

INFOWATCH

InfoWatch Traffic Monitor 7.4

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 19

2.4 Настройка удаленной базы данных 20

3 Установка Системы 25

3.1 Установка InfoWatch Traffic Monitor 26

3.1.1 Установка TM в режиме "Все-в-одном" 27

3.1.2 Распределенная установка TM 45

3.1.3 Установка в тихом режиме с файлом параметров 81

Файл параметров (option file) 83

Тихий режим установки 83

Полный состав файла параметров 84

3.2 Установка InfoWatch Device Monitor 98

3.2.1 Схема развертывания InfoWatch Device Monitor 98

3.2.2 Установка серверной части InfoWatch Device Monitor 102

Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server 102

Рекомендации по развертыванию базы данных под управлением СУБД Oracle 103

Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL 104

Рекомендации по установке Сервера InfoWatch Device Monitor 105

Порядок установки серверной части InfoWatch Device Monitor 106

3.2.3 Установка Агента InfoWatch Device Monitor 116

Локальная установка Агента 118

Установка Агента с помощью средств распространения программного обеспечения 121

3.3 Предустановленные серверные параметры 125

4 Обновление Системы 127

4.1 Обновление TM Все-в-одном (All-in-one) 130
4.1.1 Файл параметров (option file) 146
4.1.2 Тихий режим обновления 147
4.1.3 Полный состав файла параметров 148
4.2 Обновление TM при распределенной установке 152
4.2.1 Файл параметров (option file) 169
4.2.2 Тихий режим обновления 170
4.2.3 Полный состав файла параметров 171
4.3 Обновление InfoWatch Device Monitor 179
4.3.1 Обновление серверной части InfoWatch Device Monitor 180
4.3.2 Обновление Агента InfoWatch Device Monitor 182
4.4 Объединение конфигурационных файлов 183
4.4.1 Объединение конфигурационных файлов в Midnight Commander 183
4.4.2 Объединение конфигурационных файлов с помощью vimdiff 185
5 Удаление Системы 187
5.1 Удаление схемы базы данных 187
5.2 Удаление InfoWatch Device Monitor 188
5.2.1 Удаление Агента, установленного с помощью средств распространения программного обеспечения 190
5.3 Удаление Traffic Monitor 191
6 Приложение А. Рекомендации по составлению имен и паролей 193
7 Приложение В. Лицензии на стороннее программное обеспечение 194

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:

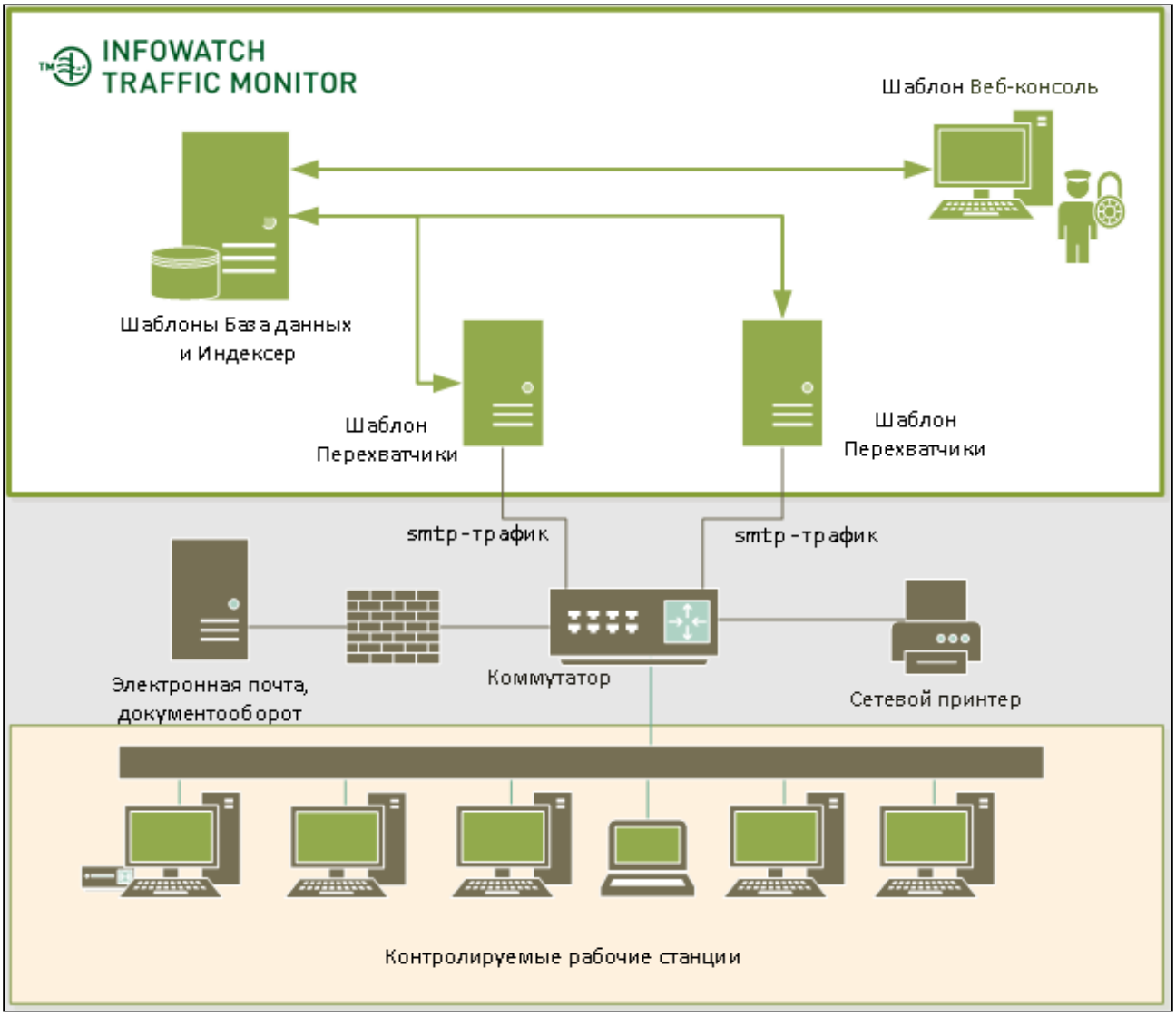
- *Все-в-одном* – все компоненты Системы (с СУБД PostgreSQL) устанавливаются на один сервер с возможностью подключения к удаленной базе данных. Такая установка используется, если с учетом предполагаемой нагрузки на сервере будет обеспечен ресурс как для СУБД, так и для сервисов Traffic Monitor. Является 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.

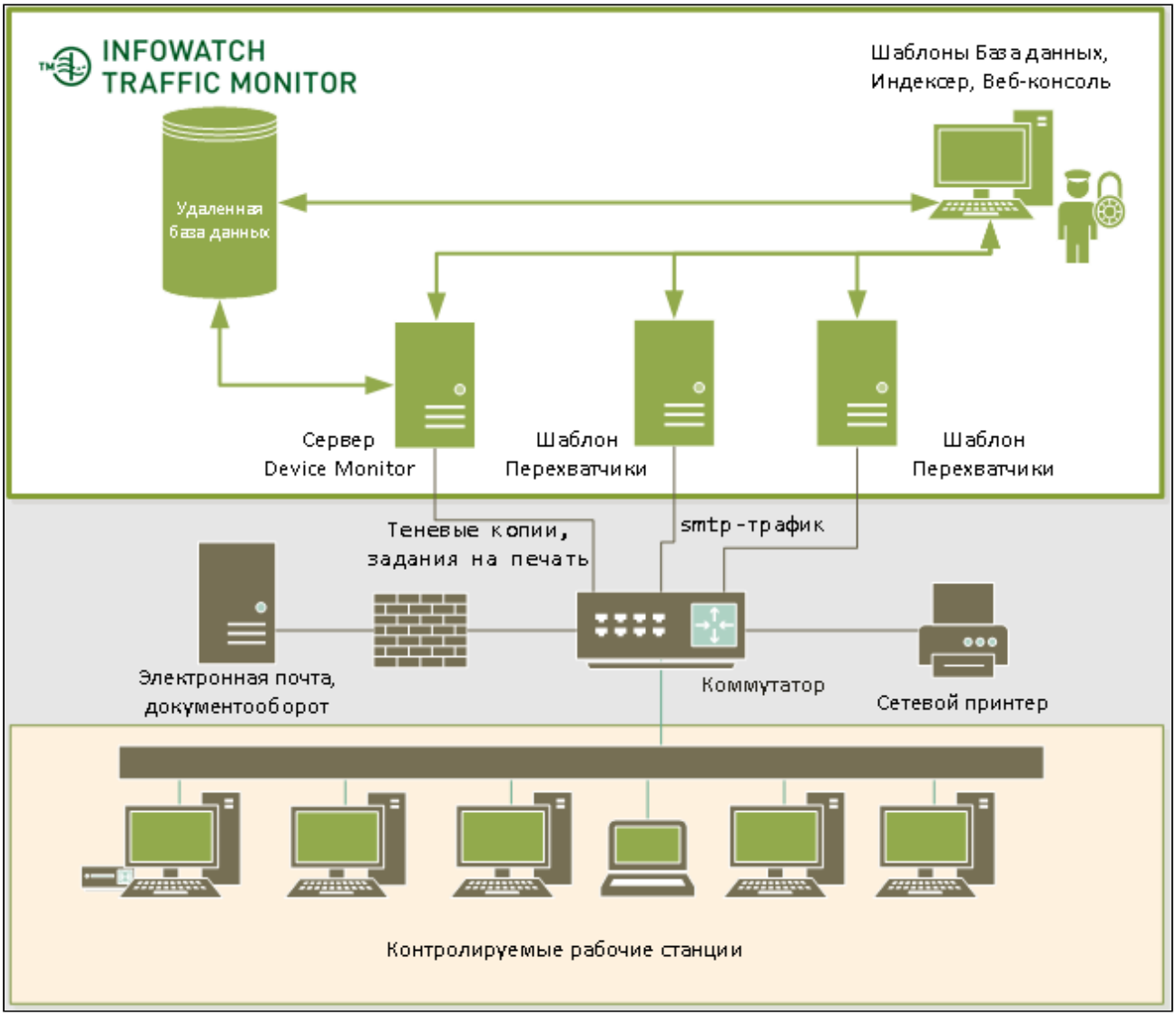


В данном примере для распределения нагрузки Перехватчики установлены на двух серверах. В зависимости от целей перехвата, на каждом из этих серверов могут быть дополнительно отключены неиспользуемые модули перехвата.

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, работающий на Windows-системах. *Требования см. ниже*.
- **Консоль управления** – автоматически устанавливается вместе с сервером Traffic Monitor и не предъявляет дополнительных программно-аппаратных требований к серверу. Для доступа к Консоли следует использовать браузер Google Chrome или Mozilla Firefox актуальной версии.

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

Также на количество и назначение серверов Traffic Monitor может влиять существенная разница в нагрузке на те или иные каналы перехвата: например, для эффективной обработки трафика с Device Monitor 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 • 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.

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Сервер TM Enterprise, от 10 до 50 GB трафика в день				
RAID-массив с fault tolerance	2SRVx2CPU 10xC	32-48 GB на каждый из серверов	ОС Astra Linux Special Edition "Смоленск" 1.7.0 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 TM Enterprise, более 50 GB трафика в день				
RAID-массив с fault tolerance	Рассчитывается по запросу	От 32GB на каждый из серверов	ОС Astra Linux Special Edition "Смоленск" 1.7.0 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 БД PostgreSQL (Обеспечивает хранение трафика для 1-2 тыс. пользователей, сроком до 3 месяцев; в случае использования OCR и Device Monitor требования рассчитываются по запросу)				
RAID-массив с fault tolerance: 500 GB	2CPU от 6xC, 2,6 GHz	От 16GB и более в зависимости от объема	ОС Astra Linux Special Edition "Смоленск" 1.7.0	

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
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.		данных, интенсивности вставки и обработки	Требуется 2 диска: • Astra-Linux-Smolensk • Astra-Linux-Smolensk-Devel	
Сервер Device Monitor				
Не менее 1 GB свободного пространства для установки	От 2-х ядер	От 2 GB	ОС (поддерживаются платформы x86 и x64): • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019. Платформа: • Microsoft .Net Framework 4.5.1. Клиент СУБД: • Oracle Database 19;	• На сервере ТМ должен быть включен автозапуск процесса **iw_xapi_xapi** • Наличие локального DNS для перевода доменных имен в адреса • Должен поддерживаться протокол TLS 1.2

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			• Microsoft SQL Server 2005, 2008, 2012, 2014, 2016, 2017, 2019 (Standard, Enterprise); • PostgreSQL версии 9.6. Ограничение: Microsoft Windows Server 2019 не поддерживает установку PostgreSQL версии 9.6.	
Агент Device Monitor для рабочих станций				
Не менее 320 GB свободного пространства для временного хранения файлов, предназначенных для передачи на анализ	От 2-х ядер	От 2.5 GB	ОС: • [1]Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 и 8.1; • Microsoft Windows 10; • Microsoft Windows 11; • [1]Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2;	• Наличие локального DNS для перевода доменных имен в адреса • Должен поддерживаться протокол TLS 1.2 Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 5 (версии ядра: 4.15.3-2-hardened, 4.15.3-2-generic) поддерживается только для установки Агента Device Monitor версии 7.1.1.

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			• Microsoft Windows Server 2016; • Microsoft Windows Server 2019. • Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 5 (20200327SE16); • Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 6 (20200722SE16); • Astra Linux Common Edition "Орел" 2.12 (x64); • РЕД ОС 7.3.1.	Astra Linux Special Edition "Смоленск" 1.6 с установленным обновлением безопасности Update 6 поддерживается только для первичной установки Агента Device Monitor. Astra Linux Common Edition "Орел" поддерживается только для установки Агента Device Monitor версий 7.1.1 и выше. **Поддерживаемые версии ядра Astra Linux Common Edition "Орел"** • 4.15.3-1-generic • 4.15.3-1-hardened • 4.15.3-2-generic • 4.15.3-2-hardened • 4.15.3-3-generic • 4.15.3-3-hardened • 4.19.0-1-generic • 4.9.135-1-generic • 5.2.13-050213-generic • 5.4.0-54-generic • 5.4.0-54-hardened

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				Microsoft Windows 11 и РЕД ОС 7.3.1 (версия ядра: 5.15.10-1) поддерживаются только для установки Агента Device Monitor версий 7.5 и выше. Для установки Агента Device Monitor 7.6 и выше поддерживаются следующие версии ядра РЕД ОС 7.3.1: • 5.15.10-1 • 5.15.10-2 • 5.15.10-3 • 5.15.10-4 • 5.15.35-1 • 5.15.35-4 • 5.15.35-5
Консоль управления Device Monitor				
Не менее 35 MB	Как у используемой ОС	Как у используемой ОС	ОС: • Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Microsoft Windows 7	

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			Service Pack 1 • Microsoft Windows 8 и 8.1; • Microsoft Windows 10.	

Примечание:

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

Примечание:

Допустима установка Системы в виртуальную среду: VMware, MS Hyper-V, Citrix 6.0, 7.6, 7.13, 7.14 и 7.15 LTSR или других систем виртуализации.

2.3 Требования к настройкам ОС и сети сервера

Для успешной установки Системы сервер должен отвечать следующим требованиям:

- На сервере должна быть установлена ОС Astra Linux Special Edition "Смоленск" (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
- Установка InfoWatch Device Monitor (опционально)

Примечание:

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

- Создание оберточных функций для чтения файлов, остановки и обрывания сессий, создания табличных пространств и выдача iwtm прав на них;
- Удаление всех представлений (view) и функций из схемы iwtm для создания в новой версии нужных с помощью обновления;

- Выдача пользователю iwtm:
  - Прав на создание объектов в БД;
  - Прав для установки, обновления и удаления схемы БД;
  - Прав для создания, удаления, архивации и восстановления табличных пространств;
  - Прав на функции обнуления статистики сервера postgres, которые используются в скрипте диагностики pgstat;
  - Прав на статистические представления (view) и таблицы, для сбора статистики работы БД;
  - Прав, используемых в коде продукта InfoWatch Traffic Monitor;
  - Прав для просмотра статистики БД;
  - Прав на схему pgagent для создания и управления заданиями (job).

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

После окончания установки серверных компонентов работа в Консоли управления 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 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.

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`**.

