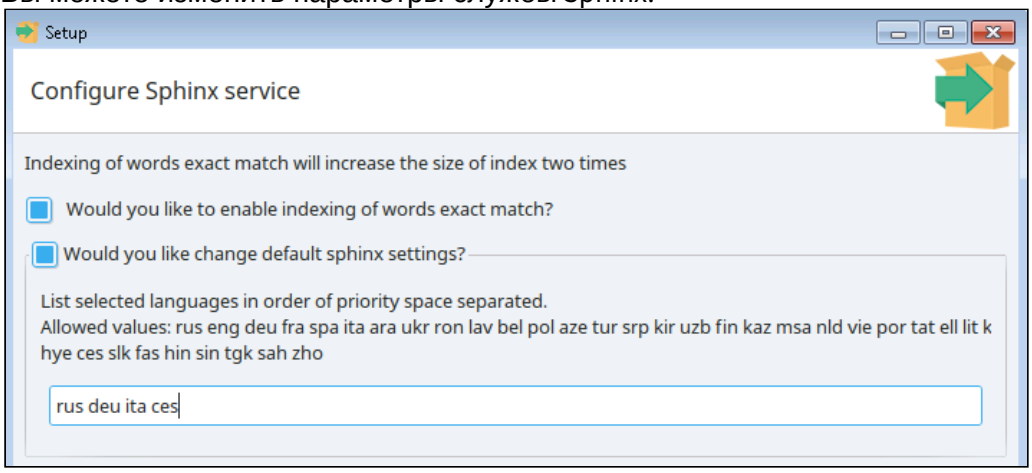
c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую.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

4. 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.

5. Вы можете изменить параметры службы Sphinx:



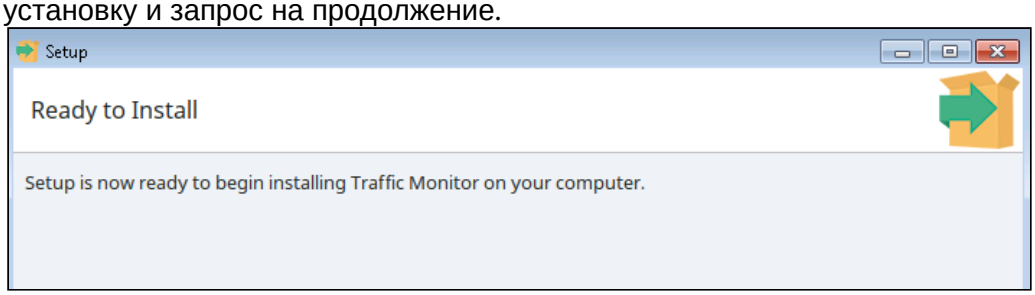
- **`Enable indexing of words exact match`** - включить индексацию на точное совпадение слов;

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

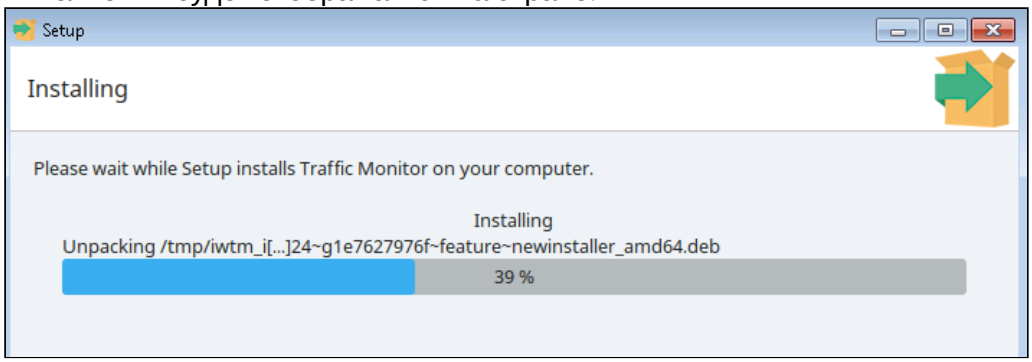
- При необходимости вы можете изменить стандартные параметры работы службы Sphinx (`default sphinx settings`). В этом случае укажите список языков с поддержкой морфологии. По этим языкам будет проводиться индексация.Вы можете указать несколько языков, используя пробел в качестве разделителя.

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

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



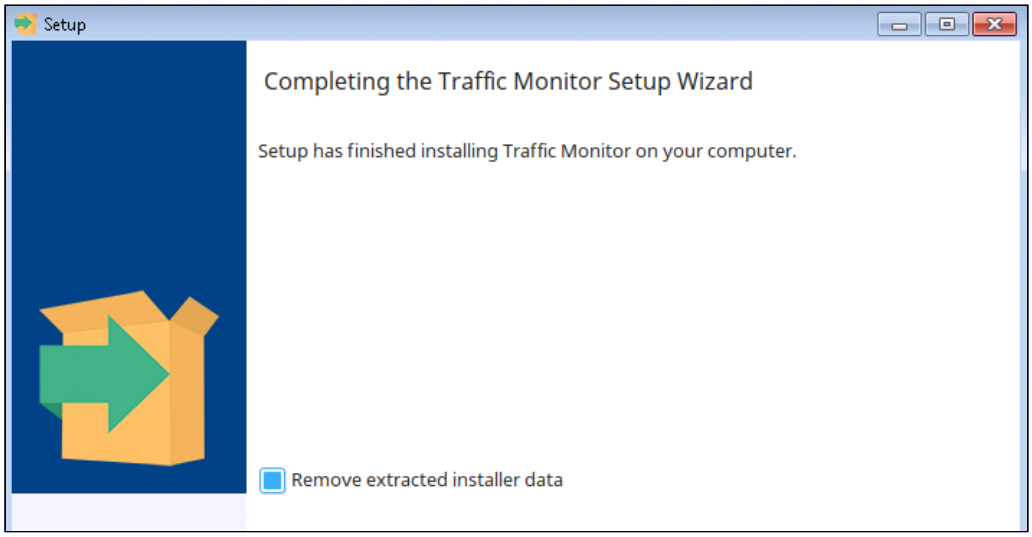
Для начала установки нажмите кнопку **Вперед**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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.

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



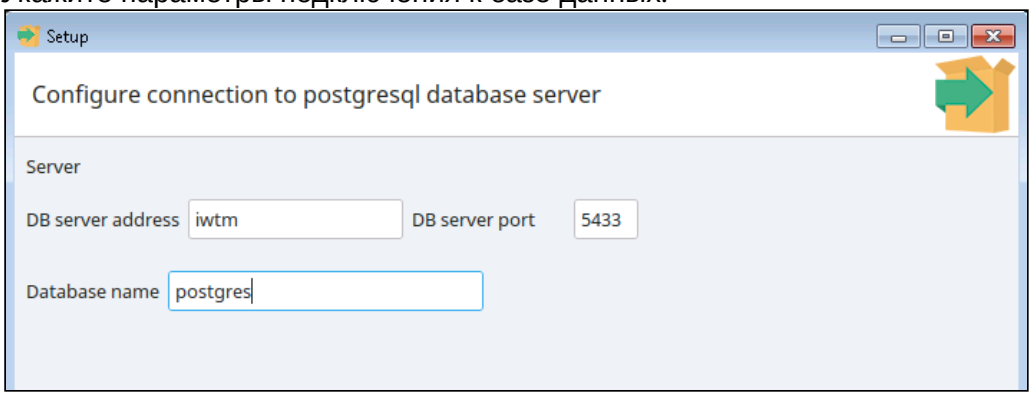
Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove exctracted installer data`**.

8. Для завершения нажмите кнопку **Finish**.
9. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
10. 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`):

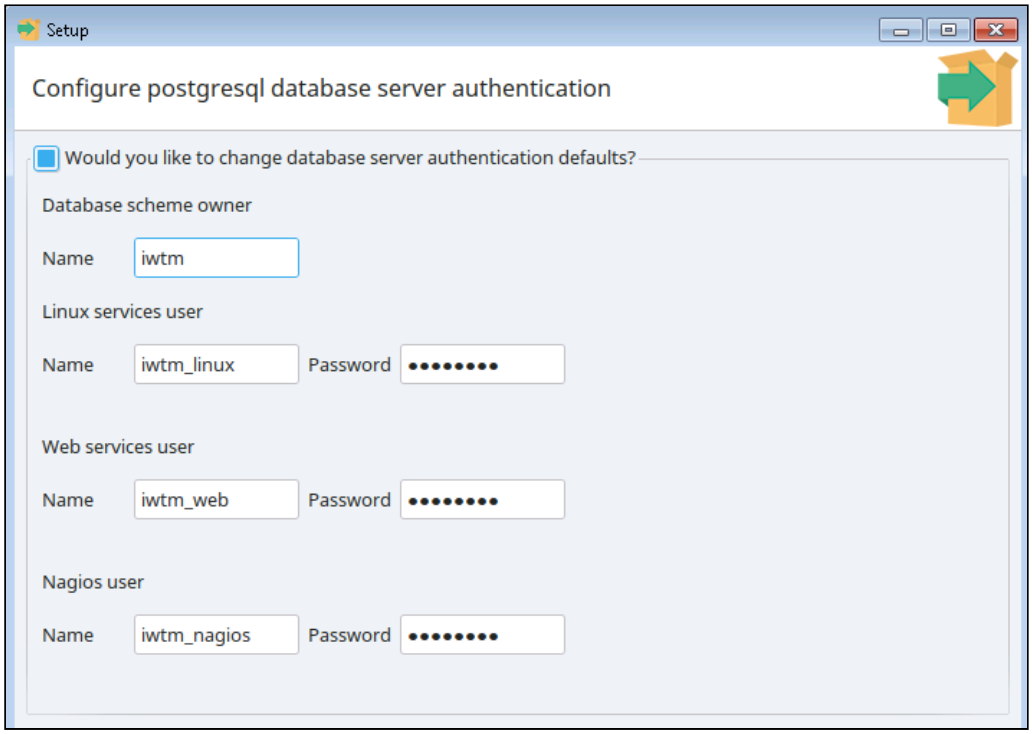
1. Укажите параметры подключения к базе данных:



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

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

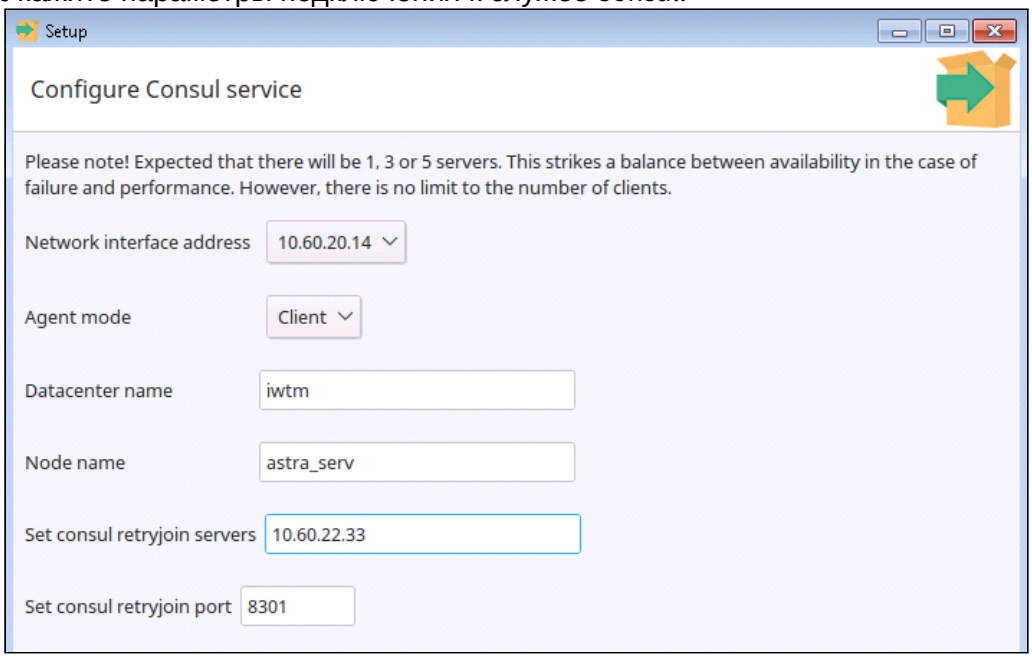
2. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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.

