

INFOWATCH

InfoWatch Data Explorer. Руководство по установке, конфигурированию и администрированию

05/08/2022

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 4

2 Комплект документов 5

3 Аппаратные и программные требования Data Explorer 6

3.1 Аппаратные требования 6

3.2 Программные требования 6

4 Установка Data Explorer 8

4.1 Чтобы установить Систему: 9

5 Обновление Data Explorer 11

6 Удаление Data Explorer 12

7 Добавление плагина Traffic Monitor 13

8 Настройка интеграции с сервером Traffic Monitor 14

9 Компонент Автолингвист 16

В настоящем руководстве вы сможете найти сведения по установке, обновлению, удалению и настройке компонентов системы InfoWatch Data Explorer.
InfoWatch Data Explorer (далее Система или Data Explorer) - программный продукт, позволяющий автоматизировать формирование политик DLP-системы с помощью выделения тематических кластеров документов в информационных потоках компании.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, работающих с Системой (выполняющих настройку конфигурации, анализ информационных объектов и т. п.).

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и СУБД PostgreSQL.

2 Комплект документов

В комплект документации по InfoWatch Data Explorer входят:

- «InfoWatch Data Explorer. Руководство по установке, конфигурированию и администрированию». Содержит описание установки, обновления, удаления и настройки продукта.
- «InfoWatch Data Explorer. Руководство пользователя». Содержит описание порядка работы с продуктом.

Сопутствующая документация по продукту InfoWatch Traffic Monitor включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание порядка установки, настройки и удаления системы InfoWatch Traffic Monitor (далее 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.

3 Аппаратные и программные требования Data Explorer

Data Explorer для получения данных обязательна интеграция с InfoWatch Traffic Monitor 7.2.1 и выше.

3.1 Аппаратные требования

Системные требования, необходимые для установки:

Процессор	ОЗУ	Жесткий диск
Количество ядер - 4; Частота - 3.1 ГГц; Разрядность - 64 bit; Поддержка инструкций SSE 4.2.	16 Гбайт	от 100 Гбайт

Важно!

Минимальное количество последовательных операций ввода-вывода в секунду для диска 7200 оборотов в минуту равно 50 IOPS. В момент первоначальной загрузки данных в Систему нагрузка возрастает и может потребоваться скорость 500 IOPS. При дальнейшей периодической синхронизации нагрузка будет снижена.

Важно!

Устанавливайте Data Explorer на отдельный сервер - на центральной ноде кластера.

Примечание:

Для точного расчета требований под конкретный проект обратитесь к специалистам компании InfoWatch.

3.2 Программные требования

Для установки и работы Data Explorer может быть использовано следующее программное обеспечение:

Тип ПО	Варианты
Операционная система	• Astra Linux Special Edition 1.6 "Смоленск": • Update 10; • Astra Linux Special Edition 1.7 "Смоленск": • версии 1.7.x (1.7.0-11.06.2021_12.40 и выше); • Red Hat Enterprise Linux: • версии 7.x (7.7 и выше); • версии 8.x (8.0 и выше);

Тип ПО	Варианты
	• Oracle Linux: • версии 7.x (7.9 и выше); • версии 8.x (8.4 и выше); • РЕД ОС: • версии 7.x.x (7.3.1 и выше), ядро версии 5.4 и выше.
СУБД	PostgreSQL 12
Браузер	• Google Chrome; • Яндекс.Браузер. **Важно!** В браузере должна быть реализована аппаратная поддержка WebGL/WebGL2

Важно!

Data Explorer должен быть установлен на отдельный сервер. Не рекомендуется совместная установка с другими продуктами.

4 Установка Data Explorer

Важно!

Устанавливайте Data Explorer на отдельный сервер. Не рекомендуется совместная установка с другими продуктами.

В одном кластере может быть один сервер Data Explorer Поддерживается установка только на центральной ноде кластера.

Важно!

Перед установкой продукта настройте правила POD сети или отключите межсетевой экран (подробнее см. статьи Базы знаний "Конфликты при взаимодействии службы firewalld и Kubernetes", "Полное отключение межсетевого экрана"). В противном случае установка продукта будет невозможна.

Важно!

Data Explorer использует Kubernetes. Для корректной установки продукта и работы Kubernetes установите пакеты:

- **socat**;
- **conntrack** или **conntrack-tools** (пакет необходимо установить, даже если **libnetfilter_conntrack** уже установлен).

Пакеты не входят в состав дистрибутива продукта.