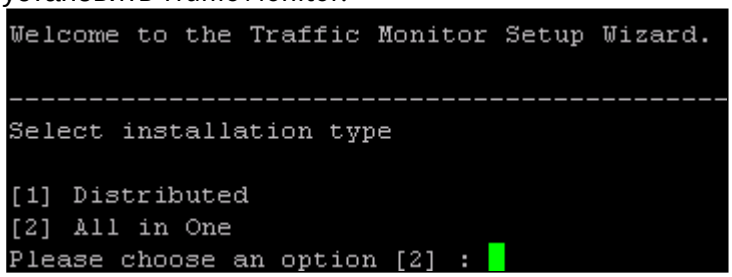
   В нашем примере:
   - **`iwtm-installer-7.4.0.140-astra-smolensk-1.7`**;
   - **`iwtm-postgresql-11.10-7.4.0.140-astra-smolensk-1.7.tar.gz`**.
6. Выполните следующую команду:
```
sudo apt-get update
```
7. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
```
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-7.4.0.140-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-7.4.0.140-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:

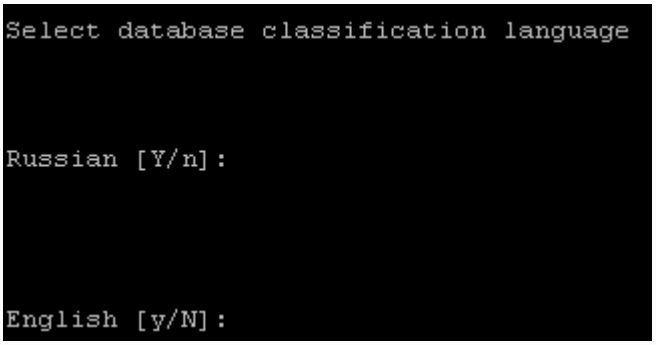


2. На этапе выбора типа установки выберите **`All in one`**.
Для этого введите цифру, указанную напротив выбранного варианта, и нажмите **Enter**.

> **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.

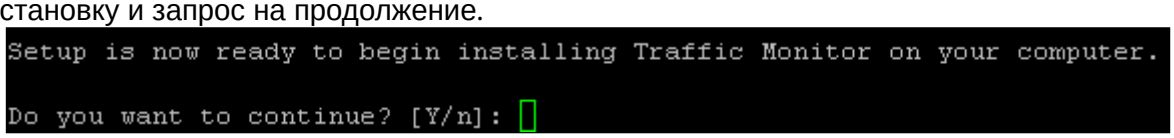
    Для каждого следующего параметра предварительно будет выведен запрос на использование:
    - `Archive non-violation events` - включить автоматическое архивирование событий, которые не являются нарушениям. В случае включения укажите число дней до архивирования, значение по умолчанию - 45.
    - `Archive 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.

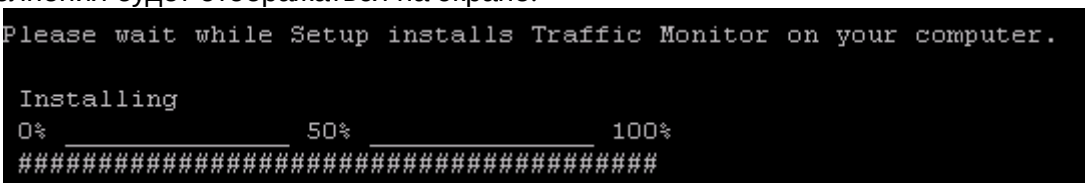
15. При необходимости вы можете изменить стандартные параметры работы службы Sphinx.
    В этом случае будет предложено задать список языков с поддержкой морфологии. По этим языкам будет проводиться индексация.
    Вы можете указать несколько языков, используя пробел в качестве разделителя.

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

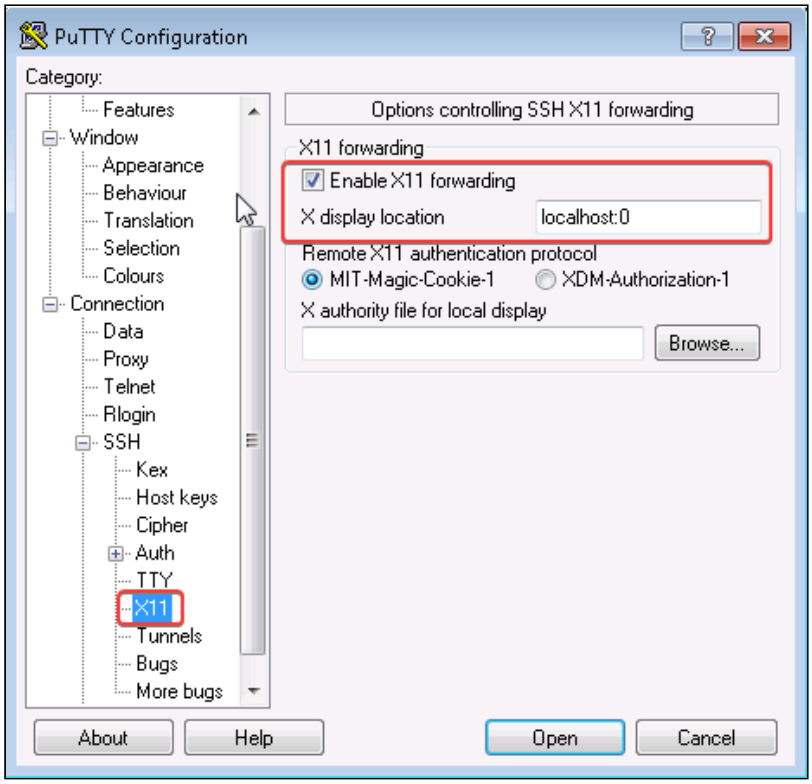
Установка с использованием графического режима инсталлятора

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

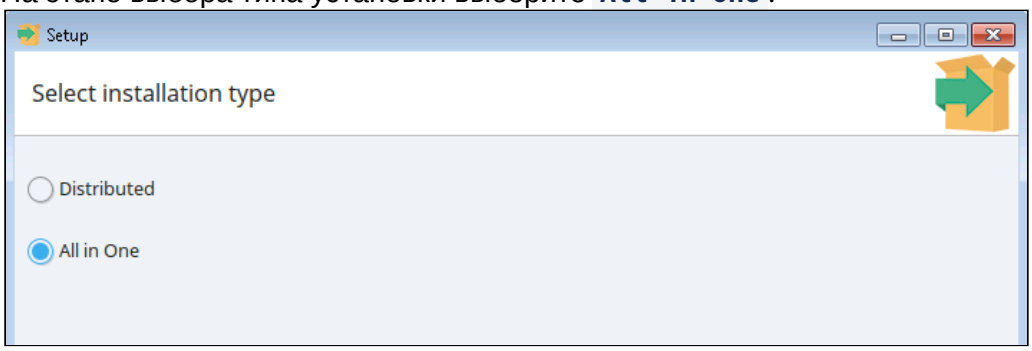


5. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
   `sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
   В нашем примере команда будет следующей:
   `sudo ./iwtm-installer-7.4.0.140-astra-smolensk-1.7`
   Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов. По завершении откроется окно с приглашением установить Traffic Monitor:



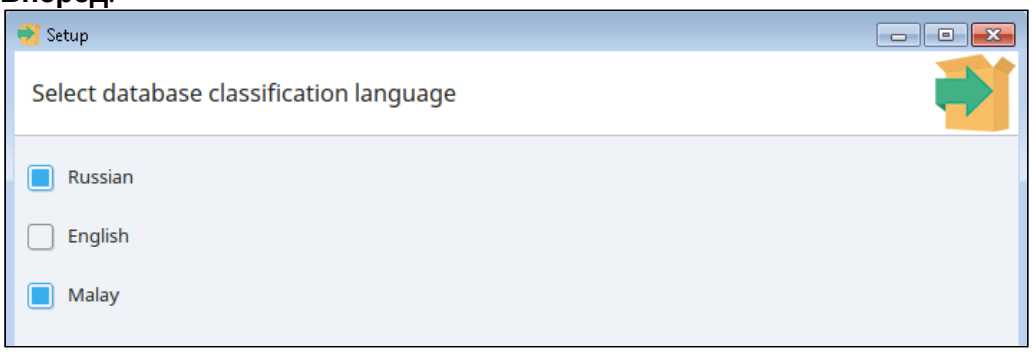
Для перехода к следующему параметру используется кнопка **Вперед**, для возврата к предыдущему - **Назад**. Для выхода из инсталлятора - кнопка **Отменить**.

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.

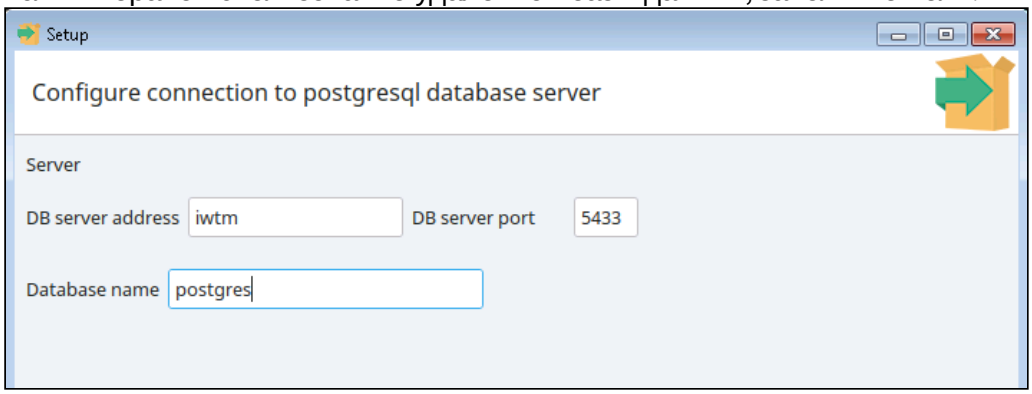
9. Выберите расположение базы данных:



   - `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.

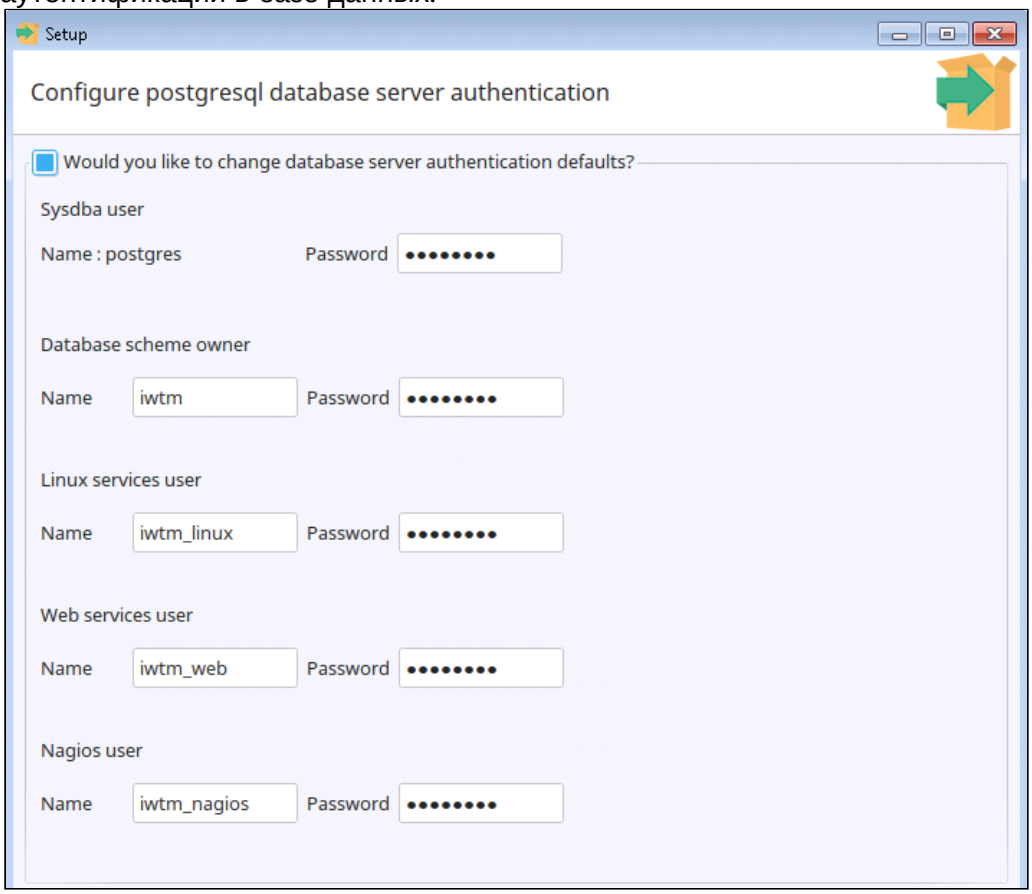
10. Если выбрано использование удаленной базы данных, заполните поля:



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.

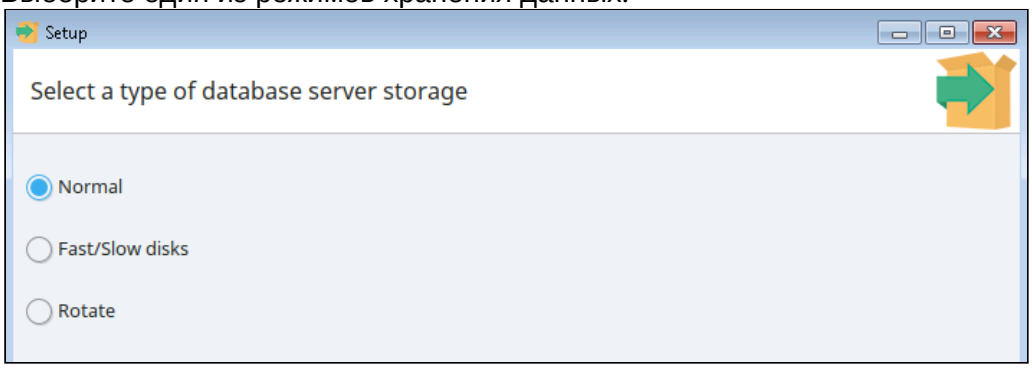


Чтобы отредактировать значения, установите флажок напротив поля с вопросом. Это сделает доступными для редактирования следующие разделы:

- **`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.

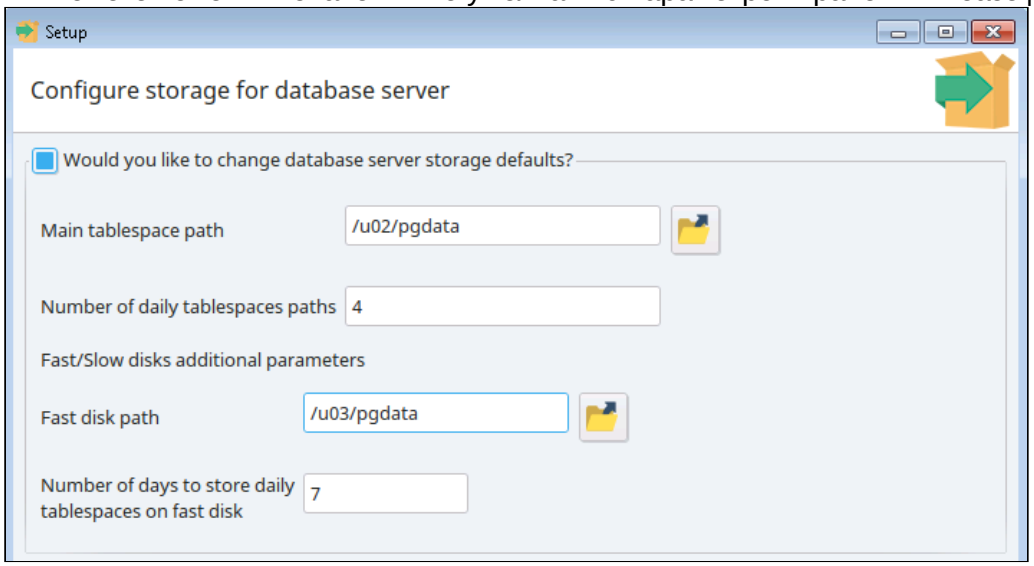
12. Выберите один из режимов хранения данных:



- **`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.

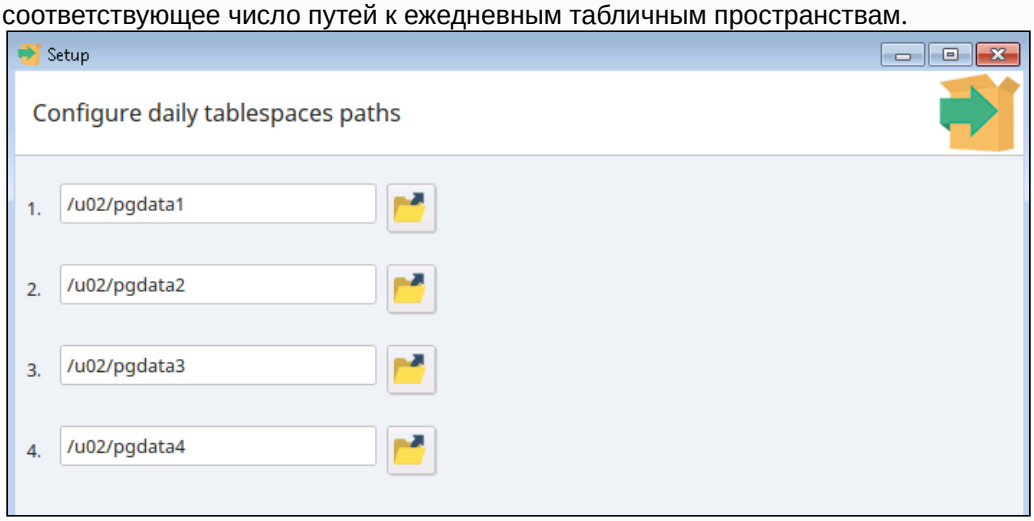
13. Вы можете изменить значения по умолчанию параметров хранения в базе данных.



- **`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;

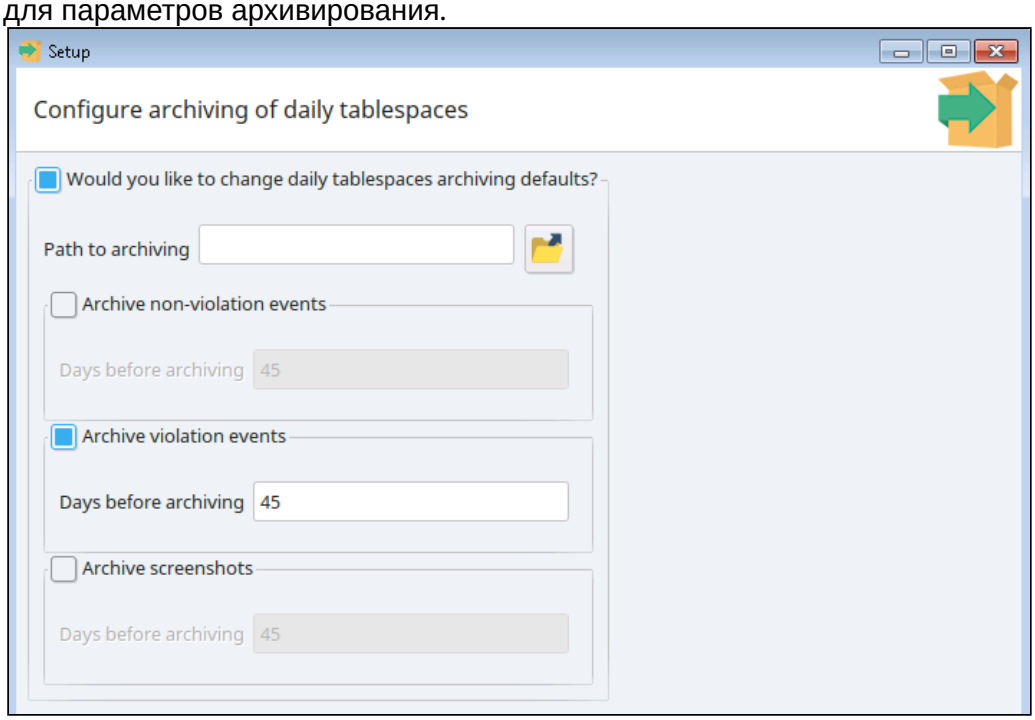
> **Примечание:**

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.



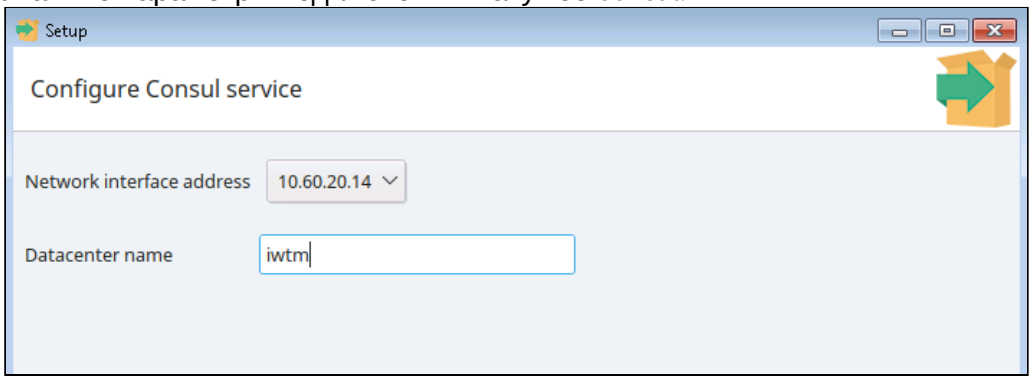
- **`Path to archiving`** - путь к директории хранения файлов архивированных табличных пространств.

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.

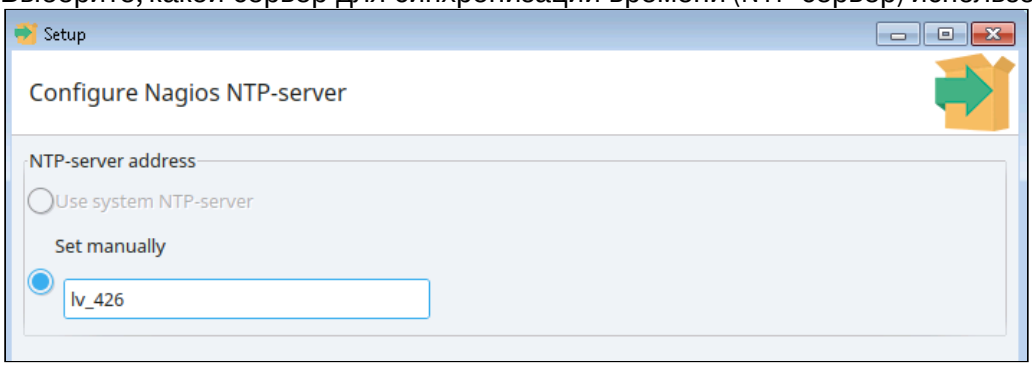
15. Аналогично предыдущему пункту вы можете настроить параметры удаления ежедневных табличных пространств. В случае включения для всех параметров значение по умолчанию - 90.
16. Укажите параметры подключения к службе Consul:



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

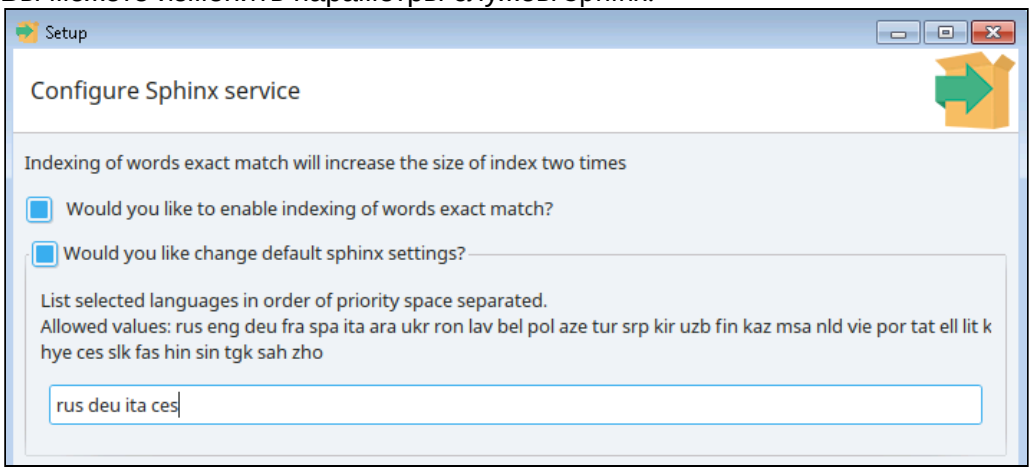
    Для выбора из списка параметров нажмите на кнопку  и в раскрывшемся списке выберите требуемое значение.

    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:



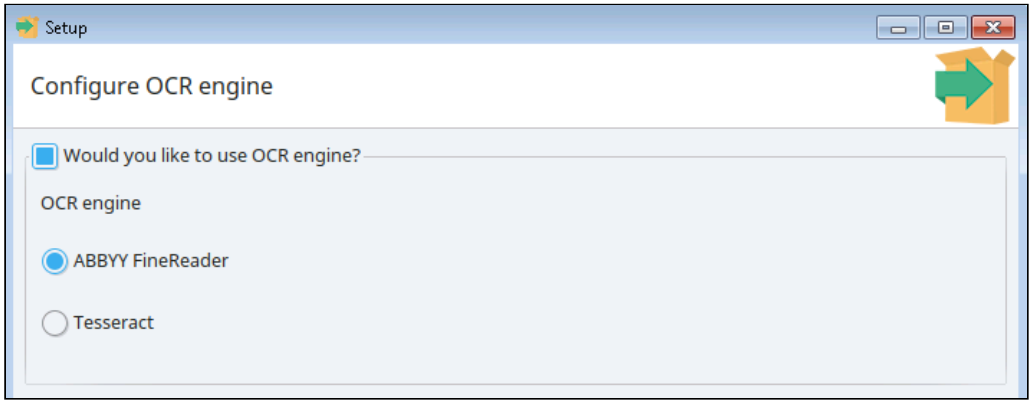
- `Enable indexing of words exact match` - включить индексацию на точное совпадение слов;

> **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.

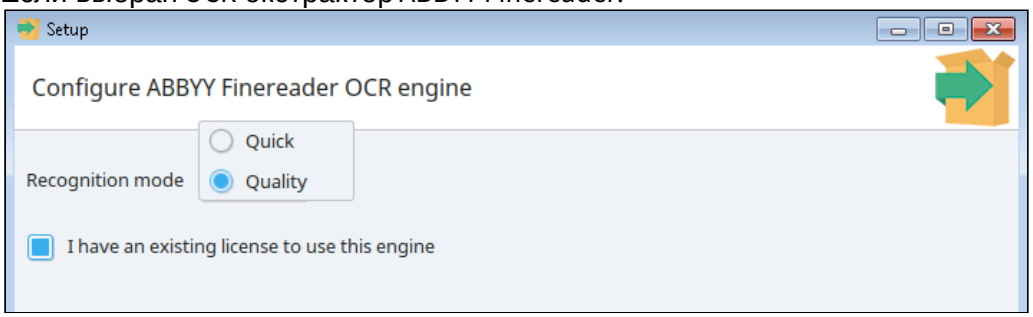
> **Примечание:**
>
> Приоритет языков соответствует последовательности их выбора. Английский язык будет добавлен по умолчанию, имеет самый высокий приоритет.

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:

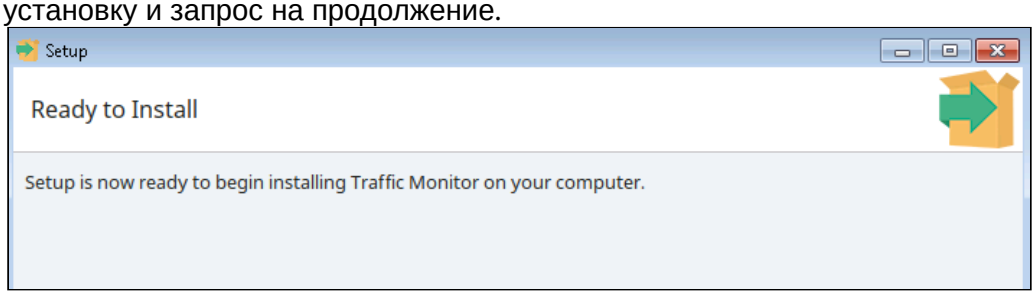


a. Выберите один из режимов распознавания (`Recognition mode`):
   - `Quick` – быстрый режим;
   - `Quality` – тщательный режим, обеспечивающий более высокое качество распознавания.

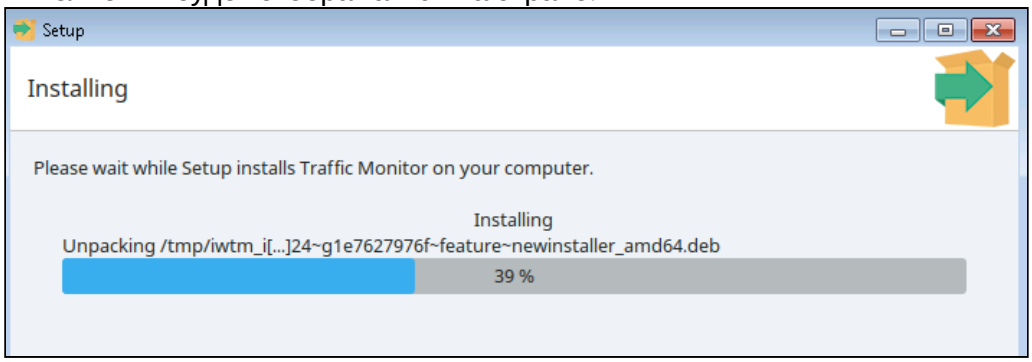
b. Подтвердите наличие у вас активной лицензии на использование ABBYY Finereader.

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.



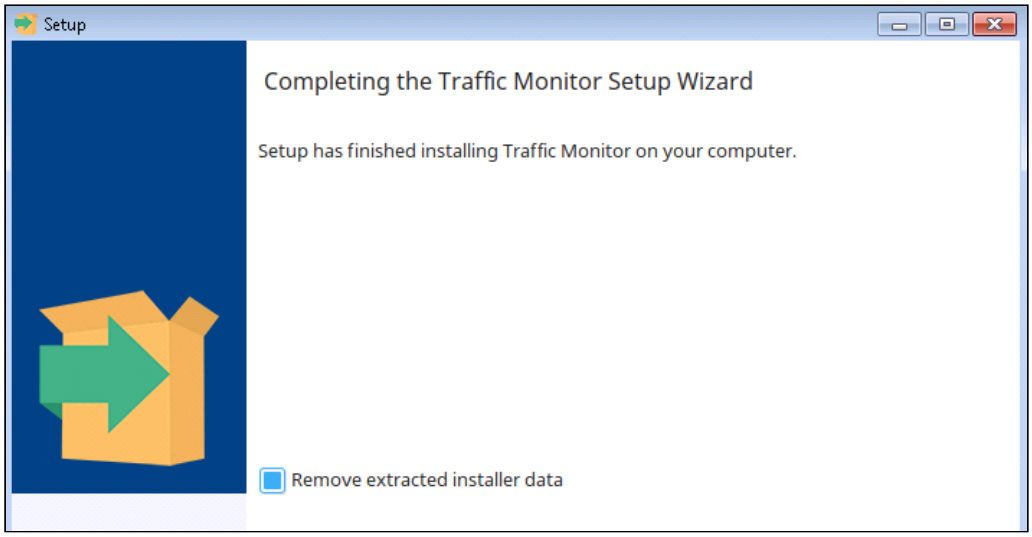
Для начала установки нажмите кнопку **Вперед**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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.

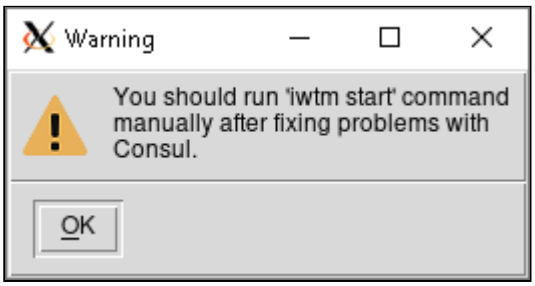
22. После завершения установки вы можете удалить пакеты, созданные инсталлятором для установки.



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 в ОС они были включены до установки, 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 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.

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`**.

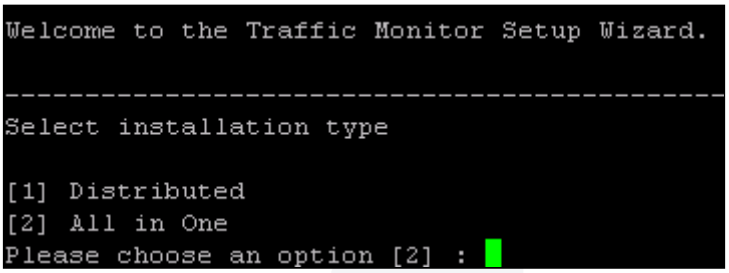
   В нашем примере:
   - **`iwtm-installer-7.4.0.140-astra-smolensk-1.7`**;
   - **`iwtm-postgresql-11.10-7.4.0.140-astra-smolensk-1.7.tar.gz`**.
6. Выполните следующую команду:
   `sudo apt-get update`
7. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
   `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-7.4.0.140-astra-smolensk-1.7`

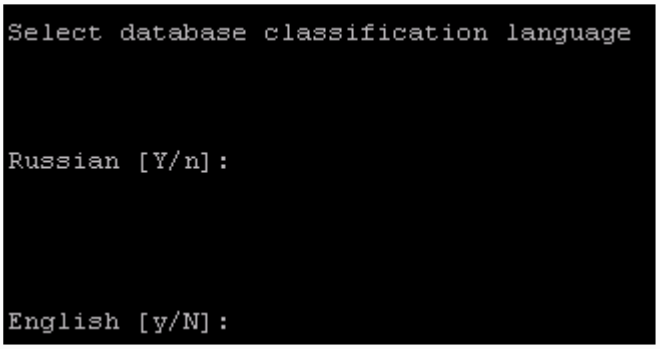
Установка в текстовом режиме в консоли сервера

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-7.4.0.140-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.

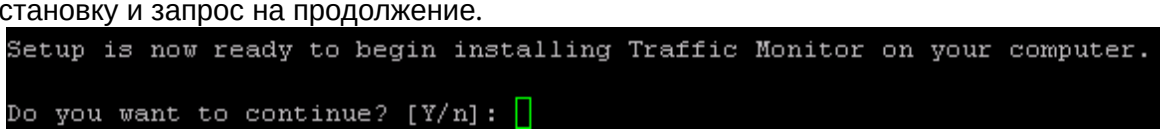
   Для каждого следующего параметра предварительно будет выведен запрос на использование:
   - **`Archive non-violation events`** - включить автоматическое архивирование событий, которые не являются нарушениям. В случае включения укажите число дней до архивирования, значение по умолчанию - 45.
   - **`Archive 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.

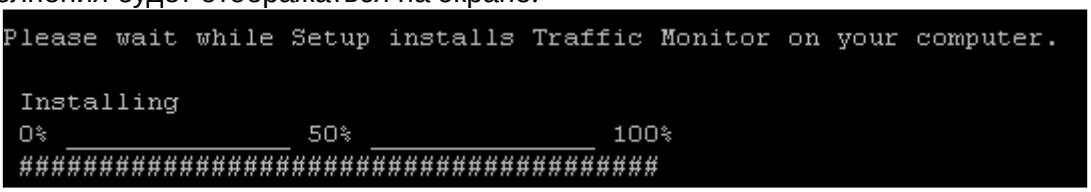
    c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
    d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
    e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через 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.

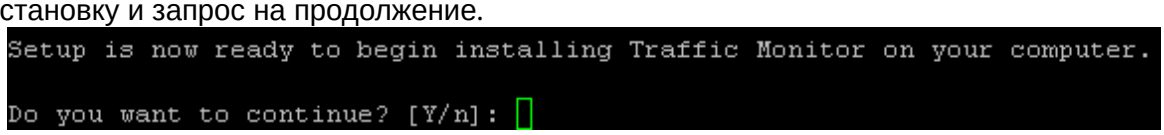
4. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:
   - **`Use system NTP-server`** - использовать системный NTP-сервер;
   - **`Set manually`** - указать NTP-сервер вручную. При выборе данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.
5. Далее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

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

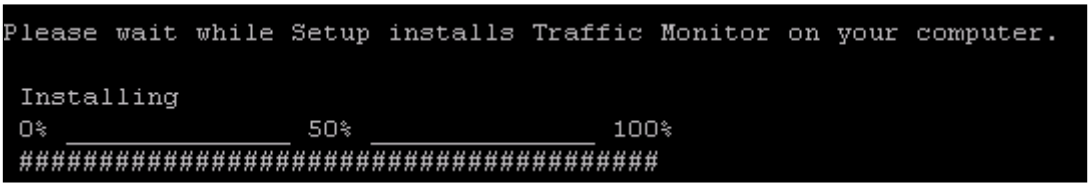
6. При необходимости вы можете изменить стандартные параметры работы службы Sphinx.
   В этом случае будет предложено задать список языков с поддержкой морфологии. По этим языкам будет проводиться индексация.
   Вы можете указать несколько языков, используя пробел в качестве разделителя.

> **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.



   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.