3. Укажите параметры подключения к службе Consul:



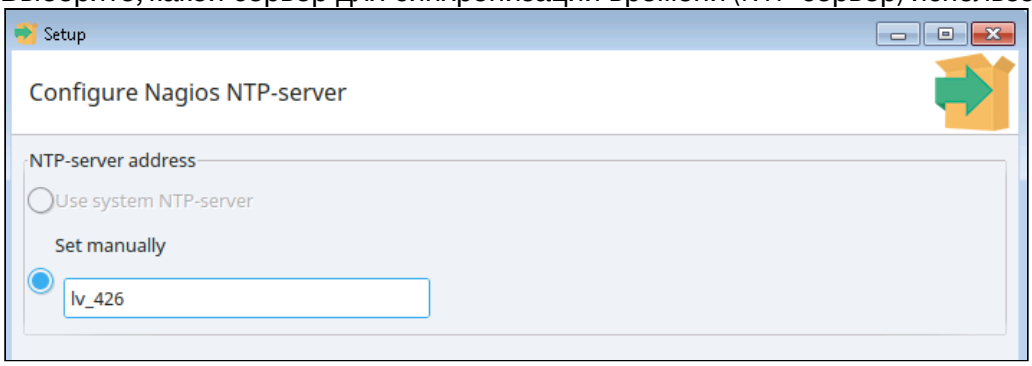
a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите на кнопку и в раскрывшемся списке выберите требуемое значение.
b. Режим работы Consul. Доступны два режима:

- **`Server`**
- **`Client`**

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

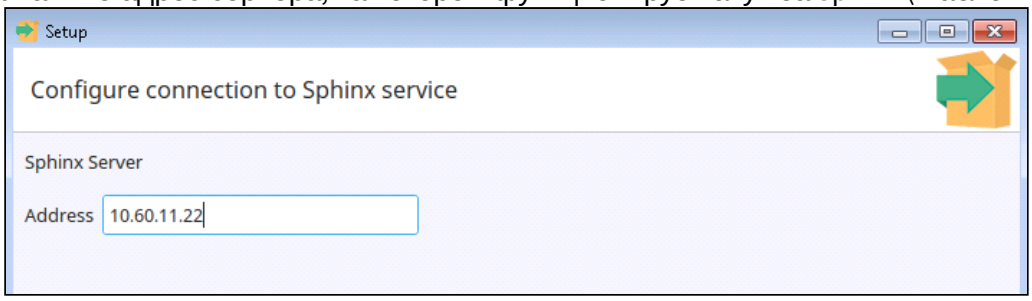
c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую.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

4. 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.

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



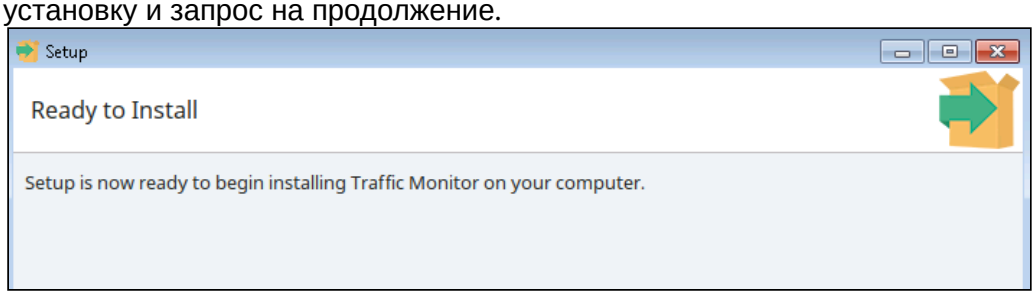
> **Примечание:**
>
> Если шаблоны Индексер и Веб-консоль устанавливаются на один сервер, данный параметр не будет запрошен инсталлятором.

6. Вы можете включить использование технологии OCR.

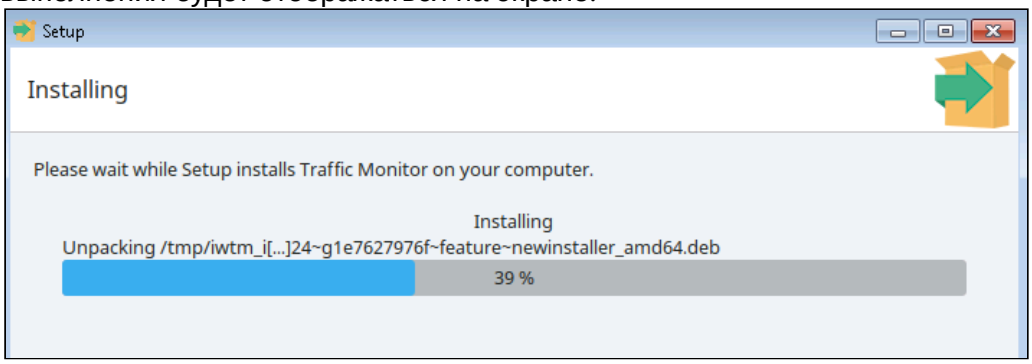


> **Примечание:**
>
> OCR-экстрактор выбирается при установке шаблона Перехватчики.

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



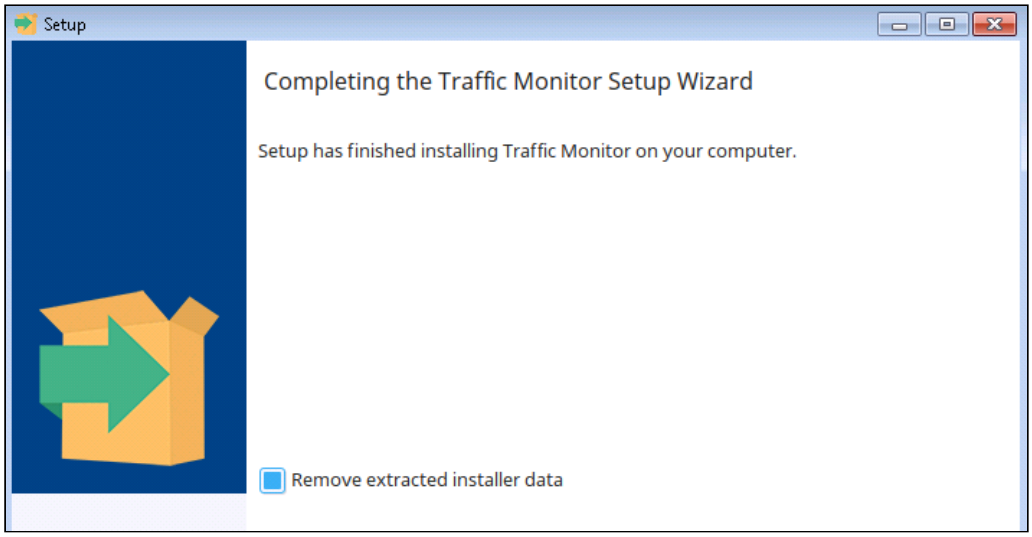
Для начала установки нажмите кнопку **Вперед**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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.

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



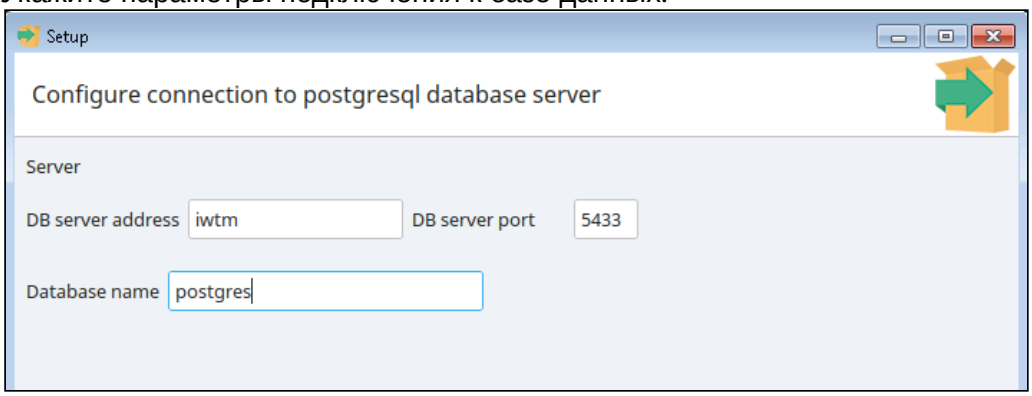
Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove exctracted installer data`**.

9. Для завершения нажмите кнопку **Finish**.
10. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
11. Если необходимо вывести список сервисов Traffic Monitor и их статусы, введите команду:
    `iwtm status`

Установка шаблона Перехватчики

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

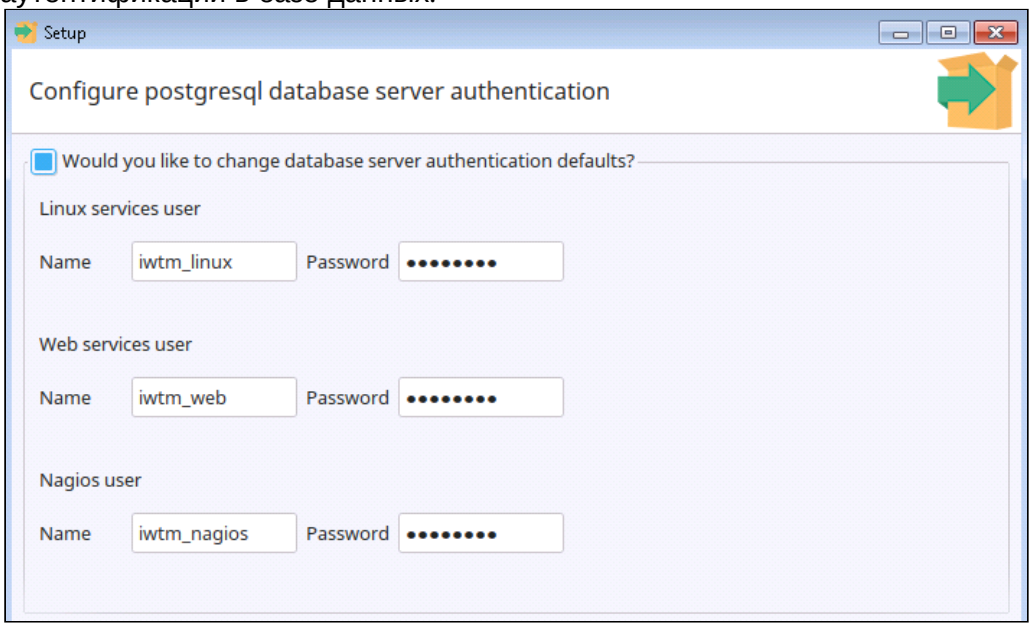
1. Укажите параметры подключения к базе данных:



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

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

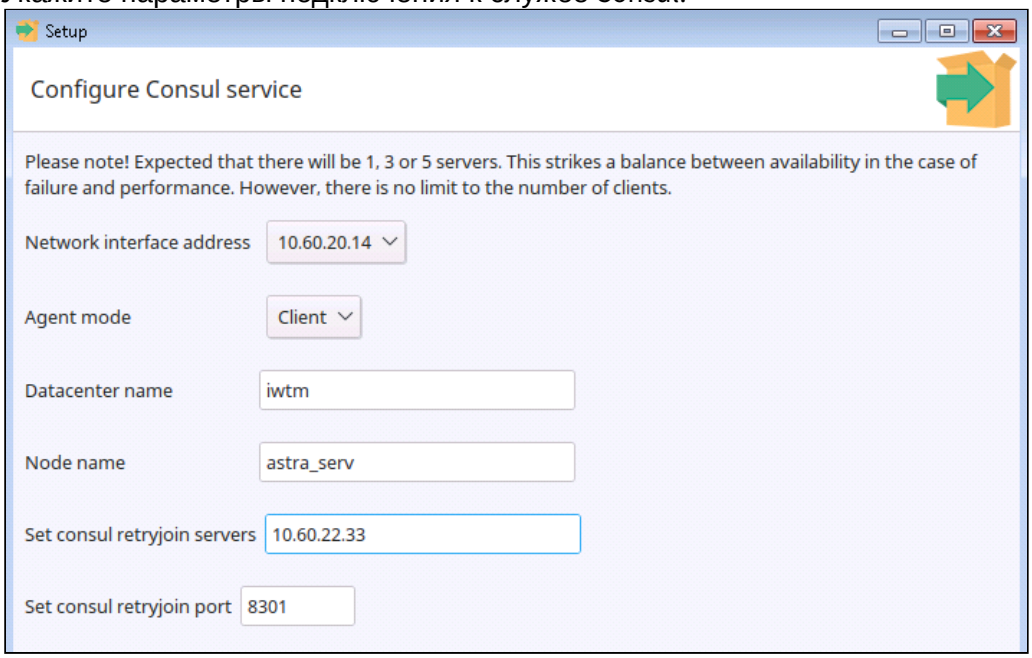
2. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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.