Пакеты могут отсутствовать в репозиториях в Astra Linux. В этом случае требуется загрузить и установить требуемые пакеты вручную.

Важно!

Если в операционной системе, куда планируется установить Data Explorer, используется SELinux, установите пакет **container-selinux**. Данный пакет необходим для корректной работы Docker.

Пакет не входит в состав дистрибутива продукта.

Пакет может отсутствовать в репозиториях в Astra Linux. В этом случае требуется загрузить и установить требуемый пакет вручную.

Важно!

Для установки и корректной работы Data Explorer в операционной системе Astra Linux Special Edition отключите настройку `astra-nochmodx-lock`, выполнив команду:
`astra-nochmodx-lock disable`

Для установки продукта используется архив iw_de_setup_x.x.x.xx.tar.xz из состава дистрибутива, где x.x.x.xx - номер версии. Архив содержит полный набор бинарных модулей образов контейнеров,

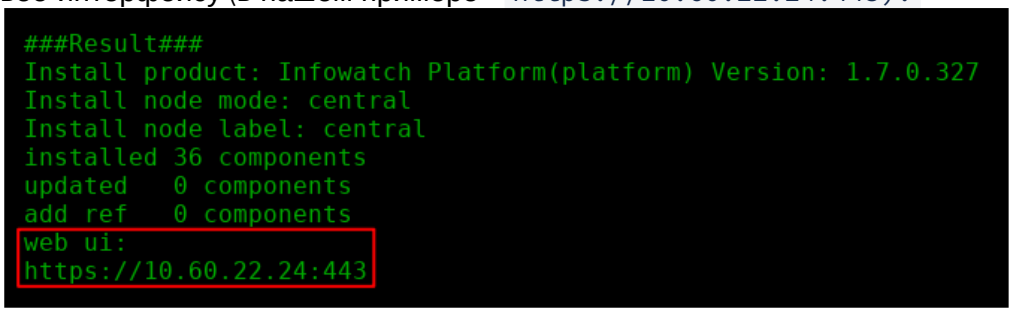
необходимых для развертывания продукта без доступа к сети Интернет (offline-установка). Также архив содержит программу установки. Программа установки написана на языке Python версии 2.7, поэтому для установки продукта в целевой ОС установите интерпретатор этого языка.

4.1 Чтобы установить Систему:

1. Создайте новую директорию на диске (например, `de`):
   `mkdir de`
2. Скопируйте архив **`iw_de_setup_1.2.0.xxx.tar.xz`** в созданную директорию.
3. Перейдите в директорию, в которую был скопирован архив.
4. Распакуйте архив с дистрибутивом продукта в эту директорию:
   `tar -xvf iw_de_setup_1.2.0.xxx.tar.xz`
5. Запустите программу установки продукта:
   `./setup.py install`
6. Ознакомьтесь с условиями лицензионного соглашения. Лицензионное соглашение содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
7. Введите "**y**", чтобы принять лицензионное соглашение, и нажмите Enter.
8. Введите IP-адрес сетевого интерфейса для взаимодействия с кластером в формате IPv4: "xxx.xxx.xxx.xxx" (по умолчанию: `0.0.0.0`) и нажмите **Enter**.

   > **Примечание:**
   >
   > Здесь и далее для использования значений, предложенных по умолчанию, нажмите **Enter** без ввода значений.

9. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию: `80%`) и нажмите **Enter**.
10. Укажите путь для размещения данных Clickhouse (по умолчанию: `/mnt/chdata`) и нажмите **Enter**.
11. Укажите путь для размещения данных Tarantool (по умолчанию: `/mnt/trdata`) и нажмите **Enter**.
12. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/mnt/pgdata`) и нажмите **Enter**.
13. Укажите путь для размещения бинарных данных (по умолчанию: `/mnt/dsdata`) и нажмите **Enter**.
14. Укажите порт подключения к веб-интерфейсу (по умолчанию: `443`) и нажмите **Enter**.
15. Дождитесь окончания процесса установки продуктовой платформы.
16. Ознакомьтесь с отчетом об установке платформы (в нашем примере была установлена платформа версии 1.7.0.327). В графе **`web ui`** указаны адрес и порт для подключения к веб-интерфейсу (в нашем примере – `https://10.60.22.24:443`):



17. Дождитесь окончания процесса установки продукта Data Explorer.
18. Ознакомьтесь с отчетом об установке продукта.
19. Убедитесь что все сервисы запущены, выполнив команду:
    `kubectl get pods -n infowatch`
    Команда выведет список сервисов. Каждый сервис должен иметь статус `Running`.
20. Введите адрес и порт для подключения к веб-интерфейсу (в нашем примере – `https://10.60.22.24:443`) в браузере, чтобы начать использование Системы (см. Шаг 16 данной инструкции).