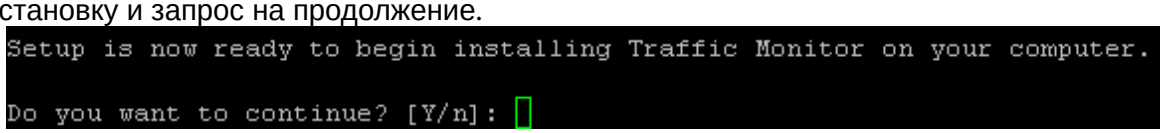
4. Выберите, какой сервер для синхронизации времени (NTP-сервер) использовать:
   - **`Use system NTP-server`** - использовать системный NTP-сервер;
   - **`Set manually`** - указать NTP-сервер вручную. При выборе данного варианта будет необходимо ввести IP-адрес или имя доступного NTP-сервера.
5. Укажите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

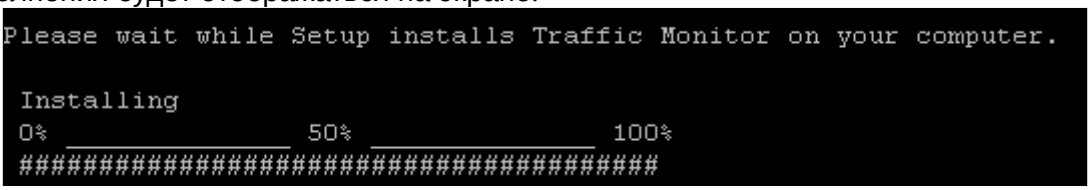
6. Вы можете включить использование технологии OCR.

> **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):

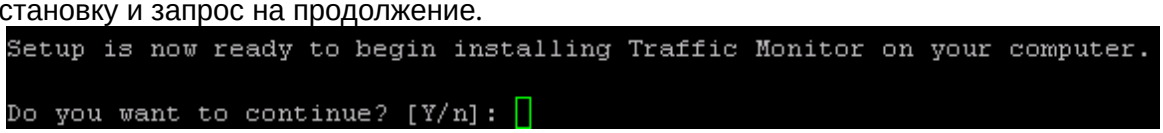
1. Последовательно укажите параметры подключения к базе данных:
   a. IP-адрес или доменное имя сервера с базой данных.
   b. Порт подключения.
   c. Имя используемой базы данных.
2. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.
   В случае утвердительного 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.

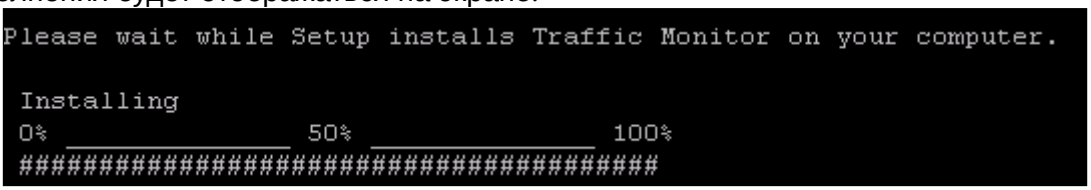
   c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
   d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
   e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. 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 в ОС они были включены до установки, не выключайте их, и наоборот.
>
> В противном случае корректная работа Системы не гарантируется.

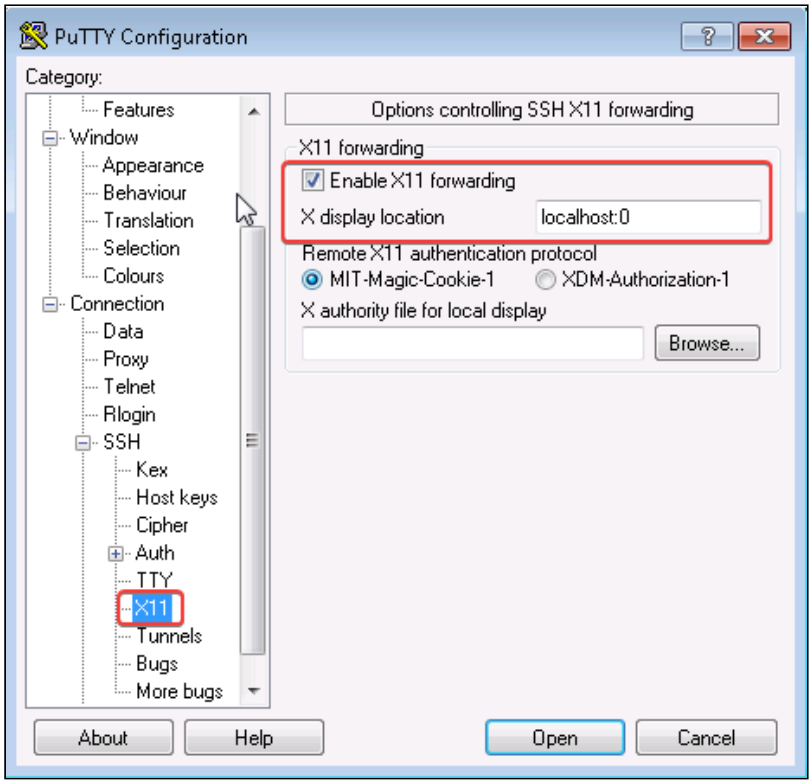
Установка с использованием графического режима инсталлятора

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

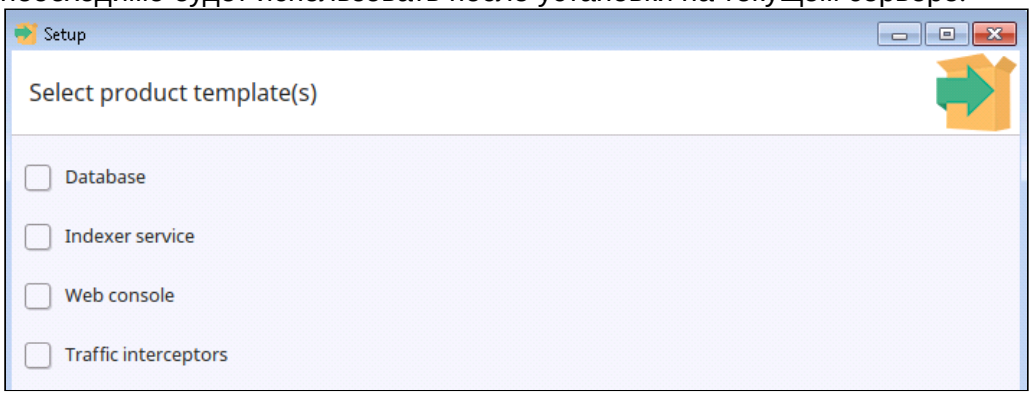


5. Для установки Traffic Monitor запустите инсталлятор, выполнив следующую команду:
   `sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
   В нашем примере команда будет следующей:
   `sudo ./iwtm-installer-7.4.0.140-astra-smolensk-1.7`
   Начнется подготовка к запуску инсталлятора. На данном этапе 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**.

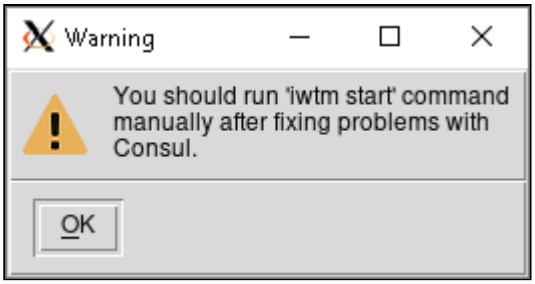
6. На этапе выбора типа установки выберите `Distributed`.
   Для выбора установите флажок напротив соответствующего значения и нажмите кнопку **Вперед**.
7. Далее с помощью выбора шаблонов вы можете указать, какие наборы компонентов необходимо будет использовать после установки на текущем сервере.



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).

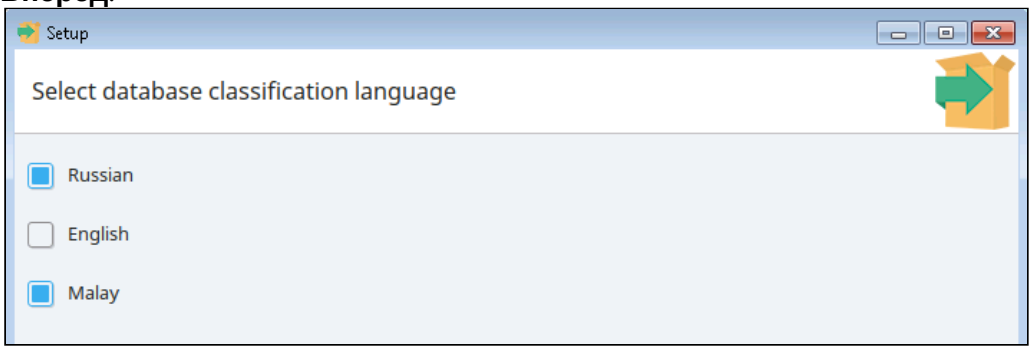
При данной ошибке инсталлятор не запустит сервисы Traffic Monitor при завершении работы, их нужно будет запустить вручную.

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

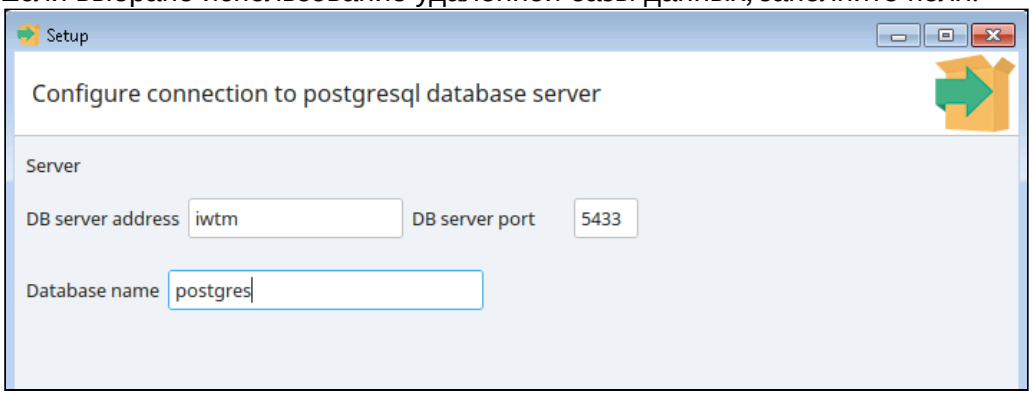
Если нет необходимости устанавливать базу классификации, не выбирайте ни один из языков.

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.

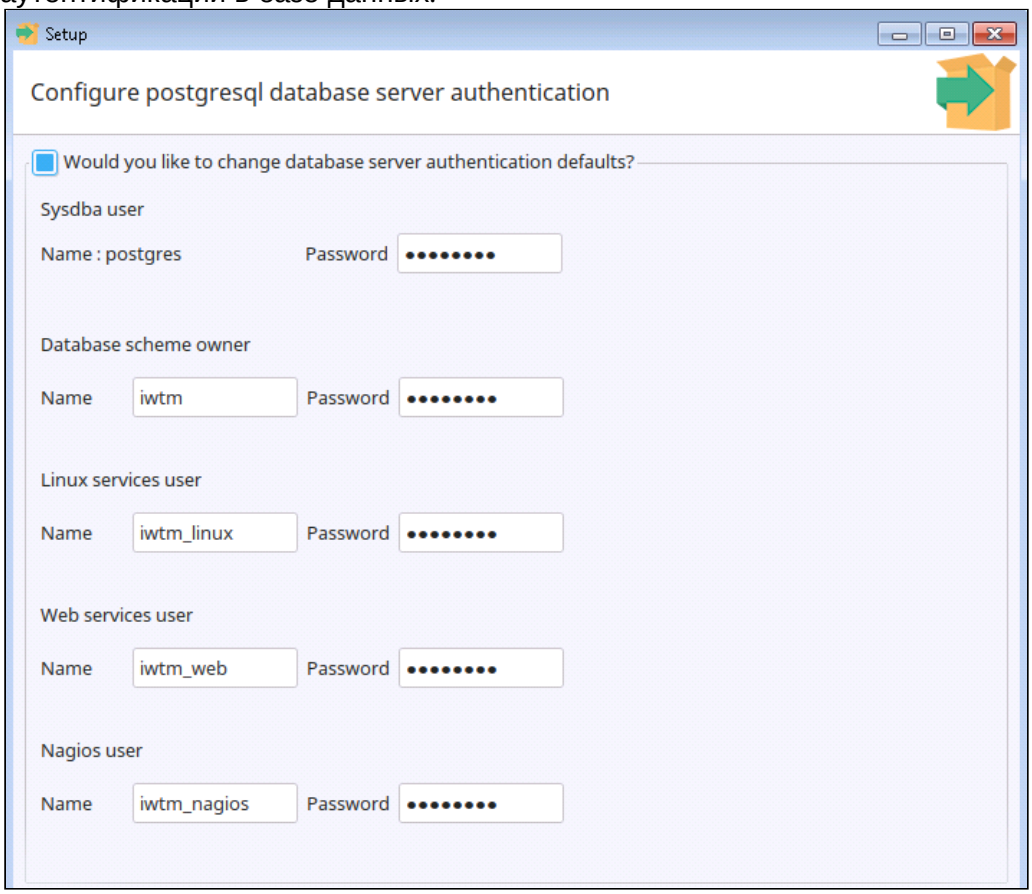
4. Если выбрано использование удаленной базы данных, заполните поля:



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.

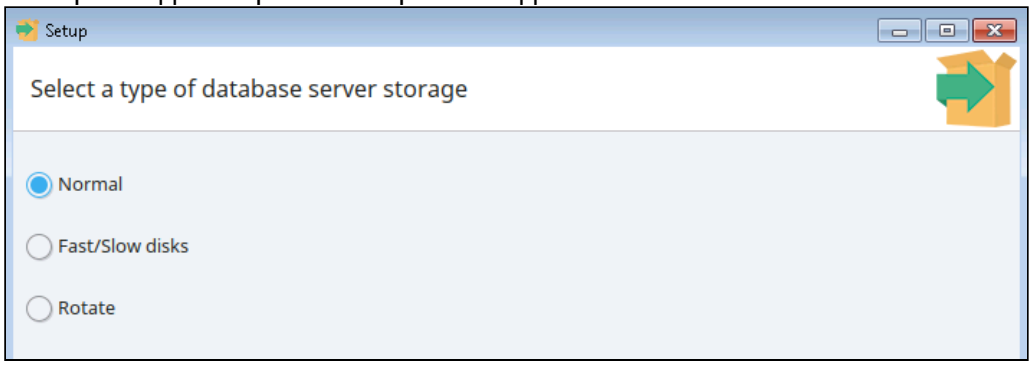
5. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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:

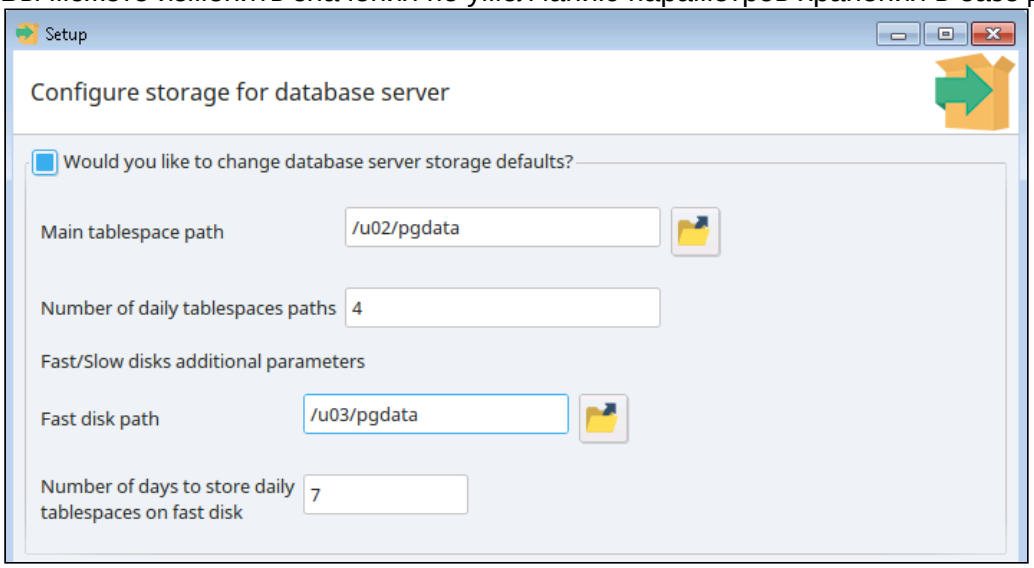


- **`Norma`** l - (обычный) - переключение на следующий раздел, если он указан, происходит при переполнении предыдущего.
- **`Fast/Slow disks`** - разделение пулов на быстрый и медленный. Новые данные сохраняются в быстром разделе и через указанное количество дней

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

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

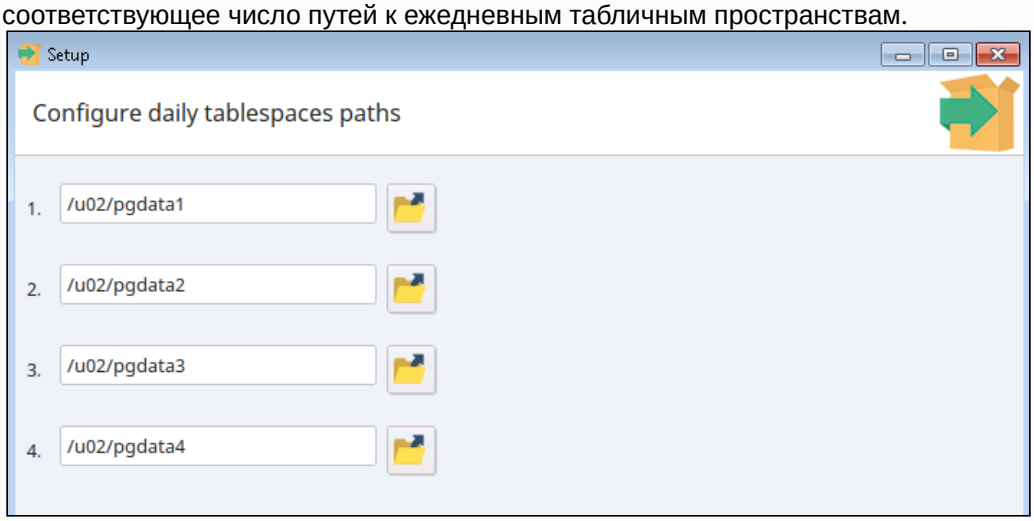
7. Вы можете изменить значения по умолчанию параметров хранения в базе данных.



- **`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;

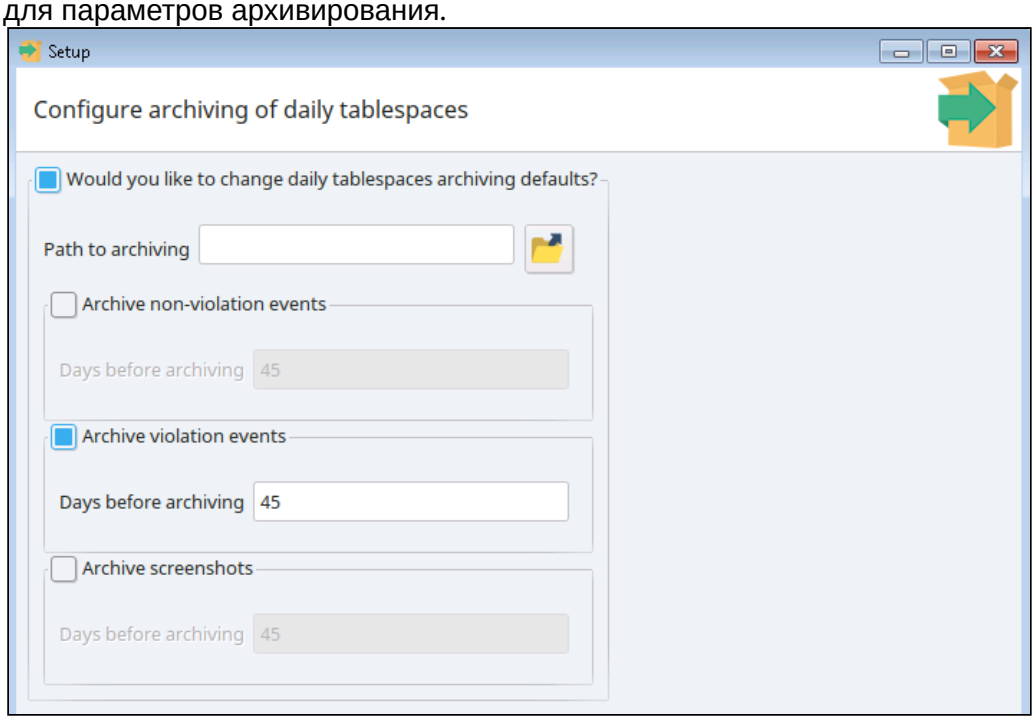
> **Примечание:**

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.



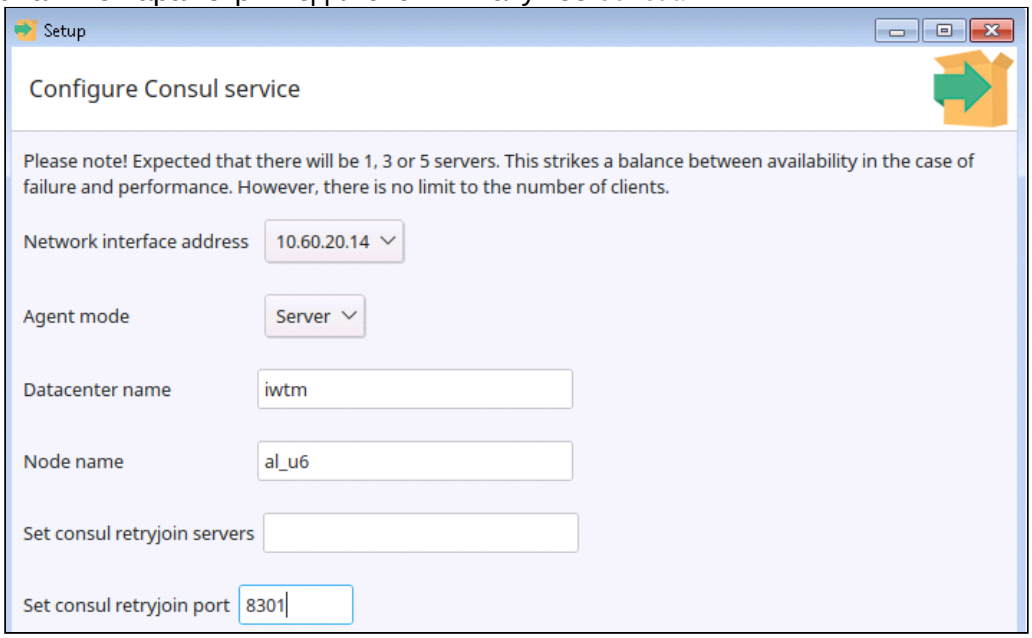
- **`Path to archiving`** - путь к директории хранения файлов архивированных табличных пространств.

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.

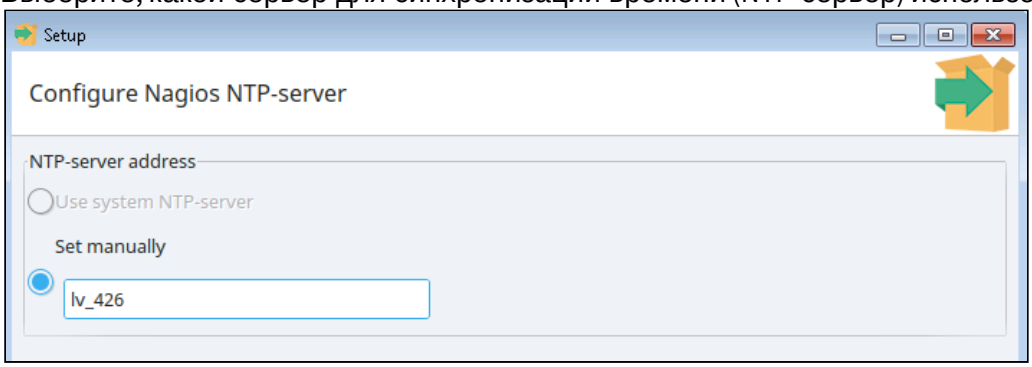
   Для выбора из списка параметров нажмите на кнопку  и в раскрывшемся списке выберите требуемое значение.

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

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

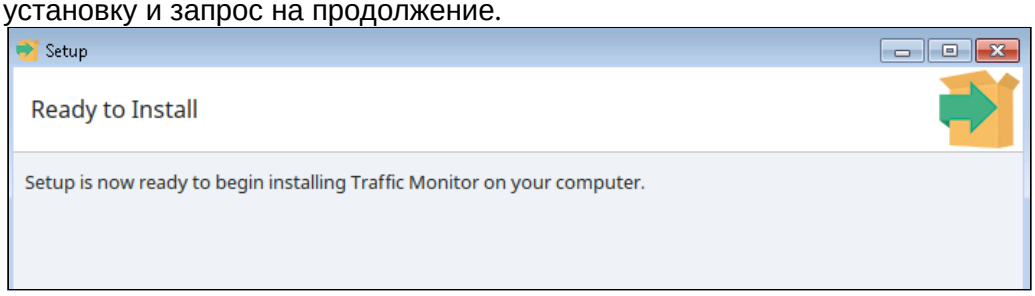
c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. 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:

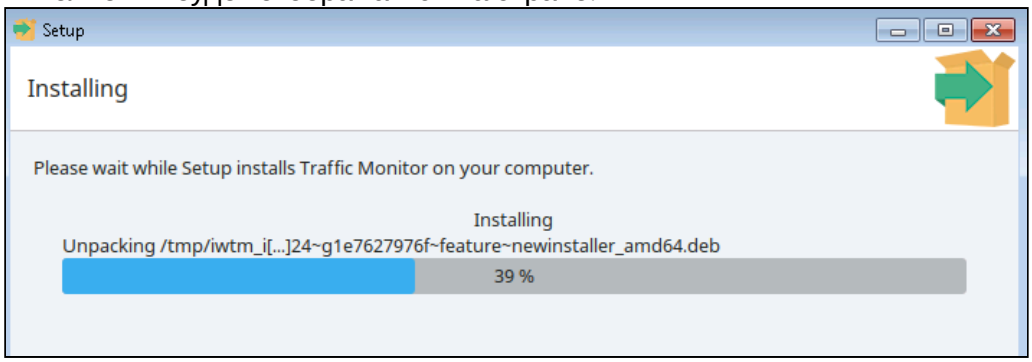


- **`Use system NTP-server`** - использовать системный NTP-сервер;
- **`Set manually`** - указать NTP-сервер вручную. При выборе данного варианта укажите IP-адрес или имя доступного NTP-сервера.

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



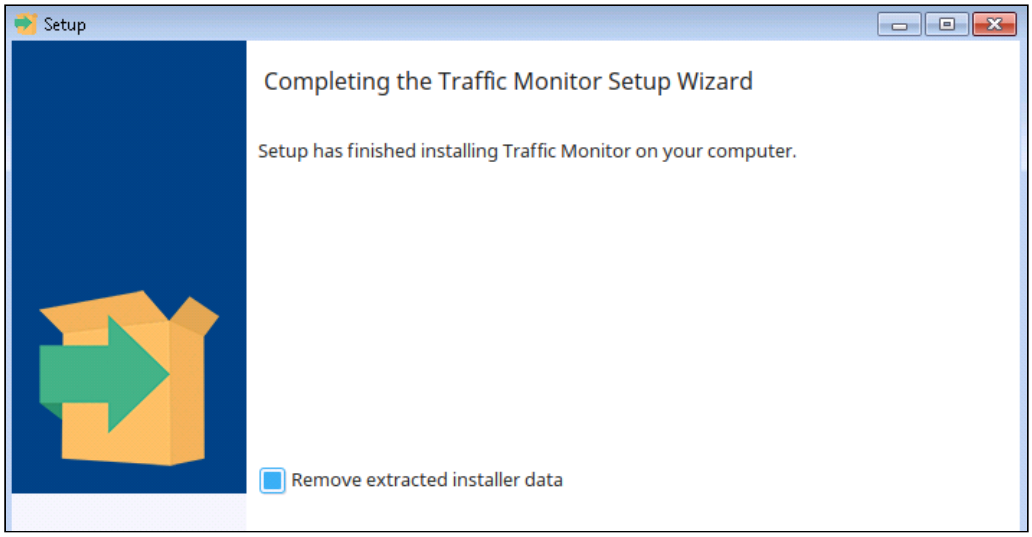
Для начала установки нажмите кнопку **Next**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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.



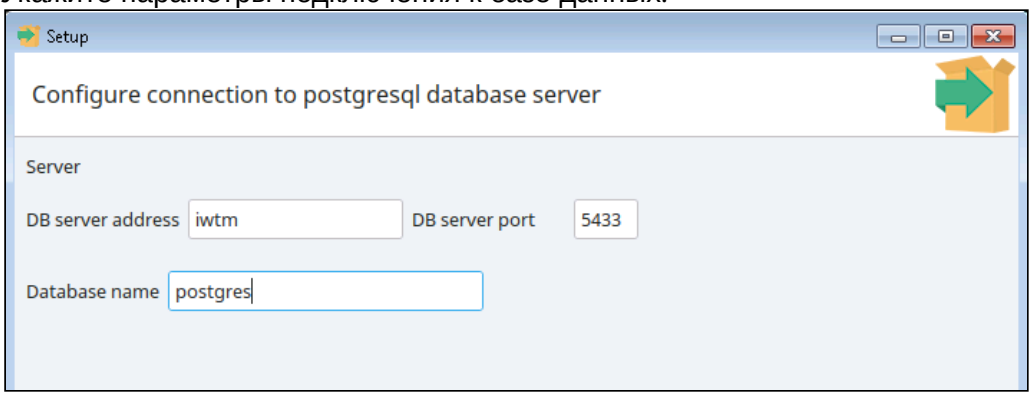
Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove exctracted installer data`**.

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`):

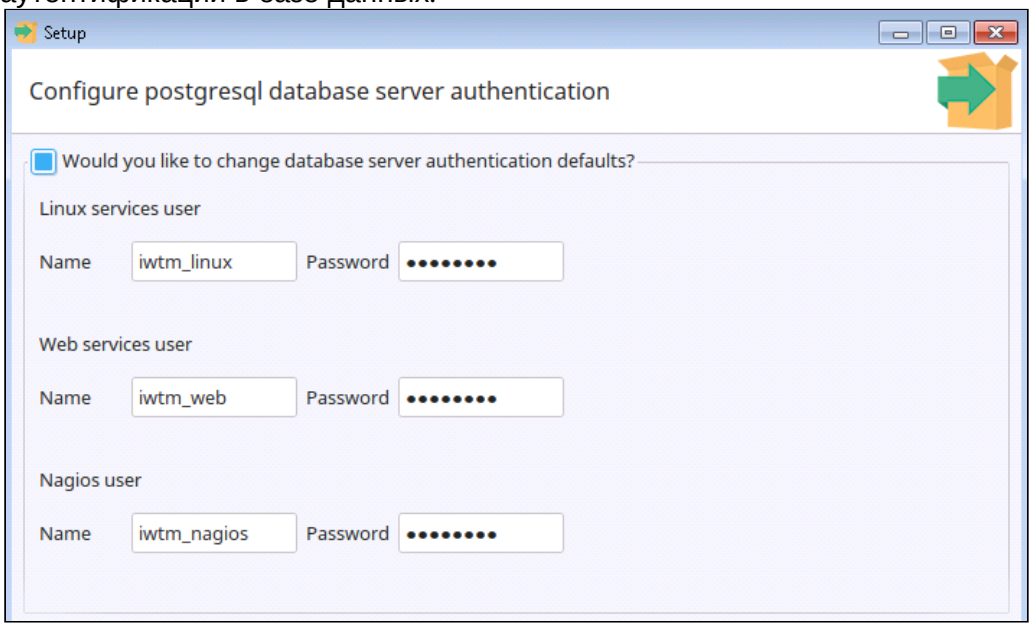
1. Укажите параметры подключения к базе данных:



   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.

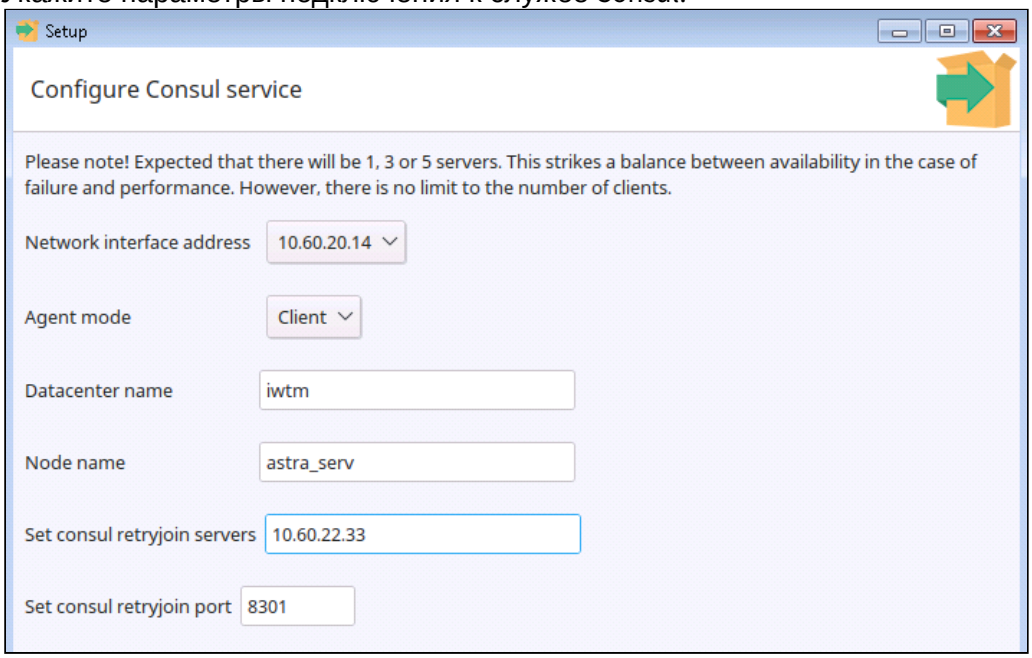
2. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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:

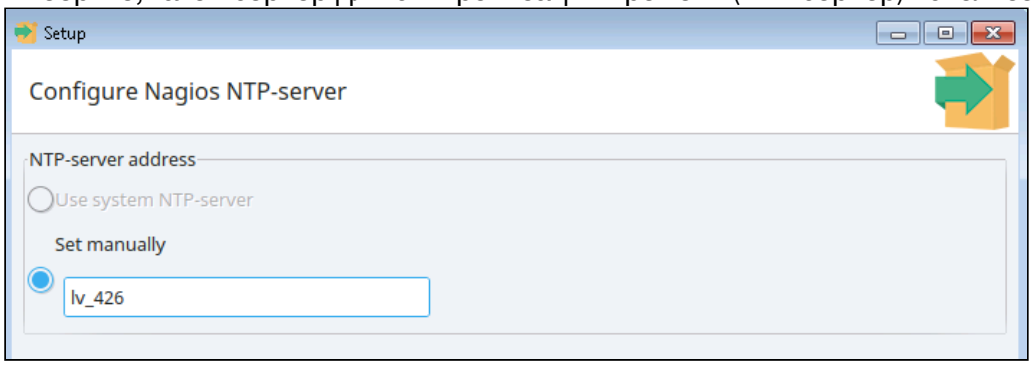


a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите на кнопку и в раскрывшемся списке выберите требуемое значение.
b. Режим работы Consul. Доступны два режима:
   - **`Server`**
   - **`Client`**

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

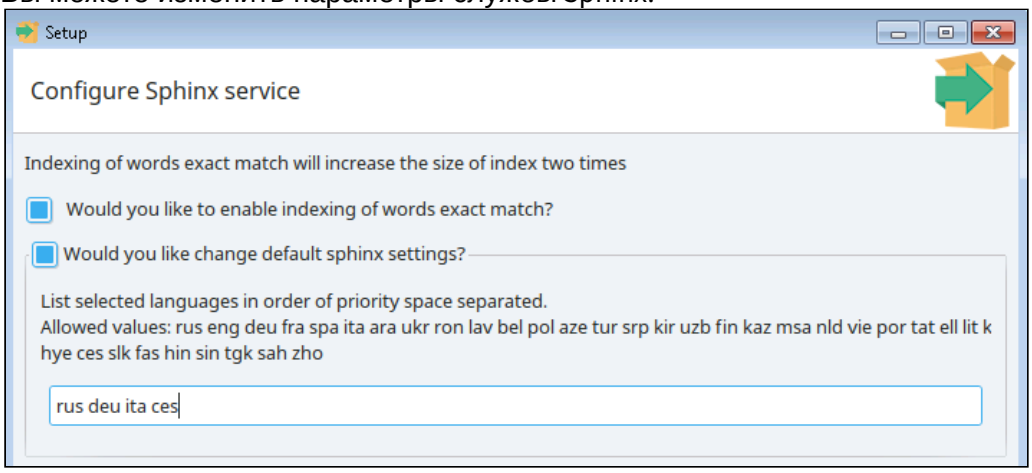
c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. 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:



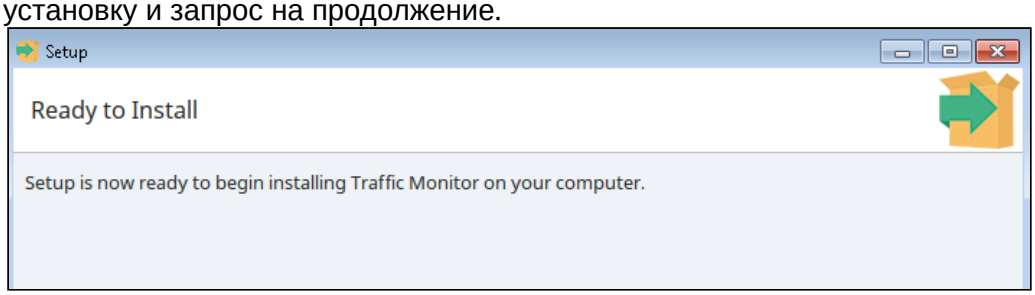
- **`Enable indexing of words exact match`** - включить индексацию на точное совпадение слов;

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

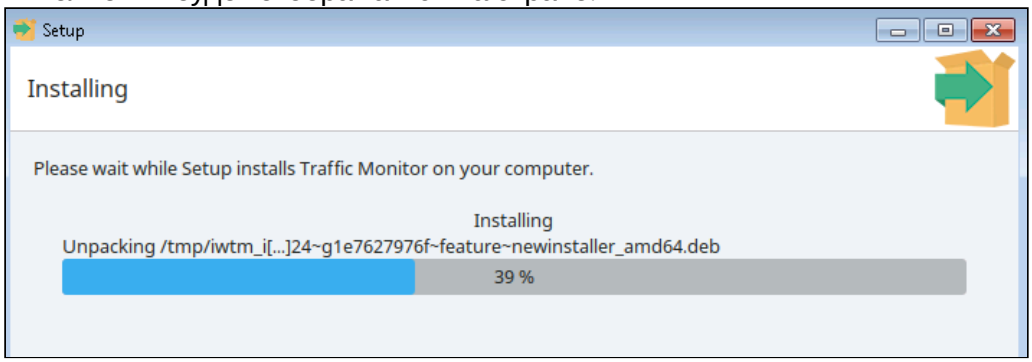
- При необходимости вы можете изменить стандартные параметры работы службы Sphinx (`default sphinx settings`). В этом случае укажите список языков с поддержкой морфологии. По этим языкам будет проводиться индексация.Вы можете указать несколько языков, используя пробел в качестве разделителя.

  > **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.



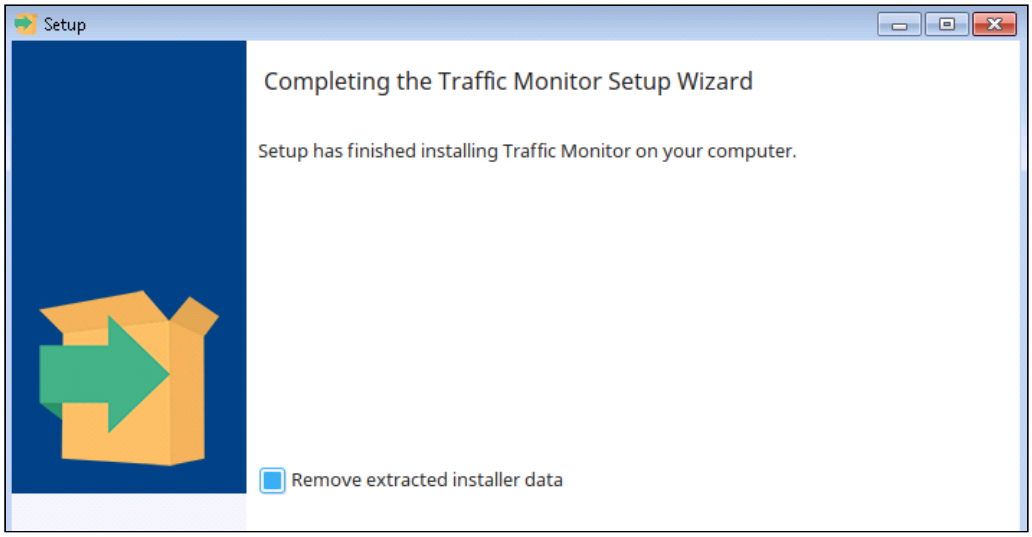
Для начала установки нажмите кнопку **Вперед**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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.



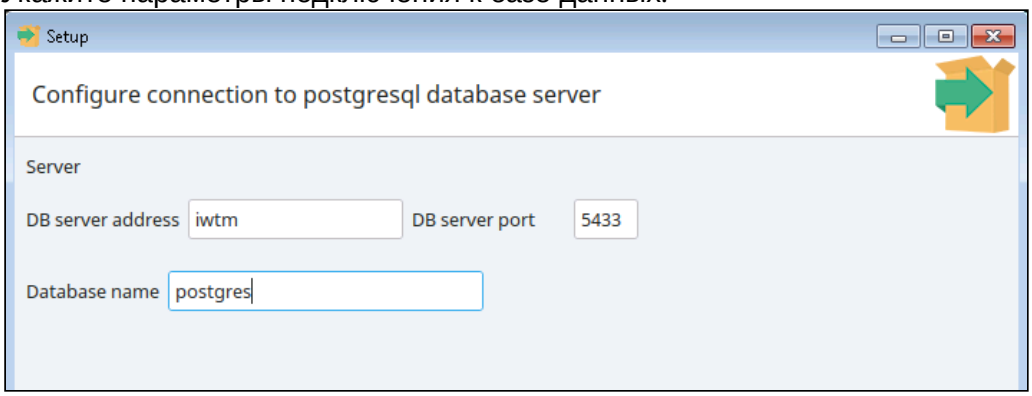
Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove exctracted installer data`**.

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`):

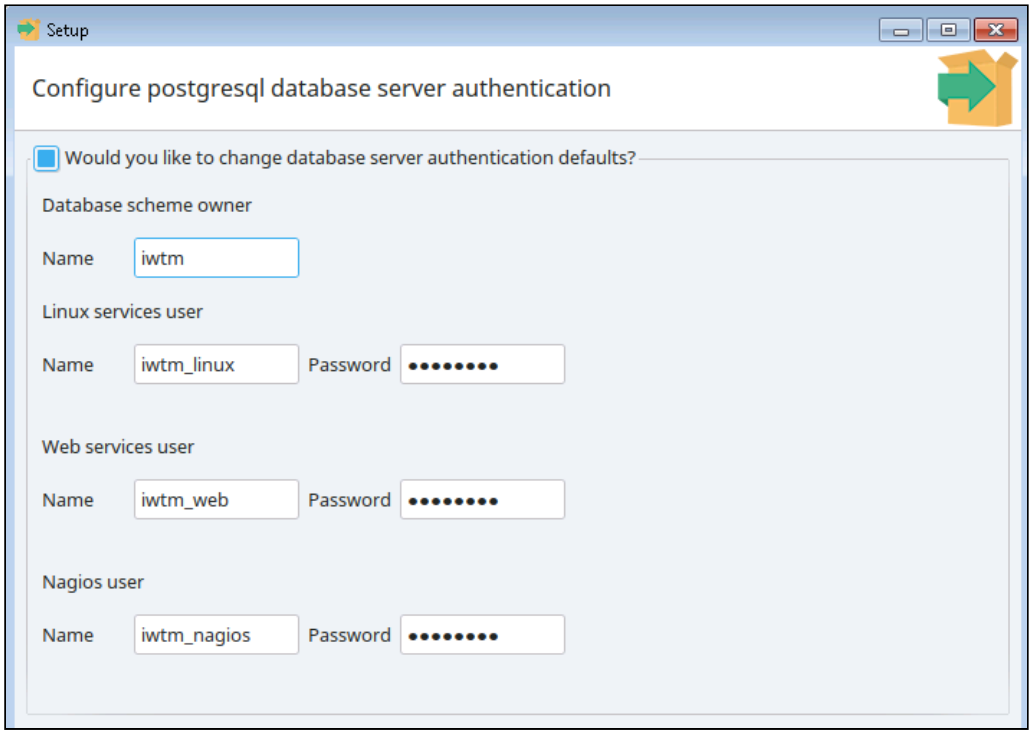
1. Укажите параметры подключения к базе данных:



   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.

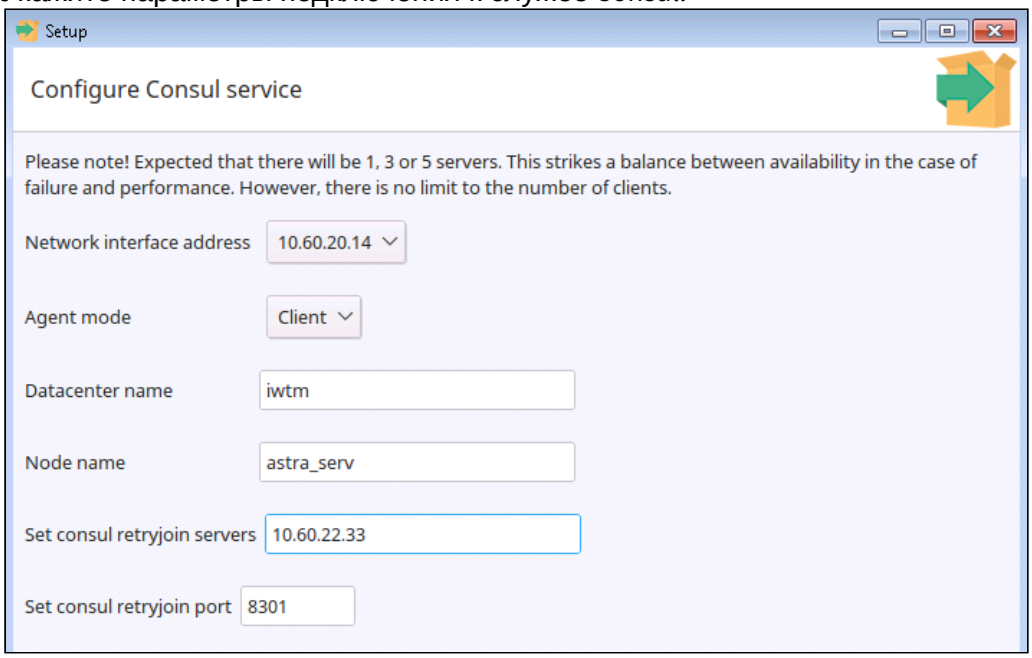
2. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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:



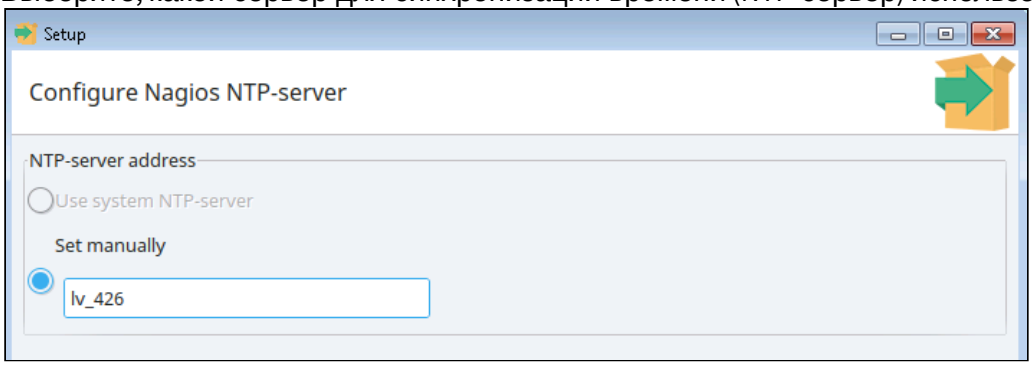
a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите на кнопку и в раскрывшемся списке выберите требуемое значение.
b. Режим работы Consul. Доступны два режима:

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

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

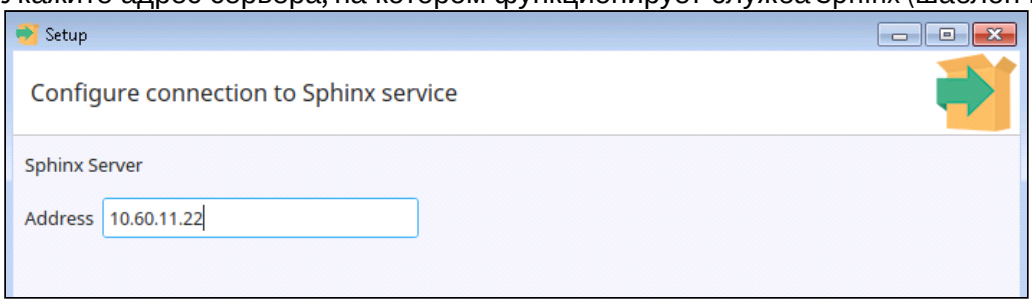
c. **Datacenter name** - введите название дата-центра Consul. По умолчанию - `iwtm`.
d. **Node name** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
e. **Consul retryjoin servers** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. Если 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).