3. Укажите параметры подключения к службе Consul:

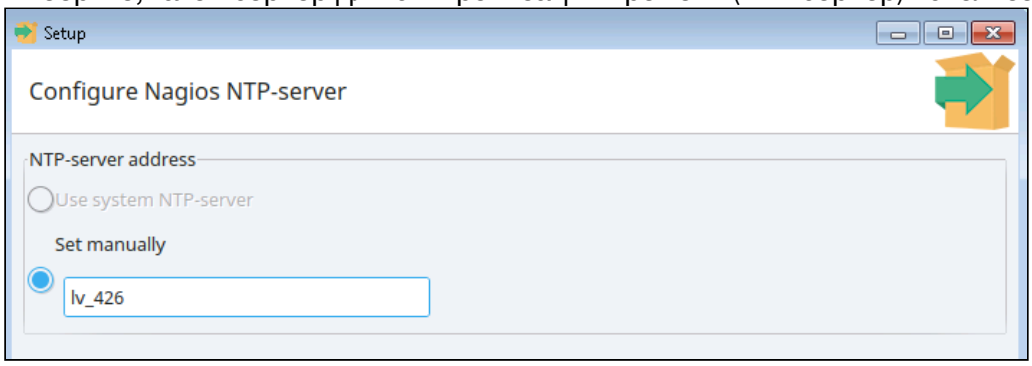


a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите на кнопку и в раскрывшемся списке выберите требуемое значение.
b. Режим работы Consul. Доступны два режима:
   - **`Server`**
   - **`Client`**

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

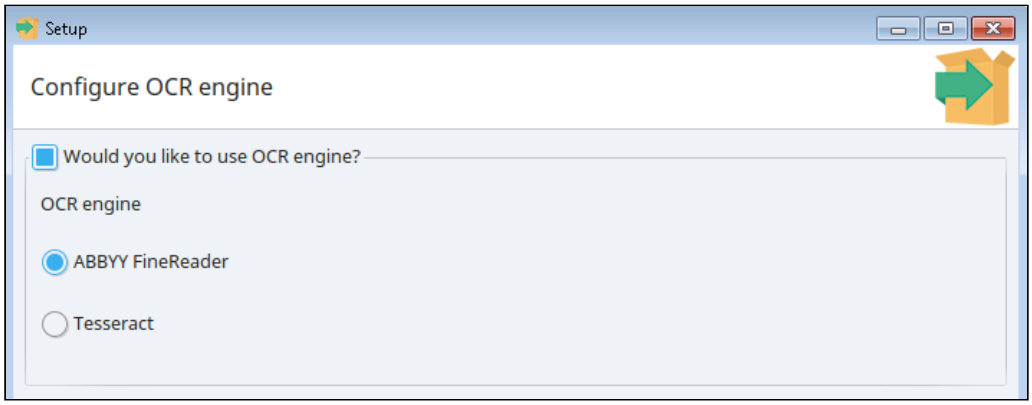
c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую.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

4. 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.

5. Вы можете включить использование технологии OCR.

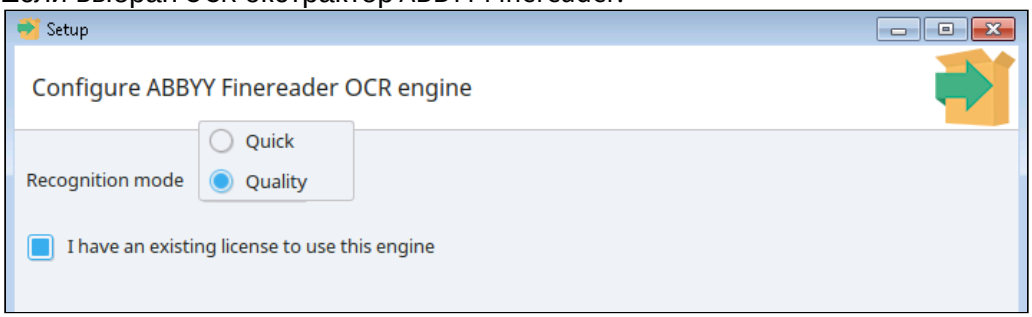


В случае включения необходимо выбрать для использования одну из систем:

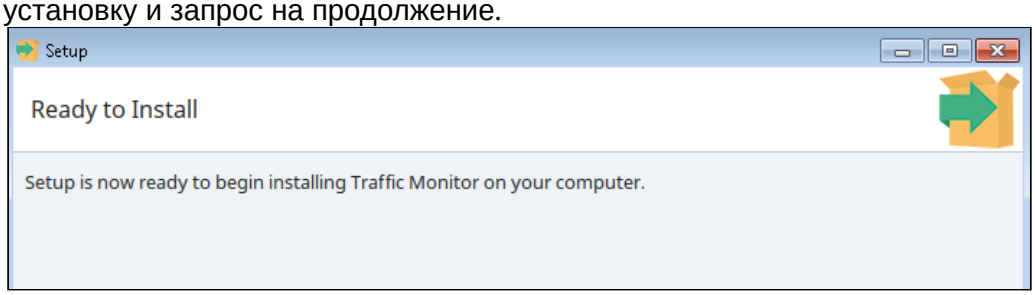
- **`ABBYY FineReader`**;
- **`Tesseract`**.

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

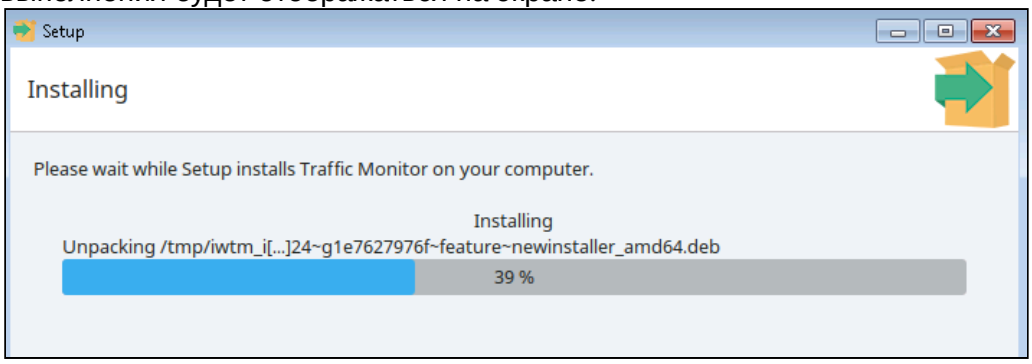
6. Если выбран OCR-экстрактор ABBYY Finereader:



   a. Выберите один из режимов распознавания (**`Recognition mode`**):
      - **`Quick`** – быстрый режим;
      - **`Quality`** – тщательный режим, обеспечивающий более высокое качество распознавания.
   b. Подтвердите наличие у вас активной лицензии на использование 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".
7. 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.

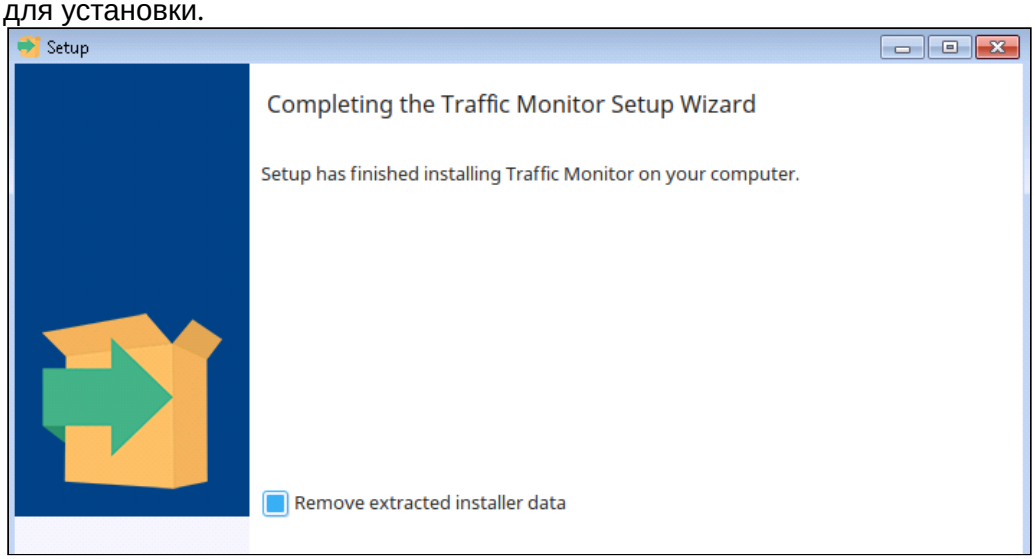


Процесс может занять некоторое время.

> **Примечание:**

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

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



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

9. Для завершения нажмите кнопку **Finish**.
10. Для перехвата `smtp` с учетом мандатных меток:
    a. Введите команду для вызова файлового менеджера:
    `sudo mc`
    b. Перейдите в директорию `/opt/iw/tm5/etc` и откройте на редактирование файл **`smtpd.conf`**.
    c. Установите параметру `"EnablePrivSock"` значение `true`, сохраните изменения и закройте файл.
    d. Для выхода из файлового менеджера введите команду:
    `exit`
11. Чтобы применить изменения окружения, обязательно выйдите из системы и повторно авторизуйтесь или перезагрузите сервер.
12. 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. Если до установки в ОС они были включены, не выключайте их, и наоборот.

В противном случае корректная работа Системы не гарантируется.

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".

3.1.3 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 7.4 на сервере должна быть установлена ОС Astra Linux Special Edition 1.7.0.
>
> Чтобы узнать версию установленной ОС, выполните команду:
>
> ```
> cat /etc/astra_version
> ```
>
> Не удаляйте репозитории, подключенные в процессе установки ОС Astra Linux Special Edition. Для установки потребуются репозитории с 2-х дисков:
>
> - Astra-Linux-Smolensk;
> - Astra-Linux-Smolensk-Devel.

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.

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

   Примечание:

   Если используется подключение по SSH, выполните повторное подключение.

4. 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`
5. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch Traffic Monitor:
   - **`iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`** (где x.x.x.xxx - номер сборки);
   - **`iwtm-postgresql-11.10-x.x.x.xxx-astra-smolensk-1.7.tar.gz`**.

   В нашем примере:
   - **`iwtm-installer-7.5.0.120-astra-smolensk-1.7`**;
   - **`iwtm-postgresql-11.10-7.5.0.120-astra-smolensk-1.7.tar.gz`**.
6. Выполните следующую команду:
   `sudo apt-get update`

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-7.5.0.120-astra-smolensk-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-7.5.0.120-astra-smolensk-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 после установки:

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. Если до установки в ОС они были включены, не выключайте их, и наоборот.

В противном случае корректная работа Системы не гарантируется.

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 инсталятора	
`skip_check_swap`	`0`	`0, 1`	Отключение проверки	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
			объема Swap-пространства	
`skip_check_space`	`0`	`0, 1`	Отключение проверки объема свободного пространства на диске	
`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	
`product_language`	`rus`	`rus, eng`	Основной язык продукта	
`installation_type`	`all_in_one`	`distributed, all_in_one`	Тип установки	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`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	
`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_installat`

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`db_server_port`			Порт сервера с базой данных	`ion_type=remote`)
`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`)
`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 (

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				`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 табличному пространству	
`db_storage_dtbs_paths_number`	`1`	1 - 10	Количество путей к ежедневным табличным пространствам	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`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_dtbs_paths_number`
`db_storage_dtbs_path_2`	`/u02/pgdata2`		Путь к ежедневному табличному пространству №2	
`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	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`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	
`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 (

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				`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`)
`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`

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`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_type=all_in_one`) или шаблон База данных (`template_database=1`)
`db_archiving_dtbs_change_defaults`	`0`	`0, 1`	Изменить параметры архивирования по умолчанию	

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
`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 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

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				(`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`)
`db_removing_dtbs_change_defaults`	`0`	`0, 1`	Изменить параметры удаления по умолчанию	
`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_one`), шаблон Перехватчики

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
				(`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.
`packages_unpack_dir`	`/tmp/iwtm_instal`	Строка - путь к	В директорию будут распакованы установочные	Директория будет создана автоматически. Допускается

Название	Значение по умолчанию	Допустимые значения	Описание	Примечание
	`ler/packages`	директории	пакеты Traffic Monitor	указать существующую директорию. Если установка завершится без ошибок, директория будет автоматически удалена.