После установки выполните настройку интеграции InfoWatch Data Explorer с сервером InfoWatch Traffic Monitor.

5 Обновление Data Explorer

Чтобы обновить Data Explorer:

1. Скопируйте архив `iw_de_setup_x.x.x.xx.tar.xz` из состава дистрибутива в директорию на сервере, в которой не был распакован инсталлятор предыдущей версии.
   В нашем примере будет использована версия `1.2.1.88`, соответственно, архив - `iw_de_setup_1.2.1.88.tar.xz`.
2. Распакуйте архив с помощью команды:
   `tar -xzvf iw_de_setup_1.2.1.88.tar.xz`
3. Перейдите в директорию, созданную после распаковки архива.
4. Для запуска обновления Data Explorer введите команду:
   `./setup.py update`
5. Дождитесь завершения процесса обновления. Программа обновит компоненты продукта и требуемое окружение.
6. Чтобы вывести на экран версию обновленного продукта, выполните команду:
   `./setup.py showproducts`

6 Удаление Data Explorer

Data Explorer удаляется с помощью командной строки.

Чтобы удалить Data Explorer:

1. Перейдите в папку, в которой был распакован инсталлятор с последней версией продукта.
2. Выполните команду:
   `./setup.py remove`
3. Дождитесь завершения процесса.

> **Примечание:**
>
> Инсталлятор удалит сервисы и компоненты Системы. После удаления на сервере останутся результаты работы продукта и база данных. Данные останутся в директориях, которые были указаны при установке Data Explorer.

7 Добавление плагина Traffic Monitor

Для установки соединения и последующего получения данных в Traffic Monitor необходимо добавить плагин в Консоли управления и разместить дополнительные файлы в соответствующих директориях Traffic Monitor. Плагин и файлы находятся в составе дистрибутива и представляют собой архивы в формате .zip. Архив плагина имеет вид: `tmplugin/de.zip`, дополнительные файлы в формате .php размещены в архиве `tmpatch/extend_api.zip.`

Чтобы разместить дополнительные файлы:

1. Перенесите поставляемый в составе дистрибутива файл `ObjectExtendController.php` в директорию Traffic Monitor `/opt/iw/tm5/www/backend/protected/controllers/`
2. Перенесите поставляемый в составе дистрибутива файл `SelectionWorkerActions.php` в директорию Traffic Monitor `/opt/iw/tm5/www/backend/protected/components/workers`

Чтобы добавить плагин:

1. Перейдите в раздел **Управление - Плагины**;
2. В области **Плагины** нажмите .
3. Нажмите **Добавить**.
4. Просмотрите описание плагина и нажмите **Установить**.

Информация о плагине будет доступна в разделе **Управление** -> **Плагины**. Для последующей отправки данных в Traffic Monitor необходим токен, который создается автоматически и доступен в разделе **Управление** -> **Плагины** -> **Токены**. Скопируйте выданный вам токен и укажите его в поле **Токен** в Консоли управления Data Explorer при последующей настройке интеграции с InfoWatch Traffic Monitor.

8 Настройка интеграции с сервером Traffic Monitor

Data Explorer использует данные, извлекаемые из событий Traffic Monitor.
Для доступа компонента Data Explorer к событиям обязательно настройте интеграцию с сервером Traffic Monitor.