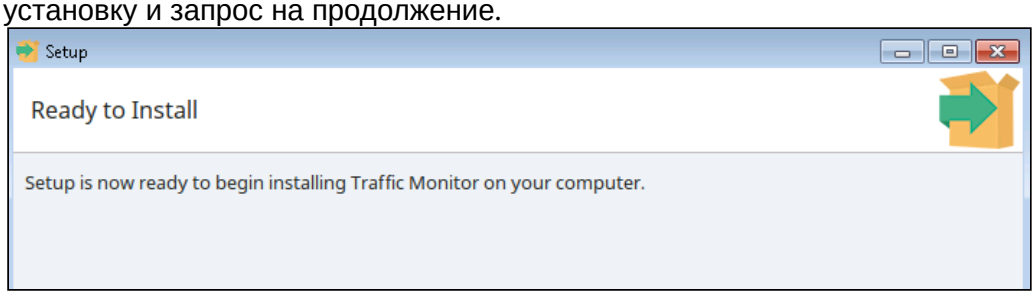
> **Примечание:**
>
> Если шаблоны Индексер и Веб-консоль устанавливаются на один сервер, данный параметр не будет запрошен инсталлятором.

6. Вы можете включить использование технологии OCR.

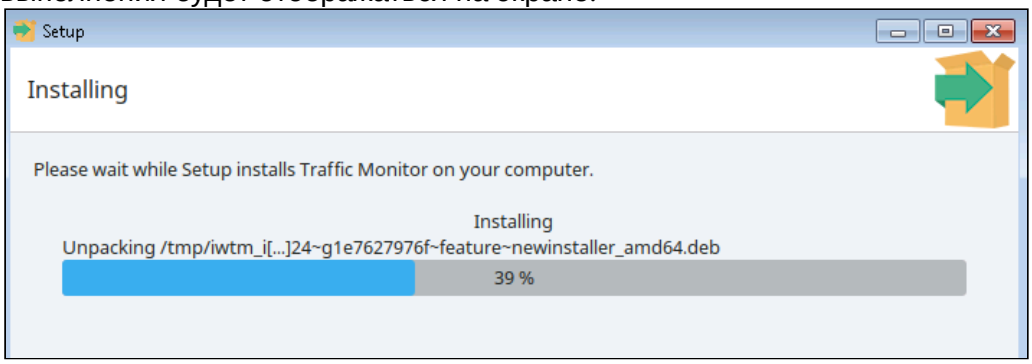


> **Примечание:**
>
> OCR-экстрактор выбирается при установке шаблона Перехватчики.

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



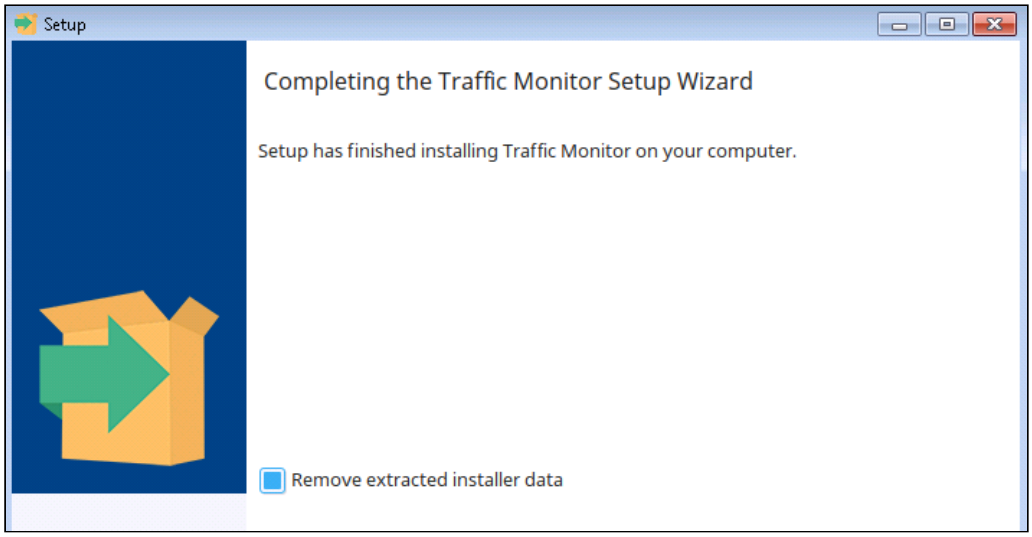
Для начала установки нажмите кнопку **Вперед**.
Начнется распаковка пакетов и установка всех компонентов Traffic Monitor. Прогресс выполнения будет отображаться на экране.



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.



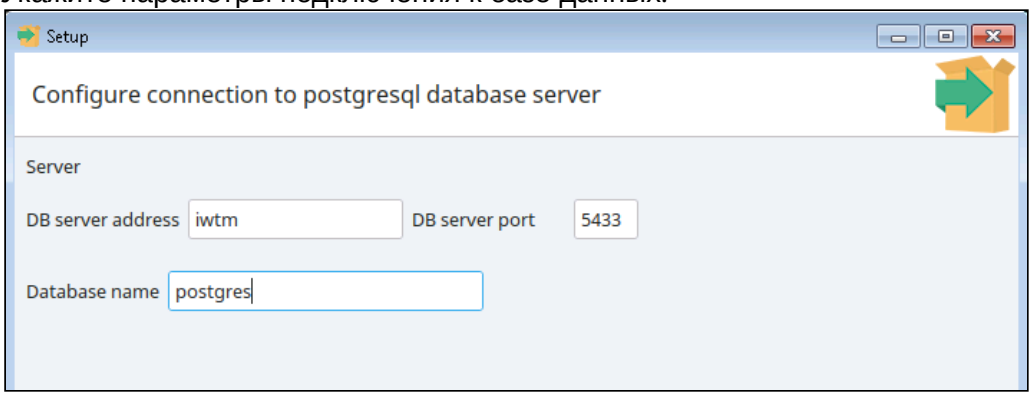
Если установка прошла успешно, данные рекомендуется удалить. Для удаления данных поставьте флажок напротив пункта **`Remove exctracted installer data`**.

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`):

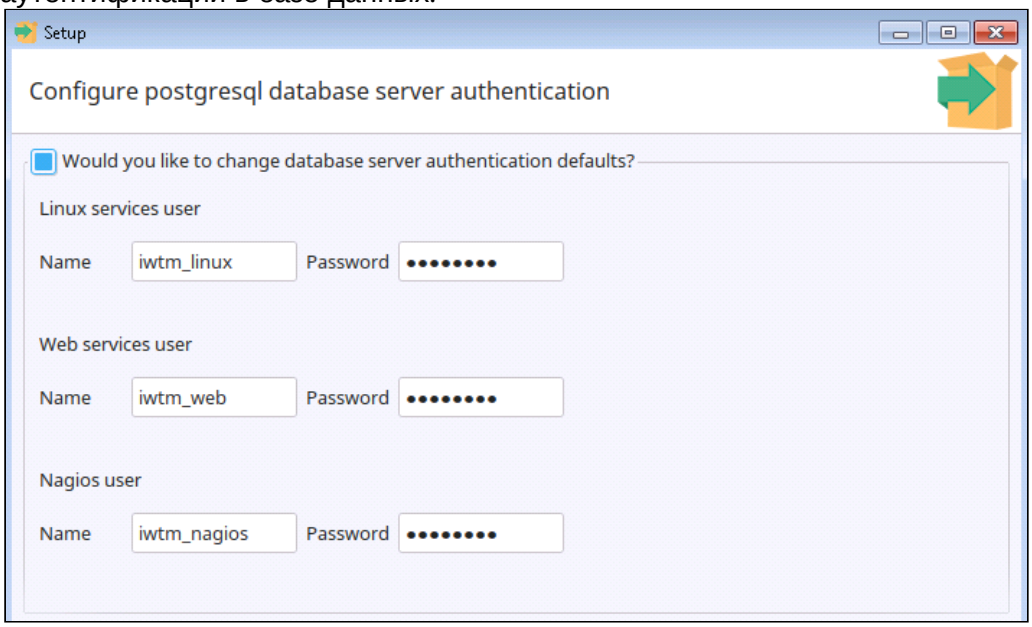
1. Укажите параметры подключения к базе данных:



   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.

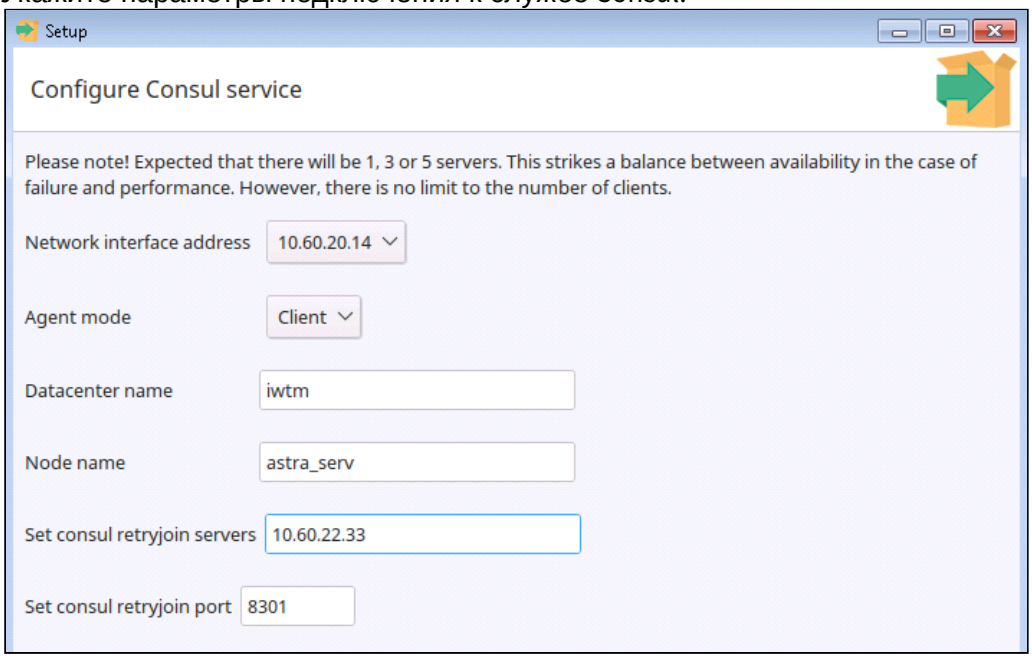
2. При необходимости вы можете изменить значения по умолчанию параметров аутентификации в базе данных.



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:

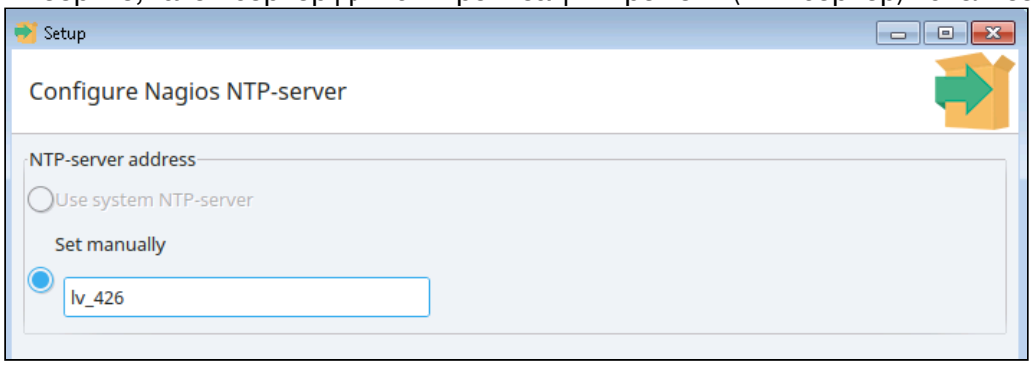


a. **`Network interface address`** - выберите IP-адрес сетевого интерфейса. Для выбора из списка параметров нажмите на кнопку и в раскрывшемся списке выберите требуемое значение.
b. Режим работы Consul. Доступны два режима:
   - **`Server`**
   - **`Client`**

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

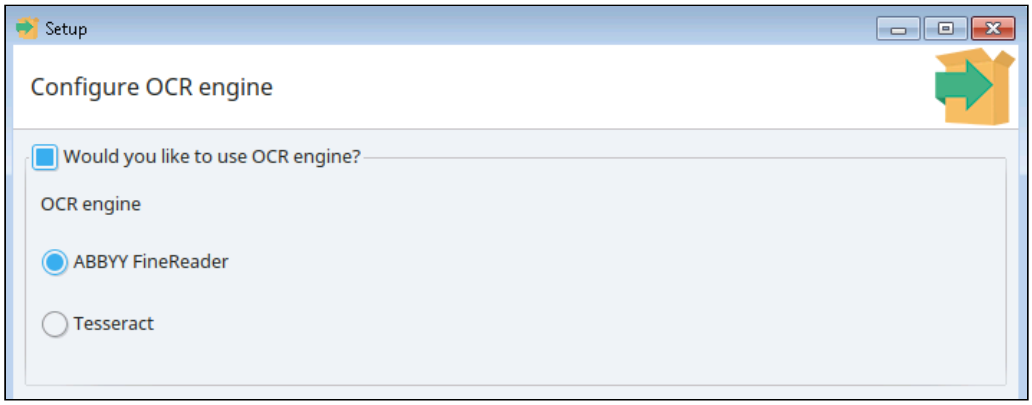
c. **`Datacenter name`** - введите название дата-центра Consul. По умолчанию - `iwtm`.
d. **`Node name`** - имя сервера, на который устанавливаются компоненты Traffic Monitor.
e. **`Consul retryjoin servers`** - список серверов Consul, к которым необходимо подключиться. Вводите значения через запятую. 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.

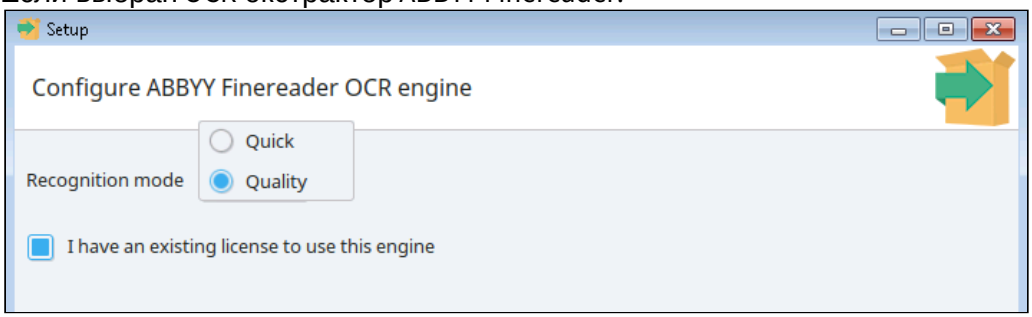


В случае включения необходимо выбрать для использования одну из систем:

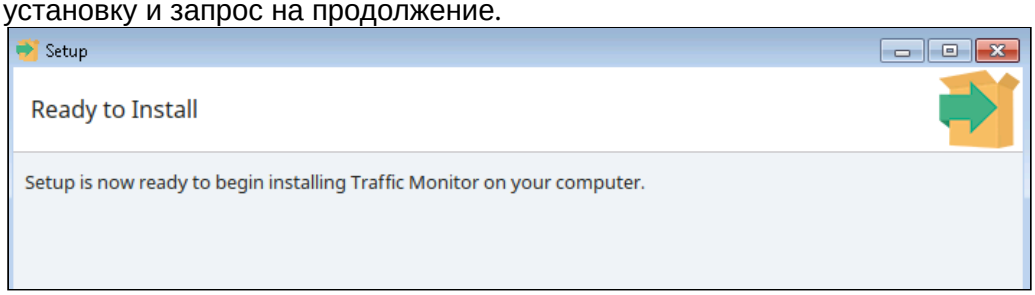
- **`ABBYY FineReader`**;
- **`Tesseract`**.

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

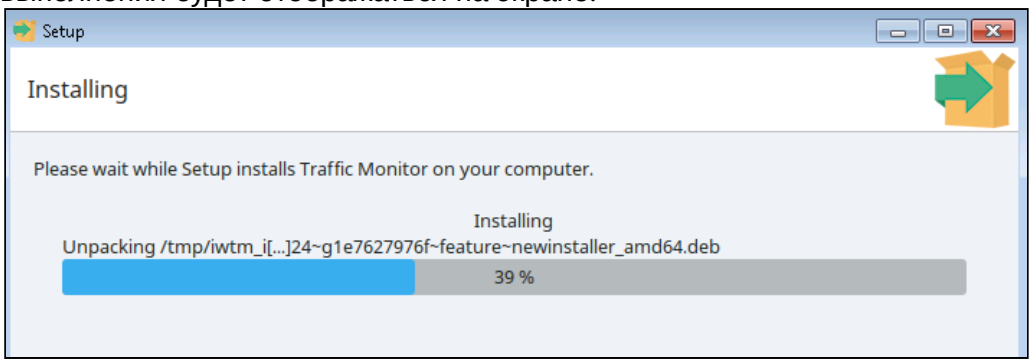
6. Если выбран OCR-экстрактор ABBYY Finereader:



   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.

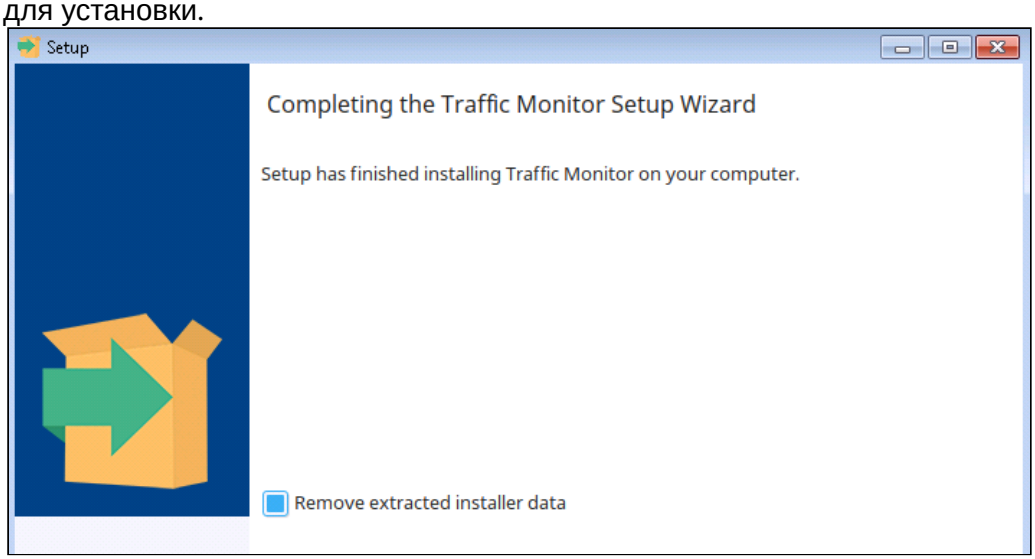


Процесс может занять некоторое время.

> **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 в ОС они были включены до установки, 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-7.4.0.140-astra-smolensk-1.7`**;
   - **`iwtm-postgresql-11.10-7.4.0.140-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-7.4.0.140-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-7.4.0.140-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 в ОС они были включены до установки, 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 Установка InfoWatch Device Monitor

Процесс установки выполняется в следующей последовательности:

1. Установка серверной части InfoWatch Device Monitor.
   В состав серверной части входят следующие компоненты:
   - база данных,
   - сервер InfoWatch Device Monitor,
   - консоль управления InfoWatch Device Monitor,
   - сервис распространения дистрибутивов.
2. Установка агента InfoWatch Device Monitor.
   Агент устанавливается на каждый компьютер, который необходимо контролировать с помощью InfoWatch Device Monitor.

До начала установки убедитесь, что среда, в которой будет развернут InfoWatch Device Monitor, удовлетворяет аппаратным и программным требованиям (см. "Аппаратные и программные требования").

Важно!

Для корректной работы и доступа ко всей функциональности версии Traffic Monitor и Device Monitor должны быть совместимы. Подробнее о совместимости Device Monitor см. в статье Базы знаний InfoWatch "Особенности совместимости разных версий TM, DM и Агентов".

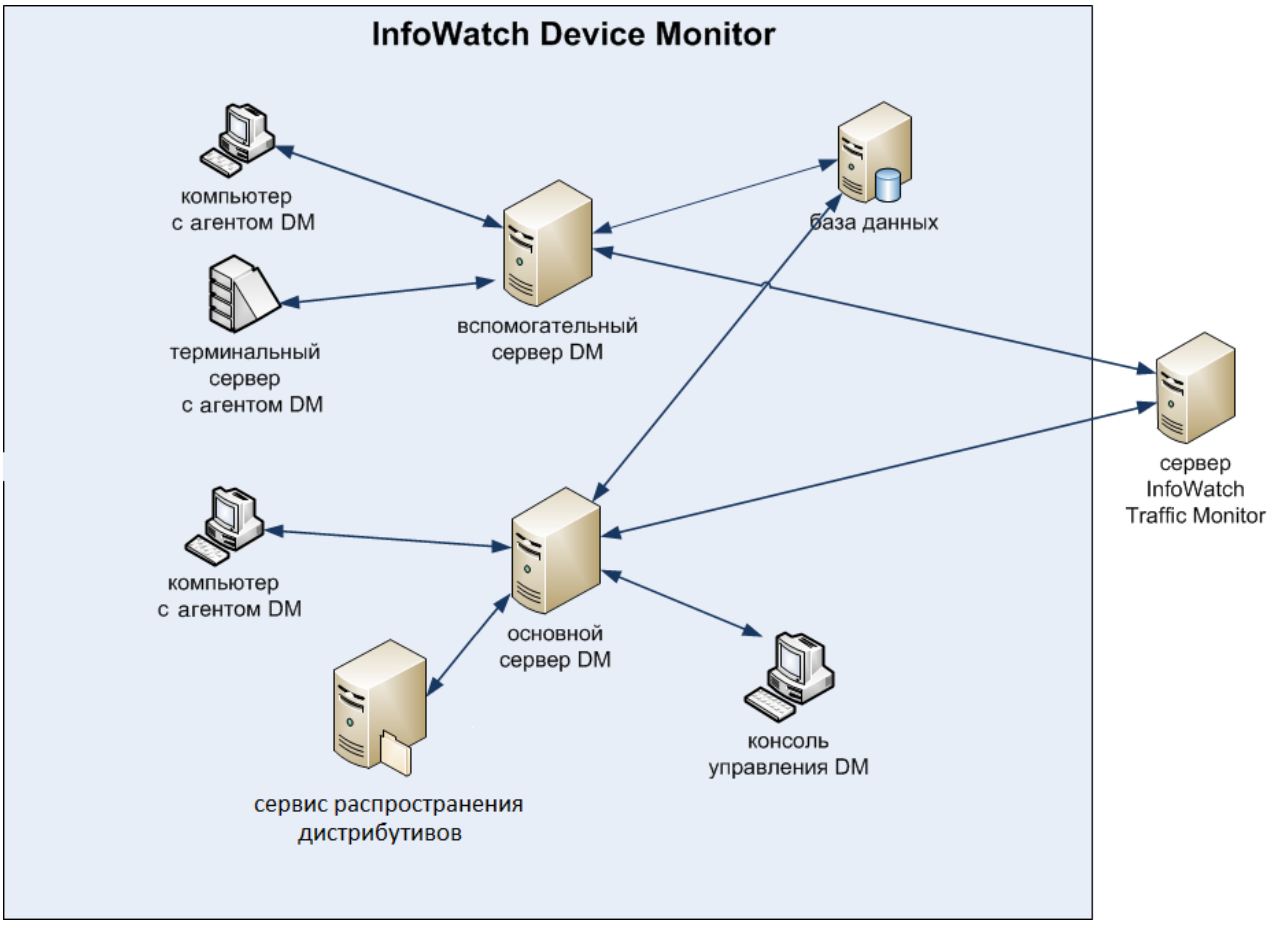
3.2.1 Схема развертывания InfoWatch Device Monitor

Компоненты, входящие в состав InfoWatch Device Monitor, перечислены в следующей таблице:

Компонент	Назначение
InfoWatch Device Monitor Client (клиентское приложение InfoWatch Device Monitor, Агент)	Перехват действий сотрудников на контролируемых рабочих станциях

Компонент	Назначение
InfoWatch Device Monitor Server (сервер InfoWatch Device Monitor, Сервер)	Конфигурирование клиентских приложений, сбор данных от клиентских приложений и передача этих данных системе InfoWatch Traffic Monitor, распространение deploy-агентов на рабочие станции
InfoWatch Device Monitor Database (база данных)	Хранение информации, необходимой для работы Device Monitor
Консоль управления InfoWatch Device Monitor (Консоль управления)	Управление модулем Device Monitor
Сервис распространения дистрибутивов (Сервис распространения)	Получение и хранение новой версии дистрибутива агента Device Monitor
Менеджер управления серверами	Изменение ролей и других атрибутов серверов Device Monitor

Взаимодействие компонентов Device Monitor показано на рисунке:



Для повышения производительности Device Monitor, можно использовать кластеризацию. При этом одна схема базы данных будет использоваться несколькими серверами для хранения и распространения общей схемы безопасности.

Сервер и база данных могут находиться на одном компьютере. Однако для увеличения производительности рекомендуется размещать базу данных и сервер на разных компьютерах.

Консоль управления может подключаться только к основному серверу. Используя Консоль управления можно управлять всеми серверами в кластере.

Система разворачивается и работает следующим образом:

1. Первым устанавливают **основной сервер** (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Работа с Менеджером управления серверами").
2. При установке основного сервера определяют используемый сервер **базы данных**: СУБД может располагаться как отдельно, так и на том же компьютере, что и основной сервер.
3. При установке основного сервера создается **схема базы данных**, где будет храниться **схема безопасности** и другие параметры Device Monitor.
4. При необходимости, можно установить **вспомогательные серверы**, которые будут обеспечивать балансировку нагрузки.
5. **Консоль управления** может устанавливаться на любую рабочую станцию. Консоль управления подключается к основному серверу. Из Консоли управления выполняется настройка схемы безопасности в соответствии с требованиями корпоративной политики безопасности.
6. **Сервер распространения дистрибутивов** устанавливается вместе с **основным сервером Device Monitor** по умолчанию, имеет хранилище с дистрибутивами Агентов для используемых ОС и платформы.
7. С **основного сервера** на **рабочие станции** распространяются deploy-агенты (агентом распространения) Device Monitor, которые затем скачивают дистрибутивы Агентов с ближайшего **сервера распространения** из указанных точек публикации дистрибутивов. Скачивание Агентов может происходить параллельно несколькими рабочими станциями одновременно.
8. Агенты выполняют подключение к серверу Device Monitor по зашифрованному каналу, с привязкой к серверу на основании ключа, используемого для шифрования трафика. Агенты Device Monitor обеспечивают реализацию схемы безопасности, а также получение теневых копий и их отправку на сервер Device Monitor.
9. Серверы Device Monitor получают из базы данных обновленные версии схемы безопасности и распространяют их на контролируемые рабочие станции. С контролируемых рабочих станций на сервер передается информация о событиях, подпадающих под действие правила схемы безопасности, а также теневые копии файлов. Информация о событиях передается в базу данных. Теневые копии передаются в систему InfoWatch Traffic Monitor.