3.2 Предустановленные серверные параметры

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

Директории установки Системы (могут располагаться на разных серверах):

- компоненты Traffic Monitor – `/opt/iw`
- компоненты базы данных – `/u01` и `/u02`

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`	Без пароля

Назначение	Имя	Пароль
Владелец схемы базы данных	`iwtm`	`xxXX1234`
Пользователь, от имени которого будут запускаться серверные процессы базы данных PostgreSQL	`postgres`	`xxXX1234`

Учетные записи баз данных:

Учетные записи доступны после запуска `psql` для PostgreSQL.

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

Учетные записи Веб-консоли управления:

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

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

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

4 Обновление Системы

Важно!

В Traffic Monitor 7.5 на ОС Astra Linux поддерживается обновление **только** с версии **7.4.x**. Обновление с версий ниже 7.4.0 не поддерживается.

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 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).

Перед обновлением убедитесь в наличии:

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

Также до начала обновления требуется выяснить:

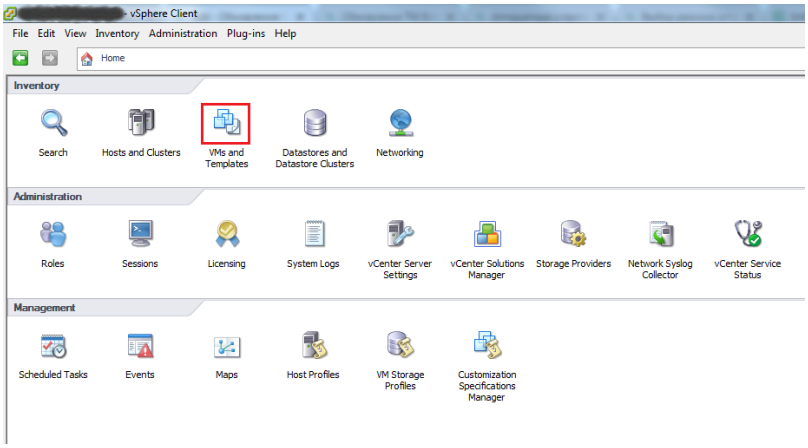
- какой тип установки в Системе (могут быть типы *Все-в-одном (All-in-one)* и *Распределенная установка*) - данная информация понадобится для выбора инструкции по обновлению;
- на каком сервере установлен пакет `web-gui` - данная информация понадобится для очистки кеша сервера после обновления схемы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

До начала обновления выполните следующие действия:

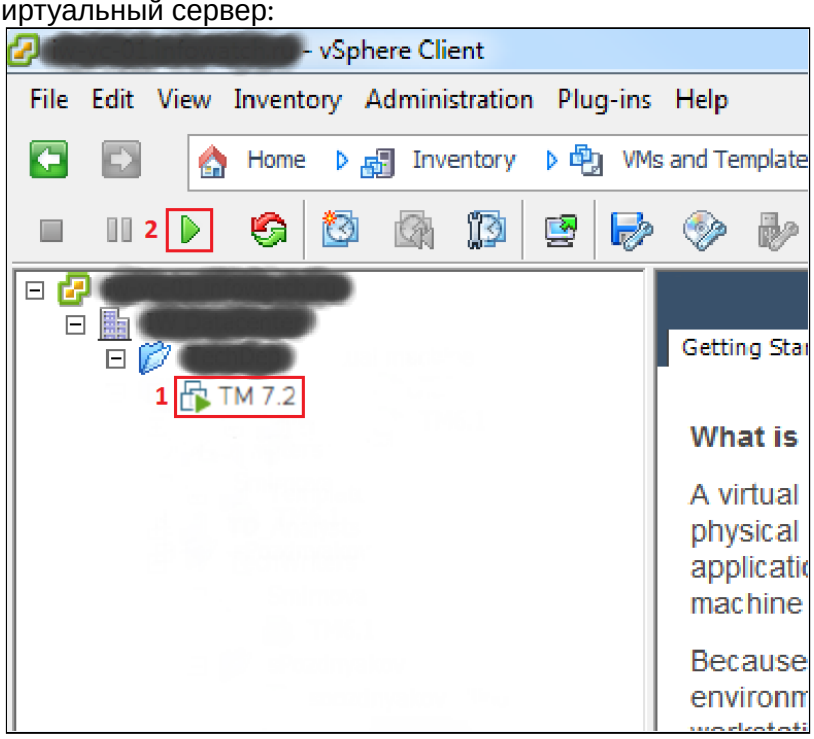
1. Включите (если он был выключен) каждый сервер, предназначенный для обновления:
   - в случае физического сервера - нажмите кнопку включения, расположенную на корпусе сервера (подробнее см. в инструкции к серверу);
   - в случае виртуального сервера - выполните команду **Power On** (см. пример ниже).

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

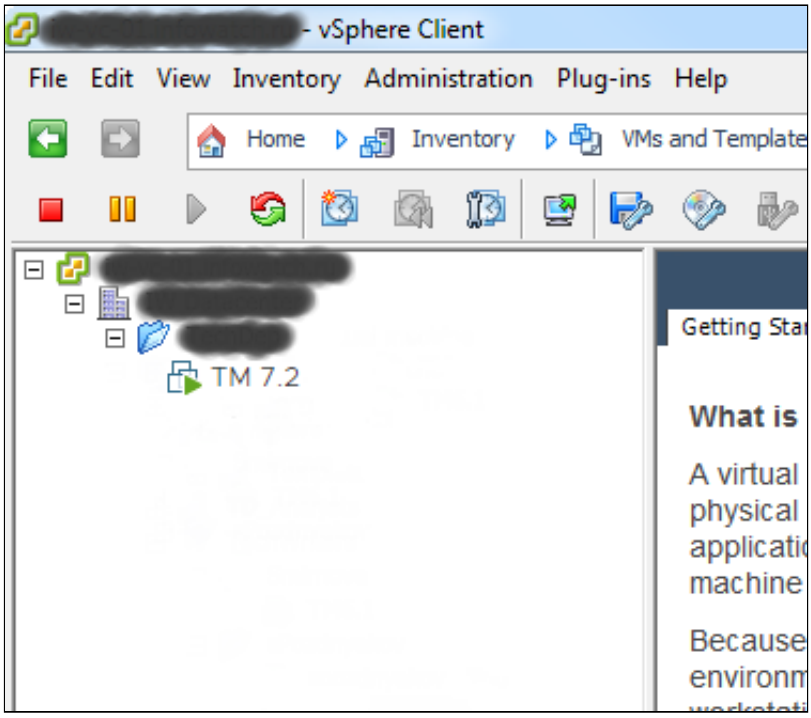
   Запустите клиентское приложение VMware vSphere Client от имени администратора (щелкните правой кнопкой мыши на иконке приложения и выберите **Запуск от имени администратора**). Войдите в приложение, используя логин и пароль, выданные администратором вашей информационной сети. Перейдите в раздел с виртуальными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



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



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



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

Обновите серверы согласно следующим инструкциям:

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

Примечание:

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.

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

Важно!

Перед обновлением Traffic Monitor обновите сервер Device Monitor.

Поддерживается обновление **только** с версий **7.4.x**.

Для обновления потребуются 2 диска:

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

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": "7.4.2.190",
"all_in_one": true,
```

   Запись из примера соответствует серверу с типом установки *Traffic Monitor Enterprise All-in one* и версией *7.4.2.190*.
7. Откройте файл `/etc/apt/sources.list` и проверьте соответствие его содержимого следующему виду:
   ```
   deb file:///директория_1/ smolensk main non-free contrib
   deb file:///директория_2/ smolensk main non-free contrib
   ```
   где:
   a. `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
   b. `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel
8. Закройте файл `sources.list`.
   Перейдите в указанные в файле директории, и убедитесь в наличии в них папок и файлов репозиториев.
9. Для выхода из файлового менеджера (требуется для лучшего контроля выполнения команд) введите команду:
   `exit`

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. Введите команду:
   `systemctl stop iwtm-php-fpm`
   c. 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-smolensk-1.7`** (где x.x.x.xxx - номер сборки);
   - **`iwtm-postgresql-11.10-x.x.x.xxx-astra-smolensk-1.7.tar.gz`**.

   В нашем примере:
   - **`iwtm-installer-7.5.0.125-astra-smolensk-1.7`**;
   - **`iwtm-postgresql-11.10-7.5.0.125-astra-smolensk-1.7.tar.gz`**.
3. Чтобы сделать файл **`iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`** исполняемым, введите команду:
   `sudo chmod u+x /root/iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
   В нашем примере команда будет следующей:
   `sudo chmod u+x /root/iwtm-installer-7.5.0.125-astra-smolensk-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_05.05.2022_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-7.4.2.152-2022-09-10_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**

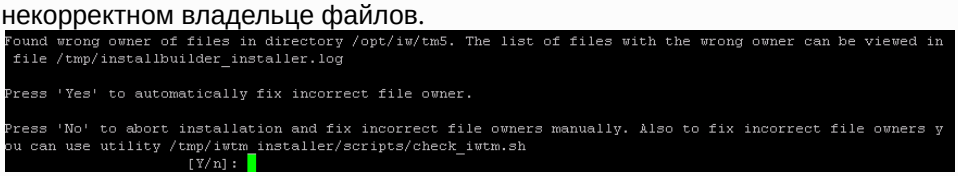
  Чтобы обновить Traffic Monitor в консоли сервера, выполните следующие действия:

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

`sudo ./iwtm-installer-7.5.0.125-astra-smolensk-1.7`
Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

Примечание:

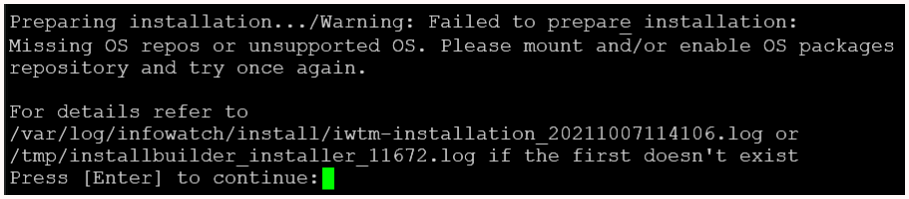
Перед запуском инсталлятора может быть выведено предупреждение о некорректном владельце файлов.



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!

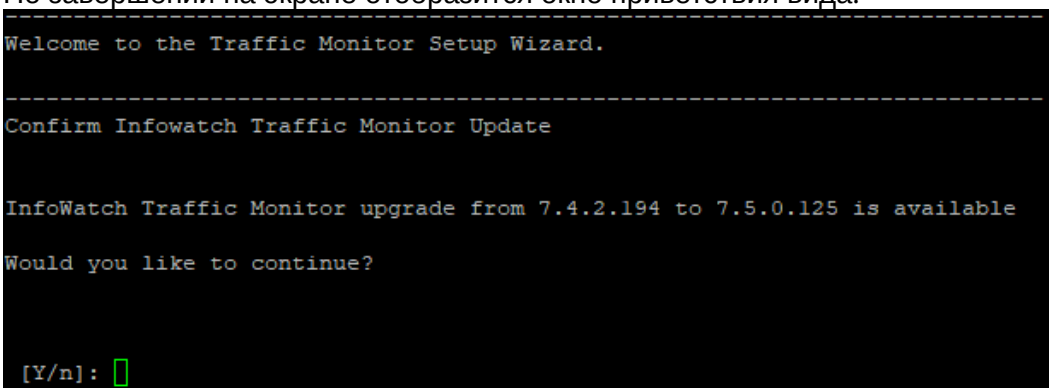
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



При возникновении данной ошибки нажмите **Enter** для завершения работы инсталлятора, затем подключите репозитории с дисков Astra-Linux-Smolensk и Astra-Linux-Smolensk-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:



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

b. Для продолжения введите **Y** и нажмите **Enter**. Для выхода из инсталлятора введите **N** и нажмите **Enter**.

> **Примечание:**
>
> При обновлении в консоли сервера перед полем ввода в квадратных скобках цифрой или заглавной буквой указано значение по умолчанию. Оно будет использовано, если оставить поле ввода пустым и нажать **Enter**.

c. Подтвердите остановку сервисов Traffic Monitor и Базы данных. Шаги подтверждения и выбора режима остановки будут пропущены, если сервисы были остановлены вручную до запуска инсталлятора.

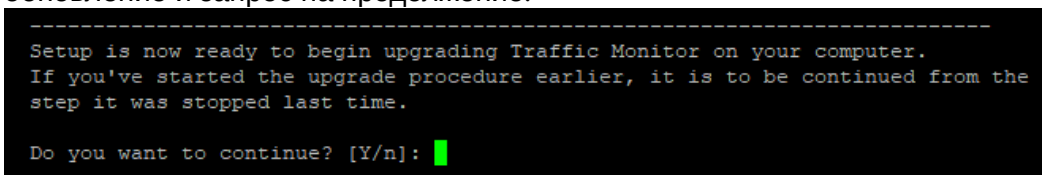
d. Выберите режим остановки Traffic Monitor:
   - `Quick stop` - быстрая остановка без обработки событий;
   - `Waiting for stop` - перед остановкой дождаться завершения текущей обработки событий;
   - `Waiting for emptying file queues` - перед остановкой дождаться обработки всех событий и очистки файловых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

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

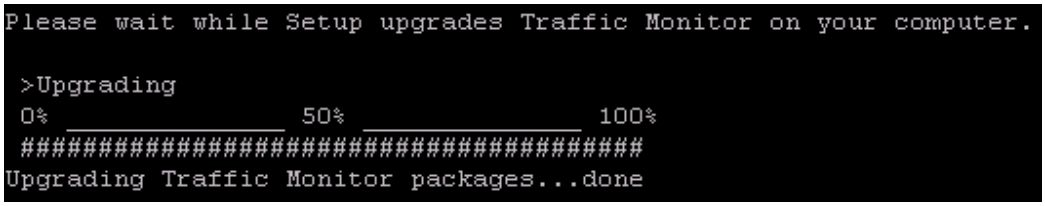
> **Примечание:**
>
> Если выбран `Quick stop`, остановленные сервисы до запуска будут иметь статус `failed (failed)`.

e. 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.

f. 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.

g. После обновления инсталлятор предложит запустить остановленные сервисы.

> **Важно!**
>
> После обновления настройки системы мониторинга Nagios были 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.

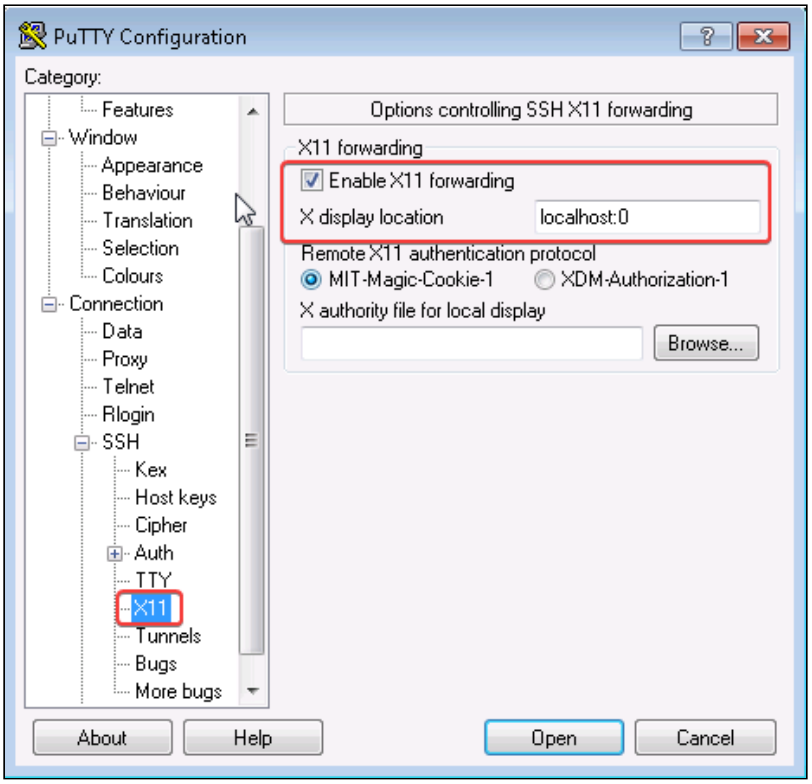
h. Перед завершением работы инсталлятор предложит удалить пакеты, созданные для обновления.
   Если обновление прошло успешно, данные рекомендуется удалить.
i. Дождитесь завершения работы инсталлятора.

- **обновление с использованием графического режима инсталлятора**

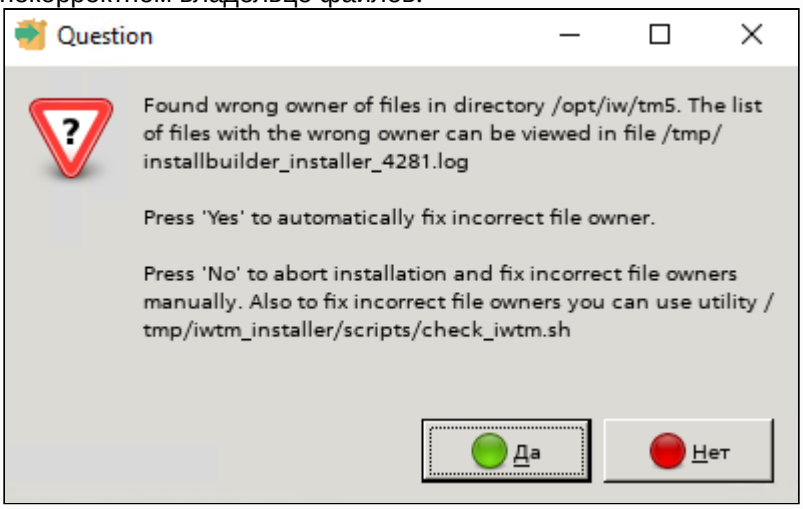
  В ОС оконная система X Window System использует клиент-серверную модель. Для запуска инсталлятора в графическом режиме используется перенаправление графического вывода удаленной подсистемы (**X11 Forwarding**). Это позволит работать напрямую с графическими приложениями среды Linux на компьютере, с которого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



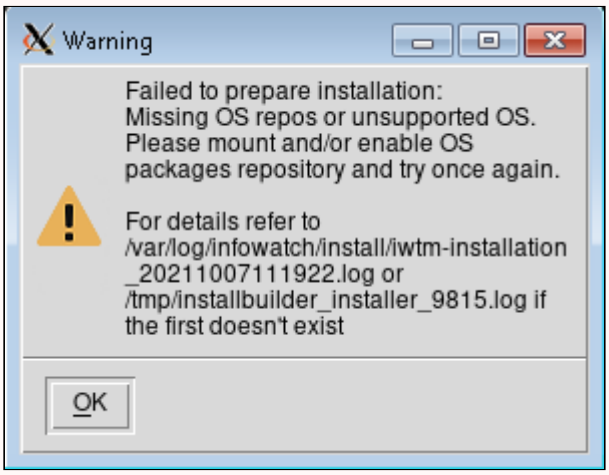
e. Запустите инсталлятор, выполнив следующую команду:
`sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
В нашем примере команда будет следующей:
`sudo ./iwtm-installer-7.5.0.125-astra-smolensk-1.7`
Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

> **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!

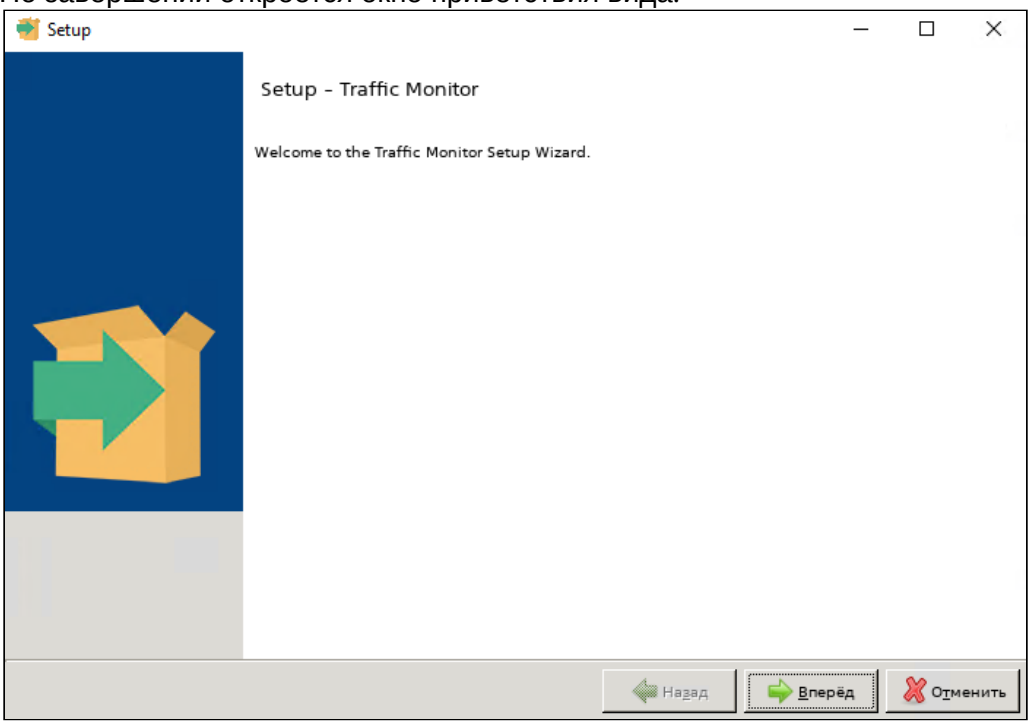
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



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

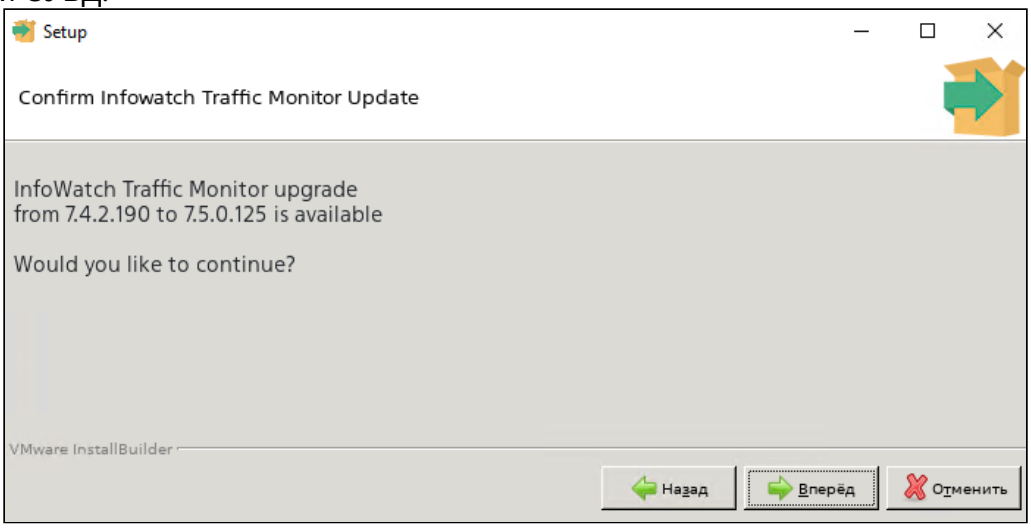
Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

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



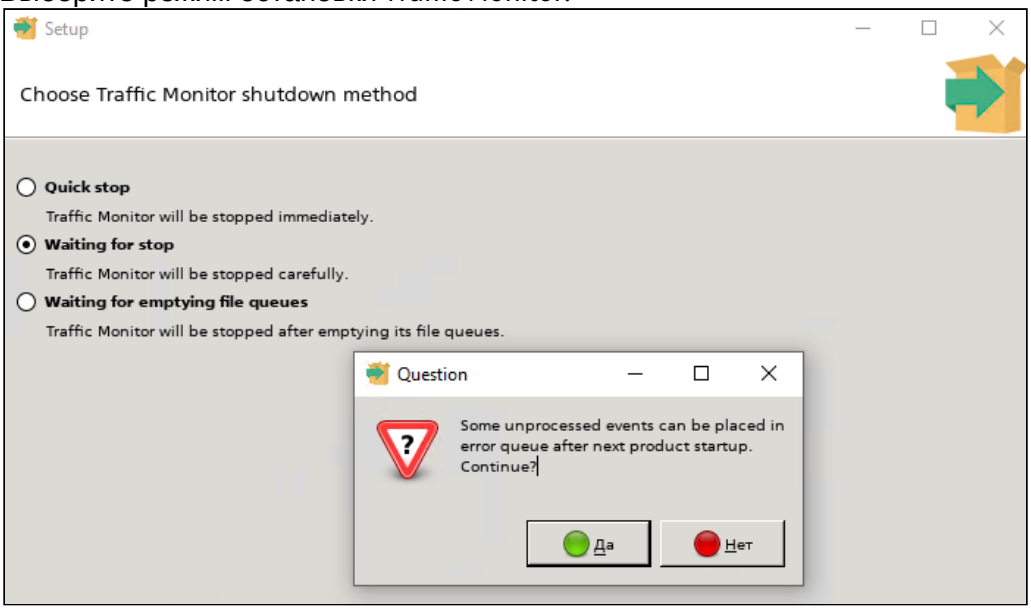
Для продолжения нажмите **Вперед**.

g. Подтвердите остановку сервисов Traffic Monitor и Базы данных. Шаги подтверждения и выбора режима остановки будут пропущены, если

сервисы были остановлены вручную до запуска инсталлятора.



h. Выберите режим остановки Traffic Monitor:



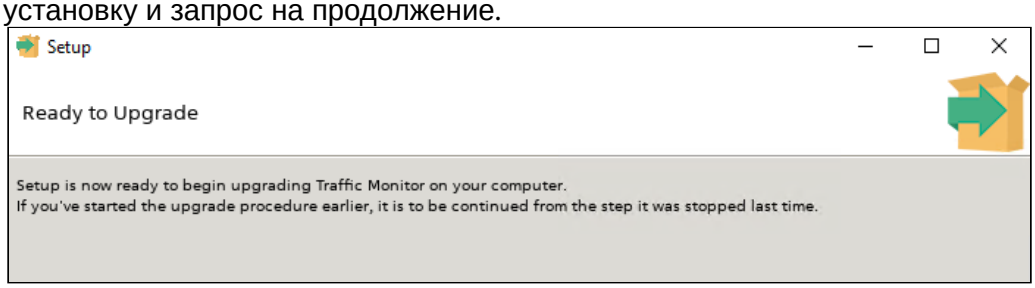
- `Quick stop` - быстрая остановка без обработки событий;
- `Waiting for stop` - перед остановкой дождаться завершения текущей обработки событий;
- `Waiting for emptying file queues` - перед остановкой дождаться обработки всех событий и очистки файловых очередей.

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

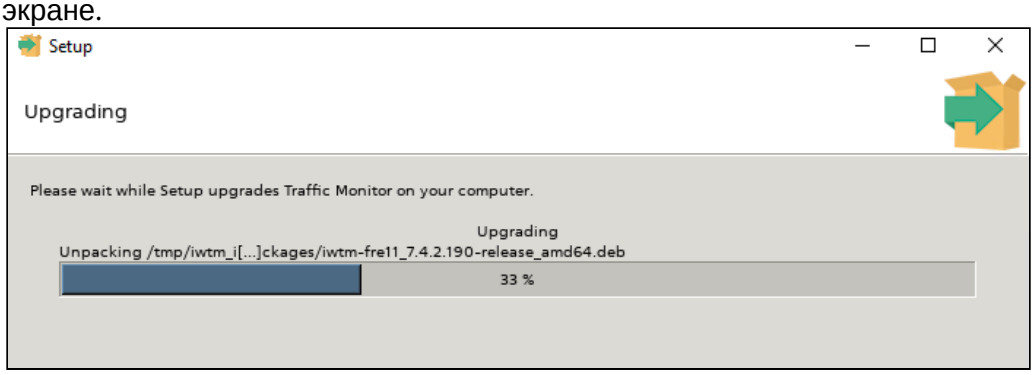
> **Примечание:**
>
> Если выбран `Quick stop`, остановленные сервисы до запуска будут иметь статус `failed (failed)`.

i. 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.

j. 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.

k. 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!

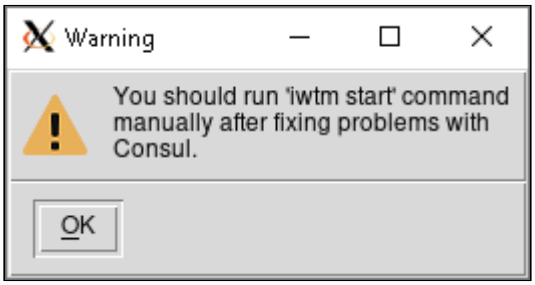
После обновления настройки системы мониторинга Nagios были изменены на значения по умолчанию. Если до обновления конфигурационные файлы Nagios редактировались, в директории `/etc/infowatch/nagios/iwmon` будут созданы их копии с расширением `.saved`. Перед запуском сервисов Traffic Monitor перенесите 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.

l. 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-7.5.0.125-astra-smolensk-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:

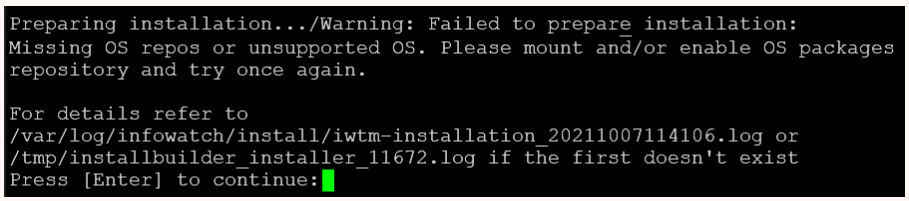
- `none` - в процессе работы инсталлятор не выводит на экран никакую информацию и не требует взаимодействия с пользователем;
- `minimal` - отображает прогресс обновления, не требует взаимодействия с пользователем;
- `minimalWithDialogs` - отображает прогресс обновления, также в процессе могут появляться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

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