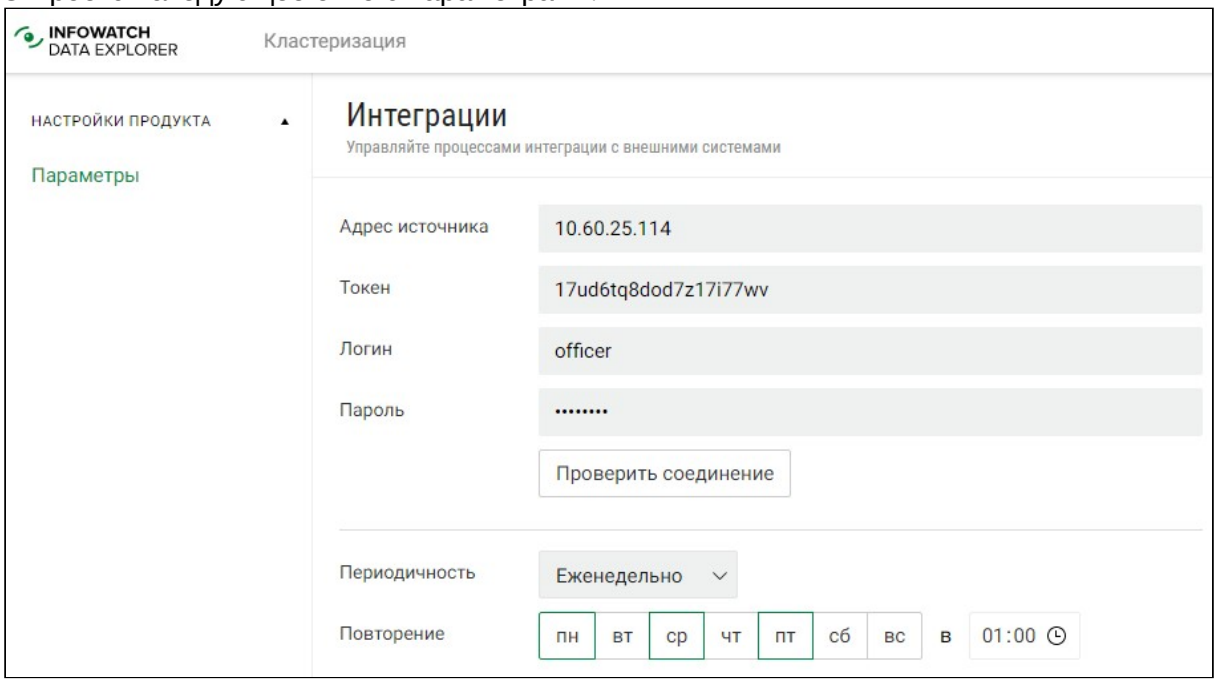
> **Примечание:**
>
> Одновременно поддерживается интеграция только с одним сервером Traffic Monitor.

Настройка интеграции выполняется в Консоли управления Data Explorer. Для настройки:

1. Откройте Консоль управления Data Explorer и авторизуйтесь.

   > **Примечание:**
   >
   > Если пароль пользователя Консоли не менялся, используйте для авторизации стандартные учетные данные:
   >
   > - логин - `officer`
   > - пароль - `xxXX1234`

2. Для перехода в раздел настроек в правом верхнем углу нажмите кнопку .
   Откроется следующее окно с параметрами:



3. Заполните все указанные поля:
   a. **Адрес источника** - IP-адрес сервера Traffic Monitor.
   В случае распределенной установки Traffic Monitor укажите адрес сервера, на котором установлены компоненты консоли управления Traffic Monitor (шаблон установки Веб-консоль).

    b. **Токен** - токен для подключения к серверу Traffic Monitor по программному интерфейсу приложения (API), полученный после добавления плагина.
    c. **Логин** - логин пользователя, от имени которого осуществляется соединение.
    d. **Пароль** - пароль пользователя, от имени которого осуществляется соединение.
4. После заполнения всех полей вы можете проверить корректность введенных данных и доступность сервера Traffic Monitor с помощью кнопки **Проверить соединение**.
5. Укажите периодичность, с которой InfoWatch Pulse будет выгружать данные из Traffic Monitor для последующей кластеризации.
   Вы можете выбрать один из вариантов:
   - **Ежечасно** - укажите интервал в часах, чтобы выгружать данные через каждые N часов;
   - **Ежедневно** - укажите время суток;
   - **Еженедельно** - укажите дни недели и время суток.

При настройках, указанных на изображении выше, Data Explorer будет подключаться к серверу Traffic Monitor по адресу *10.60.25.114* от имени пользователя *officer* и выгружать данные в *01:00* по *понедельникам*, *средам* и *пятницам*.

Важно!

Чтобы Data Explorer мог выгружать данные, на сервере Traffic Monitor должна быть добавлена действующая лицензия на экспорт в сторонние системы анализа. Наличие данной лицензии вы можете уточнить у администратора Traffic Monitor.

9 Компонент Автолингвист

Компонент Автолингвист реализован в виде технологии анализа в системе Traffic Monitor.

Установка, обновление и удаление Автолингвиста выполняются только в составе Traffic Monitor. Данные процессы описаны в документе «*InfoWatch Traffic Monitor. Руководство по установке*».

> **Примечание:**
>
> Для работы с технологией Автолингвист в Traffic Monitor должна быть добавлена соответствующая лицензия.