Пример 1

1. Сотрудник, работающий на контролируемой рабочей станции, обращается к контролируемому периферийному устройству (например, дает команду распечатать документ через USB принтер).
2. Агент проверяет, имеет ли сотрудник право на работу с периферийным устройством. Если такого разрешения нет, то сотруднику будет отказано в доступе к устройству (в рассматриваемом случае документ не будет отправлен на печать).

Печать документов на локальных и сетевых принтерах отслеживается перехватчиком Print Monitor. Копия задания на печать передается в InfoWatch Traffic Monitor для анализа. Отправка документов на

печать возможна при условии, что сотруднику разрешен доступ к принтеру (проверяется перехватчиком Device Monitor).

Пример 2

В Device Monitor задано правило, отслеживающее запись в PDF-файл на съемном устройстве. В правиле указано, что при выполнении этой операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к записи в файл на съемном устройстве (например, копирует файл на USB Flash Drive).
2. Если операция записи в файл на съемном устройстве успешно завершена, то Агент InfoWatch Device Monitor генерирует событие и создает теневую копию файла.
3. Если создать теневую копию файла невозможно (например, при отсутствии свободного места на жестком диске), операция записи в файл на съемном устройстве будет произведена без создания теневой копии, о чем будет указано в информации о событии.
4. Агент передает данные (событие и теневую копию файла) на Сервер InfoWatch Device Monitor. Если соединение с Сервером отсутствует, то данные сохраняются на контролируемом компьютере. После восстановления связи данные будут доставлены на Сервер.
5. Сервер отправляет данные в систему InfoWatch Traffic Monitor для анализа. Если соединение с сервером InfoWatch Traffic Monitor отсутствует, то данные сохраняются на компьютере. После восстановления связи данные будут доставлены в систему InfoWatch Traffic Monitor.

Попытки записи в файлы на съемных устройствах отслеживаются перехватчиком File Monitor. Полученные сведения передаются затем в InfoWatch Traffic Monitor для анализа. В то же время доступ к съемному устройству контролируется перехватчиком Device Monitor. Поэтому сотрудник может выполнять операцию записи в файл только на тех съемных устройствах, к которым у него есть доступ.

Пример 3

В Device Monitor задано правило, отслеживающее печать DOC-файлов. В правиле указано, что при выполнении подобной операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к отправке документа на печать.
2. Если задание на печать сформировано успешно, то Агент InfoWatch Device Monitor генерирует событие и создает теневую копию документа, отправленного на печать.
3. В случае если создать теневую копию документа невозможно (например, при отсутствии свободного места на жестком диске), операция печати будет произведена без создания теневой копии, о чем будет указано в информации о событии.
4. Агент передает данные (событие и теневую копию документа) на Сервер InfoWatch Device Monitor. Если соединение с Сервером отсутствует, то данные сохраняются на контролируемом компьютере. После восстановления связи данные будут доставлены на Сервер.
5. Сервер отправляет данные в систему InfoWatch Traffic Monitor для анализа. Если соединение с сервером InfoWatch Traffic Monitor отсутствует, то данные сохраняются в базе данных. После восстановления связи данные будут доставлены в систему InfoWatch Traffic Monitor.

3.2.2 Установка серверной части InfoWatch Device Monitor

Серверная часть InfoWatch Device Monitor устанавливается при помощи универсальной программы установки.
Универсальная программа установки находится на диске с дистрибутивом Device Monitor (каталог `Setup.Unified`). При помощи данной программы можно установить все компоненты, за исключением Агента: базу данных, Сервер Device Monitor и Консоль управления.
Для управления базой данных может использоваться СУБД Microsoft SQL Server, Oracle или PostgreSQL.
Консоль управления может подключаться к основному Серверу.
Подробнее об установке читайте в следующих разделах:

- Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server;
- Рекомендации по развертыванию базы данных под управлением СУБД Oracle;
- Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL;
- Рекомендации по установке Сервера InfoWatch Device Monitor;
- Порядок установки серверной части InfoWatch Device Monitor.

Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server

На компьютере, с которого будет запущен процесс создания базы данных, предварительно должен быть установлен пакет Microsoft .NET Framework 2.0 Service Pack 1, Microsoft .NET Framework 4.0 или выше.
Учетная запись, от имени которой будет создаваться база данных, должна быть подготовлена заранее.
Выбор типа учетной записи зависит от того, какой способ аутентификации вы планируете использовать для подключения к серверу базы данных. В СУБД Microsoft SQL Server поддерживаются два способа аутентификации:

- **Аутентификация Windows**. Аутентификация выполняется с использованием учетных записей, принадлежащих к домену Windows. Данные аутентификации обрабатываются системой безопасности Microsoft Windows.
- **Встроенная в SQL Server**. Используются учетные записи СУБД Microsoft SQL Server. Аутентификация выполняется средствами СУБД.

> **Важно!**
>
> Для обеспечения приемлемого уровня безопасности настоятельно рекомендуется использовать способ **Аутентификация Windows**.

Если вы планируете использовать способ Аутентификация Windows:

1. Убедитесь, что в домене Windows существует учетная запись, от имени которой будет создаваться база данных. Эта учетная запись должна иметь права локального администратора на том компьютере, с которого будет запущен процесс создания базы данных. При необходимости создайте новую учетную запись.
2. Включите учетную запись в состав учетных записей СУБД Microsoft SQL Server, выбрав при этом **Аутентификация Windows**.
3. Назначьте учетной записи роль **dbcreator**.

Если вы планируете использовать способ Встроенная в SQL Server:

1. Создайте новую учетную запись Microsoft SQL Server. При настройке параметров записи: выберите **Встроенная в SQL Server**, задайте имя и пароль.

2. Назначьте учетной записи роль **dbcreator**.

> **Примечание:**
>
> Имя и пароль встроенной учетной записи указывают при настройке параметров базы данных (см. "Порядок установки серверной части InfoWatch Device Monitor", шаг 7).

Рекомендации по развертыванию базы данных под управлением СУБД Oracle

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

- пакет Microsoft .NET Framework 4.5
- клиент СУБД Oracle (только после установки пакета Microsoft .NET Framework 4.5)
- провайдер Oracle Database Provider for .NET (ODP.NET)

> **Важно!**
>
> Выбор данного компонента рекомендуется производить путем отметки соответствующего поля при пользовательском типе установки (Custom). Проводить установку необходимо от имени администратора.

Перед тем как начать создание схемы базы данных, убедитесь, что идентификатор соединения с сервером базы данных прописан в файле **tnsnames.ora** (см. "Настройка параметров соединения с сервером СУБД ORACLE").

Настройка параметров соединения InfoWatch Device Monitor с сервером СУБД Oracle

Для корректного соединения с сервером СУБД Oracle на каждом компьютере, на котором установлен клиент СУБД Oracle, необходимо указать параметры подключения. Выберите один из двух вариантов, представленных ниже.

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

Укажите параметры подключения к серверу СУБД Oracle. Для этого добавьте в файл tnsnames.ora запись следующего вида:

```
tns_name =
 (DESCRIPTION =
 (ADDRESS = (PROTOCOL = TCP)(HOST = host_name)(PORT = port_number))
 (CONNECT_DATA =
 (SERVER = DEDICATED)
 (SERVICE_NAME = service_name)
 )
 )
```

Здесь нужно подставить действительные значения для следующих параметров:

- `tns_name` – псевдоним сервера СУБД Oracle;
- `host_name` – доменное имя или IP-адрес сервера СУБД Oracle;
- `port_number` – порт сервера, на котором запущен процесс прослушивания клиентских подключений;
- `service_name` – имя сервиса базы данных.

Пример записи в файле tnsnames.ora

```
IWDM =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = iwdm.example.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)
```

Важно!

Файл **tnsnames.ora** чувствителен к форматированию. Поэтому, если вы редактируете его, копируя приведенный пример, обратите внимание: в скопированном фрагменте не должно быть пустых строк.

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

Пример строкового представления

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

Рекомендации по развертыванию базы данных под управлением СУБД PostgreSQL

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

- ОС Microsoft Windows Server 2008 R2/2012/2012 R2/2016/2019;
- пакет Microsoft .NET Framework 4.5.2.

Скачайте на официальном сайте PostgreSQL 13 и установите с параметрами по умолчанию.

При установке будет создан супер-пользователь postgres, для которого нужно прописать пароль. Информация о нем будет доступна во входящей в комплект установки утилите pgAdmin III в секции "Роли входа".

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

Примечание:

Для увеличения быстродействия системы рекомендуется устанавливать ОС, серверную часть InfoWatch Device Monitor и СУБД PostgreSQL на разные физические жесткие диски.

Рекомендации по установке Сервера InfoWatch Device Monitor

Для повышения производительности InfoWatch Device Monitor рекомендуется развертывать Сервер и базу данных на отдельных компьютерах.

Сервер Device Monitor и Агент Device Monitor необходимо устанавливать в одном часовом поясе. Это обеспечит отображение корректного времени перехвата события.

> **Важно!**
>
> При развертывании пула из нескольких серверов, на каждом из них должна быть установлена одинаковая версия серверного приложения InfoWatch Device Monitor, соответствующая актуальной версии базы данных.

В процессе настройки параметров Сервера (см. "Порядок установки серверной части InfoWatch Device Monitor") необходимо указать учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor. Возможны следующие варианты:

- **Пользователь**. Запуск службы от имени учетной записи домена Windows,
- **Network Service**. Запуск службы от имени учетной записи, не имеющей административных привилегий на рабочей станции.

Для базы данных под управлением СУБД Microsoft SQL Server. Если для аутентификации пользователя, создающего базу данных, выбран способ Аутентификация Windows (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server"), а база данных и Сервер будут находиться на разных компьютерах, то выберите вариант Пользователь.

> **Важно!**
>
> Не рекомендуется выбирать вариант Local System. В этом случае пользователь может получить неограниченные права, что противоречит принципам создания политики безопасности.
>
> Создайте сервисную учетную запись и предоставьте ей права записи в каталог установки сервера DM: `\Program Files\InfoWatch\Device Monitor\Server`

Учетная запись домена Windows (вариант **Пользователь**) должна быть подготовлена заранее. Для этого выполните следующие действия:

1. Разрешите учетной записи запускать процесс как службу. Для этого:
   - В **Панели управления** откройте компонент **Администрирование > Локальная политика безопасности**.
   - В открывшемся диалоговом окне выберите узел **Локальные политики > Назначение прав пользователя**.
   - Справа в области сведений дважды щелкните право **Вход в качестве службы**.
   - На вкладке **Параметр локальной безопасности** добавьте подготовленную учетную запись.
- Включите учетную запись в состав учетных записей СУБД Microsoft SQL Server.
  По окончании установки предоставьте учетной записи доступ к созданной базе данных. При выборе разрешения на доступ к базе данных укажите роль **db_owner**.

Порядок установки серверной части InfoWatch Device Monitor

> **Важно!**
>
> Перед началом установки ознакомьтесь с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor".

> **Важно!**
>
> При развертывании пула из нескольких серверов, на каждом из них должна быть установлена одна и та же версия серверного приложения InfoWatch Device Monitor, соответствующая актуальной версии базы данных.

1. **Запуск мастера установки**
   Откройте папку с дистрибутивом Device Monitor. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы.
   В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите **Далее**.
2. **Принятие лицензионного соглашения**
   Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите **Далее**.
3. **Выбор устанавливаемого компонента**
   На шаге **Выборочная установка** по умолчанию выбраны все компоненты:
   - Сервер
   - Консоль управления
   - Сервис распространения дистрибутивов

   Если необходимо, измените состав устанавливаемых компонентов. По умолчанию все компоненты устанавливаются на одну рабочую станцию. Если вы рассчитываете использовать Консоль управления или Сервис распространения на другой рабочей станции, то вам не нужно устанавливать этот компонент: нажмите **Консоль управления** или **Сервис распространения дистрибутивов** и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**.
   Вы также можете изменить папку, куда будет установлен тот или иной компонент: выберите компонент в списке, нажмите и укажите другое местоположение. При установке Сервиса распространения новый дистрибутив Агентов будет автоматически размещен в директорию с дистрибутивами.
   Нажмите **Далее**.
4. **Определение параметров сервера**
   На шаге **Тип устанавливаемого сервера** выберите:
   - **Основной сервер** – должен быть установлен первым. К нему будут подключаться Агенты и Консоль управления.
   - **Вспомогательный сервер** – дополнительный сервер, обеспечивающий балансировку нагрузки от Агентов.

Важно!

Изменение имени сервера Device Monitor после установки может привести к перебоям в работе Системы.

Примечание:

Установка вспомогательного сервера возможна только после установки основного на отдельный компьютер. Установка вспомогательного сервера описана в пункте 14.

Для обеспечения быстрой актуализации информации о серверах, рекомендуется отметить **Опубликовать сервер в Active Directory**.

Важно!

Актуализируя политики безопасности, компьютеры периодически взаимодействуют с сервером Device Monitor. Поэтому, чтобы вновь добавленный сервер мог сразу же приступить к обслуживанию компьютеров, а также для своевременного уведомления Агентов о возможных изменениях портов серверов, рекомендуется при установке сервера публиковать его данные в домене.
Для публикации данных сервера Device Monitor в домене, учетной записи, от имени которой выполняется установка сервера, требуются права на создание и удаление точек подключения.

Если у вас есть СУБД со схемой БД Device Monitor того же номера версии, что устанавливается на сервер, снимите отметку **Установить новую базу данных** . Нажмите **Далее** .

5. **Файл для импорта элементов конфигурации**

   Если установка новой базы данных не производится, этот шаг будет пропущен. Чтобы использовать ранее экспортированный файл конфигурации сервера (см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Импорт/экспорт настроек и схемы безопасности"), нажмите **Выбрать** и укажите место расположения файла конфигурации.

   Важно!

   Файл конфигурации должен быть расположен на локальном диске или внешнем носителе. Расположение в сетевой папке программой установки не поддерживается.

   Нажмите **Далее**. В этом случае все существующие настройки и элементы конфигурации будут заменены на импортированные.
6. **Выбор сервера базы данных**
   Укажите СУБД, под управлением которой будет находиться база данных Device Monitor, выбрав один из следующих вариантов:

- Microsoft SQL Server
- Oracle
- PostgreSQL

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

Нажмите **Далее**.

7. **Настройка базы данных**

Этот шаг будет пропущен, если на Шаге 4 вы решили использовать уже существующую базу данных.

Принцип настройки базы данных зависит от типа используемой СУБД.

При использовании СУБД Microsoft SQL Server укажите следующие параметры:

- **Сервер БД**. NetBIOS имя сервера СУБД Microsoft SQL Server, на котором будет создана база данных.

Не задавайте в поле **Сервер БД** IP-адрес, так как в этом случае вы не сможете подключиться к серверу базы данных.

Если на сервере базы данных есть именованные экземпляры, то имя сервера нужно указывать в следующем виде: `<имя_сервера>\<имя_экземпляра>`.

- **Имя базы данных**. Имя создаваемой базы данных.

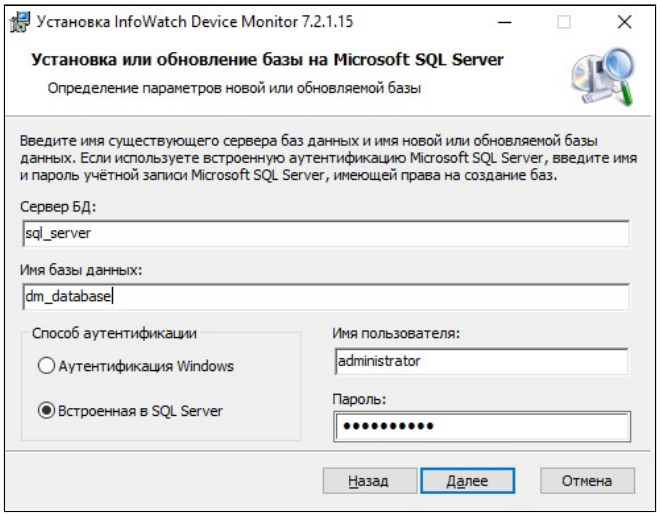
Может содержать буквы латинского алфавита, цифры и прочие символы, за исключением пробелов и специальных символов: «*», «?», «/», «\», «|», «^», «:», «"». Должно начинаться с латинской буквы.

Длина имени может составлять от 1 до 123 символов.

- **Способ аутентификации**. Способ аутентификации пользователя, от имени которого создается база данных и который будет использоваться для работы с БД. В качестве значения данного параметра укажите способ аутентификации, выбранный при подготовке учетной записи (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server").

Если учетной записи назначена аутентификация Windows, то выберите значение **Аутентификация Windows**. В этом случае процесс создания БД будет выполняться от имени доменного пользователя, выполняющего установку.

Если учетной записи назначена встроенная в SQL Server аутентификация, выберите значение Встроенная в SQL Server. Затем укажите имя и пароль подготовленной учетной записи в полях **Имя пользователя** и **Пароль** соответственно. При составлении пароля ознакомьтесь с рекомендациями в статье "Приложение А. Рекомендации по составлению имен и паролей".



Настройка базы данных Microsoft SQL Server

При использовании СУБД Oracle настройте следующие параметры:

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

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

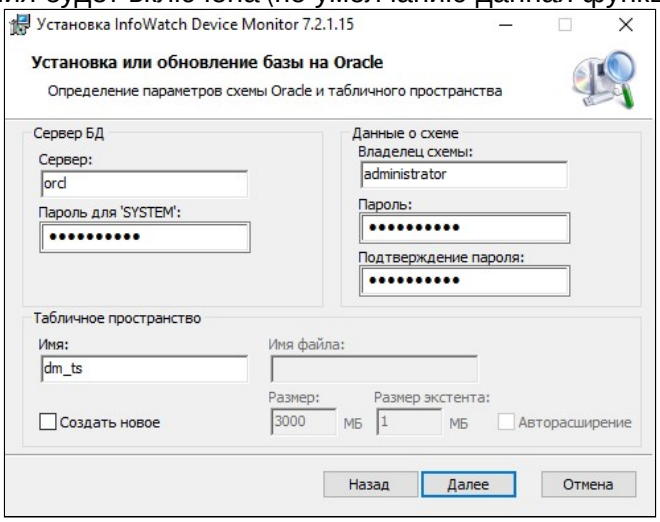
   - **Владелец схемы**. Имя учетной записи владельца схемы базы данных.
   - **Пароль, Подтверждение пароля**. Пароль учетной записи владельца схемы базы данных.

   Назначение пароля выполняется в соответствии с требованиями, указанными в документации к СУБД Oracle.
c. Настройте параметры табличного пространства в области **Табличное пространство**.

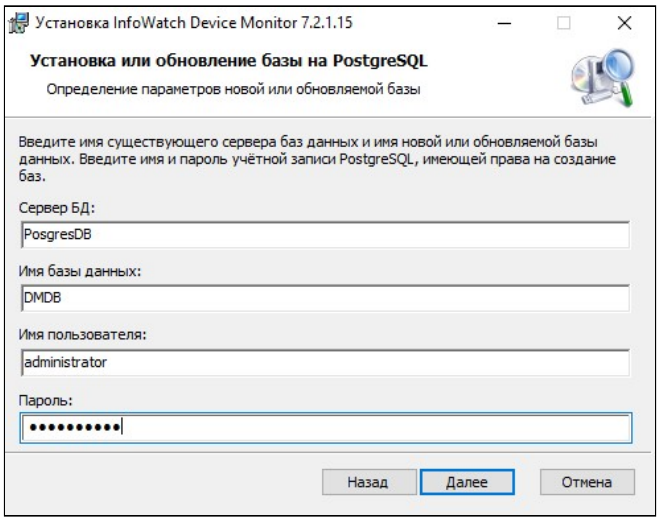
   Вы можете использовать существующее табличное пространство или создать новое. При использовании существующего табличного пространства, укажите имя табличного пространства в поле **Имя**.

   Чтобы создать новое табличное пространство, отметьте поле **Создать новое**. Затем укажите параметры табличного пространства:
   - **Имя**. Имя нового табличного пространства.
   - **Имя файла**. Имя файла данных, в котором будет храниться новое табличное пространство.
   - **Размер**. Максимальный размер (в МБ) файла данных (значение по умолчанию - 3000 МБ).
   - **Размер экстента**. Максимальный размер (в МБ) непрерывного фрагмента пространства в файле данных (значение по умолчанию - 1 МБ).
   - **Авторасширение**. Возможность автоматического расширения файла данных

средствами СУБД Oracle. Если отмечено поле **Авторасширение**, то функция авторасширения будет включена (по умолчанию данная функция отключена).



При использовании СУБД PostgreSQL укажите следующие параметры:
- **Сервер БД**. Имя сервера СУБД PostgreSQL, на котором будет создана база данных. Порт по умолчанию - 5432. Если будет использовать другой порт, необходимо его задать в формате `host:port`.
- **Имя базы данных**. Имя создаваемой базы данных.Может содержать буквы латинского алфавита, цифры и прочие символы, за исключением пробелов и специальных символов: «*», «?», «/», «\», «|», «^», «:», «"». Должно начинаться с латинской буквы.Длина имени может составлять от 1 до 123 символов.
- **Имя пользователя** - имя учетной записи, имеющей права на создание БД на PostgreSQL сервере.
- **Пароль** - пароль учетной записи, имеющей права на создание БД на PostgreSQL сервере.



После того как все необходимые параметры будут заданы, нажмите **Далее**.

8. **Настройка сетевых параметров сервера**

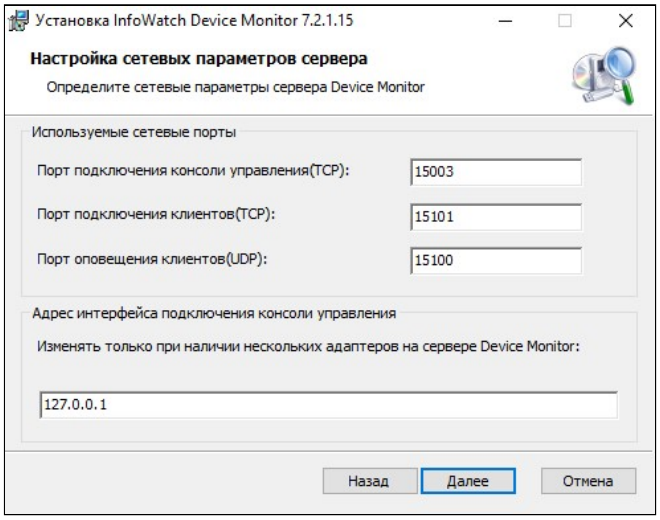
   Настройте параметры Сервера:

   a. В области **Используемые сетевые порты** задайте номера TCP и UDP портов, используемые для:
      - **подключения Консоли управления**;

- **подключения Агентов** для передачи схем безопасности на контролируемые компьютеры, отправки информации о событиях и теневых копий на сервер;
- **оповещения Агентов** об изменениях схем безопасности.

b. В области **Адрес интерфейса подключения консоли управления** укажите IP-адрес, через который будет осуществляться взаимодействие между Сервером и Консолью управления.

> **Важно!**
>
> Изменять значение данного параметра следует, только если Сервер будет установлен на компьютер с несколькими сетевыми адаптерами, подключенными к разным сетям. При наличии одного сетевого адаптера не допускается изменение данного параметра, иначе подключение Консоли управления к Серверу будет невозможно.
> Если в процессе работы на компьютер с установленным Сервером будут добавлены дополнительные сетевые адаптеры, то изменить настройку данного параметра можно в конфигурационном файле Сервера.



После того как все необходимые параметры будут указаны, нажмите **Далее**.

9. **Настройка защищенного канала**

Укажите порт, по которому будут передаваться трафик между Агентом и Сервером InfoWatch Device Monitor.

Если на Шаге 4 вы выбрали **Установить новую базу данных**, то в области **Ключ защищенного канала** выберите:

- если установка выполняется впервые - оставьте настройку **Создать новый ключ**;
- если вы использовали сервер версии 6.0 и выше и удалили его, а затем хотите опять установить, то для того, чтобы Агенты Device Monitor смогли подключиться и привязаться к новому серверу, необходимо указать ключ шифрования, который использовался на старом сервере. Рекомендации о сохранении ключа шифрования даны в разделе "Удаление InfoWatch Device Monitor". Выберите **Использовать существующий ключ** и укажите путь к файлу с имеющимся ключом шифрования.

Нажмите **Далее**.

Если была выбрана настройка **Создать новый ключ**, укажите путь, куда Система сохранит файл со сгенерированным ключом.

10. **Настройка учетной записи сервера**

    Выберите учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor, в соответствии с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor". При выборе варианта **Пользователь** укажите имя и пароль подготовленной учетной записи домена Windows. Имя задается в формате `DOMAIN\USERNAME`.
    Нажмите **Далее**.
11. **Настройка учетной записи администратора сервера**

    Укажите данные (имя и пароль) учетной записи администратора сервера. Данной учетной записи будет присвоена роль **Суперпользователь** (подробнее см. " *Infowatch Traffic Monitor. Руководство пользователя* ", статья "Управление учетными записями Консоли управления"): она используется при первом подключении к Серверу с помощью Консоли управления.
    Нажмите **Далее**.

12. **Настройка параметров соединения с сервером InfoWatch Traffic Monitor**

    Если на Шаге 4 вы решили использовать уже существующую базу данных (опция **Установить новую базу данных** не была выбрана), то этот шаг будет пропущен.
    Укажите параметры для взаимодействия с сервером InfoWatch Traffic Monitor:
    - Адрес сервера TM. Адрес сервера InfoWatch Traffic Monitor. Запись адреса должна иметь следующий формат:
      `host:port`
      Параметр host должен содержать доменное имя или IP-адрес сервера InfoWatch Traffic Monitor. Адрес сервера является стандартным URI-адресом (Uniform Resource Identifier), формальный синтаксис которого описан в RFC 3986 http://tools.ietf.org/html/rfc3986.
      В качестве параметра *port* указывается порт сервера InfoWatch Traffic Monitor, через который будет осуществляться доставка событий. По умолчанию, порт сервера InfoWatch Traffic Monitor – 9100.

      > **Важно!**
      >
      > Если планируется интеграция с Traffic Monitor версии 5.5 или ниже, используйте формат `host:port`, где `port` - 4101.

    - Количество соединений. Количество соединений с сервером InfoWatch Traffic Monitor. Вы можете задать значение от 1 до 32 соединений.
      - **Токен авторизации**. Токен для подключения к API. Необходимо указывать при работе с Traffic Monitor версии 6.0 и выше. Получите актуальный токен от администратора Traffic Monitor.
      - если в схеме развертывания Device Monitor не планируется интеграция с InfoWatch Traffic Monitor, отметьте поле **Работать в автономном режиме**. В этом случае вы можете, отметив поле **Сохранять теневые копии**, сохранять перехваченные теневые копии файлов в директорию установки сервера.

    Нажмите **Далее**.

13. **Завершение установки**

    Нажмите **Установить**, чтобы начать установку Сервера. Следуйте указаниям для завершения установки.

    > **Важно!**
    >
    > При установке на Microsoft Windows Server 2012 и Microsoft Windows Server 2012 R2, на экран будет выведено диалоговое окно **Windows Security**, которое устанавливает виртуальный принтер InfoWatch, необходимый для обработки печати из metro-приложений. Для установки виртуального принтера нажмите **Install**.

    > **Примечание:**
    >
    > Этап установки сигнатур может занимать существенное время (до получаса).

14. **Установка вспомогательного сервера**

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

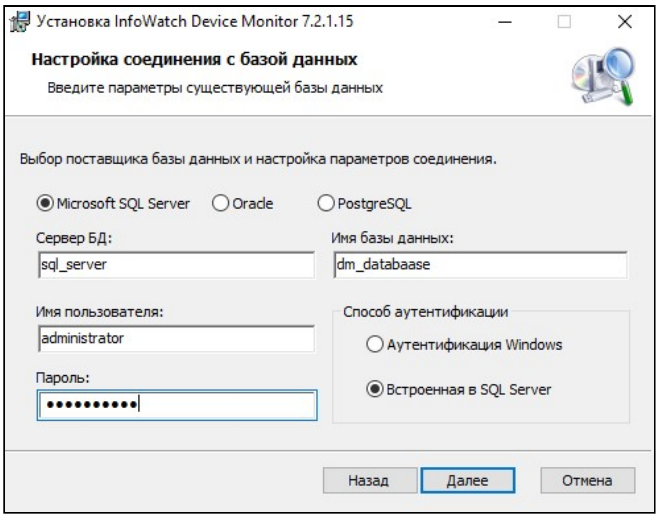
a. Запуск мастера установки
   Откройте папку с дистрибутивом Device Monitor. Затем откройте каталог `Server`. В данном каталоге найдите и запустите файл установки для требуемой платформы. В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите **Далее**.
b. Принятие лицензионного соглашения
   Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите **Далее**.
c. Выбор устанавливаемого компонента
   На шаге **Выборочная установка** по умолчанию выбраны все компоненты:
   - Сервер
   - Консоль управления
   - Сервис распространения дистрибутивов

   Если необходимо, измените состав устанавливаемых компонентов. По умолчанию все компоненты устанавливаются на одну рабочую станцию. Если вы рассчитываете использовать Консоль управления или Сервис распространения на другой рабочей станции, то вам не нужно устанавливать этот компонент: нажмите **Консоль управления** или **Сервис распространения дистрибутивов** и в раскрывшемся списке выберите пункт ✕ **Этот компонент будет полностью недоступен**.
   Вы также можете изменить папку, куда будет установлен тот или иной компонент: выберите компонент в списке, нажмите и укажите другое местоположение. При установке Сервиса распространения новый дистрибутив Агентов будет автоматически размещен в директорию с дистрибутивами.
   Нажмите **Далее**.
d. Определение параметров сервера
   На шаге **Тип устанавливаемого сервера** выберите **Вспомогательный сервер**.

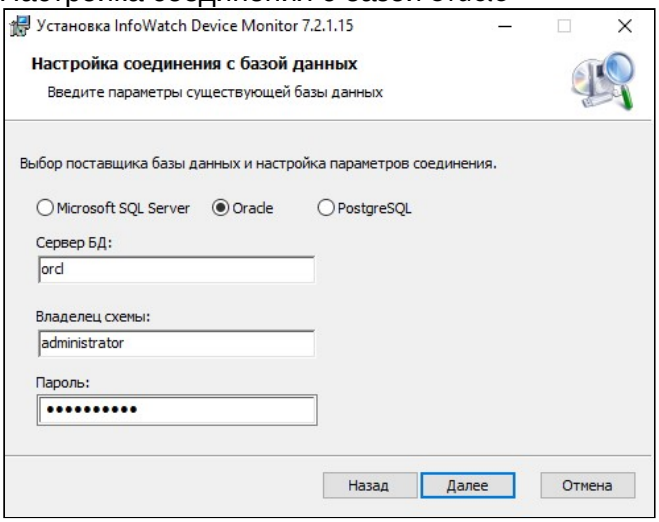
Важно!

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

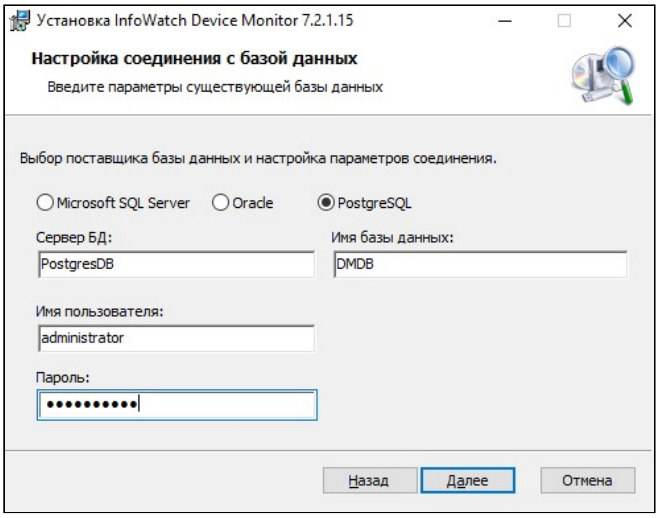
e. Настройка соединения с базой данных
Укажите СУБД, под управлением которой находится база данных Device Monitor и введите оставшиеся параметры соединения такими же, которые были использованы при установке основного сервера:
Настройка соединения с базой Microsoft SQL Server
Если учетной записи назначена аутентификация Windows, и база данных была создана от имени доменного пользователя, то выберите значение **Аутентификация Windows.** Если учетной записи назначена встроенная в SQL Server аутентификация, выберите значение **Встроенная в SQL Server** :



Настройка соединения с базой Oracle

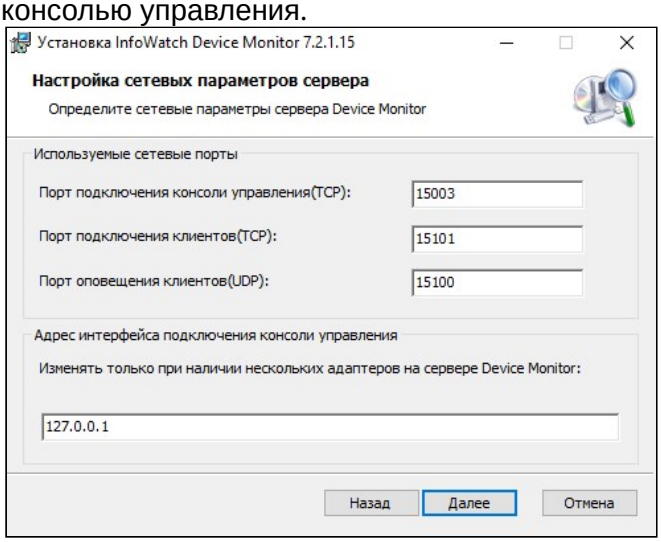


Настройка соединения с базой PostgreSQL



После того как все необходимые параметры будут указаны, нажмите **Далее**.

f. Настройка сетевых параметров сервера
Настройте параметры сервера:
В области **Используемые сетевые порты** задайте номера TCP и UDP портов, используемых для:
- подключения Консоли управления;
- подключения Агентов для передачи схем безопасности а контролируемые компьютеры, отправки информации о событиях и теневых копий на сервер;
- оповещения Агентов об изменениях схем безопасности.
В области **Адрес интерфейса подключения консоли управления** укажите IP-адрес, через который будет осуществляться взаимодействие между сервером и консолью управления.



После того как все необходимые параметры будут указаны, нажмите **Далее**.

g. Настройка учетной записи сервера
Выберите учетную запись, от имени которой будет запускаться служба Сервера InfoWatch Device Monitor, в соответствии с разделом "Рекомендации по установке Сервера InfoWatch Device Monitor". При выборе варианта **Пользователь** укажите имя и пароль подготовленной учетной записи домена Windows. Имя задается в формате `DOMAIN\USERNAME`.
Нажмите **Далее**.

h. Завершение установки
Нажмите **Установить**, чтобы начать установку сервера. Следуйте указаниям для завершения установки. Этап установки сигнатур может занять некоторое время.

Откройте папку с дистрибутивом Device Monitor

3.2.3 Установка Агента InfoWatch Device Monitor

Агент Device Monitor и Сервер Device Monitor необходимо устанавливать в одном часовом поясе. Это обеспечит отображение корректного времени перехвата события.

Важно!

Не допускается установка Агента InfoWatch Device Monitor и сервера Device Monitor на один компьютер, это может привести к неработоспособности сервера.

Если на компьютере с ОС Astra Linux 1.6 установлен Агент InfoWatch Device Monitor версии ниже 7.0, для установки Агента **обязательно** выполните следующие действия:

1. Удалите Агент InfoWatch Device Monitor;
2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 5 (20200327SE16) (см. официальную инструкцию) или Update 6 (20200722SE16) (см. официальную инструкцию).

   Примечание:

   Рекомендуется установка на ОС Astra Linux Special Edition 1.6 Update 6 (20200722SE16).

3. Установите новую версию Агента InfoWatch Device Monitor.

Агент InfoWatch Device Monitor может быть установлен на рабочие станции одним из следующих способов:

- Локальная установка. Выполняется при помощи универсальной программы установки непосредственно на каждом компьютере.
- Удаленная установка с помощью стороннего ПО. Осуществляется с использованием средств распространения программного обеспечения: например, посредством механизма групповых политик Microsoft Active Directory.
- Установка через задачи распространения. Выполняется в Консоли управления InfoWatch Device Monitor (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", раздел "Удаленная установка, обновление и удаление Агентов").
- Автоматическая установка. Выполняется в Консоли управления InfoWatch Device Monitor (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", раздел "Соединение и синхронизация со службами каталогов").

Чтобы успешно установить или обновить Агент InfoWatch Device Monitor, следуйте рекомендациям:

1. Исключите параллельное использование сторонних DLP-систем;

2. Добавьте в исключения антивируса процессы Агента InfoWatch Device Monitor (список файлов см. в статье "Список файлов Агента InfoWatch для добавления в исключения антивирусов");
3. Отключите самозащиту антивируса;
4. По возможности отключите или удалите антивирус на время установки, обновления и удаления Агента InfoWatch Device Monitor;
5. Если на рабочих станциях используется VMWare Horizon VDI 8.0.0-16530, то необходимо отключить компонент ftapihook654.dll версии 3.2.4.1. (подробнее см. "Проблема совместимости с VmWare Horizon VDI")
6. Обеспечьте доступ к портам, необходимым для работы Агента InfoWatch Device Monitor (список портов см. в "*Infowatch Traffic Monitor. Руководство администратора*", раздел "Настройка Сервера InfoWatch Device Monitor");
7. Для установления соединения убедитесь, что доменные имена сервера InfoWatch Device Monitor и машины, на которую устанавливается Агент InfoWatch Device Monitor, корректно преобразовываются (резолвятся) DNS-сервером в IP-адреса;

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

8. Если не требуется использовать компонент контроля сетевых соединений, отключите его при создании дистрибутива Агента InfoWatch Device Monitor;
9. Установите Агенты InfoWatch Device Monitor сначала на тестовые машины или небольшую группу рабочих станций;
   Если на тестовой группе в течение 2-3 дней не возникало ошибок, снижения производительности, зависания приложений, продолжайте установку на рабочие станции.

> **Важно!**
>
> Выключение питания компьютера в процессе установки/удаления Агента может привести к ошибкам, ведущим к нестабильной работе операционной системы.

> **Важно!**
>
> При установке, обновлении и удалении Агента выполняется кратковременный разрыв всех сетевых соединений. Это связано с установкой компонентов контроля сетевого трафика, используемых в Device Monitor (IWPROXY и IWNBG). Кроме того, разрыв связан как с технологическими особенностями ОС при установке модулей, так и с принудительным перезапуском сетевых карт при установке модуля «прозрачная прокси».

Важно!

В процессе установки Агента будут закрыты (если они были запущены) программы Mozilla Firefox и Mozilla Thunderbird.

Примечание:

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

Примечание:

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

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

Примечание:

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

Локальная установка Агента

Важно!

Настоятельно не рекомендуется устанавливать Агенты InfoWatch Device Monitor на компьютеры с одинаковыми именами. Такие компьютеры будут зарегистрированы как один компьютер и, соответственно, на них будет распространяться одна политика, будет вестись единая регистрация событий и т.д.

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

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью msi-пакета с последующим вводом параметров вручную:

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

каталог `Client`. В данном каталоге найдите и запустите пакет установки для требуемой платформы для развёртывания в соответствии с заданными при формировании пакетов параметрами, например, `InfoWatch.DeviceMonitor.Client.7.4.1.x64.msi.cmd.`
В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor Client. Нажмите на кнопку **Далее**, чтобы перейти к следующему окну мастера установки.

2. **Выбор каталога для установки**
   Укажите путь к каталогу, в который будет установлен **Агент**.

   > **Важно!**
   >
   > Путь к каталогу может содержать следующие символы: 0-9,a-z,A-Z, ":", ".", "_", "-", "\", " ". При наличии в пути других символов, установка Агента будет некорректной.

   Нажмите кнопку **Далее**.
3. **Настройка параметров**
   Укажите параметры соединения с Сервером InfoWatch Device Monitor:
   - **Сервер**. Имя сервера InfoWatch Device Monitor.
   - **Порт**. Номер порта, используемого для соединения между Агентом и Сервером InfoWatch Device Monitor (по умолчанию задан порт 15101).

   Нажмите кнопку **Далее**.
4. **Завершение установки**
   После перехода к окну **Подтверждение установки**, нажмите кнопку **Далее,** чтобы начать установку Агента. Следуйте дальнейшим указаниям мастера для завершения установки. По окончании установки перезагрузите компьютер.

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью cmd-пакета, уже содержащего параметры установки:

1. **Вход в командную строку Window**
   Запустите командную строку (cmd.exe) от имени Администратора.
2. **Запуск скрипта**
   a. Перейдите в каталог, где находится скрипт установки:
   `cd <путь_до_скрипта>`
   b. Запустите скрипт, полностью указав его имя, например:
   `InfoWatch.DeviceMonitor.Client.7.4.1.x64.msi.cmd`
   c. Будет запущена установка без графического интерфейса в тихом режиме и без оповещений. Дождитесь окончания установки, после чего будет сформирован лог-файл с подробной информацией.

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

> **Важно!**
>
> Если на компьютере под управлением ОС Astra Linux установлен Агент InfoWatch Device Monitor версии ниже 7.0, для установки Агента новой версии **обязательно** выполните следующие действия:

1. Удалите Агент InfoWatch Device Monitor;
2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 6 (20200722SE16) (см. официальную инструкцию);
3. Установите новую версию Агента InfoWatch Device Monitor.

Примечание:

Если на компьютере установлена кастомизированная версия системы SeLinux, корректная установка Агента не гарантируется.

Для Агентов на компьютерах под управлением РЕД ОС не поддерживается совместная работа с антивирусами.

1. **Подготовка к установке:**
   a. Если на компьютере под управлением ОС Astra Linux ранее было установлено обновление безопасности (например, Update 5):
      i. Узнайте текущую версию ядра Astra Linux (например, **4.15.3-2-generic**):
      `uname -r`
      ii. Проверьте, что директория */boot* не содержит старых пакетов ядра с более ранней версией, чем в предыдущем шаге (например, **initrd.img-4.15.3-1-generic** или **initrd.img-4.15.3-1-hardened.**
      iii. Удалите такие пакеты при наличии:
      `apt-get purge linux-image-4.15.3-1`
      iv. Удалите неиспользуемые Системой пакеты:
      `apt-get autoremove`
      `apt-get autoclean`
   b. Скопируйте на целевой компьютер архив, в котором содержаться пакет и скрипты для установки и удаления Агента Device Monitor. Архив поставляется в составе дистрибутива. Название архива может отличаться в зависимости от используемой ОС:
      - `Setup.AstraLinuxSE-1.6-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.6;
      - `Setup.AstraLinuxCE-2.12-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Common Edition 2.12;
      - `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz` - для РЕД ОС 7.3.1.

      x.x.x.xx - номер сборки.

      Примечание:

      Далее будет рассмотрен пример установки и удаления Агента на ОС Astra Linux Special Edition 1.6. Установка и удаление на других поддерживаемых ОС аналогичны.

      В нашем примере:
      `Setup.AstraLinuxSE-1.6-iwdm.x64.7.4.1.62.tar.gz`
   c. На целевом компьютере перейдите в директорию, в которую скопирован архив, и введите команду для распаковки:

`sudo tar -xvzf Setup.AstraLinuxSE-1.6-iwdm.x64.7.4.1.62.tar.gz`
В результате будут созданы файлы `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<версия_агента>.deb`.

2. **Установка Агента InfoWatch Device Monitor:**
   a. Перейдите в директорию, в которую распаковано содержимое архива **`Setup.AstraLinuxSE-1.6-iwdm.x64.7.4.1.62.tar.gz`**.
   b. Для установки Агента запустите скрипт, выполнив команду:
   `sudo ./install.sh <сервер>:<порт>`
   где `<сервер>` - ip-адрес или доменное имя Сервера Infowatch Device Monitor, `<порт>` - порт подключения к Серверу Infowatch Device Monitor.
   В нашем примере команда будет следующей:
   `sudo ./install.sh <dm-server>:<15101>`
   Продукт будет установлен в директорию `/opt/iw/dmagent`.
   c. Проверить статус сервисов можно командой:
   `sudo systemctl status iwdm*`

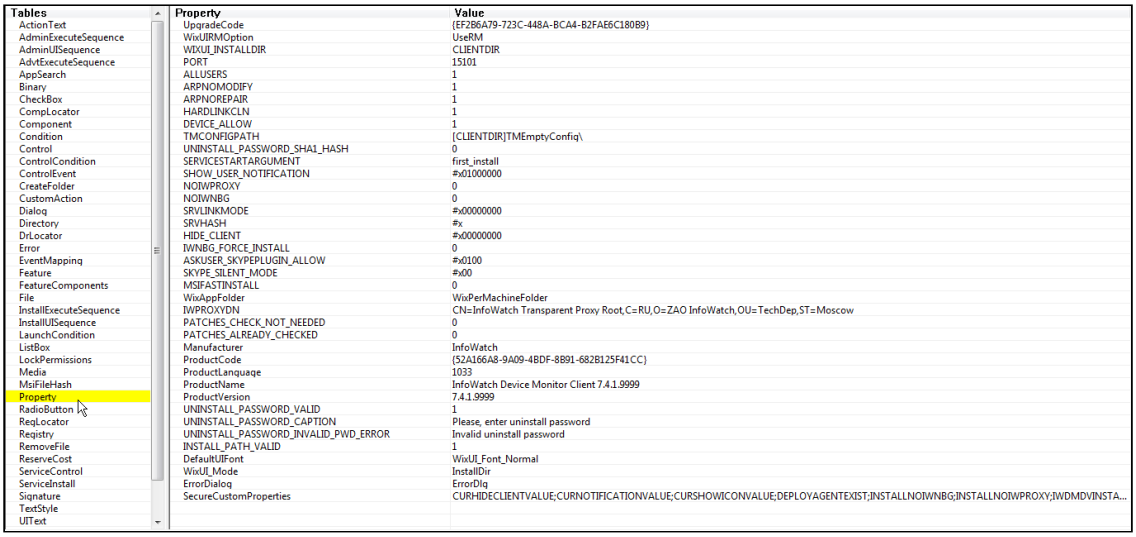
Установка Агента с помощью средств распространения программного обеспечения

Установка Агента на компьютеры может выполняться администратором корпоративной сети централизованно, с помощью средств распространения программного обеспечения. В настоящем разделе описывается пример такой установки посредством Microsoft Active Directory.

Установка Агента через Microsoft Active Directory осуществляется посредством механизма групповых политик. Для установки необходимо выбрать такую групповую политику, которая распространяется на все компьютеры, подлежащие контролю при помощи Агента. Это может быть политика, назначенная:

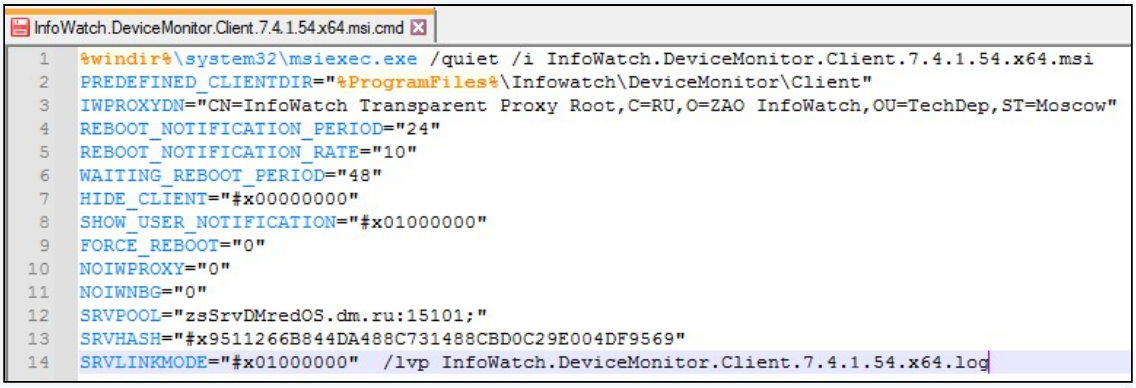
- контейнеру Active Directory, содержащему все компьютеры, на которые будет выполняться установка Агента.
- всему домену Active Directory, но не являющаяся доменной политикой по умолчанию (*Default Domain Policy*). Распространение этой политики должно быть назначено только той группе, которая включает в себя все компьютеры, подлежащие контролю при помощи Агента.

1. **Создание инсталляционного пакета**
   a. Создайте установочный cmd-пакет, например, `InfoWatch.DeviceMonitor.Client.7.4.1.x64.msi.cmd` (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", статья "Создание пакета установки").
   b. Разместите установочный пакет в сетевом каталоге, доступном для чтения всем компьютерам домена, на которые будет установлен Агент.
2. **Создание файла трансформации**
   a. Откройте установочный файл `InfoWatch.DeviceMonitor.Client.7.4.1.x64.msi` в редакторе таблиц баз данных (например, Orca) и перейдите в таблицу **Property**:



b. Выберите в главном меню **Transform → New Transform**

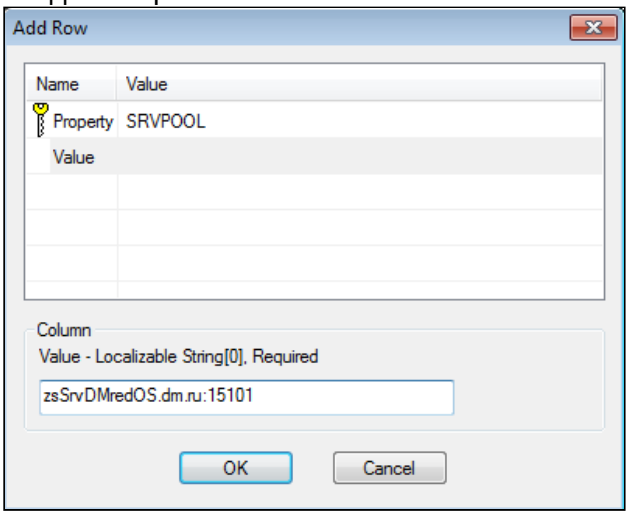
c. Откройте в текстовом редакторе ранее полученный cmd-пакет `InfoWatch.DeviceMonitor.Client.7.4.1.x64.msi.cmd`.



d. В таблице **Property** добавьте отсутствующие свойства или замените старые значения новыми из cmd-пакета. Чтобы добавить новое свойство:

   i. Кликните на пустой строке таблицы.

   ii. Введите пары значений <имя свойства>=<"новое значение"> и нажмите **Ок**



   iii. Чтобы заменить значение свойства, выберите значение двойным кликом мыши, введите новое значение и нажмите **Enter**. Выполните эти операции для всех свойств из cmd-пакета.

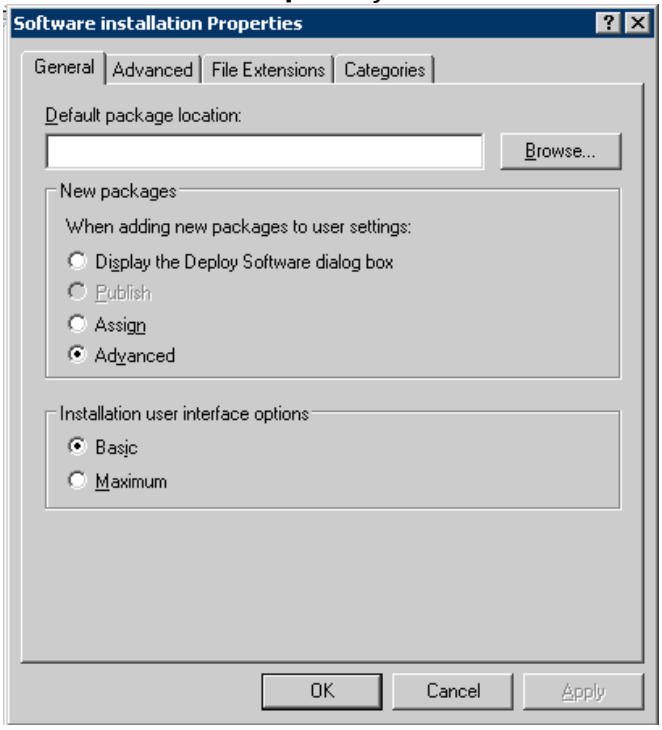
e. Перейдите в главном меню **Transform → Generate Transform**
f. Сохраните mst-файл трансформации.

3. **Редактирование групповой политики**

Перед установкой Агента средствами Active Directory необходимо отредактировать используемую групповую политику.

Чтобы отредактировать групповую политику:

a. Откройте оснастку **Active directory users and computers** (**Start** > **Settings** > **Control Panel** > **Administrative tools** > **Active directory users and computers**).
b. В дереве консоли выберите контейнер Active Directory, содержащий все компьютеры, на которые будет выполняться установка Агента.
c. Откройте оснастку **Group Policy**. Для этого в контекстном меню контейнера Active Directory выберите команду **Properties**. Затем в открывшемся диалоговом окне перейдите на вкладку **Group policy**. На данной вкладке выберите объект групповой политики и нажмите на кнопку **Edit**.
d. В дереве консоли выберите расширение **Software Installation** (**Computer Configuration** > **Software Settings**).
e. В контекстном меню расширения **Software Installation** выберите команду **Properties**. В открывшемся диалоговом окне на вкладке General выполните следующие настройки (см. рисунок):
- на панели **New packages** установите значение **Advanced**;
- на панели **Installation user interface options** установите значение **Basic**.



f. По окончании настройки нажмите на кнопку **OK**.

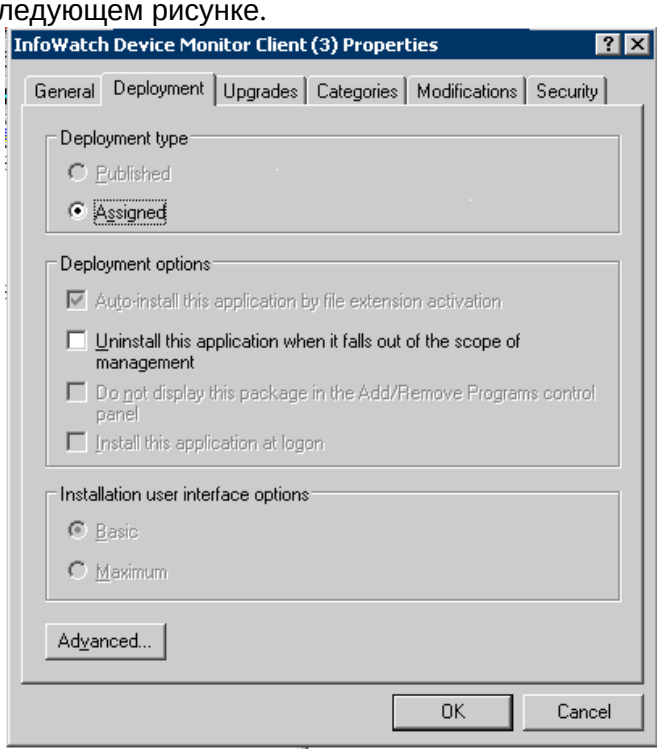
4. **Подготовка задания на установку Агента**

Создание и настройка задания на установку Агента выполняется в окне **Group Policy Object Editor**:

a. После того как окно **Group Policy Object Editor** будет открыто, в дереве консоли выберите расширение **Software Installation** (**Computer Configuration** > **Software Settings**). Щелкните правой кнопкой мыши по названию выделенного пункта и в раскрывшемся контекстном меню выберите пункт **New** > **Package**.
b. В открывшемся диалоговом окне **Open** укажите mst-файл трансформации (установочный пакет .msi должен быть предварительно размещен в сетевом каталоге, доступном для чтения всем компьютерам домена, на которые будет установлен Агент).

> **Примечание:**
>
> Некоторые системы распространения поддерживают возможность указания параметров развёртывания. В этом случае можно использовать сам cmd-пакет клиентского модуля `InfoWatch.DeviceMonitor.Client.7.4.1.x64.msi.cmd` для передачи системе распространения.

c. Выполните настройку свойств нового пакета:
- Убедитесь, что установки, заданные на вкладке **Deployment**, соответствуют показанным на следующем рисунке.



- После того как все необходимые настройки будут заданы, нажмите на кнопку **OK**.
d. В дереве консоли выберите каталог **Computer Configuration** > **Administrative templates** > **System** > **Scripts**. В области сведений выберите параметр **Run logon scripts synchronously**. Затем в окне свойств данного параметра установите значение **Enabled**.

5. **Выполнение установки**

Добавленное задание отображается в списке заданий оснастки **Software Installation**.

Задание выполняется при первой перезагрузке компьютера, на который должен быть установлен Агент. Запуск службы InfoWatch Device Monitor Client осуществляется автоматически сразу после установки.
Способ установки отображается в столбце **Deployment state**. Состояние **assigned** означает, что установка осуществляется принудительно, т.е. без учета мнения пользователя, работающего за компьютером, на который выполняется установка Агента. Состояние **published** соответствует установке с запросом согласия от пользователя.

> **Важно!**
>
> Вы можете проверить успешность установки Агента в Консоли управления InfoWatch Device Monitor. Все компьютеры, на которые Агент был успешно установлен, должны отображаться в списке раздела **Группы компьютеров**. Чтобы просмотреть список всех контролируемых компьютеров, воспользуйтесь кнопкой **Показать все компьютеры**, расположенной в верхней части Панели навигации. Чтобы получить актуальные сведения об установленных Агентах, воспользуйтесь кнопкой **Обновить**, расположенной на панели инструментов.

3.3 Предустановленные серверные параметры

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

Директории установки Системы (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
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 7.4 на ОС Astra Linux поддерживается обновление **только** с версии **7.4.x** до **7.4.y**. 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:

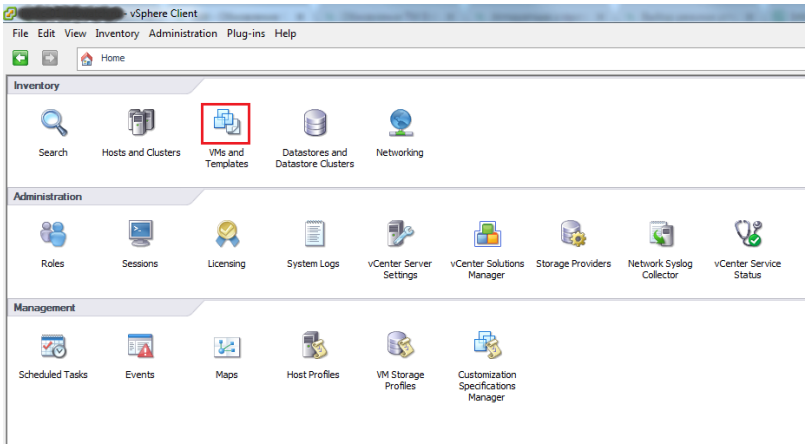
- какой тип установки в Системе (могут быть типы *Все-в-одном (All-in-one)* и *Распределенная установка*) - данная информация понадобится для выбора инструкции по обновлению;
- на каком сервере установлен пакет `web-gui` - данная информация понадобится для очистки кеша сервера после обновления схемы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

До начала обновления выполните следующие действия:

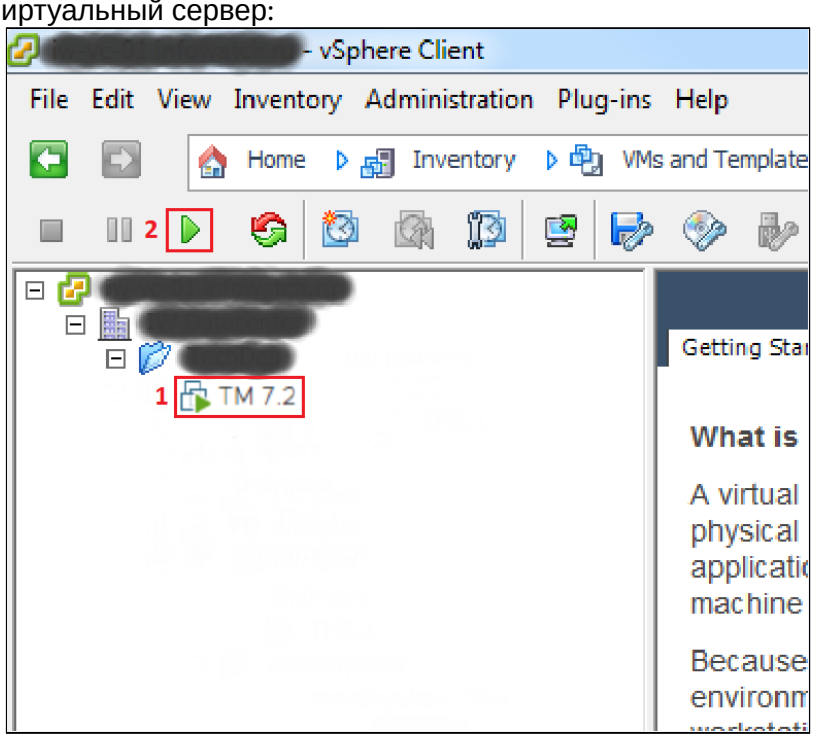
1. Включите (если он был выключен) каждый сервер, предназначенный для обновления:
   - в случае физического сервера - нажмите кнопку включения, расположенную на корпусе сервера (подробнее см. в инструкции к серверу);
   - в случае виртуального сервера - выполните команду **Power On** (см. пример ниже).

   > **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.

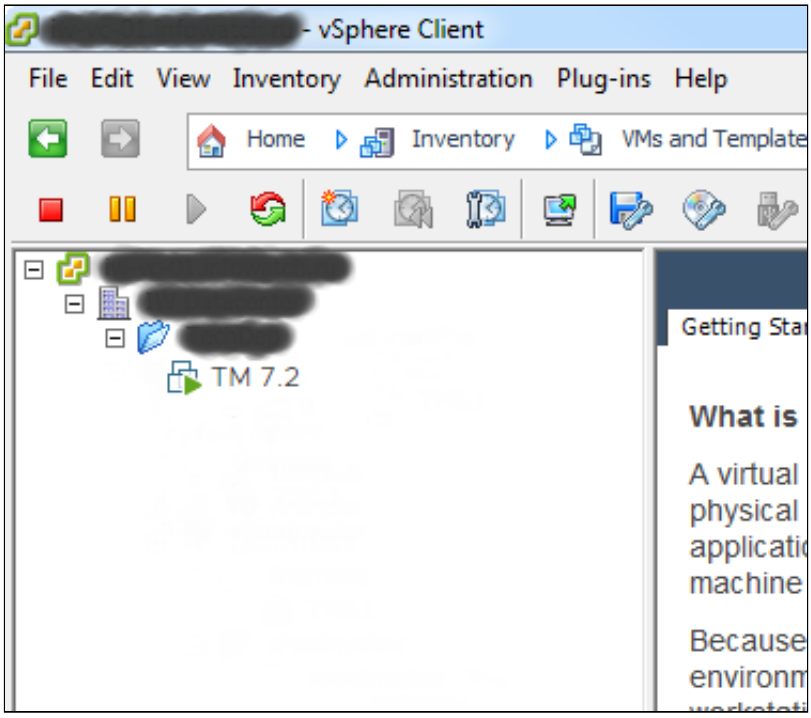
   Запустите клиентское приложение VMware vSphere Client от имени администратора (щелкните правой кнопкой мыши на иконке приложения и выберите **Запуск от имени администратора**). Войдите в приложение, используя логин и пароль, выданные администратором вашей информационной сети. Перейдите в раздел с виртуальными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

Примечание:

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

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

Важно!

Перед обновлением Traffic Monitor рекомендуется сначала обновить сервер Device Monitor.

Поддерживается **только** обновление с версии **7.4.x** до **7.4.y**. Обновление с версий ниже 7.4.0 не поддерживается.

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": "7.4.0.140",
"all_in_one": true,
```