```
./iwtm-installer-7.5.0.125-astra-smolensk-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`

8. Введите команду для поиска и вывода на экран консоли списка файлов с расширением **`.dpkg-dist`**.
   `sudo find / -name "*dpkg-dist*" -print`
   Если такие файлы найдены, их 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. 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&)
> ```

```
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.

11. Если у вас установлена система Prometheus и если сервер не был перезагружен, для запуска службы выполните команду:
    `systemctl start iwtm-postgres_exporter`
12. Введите команду для очистки кеша:
    `redis-cli flushall`
13. 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. 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 **только** с версий не ниже **7.4.x**.

Для обновления потребуются 2 диска:

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

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!

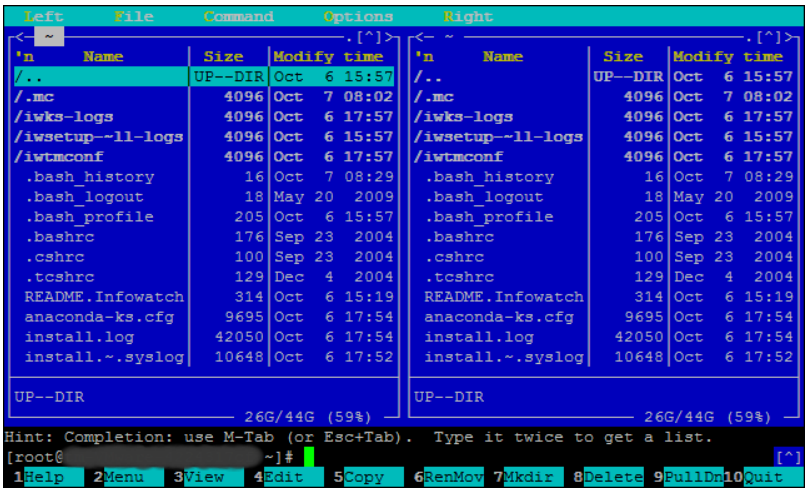
Каждый сервер должен иметь уникальный корректный FQDN.

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": "7.4.2.190",
  "all_in_one": false,
  "templates": {
    "db": {
      "local": true
    },
    "indexer": {},
  }
}
```

Запись из примера соответствует серверу с *распределенной* установкой *Traffic Monitor Enterprise* версии *7.4.2.190*. На сервере из примера активированы шаблоны *База данных* и *Индексер*. Используется *локальная* база данных.

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

> **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 с шаблоном Веб-консоль:

i. Введите команду:
`systemctl stop iwtm-php-fpm`
ii. 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.

c. На сервере с шаблоном Индексер:
i. Введите команду для остановки службы `iw_indexer`:
`iwtm stop indexer`
ii. 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

d. На сервере с шаблоном 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:
>
> 1. Перехватчики
> 2. Индексер
> 3. Веб-консоль
> 4. База данных

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

Порядок обновления следующий:

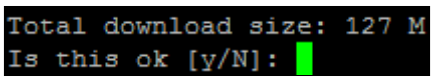
Шаг 1. Обновление всех серверов.
Шаг 2. Проверка кластера службы Consul.
Шаг 3. Проверка работоспособности внутренних сервисов Системы.
Шаг 4. Завершение обновления серверов.

ШАГ 1. ОБНОВЛЕНИЕ ВСЕХ СЕРВЕРОВ

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

1. 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-smolensk-1.7`** (где x.x.x.xxx - номер сборки);
   - **`iwtm-postgresql-11.10-x.x.x.xxx-astra-smolensk-1.7.tar.gz`**.

   В нашем примере:
   - **`iwtm-installer-7.5.0.125-astra-smolensk-1.7`**;
   - **`iwtm-postgresql-11.10-7.5.0.125-astra-smolensk-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-smolensk-1.7`** исполняемым, введите команду:
   `sudo chmod u+x ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
   В нашем примере команда будет следующей:
   `sudo chmod u+x ./iwtm-installer-7.5.0.125-astra-smolensk-1.7`
5. Откройте файл `/etc/apt/` **`sources.list`** и проверьте соответствие его содержимого следующему виду:
   ```
   deb file:///директория_1/ smolensk main non-free contrib
   deb file:///директория_2/ smolensk main non-free contrib
   ```
   где:
   a. `директория_1` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk
   b. `директория_2` - это абсолютный путь к директории, в которой сохранены данные с диска Astra-Linux-Smolensk-Devel
6. Закройте файл **`sources.list`**.
   Перейдите в указанные в файле директории, и убедитесь в наличии в них папок и файлов репозиториев.
7. Для обновления пакетов введите команду:
   `sudo apt-get update`
   Будет выведен запрос вида:

   Для продолжения наберите **Y** на клавиатуре и нажмите **Enter**.
8. Если у вас установлена система Prometheus, на сервере с шаблоном База данных для остановки службы выполните команду:
   `systemctl stop  iwtm-postgres_exporter`
9. На сервере с шаблоном База данных перед запуском инсталлятора рекомендуется запустить сервис базы данных, если ранее он был остановлен:
   `service postgresql start`
10. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor:
    `cd /root`
11. В инсталляторе реализован механизм автоматического объединения конфигурационных файлов Traffic Monitor старой и новой версии.

Важно!

Автоматическое объединение затрагивает только конфигурационные файлы Traffic Monitor с расширением **.conf**, расположенные в директории `/opt/iw/tm5/etc`.
Перед объединением в директории `/opt/iw/tm5/etc_conf_backup_<дата_время>` будут созданы резервные копии исходных конфигурационных файлов. Пример названия директории: `/opt/iw/tm5/etc_conf_backup_05.06.2022_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-7.5.0.125-2022-09-10_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:

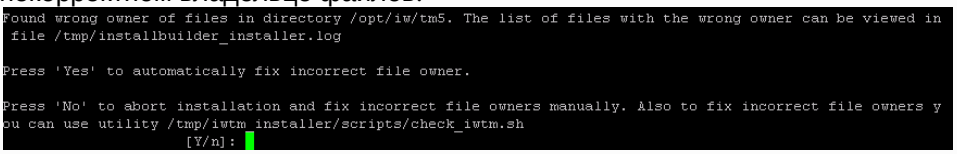
- **обновление в текстовом режиме в консоли сервера**

  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-smolensk-1.7`
  В нашем примере команда будет следующей:
  `sudo ./iwtm-installer-7.5.0.125-astra-smolensk-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:

```
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-Smolensk и Astra-Linux-Smolensk-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:

```
--------------------------------------------------------------------------------
Welcome to the Traffic Monitor Setup Wizard.

--------------------------------------------------------------------------------
Confirm Infowatch Traffic Monitor Update


InfoWatch Traffic Monitor upgrade from 7.4.2.194 to 7.5.0.125 is available

Would you like to continue?