   Запись из примера соответствует серверу с типом установки *Traffic Monitor Enterprise All-in one* и версией *7.4.0.140*.
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-7.4.2.190-astra-smolensk-1.7`**;
   - **`iwtm-postgresql-11.10-7.4.2.190-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-7.4.2.190-astra-smolensk-1.7`
4. Для обновления пакетов введите команду:
   `sudo apt-get update`
5. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor.
   В нашем примере:
   `cd /distr`
6. 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:

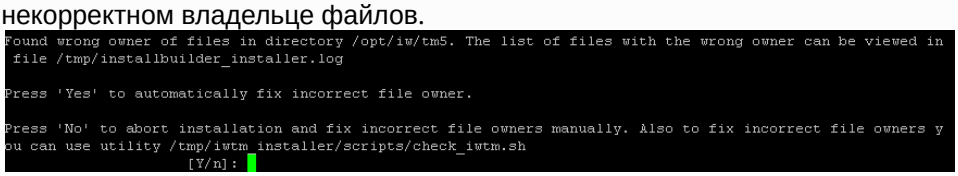
- **обновление в текстовом режиме в консоли сервера**

  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-7.4.2.190-astra-smolensk-1.7`
  Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

Примечание:

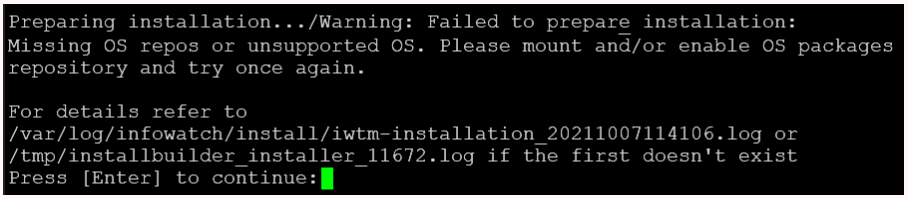
Перед запуском инсталлятора может быть выведено предупреждение о некорректном владельце файлов.



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!

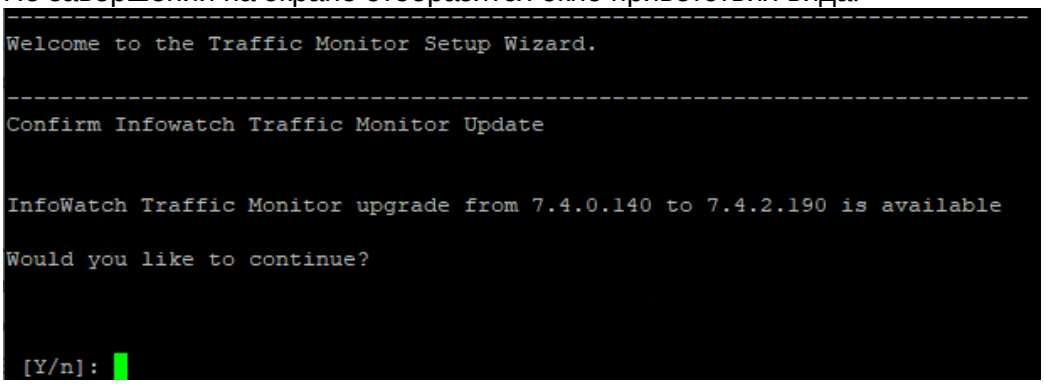
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



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**.

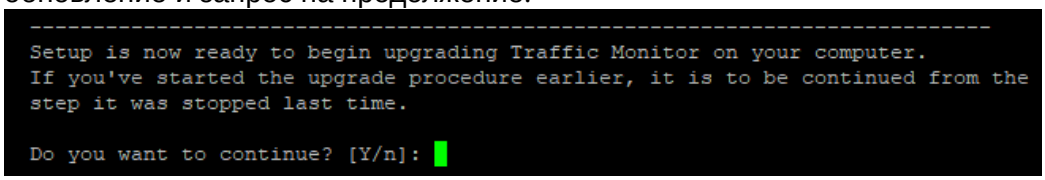
> **Примечание:**
>
> При обновлении в консоли сервера перед полем ввода в квадратных скобках цифрой или заглавной буквой указано значение по умолчанию. Оно будет использовано, если оставить поле ввода пустым и нажать **Enter**.

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.

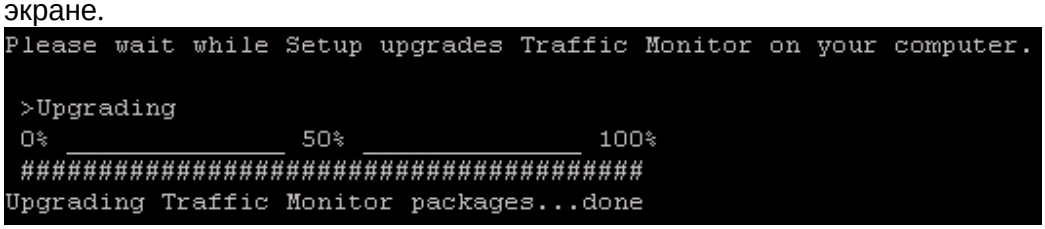
   Для выбора введите цифру, указанную напротив выбранного варианта, и нажмите **Enter**.

> **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:
>
> ```
> \Warning: You should run 'iwtm start' command manually after fixing problems with
> Consul.
> Press [Enter] to continue:
> ```
>
> Для завершения работы инсталлятора нажмите **Enter**.
>
> **Для корректной работы Системы выполните проверку и настройку кластера службы Consul**
>
> i. Запустите службу Consul, выполнив команду:
> `systemctl start iwtm-consul`
> Проверить статус службы можно командой:
> `systemctl status iwtm-consul`
> ii. Чтобы проверить службу Consul выполните команды:
> 1. Для вывода IP-адреса основного сервера (лидера) кластера:
> `curl --noproxy 127.0.0.1 http://127.0.0.1:8500/v1/status/leader ; echo`
> 2. Для вывода информации о членах кластера:
> `consul members`

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

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

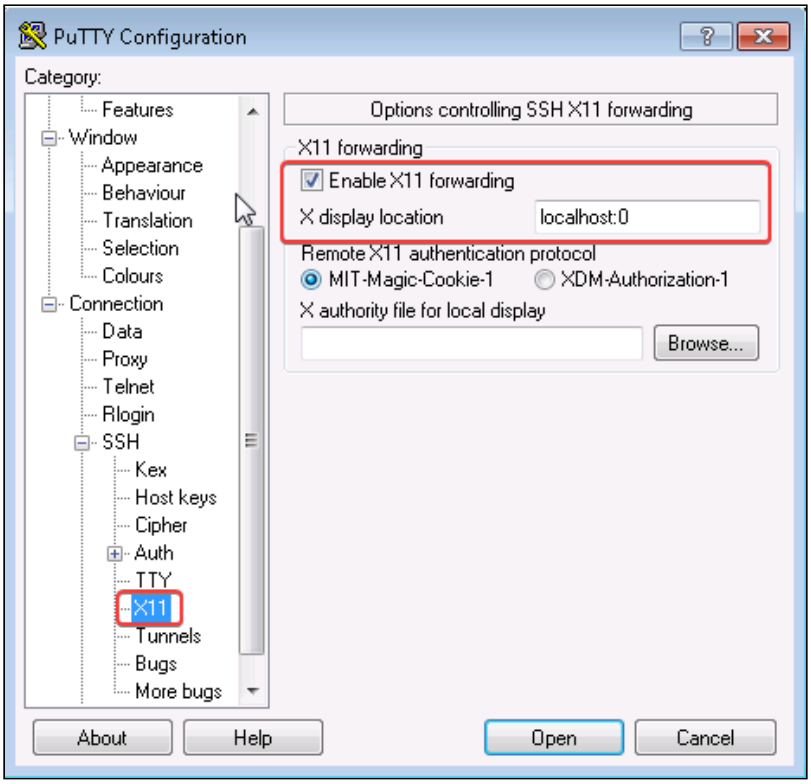
h. Перед завершением работы инсталлятор предложит удалить пакеты, созданные для обновления.
Если обновление прошло успешно, данные рекомендуется удалить.
i. Дождитесь завершения работы инсталлятора.

- **обновление с использованием графического режима инсталлятора**

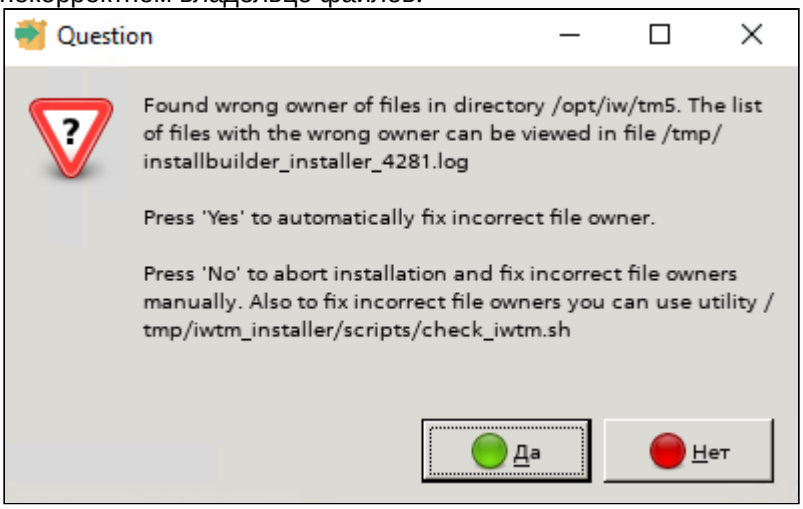
В ОС оконная система X Window System использует клиент-серверную модель. Для запуска инсталлятора в графическом режиме используется перенаправление графического вывода удаленной подсистемы (**X11 Forwarding**). Это позволит работать напрямую с графическими приложениями среды Linux на компьютере, с которого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



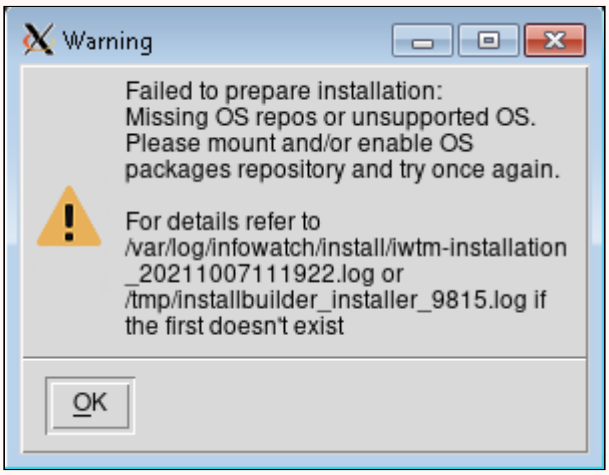
e. Запустите инсталлятор, выполнив следующую команду:
`sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
В нашем примере команда будет следующей:
`sudo ./iwtm-installer-7.4.2.190-astra-smolensk-1.7`
Начнется подготовка к запуску инсталлятора. На данном этапе не производится распаковка файлов.

> **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!

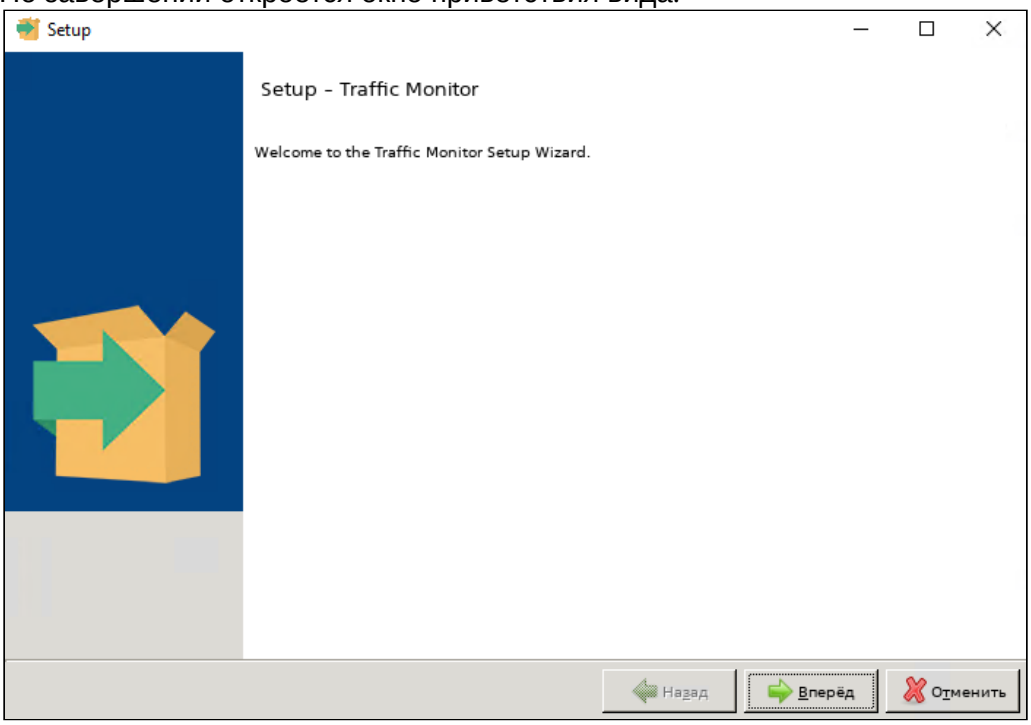
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



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.

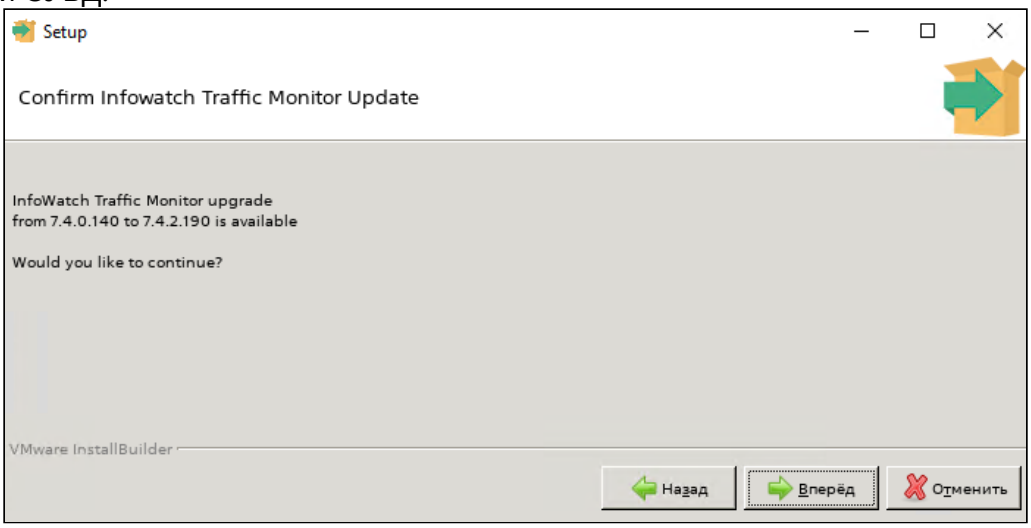
Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

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.



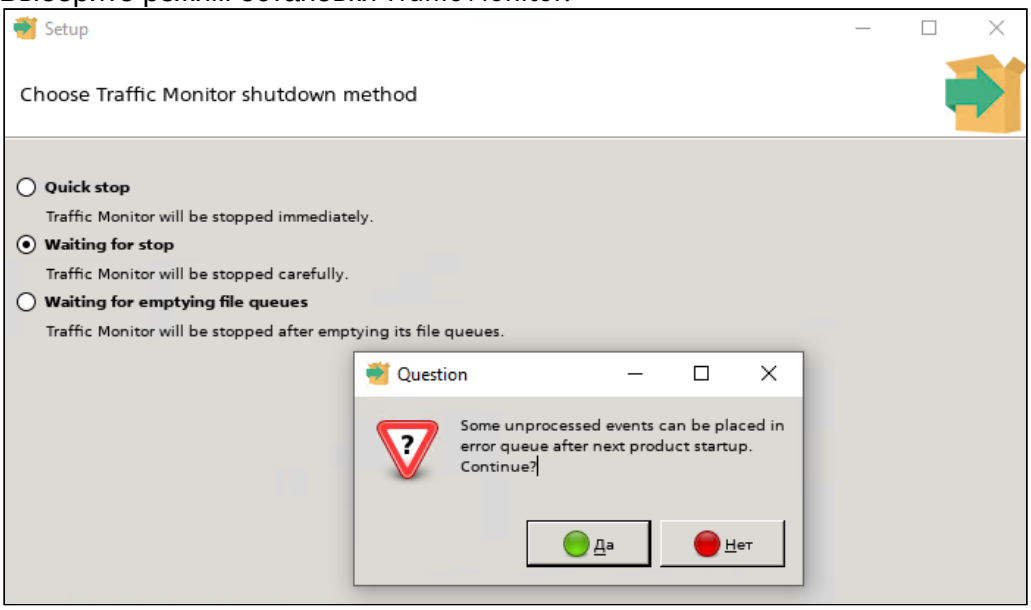
Для продолжения нажмите **Вперед**.

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:



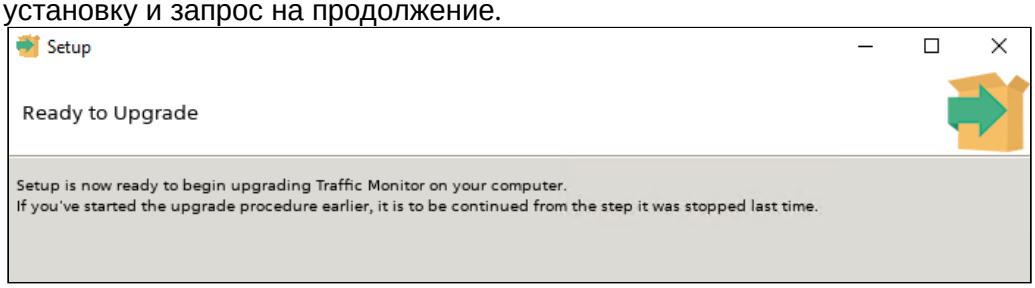
- `Quick stop` - быстрая остановка без обработки событий;
- `Waiting for stop` - перед остановкой дождаться завершения текущей обработки событий;
- `Waiting for emptying file queues` - перед остановкой дождаться обработки всех событий и очистки файловых очередей.

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

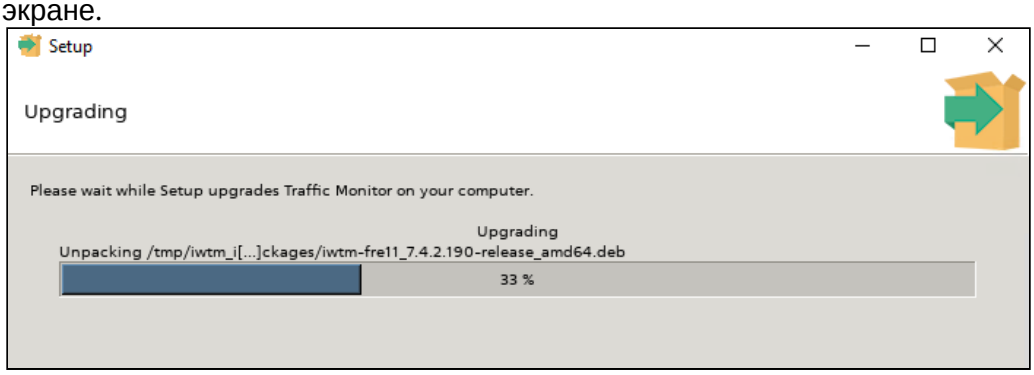
> **Примечание:**
>
> Если выбран `Quick stop`, остановленные сервисы до запуска будут иметь статус `failed (failed)`.

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!

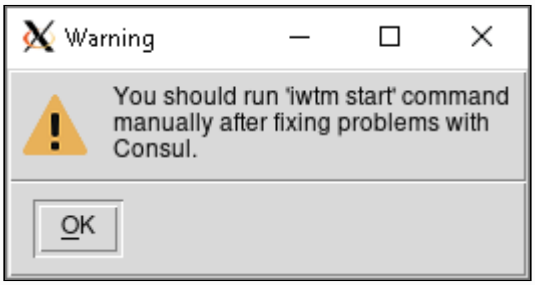
После обновления настройки системы мониторинга Nagios были изменены на значения по умолчанию. Если до обновления конфигурационные файлы Nagios редактировались, в директории `/etc/infowatch/nagios/iwmon` будут созданы их копии с расширением `.saved`. Перед запуском сервисов Traffic Monitor перенесите 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-7.4.2.190-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:

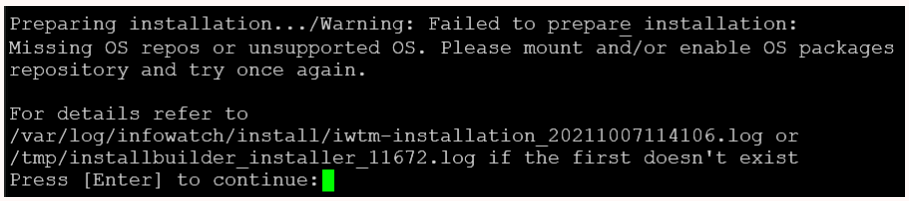
- `none` - в процессе работы инсталлятор не выводит на экран никакую информацию и не требует взаимодействия с пользователем;
- `minimal` - отображает прогресс обновления, не требует взаимодействия с пользователем;
- `minimalWithDialogs` - отображает прогресс обновления, также в процессе могут появляться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

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

```
./iwtm-installer-7.4.2.190-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`

7. 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").

8. 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").
9. 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.

10. Введите команду для очистки кеша:
    `redis-cli flushall`
11. 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 рекомендуется сначала обновить сервер Device Monitor.

Поддерживается **только** обновление с версии **7.4.x** до **7.4.y**. Обновление с версий ниже 7.4.0 не поддерживается.

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": "7.4.0.140",
  "all_in_one": false,
  "templates": {
    "db": {
      "local": true
```

```
    },
    "indexer": {},
  }
}
```

Запись из примера соответствует серверу с *распределенной* установкой *Traffic Monitor Enterprise* версии *7.4.0.140*. 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:

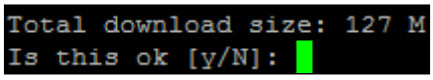
1. Создайте директорию, в которой будет располагаться инсталлятор InfoWatch Traffic Monitor. Например, для создания директории с именем `distr` в корне файловой системы выполните следующую команду:
   `sudo mkdir /distr`
2. Скопируйте в созданную директорию файлы, поставляемые в дистрибутиве InfoWatch 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-7.4.2.190-astra-smolensk-1.7**;
- **iwtm-postgresql-11.10-7.4.2.190-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-7.4.2.190-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. На сервере с шаблоном База данных перед запуском инсталлятора рекомендуется запустить сервис базы данных, если ранее он был остановлен:
`service postgresql start`
9. Введите команду для перехода в директорию с дистрибутивами Traffic Monitor:
`cd /root`
10. 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/`

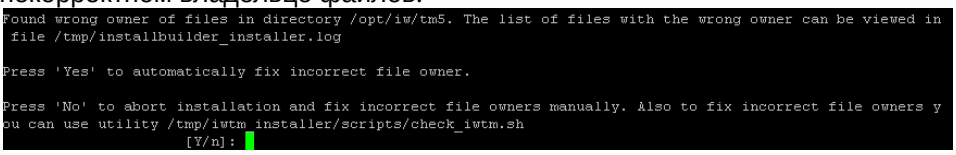
`iwtm-install-7.4.2.190-2022-09-10_09-56-25.log`.
Также информацию о процессе можно найти в директории `/var/log/infowatch/config_merge/`.
Если во время действий с конфигурационным файлом будут обнаружены ошибки, процесс будет остановлен до исправления ошибок пользователем. После исправления ошибок повторно запустите обновление.

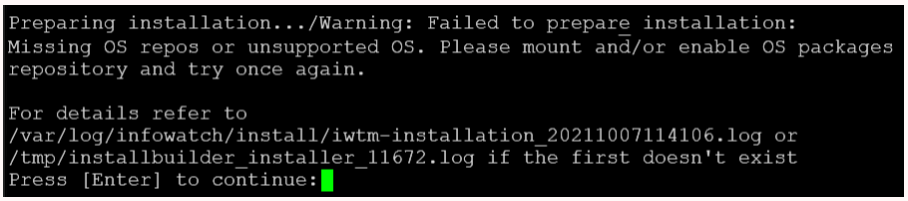
Запустите инсталлятор в одном из режимов:

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

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

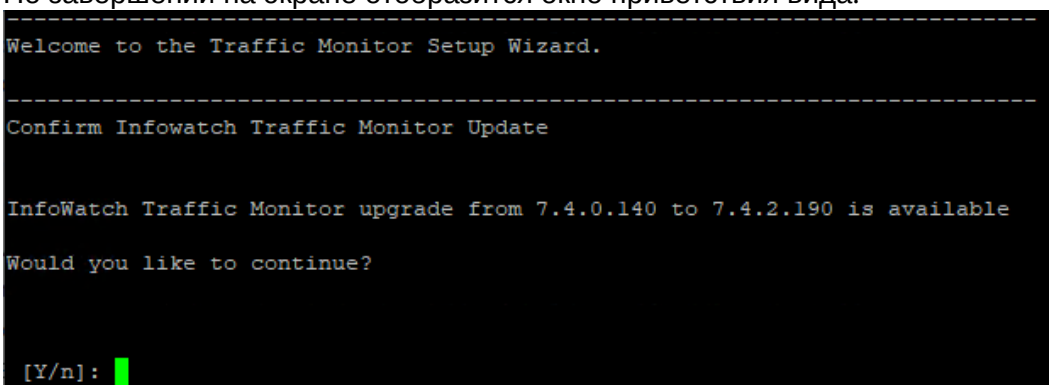
  a. Для обновления Traffic Monitor запустите инсталлятор, выполнив следующую команду:
  `sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
  В нашем примере команда будет следующей:
  `sudo ./iwtm-installer-7.4.2.190-astra-smolensk-1.7`
  Начнется подготовка к запуску инсталлятора. На данном этапе не 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. 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.

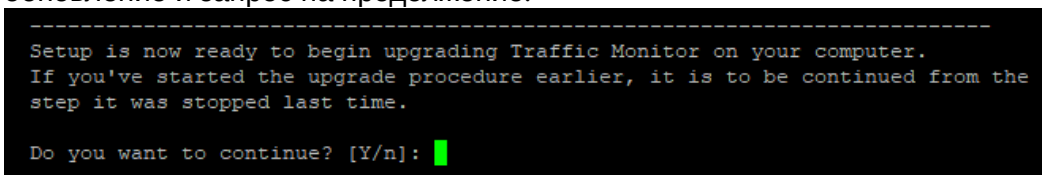
> **Важно!**
>
> Если компоненты перехвата и компоненты анализа (`iw_cas` , `iw_pas`) используются на разных серверах, остановка перехватчиков с очисткой файловых очередей может зависнуть. Рекомендуется использовать другие режимы или остановить компоненты вручную.

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

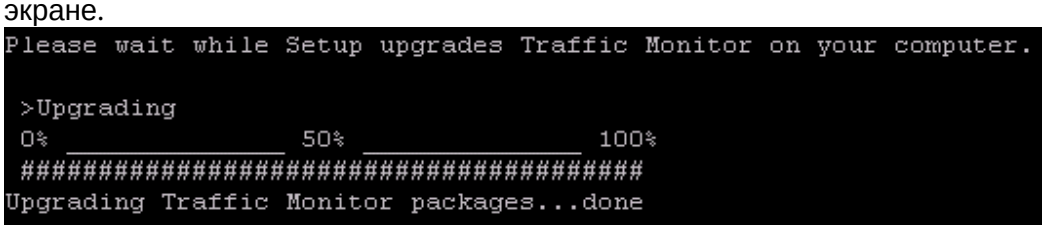
> **Примечание:**
>
> Если выбран `Quick stop` , остановленные сервисы до запуска будут иметь статус `failed (failed)` .

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:
>
> ```
> \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.

> **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:

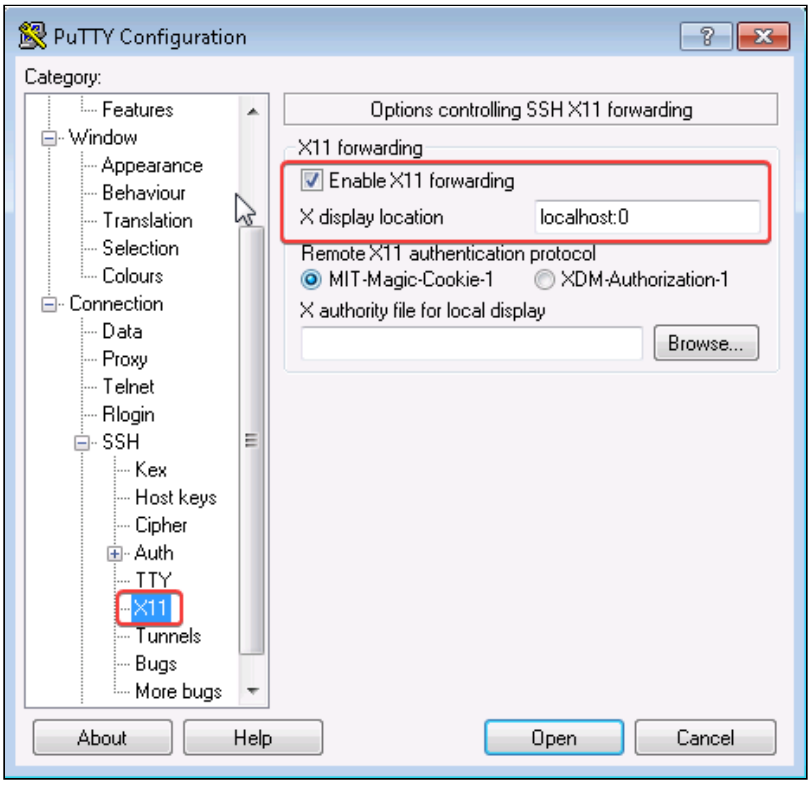
  a. На обновляемом сервере:

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

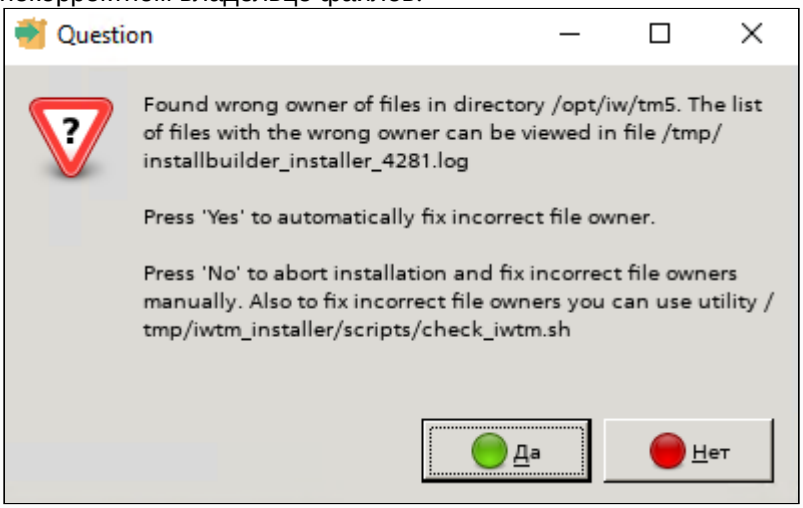


e. Для обновления Traffic Monitor запустите инсталлятор, выполнив следующую команду:
`sudo ./iwtm-installer-x.x.x.xxx-astra-smolensk-1.7`
В нашем примере команда будет следующей:
`sudo ./iwtm-installer-7.4.2.190-astra-smolensk-1.7`

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

Примечание:

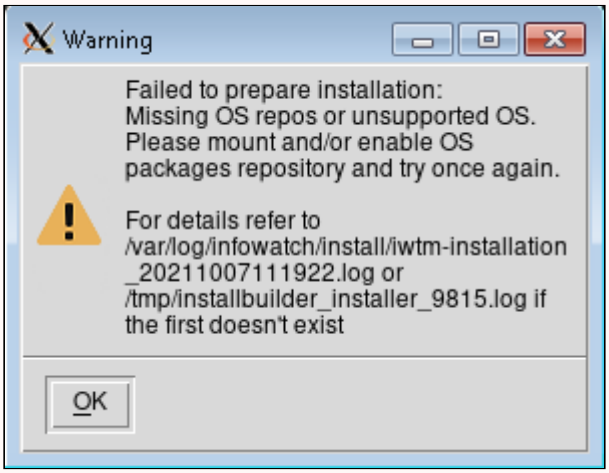
Перед запуском инсталлятора может быть выведено предупреждение о некорректном владельце файлов.



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!

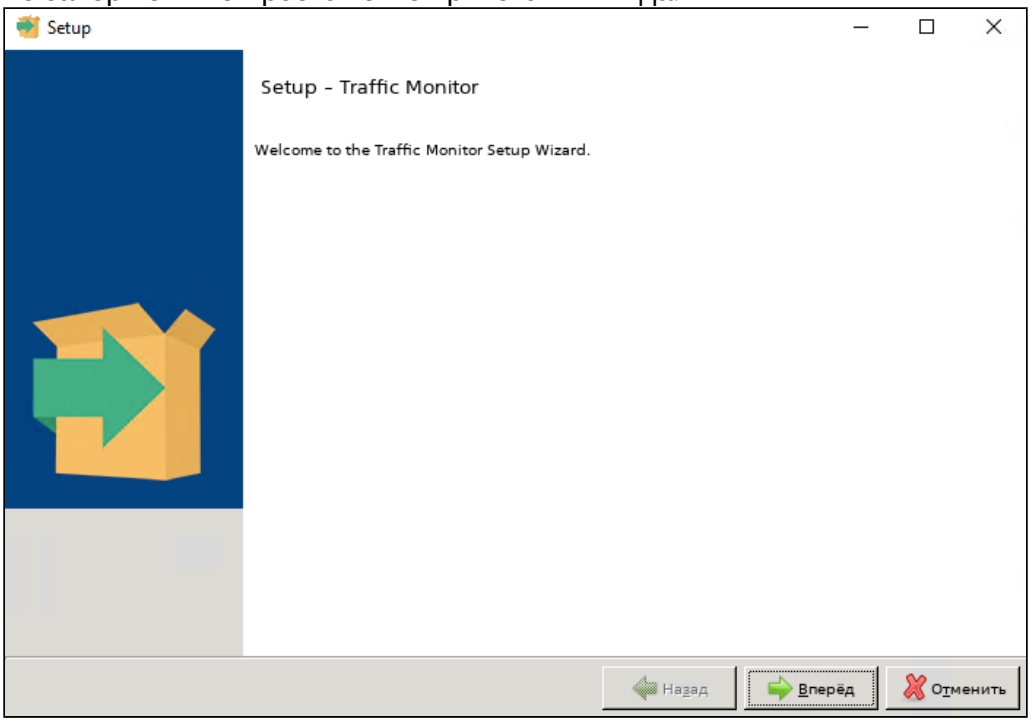
При отсутствии настроенных и доступных репозиториев ОС, запуск инсталлятора прервется со следующей ошибкой:



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.

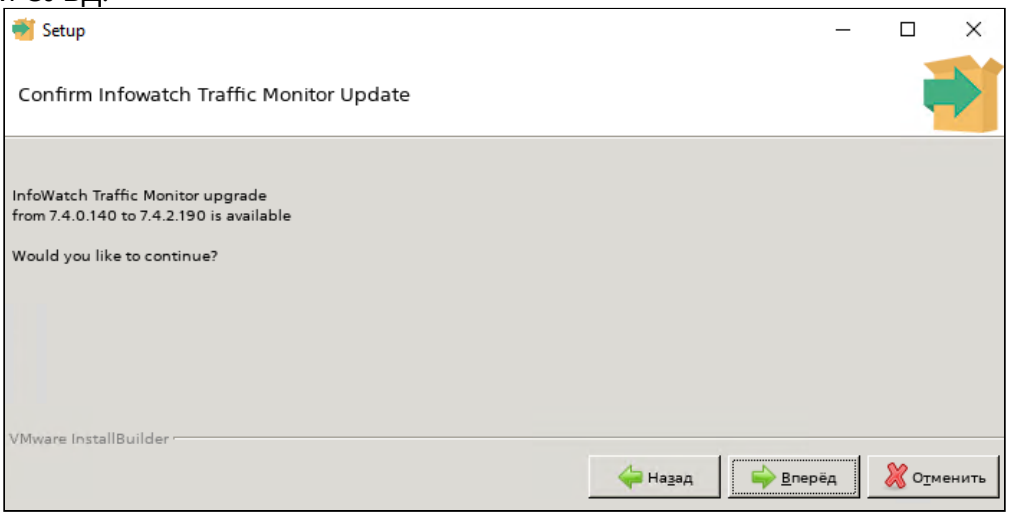
Подробную информацию об ошибке вы можете найти в лог-файлах, указанных в предупреждении.

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**.

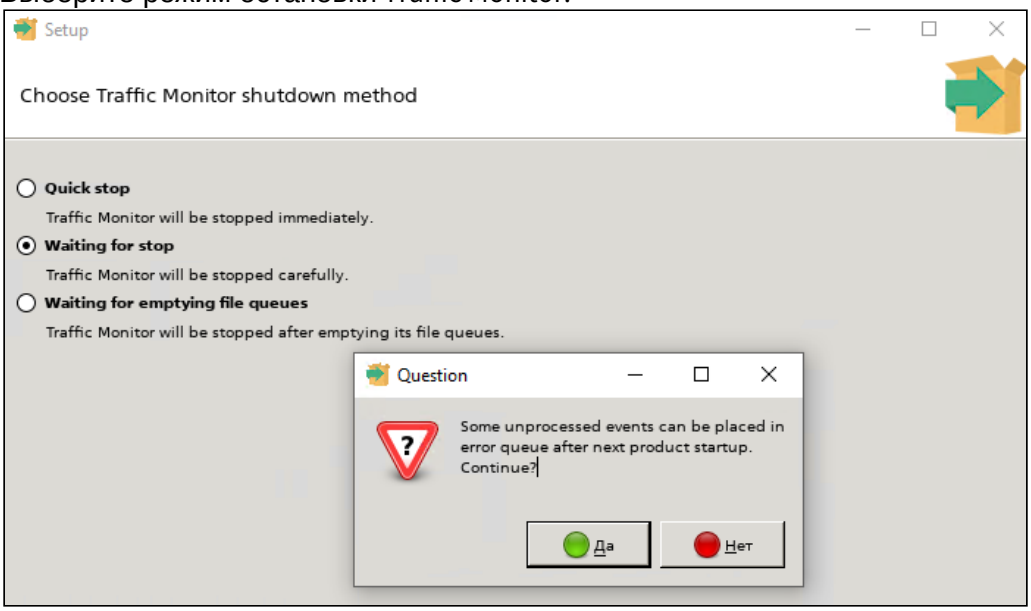
g. Подтвердите остановку сервисов. Шаги подтверждения и выбора режима остановки будут пропущены, если сервисы были остановлены вручную до

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.

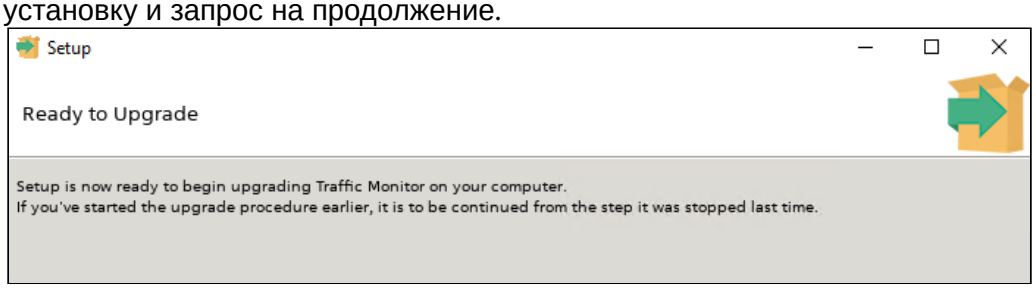
> **Важно!**
>
> Если компоненты перехвата и компоненты анализа (`iw_cas` , `iw_pas`) используются на разных серверах, остановка перехватчиков с очисткой файловых очередей может зависнуть. Рекомендуется использовать другие режимы или остановить компоненты вручную.

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

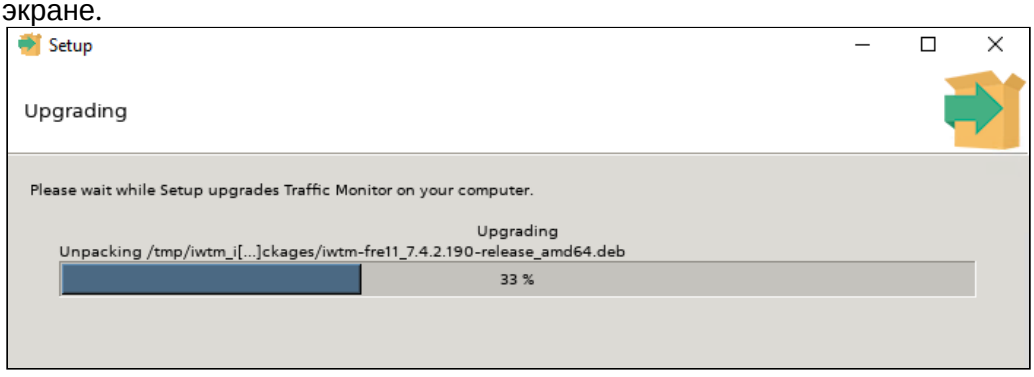
> **Примечание:**
>
> Если выбран `Quick stop` , остановленные сервисы до запуска будут иметь статус `failed (failed)` .

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:

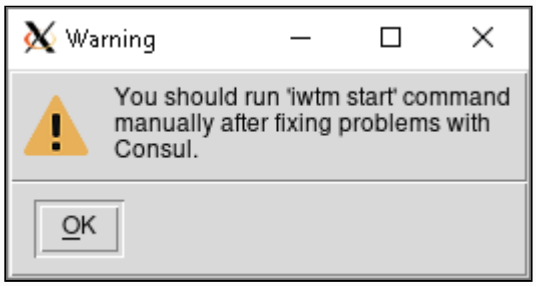


- `Remove exctracted installer data` - удалить пакеты, созданные инсталлятором для установки. Если установка прошла успешно, данные рекомендуется удалить;
- `Start Infowatch Traffic Monitor services` - запустить остановленные сервисы.

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-7.4.2.190-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-7.4.2.190-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

11. 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").
12. 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`.

13. Проверьте кластер службы Consul - описание смотрите ниже.

ШАГ 2. ПРОВЕРКА КЛАСТЕРА СЛУЖБЫ CONSUL

Для проверки кластера Consul выполните следующие действия:

1. На всех обновляемых серверах запустите службу Consul, выполнив команду:
`systemctl start iwtm-consul`
Проверить статус службы можно командой:
`systemctl status iwtm-consul`
2. Чтобы проверить службу Consul, на сервере 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. На сервере с шаблоном Веб-консоль введите команду для очистки кеша:
   `redis-cli flushall`
3. 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 Обновление InfoWatch Device Monitor

Если у вас установлен InfoWatch Device Monitor, то вы можете обновить его до более поздней версии.

Важно!

Для корректной работы и доступа ко всей функциональности версии Traffic Monitor и Device Monitor должны быть совместимы. Подробнее о совместимости Device Monitor см. в статье Базы знаний InfoWatch "Особенности совместимости разных версий TM, DM и Агентов".

Обновление Device Monitor выполняется в том же порядке, что и установка:

1. Обновление серверной части InfoWatch Device Monitor (база данных, сервер, сервис распространения дистрибутивов и консоль управления).

   Важно!

   При обновлении Системы с ранних версий:

   1. Соблюдайте следующий порядок: в первую очередь обновите Сервер Device Monitor, затем Сервер Traffic Monitor, затем Агенты DM на рабочих станциях.

   2. Если требуется обновить Device Monitor версии 3.4, удалите старую версию сервера (не удаляя базу данных) и установите сервер заново, указав при этом параметры соединения с существующей базой данных.

   3. Если требуется обновить Device Monitor, начиная с версии 4.0, то выполните обновление без удаления предыдущей версии.

4. Чтобы при обновлении Device Monitor версии 6.0 (путем удаления и повторной установки Сервера) Агенты Device Monitor смогли подключиться и привязаться к новому серверу:

- при удалении: сохраните ключ шифрования, хранящийся в папке установки сервера DM, файл `SSLServerKey.pfx`.

- при установке: укажите путь к сохраненному ключу шифрования, который использовался на старом сервере.

2. Обновление Агента InfoWatch Device Monitor.

Важно!

Обновление Агентов Device Monitor следует проводить после обновления Сервера Device Monitor и Сервера Traffic Monitor.

4.3.1 Обновление серверной части InfoWatch Device Monitor

Важно!

При использовании нескольких серверов начните установку обновления с главного сервера. При этом обязательно выключите все используемые второстепенные серверы. Обновление серверов происходит по очереди, начиная с главного сервера.

Шаг 1. Начало обновления

Откройте папку с дистрибутивом Device Monitor и запустите файл установки для требуемой платформы.

В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor. Нажмите кнопку **Далее**, чтобы перейти к следующему окну мастера установки.

Шаг 2. Принятие лицензионного соглашения

Ознакомьтесь с текстом лицензионного соглашения. Если вы принимаете условия лицензионного соглашения, отметьте поле **Я принимаю условия настоящего лицензионного соглашения** и нажмите **Далее**.

Шаг 3. Настройка базы данных

При обновлении база данных сохраняется, и в окне **Установка или обновление базы** по умолчанию указываются параметры ранее использовавшейся базы данных. Однако вам потребуется указать некоторые параметры, в зависимости от используемой СУБД.

Обновление базы данных под управлением СУБД Microsoft SQL Server

На панели **Способ аутентификации** выберите способ аутентификации, назначенный пользователю, от имени которого обновляется база данных. В качестве значения данного параметра укажите способ аутентификации, выбранный при подготовке учетной записи (см. "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server").

Если учетной записи назначена аутентификация Windows, то выберите значение **Аутентификация Windows**.

Если учетной записи назначена встроенная аутентификация SQL Server, выберите значение **Встроенная в SQL Server**. Затем укажите имя и пароль подготовленной учетной записи в полях **Имя пользователя** и **Пароль** соответственно.

> **Примечание:**
>
> В процессе обновления вы можете указать прежние параметры аутентификации или задать новые. Рекомендации по выбору способа аутентификации и подготовке необходимой учетной записи приведены в статье "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server".

Обновление базы данных под управлением PostgreSQL

Укажите имя пользователя и пароль учетной записи, используемой для работы с обновляемой базой данных. Имя по умолчанию - `postgres`.

После того как необходимые параметры будут настроены, нажмите кнопку **Далее**.

Шаг 4. Завершение обновления

После перехода к следующему окну, нажмите на кнопку **Установить**, чтобы запустить процесс обновления серверной части Device Monitor.

Следуйте дальнейшим указаниям мастера установки, чтобы завершить обновление серверной части.

> **Примечание:**
>
> При обновлении сервера Device Monitor не гарантируется работа фильтров отображения данных в консоли (фильтры событий, логов журнала аудита и т.д.), которые были настроены в предыдущей версии.

> **Важно!**
>
> Если после обновления Device Monitor Server в конфигурационном файле `InfoWatch.DeviceMonitor.Server.exe.config` отсутствуют параметры для интеграции с InfoWatch Activity Monitor, выполните действия из статьи базы знаний.

> **Примечание:**
>
> При обновлении сервера до версии 7.4 в поле **Статус** возможны следующие значения:
>
> - **Не установлен** - если не было ни одного обращения Агента к серверу;
> - **Установлен** - если Агент хотя бы один раз обращался к серверу.
>
> Для поля **Активность агента** актуальный статус будет установлен в соответствии со значениями, указанными в настройках.
>
> При обновлении на новую версию переименование рабочих станций, которые уже находятся в схеме безопасности, не производится. Новый механизм проверки и регистрации распространяется на компьютеры, которые обращаются к серверу после обновления. Он подразумевает проверку только идентификатора: если он совпадает, у рабочей станции меняется имя, а прежнее имя будет только отображаться в Консоли до тех пор, пока Пользователь не удалит её.

Прежний механизм также включал проверку имени, что приводило к возникновению в Консоли DM двух записей для одной рабочей станции, с новым и старым именем.

4.3.2 Обновление Агента InfoWatch Device Monitor

Device Monitor поддерживает совместимость с Агентами версий 7.2 и выше. Таким образом, обновленные компоненты Device Monitor могут работать со старыми версиями Агента. Однако вы можете обновить Агент до более поздней версии.

Важно!

Если на компьютере под управлением ОС Astra Linux установлен Агент InfoWatch Device Monitor версии ниже 7.0, для обновления Агента **обязательно** выполните следующие действия:

1. Удалите Агент InfoWatch Device Monitor;
2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 6 (20200722SE16) (см. официальную инструкцию);
3. Установите новую версию Агента InfoWatch Device Monitor.

Обновление Агента выполняется аналогично установке:

- локальное обновление с использованием мастера установки;
- удаленное обновление с помощью средств распространения программного обеспечения;
- автоматическое обновление (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", раздел "Автоматическое обновление Агентов").
- централизованное обновление через Консоль управления (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", раздел "Удаленная установка, обновление и удаление Агентов").

Чтобы успешно установить или обновить Агент InfoWatch Device Monitor, следуйте рекомендациям, указанным на странице Установка Агента InfoWatch Device Monitor.

При обновлении Агента Device Monitor до новой версии следует действовать следующим образом:

1. Произвести обновление на группе не более 10 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
2. Произвести обновление на группе не более 50 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
3. Произвести обновление на группе не более 500 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
4. Произвести обновление на группе не более 1000 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
5. Произвести обновление на оставшихся компьютерах до полного завершения процесса обновления.

Примечание:

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

Если компонент Контроль сетевых соединений был установлен ранее, при обновлении Агента он будет удален. При необходимости, данный компонент возможно установить вручную, используя командную строку.

Warning!

После обновления Агента обязательно перезагрузите рабочую станцию, чтобы использовать новый механизм перехвата для приложений, запущенных до обновления.

4.4 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.

4.4.1 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:

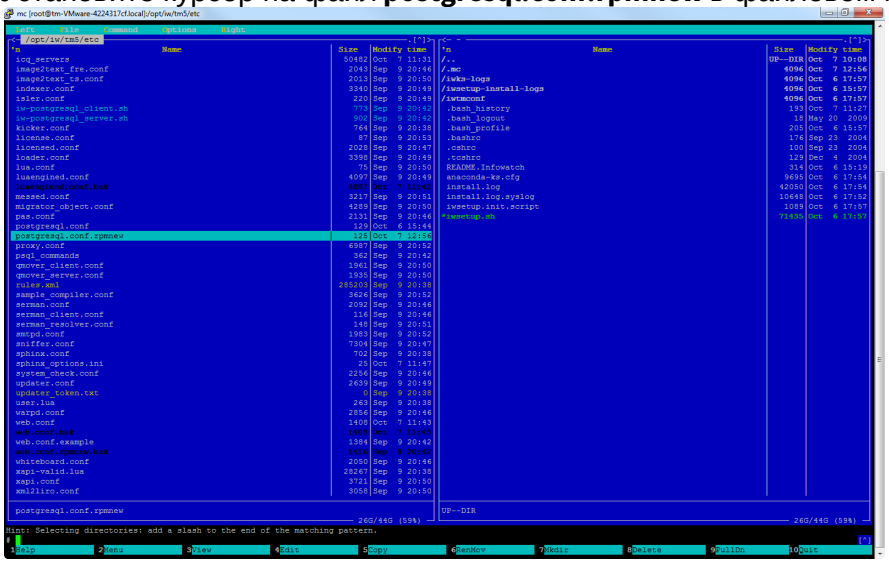
```
{
    "DB": "postgres",
    "Host": "localhost",
    "Password": "xxXX1234",
    "Port": 5433,
    "Username": "iwtm_linux"
}
```

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"
}
```

4.4.2 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 (как Oracle, так и PostrgreSQL) см. "Удаление схемы базы данных".
- О порядке удаления Device Monitor (серверная и клиентская часть) см. "Удаление InfoWatch Device Monitor".
- О порядке удаления Traffic Monitor (все установленные на сервере компоненты: веб-консоль, модули перехвата и другие) см. "Удаление Traffic Monitor".

По окончании удаления Сервера Traffic Monitor верните внешнюю инфраструктуру, настроенную на Traffic Monitor, в исходное состояние:

- если выполнялась интеграция с почтовым relay-сервером - убедитесь, что параметры Postfix возвращены в исходное состояние;
- если Система выполняла перехват и фильтрацию SMTP-трафика - настройте доставку SMTP-писем через корпоративный почтовый сервер, минуя InfoWatch Traffic Monitor.

5.1 Удаление схемы базы данных

> **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 InfoWatch Device Monitor

Важно!

Если вы планируете вновь устанавливать сервер Device Monitor, то для обеспечения Агентам Device Monitor возможности подключаться и привязываться к новому серверу, начиная с версии 6.0, рекомендуется сохранить ключ шифрования старого сервера.

Ключ шифрования хранится в папке установки сервера InfoWatch Device Monitor, файл `SSLServerKey.pfx`.

Чтобы удалить серверную часть InfoWatch Device Monitor вместе с Консолью управления и Сервисом распространения дистрибутивов:

1. Выполните одно из следующих действий:
   - На диске с дистрибутивом системы откройте каталог `Setup\Unified`. В данном каталоге найдите и запустите файл установки для требуемой платформы.
   - В оснастке **Добавить или удалить программы** (**Add or remove programs**), входящей в состав операционной системы Windows, выберите **InfoWatch Device Monitor Server** и нажмите на кнопку **Изменить** (**Change**).
2. В окне **Изменение, восстановление или удаление…** выберите команду **Удалить**.
3. Если вы хотите удалить систему вместе с базой данных, в окне **Удаление базы данных…** отметьте поле **Удалить базу**. В этом случае вам потребуется задать параметры удаления; параметры зависят от вида используемой СУБД:
   - **Microsoft SQL Server** – укажите используемый способ аутентификации, выбрав нужный вариант на панели **Способ аутентификации** (см. также "Рекомендации по развертыванию базы данных под управлением СУБД Microsoft SQL Server"). Если аутентификация выполнялась средствами SQL-сервера (**Встроенная в SQL Server**), то на панели **Администратор базы данных**, в полях **Имя пользователя** и **Пароль** укажите параметры той учетной записи, при помощи которой осуществлялось подключение к базе данных.
   - **Oracle** – в поле **Пароль учетной записи SYSTEM** укажите необходимый пароль. В результате будет удалена учетная запись владельца схемы базы данных, а также все объекты, за исключением табличного пространства.
   - **PostgreSQL** – в полях **Имя пользователя** и **Пароль** укажите имя и пароль учетной записи, от имени которой была создана эта БД при установке сервера (см. "Порядок установки серверной части InfoWatch Device Monitor").

     Важно!

     Если БД не функционирует или ограниченно функционирует, то для удаления InfoWatch Device Monitor рекомендуется снять отметку с поля **Удалить базу**, иначе удаление может произойти не полностью.

4. После того как необходимые параметры будут заданы, нажмите **Далее**, а затем – **Удалить**, чтобы запустить процесс удаления.

Чтобы удалить серверную часть InfoWatch Device Monitor, или Консоль управления, или Сервис распространения дистрибутивов отдельно:

1. В оснастке **Добавить или удалить программы** (**Add or remove programs**) воспользуйтесь кнопкой **Изменить** (**Change**).
2. В окне **Выборочная установка** нажмите  слева от компонента, который вы намерены удалить, и в раскрывшемся списке выберите пункт **Этот компонент будет полностью недоступен**. Нажмите **Далее**.
3. Если на предыдущем шаге вы выбрали для удаления сервер, то в окне **Удаление базы данных…** определите необходимость удаления базы данных и при необходимости задайте параметры учетной записи, имеющей на это права (подробнее см. выше).
4. Нажмите **Изменить**, чтобы запустить процесс удаления.

Важно!

В результате удаления Сервиса распространения дистрибутивов будет удалена зарегистрированная в Системе точка распространения и директория со всеми размещенными в ней дистрибутивами.

Чтобы удалить Агент InfoWatch Device Monitor:

на компьютере, где он установлен, в оснастке **Добавить или удалить программы** (**Add or remove programs**) выберите **InfoWatch Device Monitor Client** и воспользуйтесь кнопкой **Удалить** (**Remove**).

Чтобы удалить Агент InfoWatch Device Monitor на ОС Astra Linux и РЕД ОС:

1. Перейдите в директорию, в которую при установке было распаковано содержимое архива:
   - `Setup.AstraLinuxSE-1.6-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.6;
   - `Setup.AstraLinuxCE-2.12-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Common Edition 2.12;
   - `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz` - для РЕД ОС 7.3.1.
2. Для удаления Агента запустите скрипт, выполнив команду:
   `sudo ./remove.sh`
3. Для удаления средств распространения агента выполните команду:
   `rpm -e iwdeployagent` - на РЕД ОС
   `dpkg --purge iwdeployagent` - на ОС Astra Linux

Удаление Агентов можно также выполнять централизованно:

- с помощью средств Active Directory (если Агенты были установлены при помощи средств распространения программного обеспечения), как описано в статье "Удаление Агента, установленного с помощью средств распространения программного обеспечения".
- с помощью задач распространения в Консоли управления (подробнее см. "*Infowatch Traffic Monitor. Руководство пользователя*", раздел "Удаленная установка, обновление и удаление Агентов").

Важно!

Выключение питания компьютера в процессе установки/удаления Агента может привести к ошибкам, ведущим к нестабильной работе операционной системы.

В случае возникновения трудностей при удалении Агента рекомендуем обратиться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.
Вы также можете посетить раздел технической поддержки на нашем сайте: http://www.infowatch.ru/services/support.

5.2.1 Удаление Агента, установленного с помощью средств распространения программного обеспечения

Агенты, установленные с помощью средств распространения программного обеспечения, могут быть удалены тем же способом.

Например, если установка Агентов была выполнена через Microsoft Active Directory, то администратор корпоративной сети может удалить назначенное задание на установку из соответствующей групповой политики. Порядок редактирования групповой политики описывается в статье "Установка Агента с помощью средств распространения программного обеспечения", шаг 3.

Чтобы удалить Агент со всех контролируемых компьютеров:

1. Выделите задание на установку, которое нужно удалить. Затем щелкните правой кнопкой мыши по выделенной строке и в раскрывшемся контекстном меню выберите пункт **All tasks** > **Remove**.
2. В открывшемся диалоговом окне **Remove software** выберите **Immediately uninstall thesoftware from users and computers**.

   > **Примечание.**
   >
   > Если будет выбрано другое действие, то задание на установку будет удалено, но все ранее установленные Агенты останутся. Удаление этих Агентов средствами Microsoft Active Directory в дальнейшем будет невозможно.

3. Нажмите **OK**. Агент будет удален со всех компьютеров, на которые распространяется выбранная групповая политика.

Удалить Агент InfoWatch Device Monitor, установленный на ОС Astra Linux или РЕД ОС, можно несколькими способами:

- Локально, при это также необходимо отдельно удалить средство распространения. Для этого выполните команды:
  - На ОС Astra Linux:
    ```
    dpkg --purge iwdm
    dpkg --purge iwdeployagent
    ```
  - На РЕД ОС:
    ```
    rpm -e iwdm
    rpm -e iwdeployagent
    ```
- Предварительно обновить Агент через задачу первичного распространения и после этого запустить задачу на удаление продукта.

5.3 Удаление Traffic Monitor

> **Важно!**
>
> Если база данных находится на сервере, на котором будет запущен процесс удаления, сначала удалите схему базы данных.
>
> Удаление затронет **только** тот сервер, на котором будет выполнена команда удаления. Для возможности восстановления событий в случае переустановки Traffic Monitor рекомендуем перед удалением создать резервную копию базы данных (см. "*InfoWatch Traffic Monitor. Руководство администратора*", раздел Администрирование базы данных > PostgreSQL > Резервное копирование базы данных, статья "Создание резервной копии базы данных"). Также рекомендуется создать резервные копии конфигурации и настроек.

Процесс удаления Traffic Monitor запускается в консоли сервера. Удаление выполняется средствами ОС.

Чтобы удалить Traffic Monitor выполните следующие действия:

1. Введите логин и пароль, чтобы войти в операционную систему (вход выполняется от имени пользователя, созданного при установке).
2. Остановите процессы Traffic Monitor с помощью команды:
   `iwtm stop`
3. Для удаления пакетов Traffc Monitor и символических ссылок последовательно выполните команды:
   ```
   sudo dpkg-query -f '${Package}\n' -W | grep -E "iwtm" | 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