 [Y/n]:
```

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

b. Для продолжения введите **Y** и нажмите **Enter**. Для выхода из инсталлятора введите **N** и нажмите **Enter**.

> **Примечание:**
>
> При обновлении в консоли сервера перед полем ввода в квадратных скобках цифрой или заглавной буквой указано значение по умолчанию. Оно будет использовано, если оставить поле ввода пустым и нажать **Enter**.

c. 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

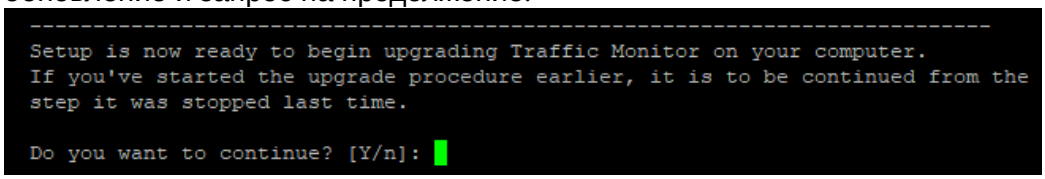
d. Выберите режим остановки Traffic Monitor:
   - `Quick stop` - быстрая остановка без обработки событий;
   - `Waiting for stop` - перед остановкой дождаться завершения текущей обработки событий;
   - `Waiting for emptying file queues` - перед остановкой дождаться обработки всех событий и очистки файловых очередей. Режим обработки всех событий и очистки файловых очередей доступен только на серверах с шаблоном 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.

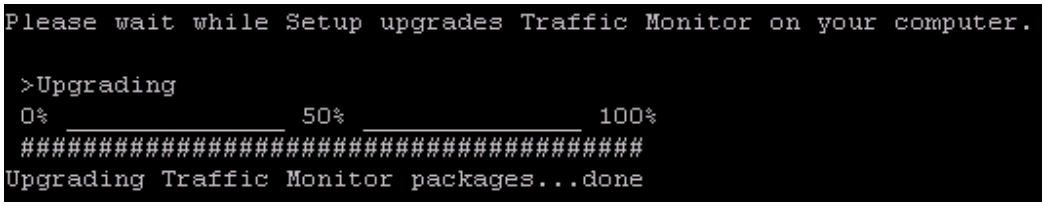
   Для выбора введите цифру, указанную напротив выбранного варианта, и нажмите **Enter**.

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

e. 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.
f. 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.

g. Перед завершением работы инсталлятор предложит удалить пакеты, созданные для обновления.
Если обновление прошло успешно, данные рекомендуется удалить.
h. 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 шаблоном База данных.
>
> После обновления настройки системы мониторинга Nagios были 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.

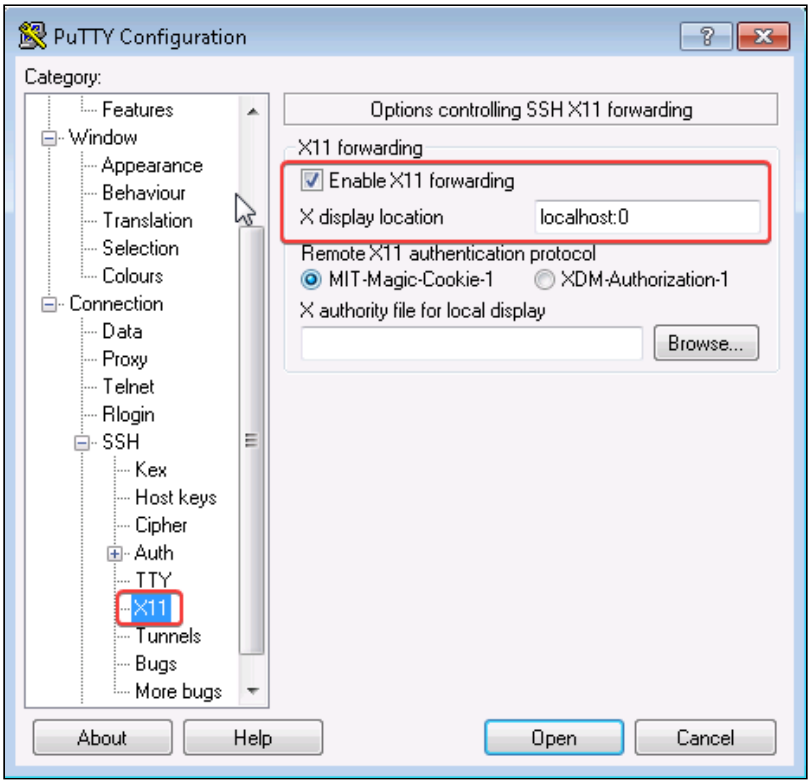
После обновления для управления системой мониторинга используйте службу iwtm-nagios.
Например, для просмотра статуса Nagios используйте команду:
`systemctl status iwtm-nagios`

- **обновление с использованием графического режима инсталлятора**

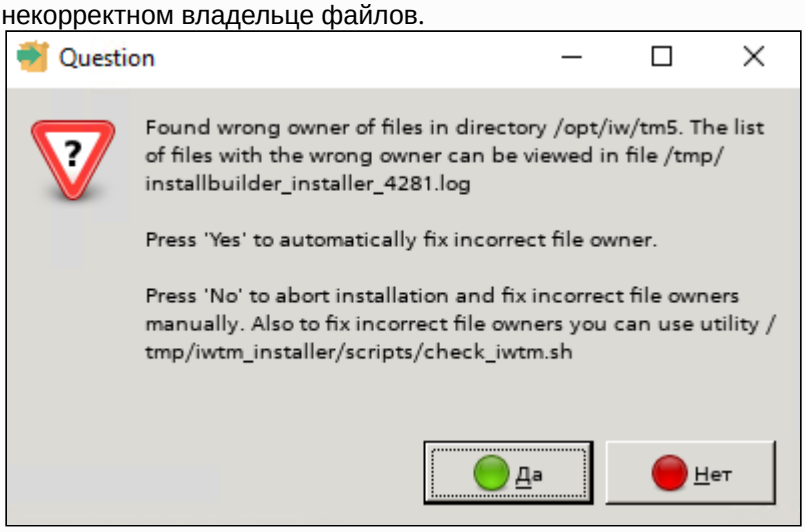
  В ОС оконная система X Window System использует клиент-серверную модель. Для запуска инсталлятора в графическом режиме используется перенаправление графического вывода удаленной подсистемы (**X11 Forwarding**). Это позволит работать напрямую с графическими приложениями среды Linux на компьютере, с которого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



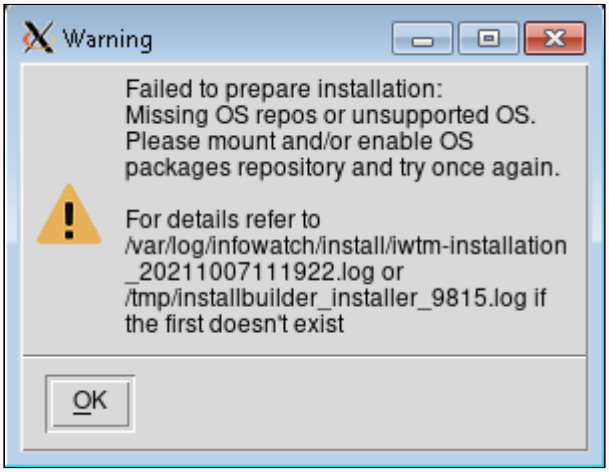
e. Для обновления Traffic Monitor запустите инсталлятор, выполнив следующую команду:
`sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
В нашем примере команда будет следующей:
`sudo ./iwtm-installer-7.5.0.125-astra-smolensk-1.7`
Начнется подготовка к запуску инсталлятора. На данном этапе не производится 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!

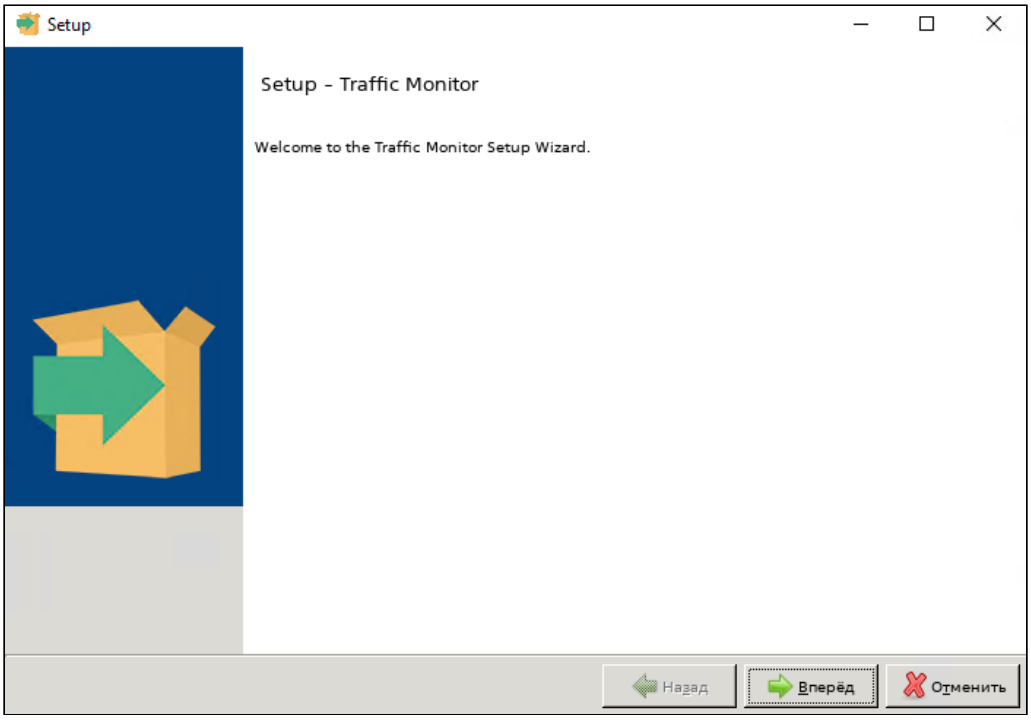
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



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

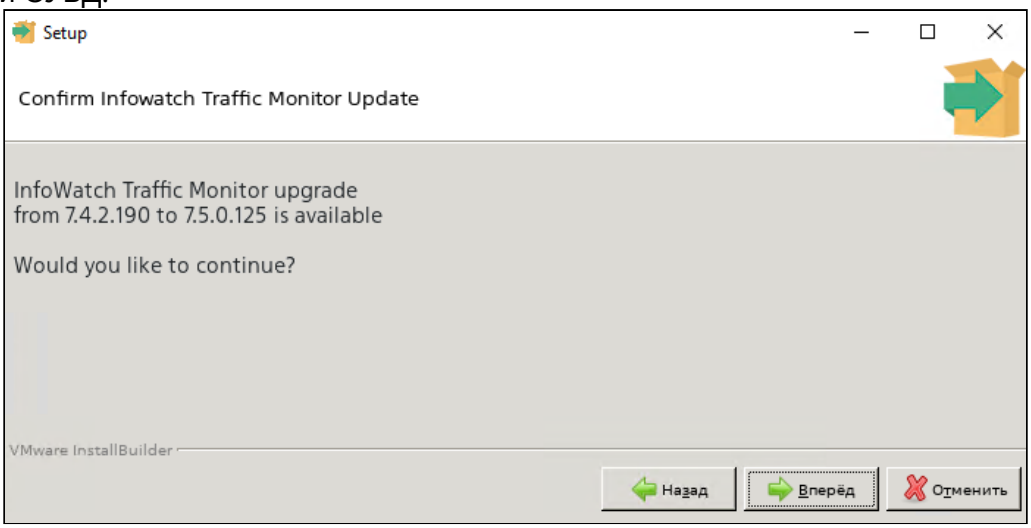
Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

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



Для продолжения нажмите **Вперед**.

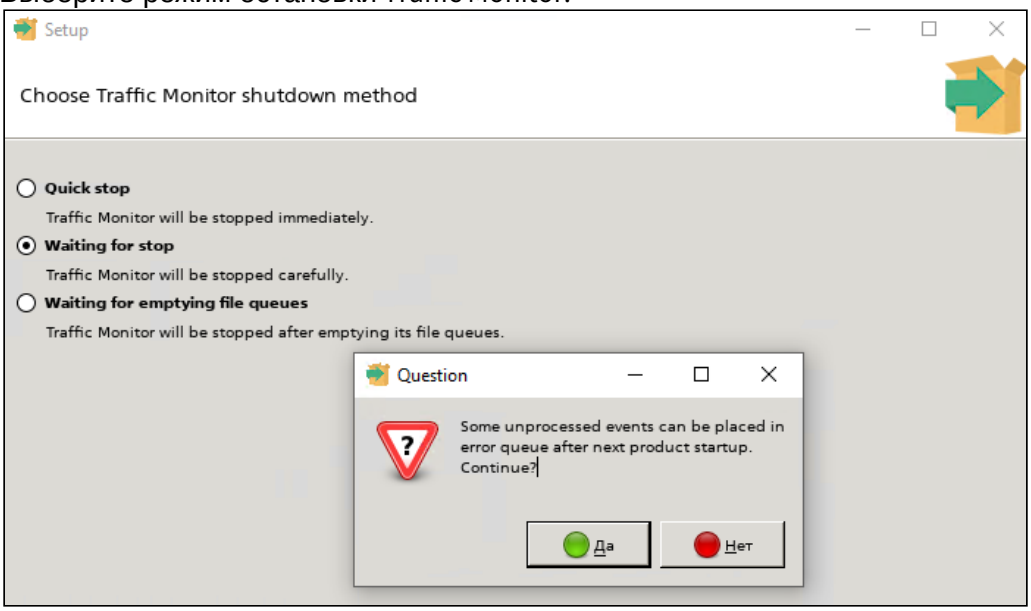
g. Подтвердите остановку сервисов. Шаги подтверждения и выбора режима остановки будут пропущены, если сервисы были остановлены вручную до

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

h. 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 с шаблоном Перехватчики.

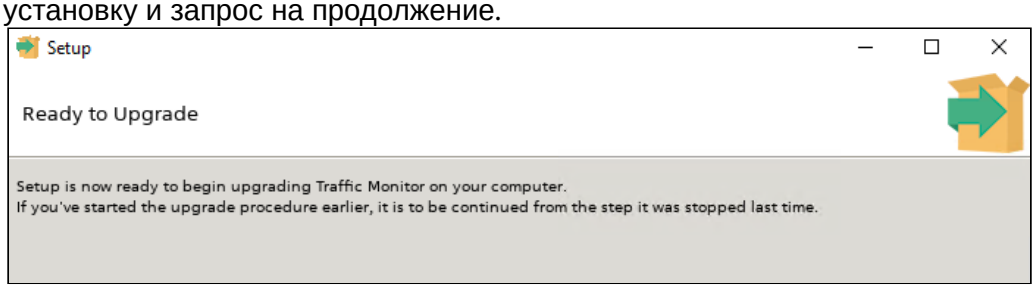
> **Важно!**
>
> Если компоненты перехвата и компоненты анализа (`iw_cas` , `iw_pas`) используются на разных серверах, остановка перехватчиков с очисткой файловых очередей может зависнуть. Рекомендуется использовать другие режимы или остановить компоненты вручную.

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

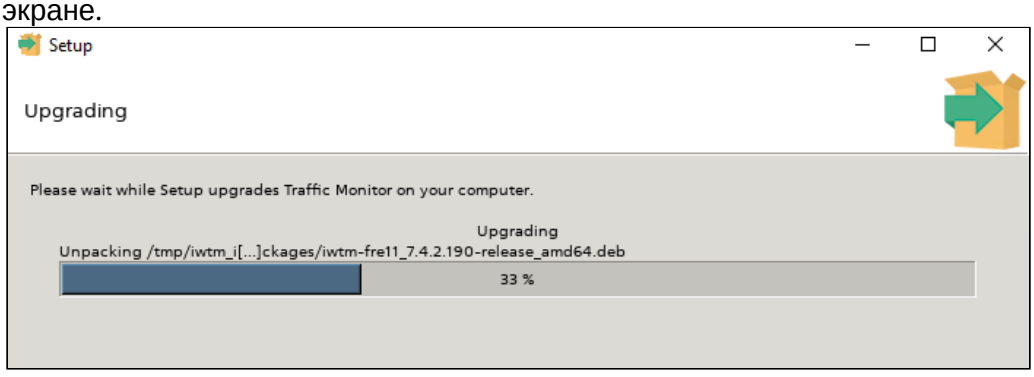
> **Примечание:**
>
> Если выбран `Quick stop` , остановленные сервисы до запуска будут иметь статус `failed (failed)` .

i. 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.

j. 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.

k. После завершения обновления вы можете:

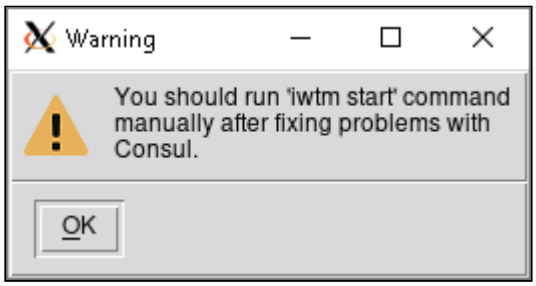


- `Remove exctracted installer data` - удалить пакеты, созданные инсталлятором для установки. Если установка прошла успешно, данные рекомендуется удалить;
- `Start Infowatch Traffic Monitor services` - запустить остановленные сервисы.

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 шаблоном База данных.

После обновления настройки системы мониторинга Nagios были 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`

l. 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-7.5.0.125-astra-smolensk-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-7.5.0.125-astra-smolensk-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-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 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 с шаблоном 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

12. Введите команду для поиска и вывода на экран консоли списка файлов с расширением **`.dpkg-dist`**.
`sudo find / -name "*dpkg-dist*" -print`
Если такие файлы найдены, их необходимо корректно объединить с конфигурационными файлами (см. статью "Объединение конфигурационных файлов").
13. На серверах с шаблоном 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`.

14. 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 с шаблонов 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 с шаблоном 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:

```
[
    {
        "CheckID": "service:iw-bookworm8a27e90e-d7fe-4175-a915-1d83aece7f6e",
        "CreateIndex": 81927,
        "Definition": {},
        "ModifyIndex": 81927,
        "Name": "Service 'iw-bookworm' check",
        "Node": "tm-VMware-420c0d195.local",
        "Notes": "",
        "Output": "TCP connect localhost:8091: Success",
        "ServiceID": "iw-bookworm8a27e90e-d7fe-4175-a915-1d83aece7f6e",
        "ServiceName": "iw-bookworm",
        "ServiceTags": [],
        "Status": "passing"
    }
]
```


3. Проверьте значения блоков "Node" и "Status":
    a. В блоке "Node" должно быть указано имя ноды в кластере Consul, на которой установлена проверяемая служба;
    b. В блоке "Status" должно быть указано "passing".
4. Служба **`iw_licensed`** должна быть запущена в единственном экземпляре на кластер. Выполните команду для запуска службы `iw_licensed`:
   `iwtm start licensed`
5. Службе может потребоваться время на включение. Для проверки состояния службы `iw_licensed` введите команду:
   `curl -s http://localhost:8500/v1/health/checks/iw-licensed | python -mjson.tool`
   Выполните действие 3 текущего шага.
6. Выполните команду для запуска службы `iw_updater`:
   `iwtm start updater`
7. Службе может потребоваться время на включение. Для проверки состояния службы `iw_updater` введите команду:
   `curl -s http://localhost:8500/v1/health/checks/iw-updater | python -mjson.tool`
   Выполните действие 3 текущего шага.
8. Для проверки службы `iw_kicker` необходимо запустить службу `iw_blackboard`:
   `iwtm start blackboard`
9. Служба **`iw_kicker`** должна быть запущена в единственном экземпляре на кластер. Выполните команду для запуска службы `iw_kicker`:
   `iwtm start kicker`
10. Службе может потребоваться время на включение. Для проверки состояния службы `iw_kicker` необходимо проверить файл `/opt/iw/tm5/log/web-console-error.log` на наличие ошибок в процессе обновления. Введите команду:
    `grep -r 'error' /opt/iw/tm5/log/web-console-error.log || echo "All good"`
    Убедитесь, что адрес в команде указан верно. В случае отсутствия ошибок будет выведено сообщение `All good`.
11. Выполните команду для остановки служб:
    `iwtm stop`
12. Завершите обновление серверов - описание смотрите ниже.

Важно!

Если служба не запустилась успешно, проверьте соответствующий лог-файл на наличие ошибок в процессе обновления и обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.
Вы также можете посетить раздел технической поддержки на нашем сайте:

www.infowatch.ru/services/support.

Лог-файлы служб для проверки:

- `/opt/iw/tm5/log/bookworm.log` - для службы `iw_bookworm`
- `/opt/iw/tm5/log/updater.log` - для службы `iw_updater`
- `/opt/iw/tm5/log/licserv.log` - для службы `iw_licensed`
- `/opt/iw/tm5/log/web-console-error.log` - для службы `iw_kicker`

Лог-файлы служб рекомендуется проверить и в случае успешного запуска служб, чтобы исключить возникновение ошибок.
Рекомендованный уровень логирования для проверки - не ниже INFO. Лог-файл может отсутствовать, если не было записей об ошибках.

ШАГ 4. ЗАВЕРШЕНИЕ ОБНОВЛЕНИЯ СЕРВЕРОВ

Чтобы завершить обновление серверов, на каждом из них выполните следующие действия:

1. Если ранее работа инсталлятора не была завершена, выберите запуск сервисов и завершите обновление.
   Если ранее инсталлятор завершил работу без запуска сервисов, запустите их вручную или перезагрузите сервер для запуска всех остановленных сервисов.
   Команда для перезагрузки сервера:
   `reboot`

Важно!

Компоненты Traffic Monitor должны быть запущены в следующей последовательности:

a. База данных
b. Веб-консоль
c. Индексер
d. Перехватчики

Важно!

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

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

Запись об ошибке вида

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

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

Запись об ошибке вида

```
1 2019-10-03 17:39:13.348146 (14262:0x00007fe83892ba80) [WARNING] :
<Root> Prometheus server is off, therefore the statistics is
unavailable. That's what you wanted, isn't it?
2 2019-10-03 17:39:14.364655 (14262:0x00007fe83892ba80) [ERROR  ] :
<Root> Error when loading config of tech: Cannot open xml file with
 cas configuration: etc/config/cas/cas_config.xml
3 2019-10-03 17:39:14.364856 (14262:0x00007fe83892ba80) [ERROR  ] :
<Root> failed to initialize thrift server
Diagnostic information.
/sandbox/src/cas3/handler.cpp(682): Throw in function
 cas::Handler::LoadedConfigData
cas::Handler::GetLoadedConfigData(const prop::Property&, const Ptr&)
Dynamic exception type:
boost::exception_detail::clone_impl<tech::ExceptionTechLoadConfig>
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. Если у вас установлена система Prometheus и если сервер с шаблоном База данных не был перезагружен, для запуска службы выполните на нем команду:
   `systemctl start iwtm-postgres_exporter`
3. На сервере с шаблоном Веб-консоль введите команду для очистки кеша:
   `redis-cli flushall`
4. 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. 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:

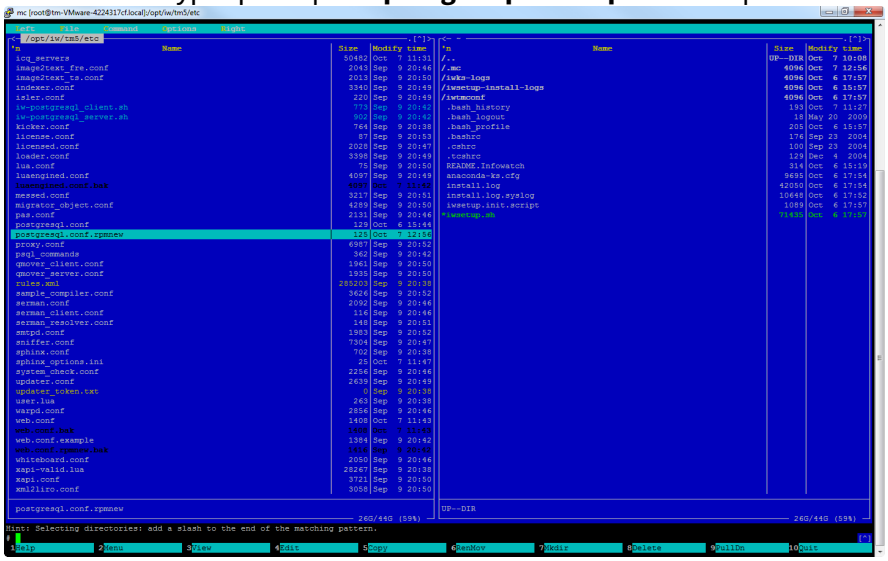
```
{
    "DB": "postgres",
    "Host": "localhost",
    "Password": "xxXX1234",
    "Port": 5433,
    "Username": "iwtm_linux"
}
```

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-9.6.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 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 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 с шаблоном установки 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. Остановить 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`

5.2 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