

INFOWATCH

InfoWatch Data Explorer. Руководство по установке

28/04/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 4

2 Комплект документов 5

3 Техническая поддержка пользователей 6

4 Типы установки, совместимость с другими продуктами, аппаратные и программные требования 7

4.1 Типы установки и совместимость с другими продуктами InfoWatch 7

4.2 Типы обновления 8

4.3 Аппаратные требования 8

4.4 Программные требования 9

5 Подготовка сервера 10

6 Настройка сетевых правил доступа 18

7 Установка Data Explorer 19

8 Устранение неполадок 23

9 Удаление Data Explorer 24

В настоящем руководстве вы можете найти сведения по установке и удалению InfoWatch Data Explorer. InfoWatch Data Explorer (далее Модуль/Система или Data Explorer) это – модуль, позволяющий автоматически систематизировать документы, найденные с помощью InfoWatch Data Discovery. Для работы Data Explorer необходим InfoWatch Data Analysis Service.

1 Аудитория

Данное руководство предназначено для пользователей Модуля, выполняющих ее установку и удаление.

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

2 Комплект документов

В документацию по InfoWatch Data Explorer входят:

- *InfoWatch Data Explorer. Руководство по установке*. Содержит описание установки и удаления Модуля;
- *InfoWatch Data Explorer. Руководство администратора*. Документ содержит информацию по настройке Модуля.
- *InfoWatch Data Explorer. Руководство пользователя*. Содержит описание работы с Модулем.

Сопутствующая документация по продукту InfoWatch Data Discovery включает в себя:

- *InfoWatch Data Discovery. Руководство по установке*. Документ содержит описание процесса установки, обновления и удаления Data Discovery.
- *InfoWatch Data Discovery. Руководство администратора*. Документ содержит информацию по настройке Data Discovery.
- *InfoWatch Data Discovery. Руководство пользователя*. Содержит описание работы с задачами сканирования.

Сопутствующая документация по сервису InfoWatch Data Analysis Service включает в себя:

- *InfoWatch Data Analysis Service. Руководство по установке, конфигурированию и администрированию*. Содержит описание установки, обновления, удаления и настройки Data Analysis Service.

Сопутствующая документация по продукту InfoWatch Traffic Monitor включает в себя:

- *InfoWatch Traffic Monitor. Руководство по установке*. Содержит описание установки, настройки и удаления системы InfoWatch Traffic Monitor;
- *InfoWatch Traffic Monitor. Руководство администратора*. Содержит информацию по администрированию InfoWatch Traffic Monitor (база данных, серверная часть);
- *InfoWatch Traffic Monitor. Руководство пользователя*. Содержит описание 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 Техническая поддержка пользователей

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

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

Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

4 Типы установки, совместимость с другими продуктами, аппаратные и программные требования

4.1 Типы установки и совместимость с другими продуктами InfoWatch

Для работы **Data Explorer** необходимо, чтобы в одном кластере с ним были установлены:

- **Data Discovery 2.2**
- **Data Analysis Service 1.6**

Data Explorer является частью Центра расследований InfoWatch.

Центр расследований InfoWatch - это единый интерфейс для работы и эффективного взаимодействия продуктов InfoWatch.

Основой для установки каждого продукта Центра расследований выступает Платформа. Инсталлятор каждого продукта содержит и Платформу, и продуктовые компоненты. Обе части обязательны к установке при развертывании продуктов.
И продуктовые компоненты, и Платформа поддерживают установку в двух режимах:

- `central`;
- `office`.

Режимы установки продукта и Платформы вы указываете при запуске инсталлятора. Если оба режима не указаны пользователем, инсталлятор по умолчанию использует значение `central` для обоих компонентов.

Центр расследований поддерживает **распределенную установку**: центральная (`central`) и офисные (`office`) ноды Платформы объединены в кластер.
Вы можете установить компоненты продуктов и на центральную, и на офисные ноды Платформы. Это позволяет создать кластер Платформы с несколькими продуктами с учетом инфраструктуры, требований к безопасности и доступных мощностей компании.

Важно!

При распределенной установке примите во внимание следующие ключевые аспекты:

- Продукты в кластере должны быть установлены на одной версии Платформы – в номерах версий должны совпадать первые два числа. Версия центральной ноды Платформы должна быть самой новой в кластере.
- Если вы устанавливаете в кластер продукт на новой версии Платформы, то после этого обновите остальные продукты.
- В одном кластере можно развернуть только одну центральную ноду Платформы и каждый продукт в режиме central только в единственном экземпляре.
- Если в кластере уже установлен продукт в режиме `central`, еще одна установка этого продукта в режиме `central` в том же кластере будет прервана ошибкой.
- Data Explorer поддерживает установку только в режиме `central`. При этом модуль может быть установлен как на центральную, так и на офисную ноду Платформы.

Продукты в одном кластере имеют:

- доступ ко всей функциональности в одной консоли управления;
- общие настройки;
- общую ролевую модель;
- общий доступ к данным независимо от того, на каком из них выполнена интеграция с источником, а также доступ к обработанным данным.

> **Важно!**
>
> Для подключения к веб-интерфейсу Центра расследований **всегда** используйте адрес или имя сервера, на котором установлена **Платформа в режиме** `central`.
>
> Если в распределенной установке продукт в режиме `central` установлен на офисной ноде Платформы, для работы все равно используйте центральную ноду Платформы (`central`).

Продукты Центра расследований InfoWatch поддерживают **совместную установку** на одном сервере.

Вы можете установить **Data Explorer 2.0 совместно** с:

- **Data Discovery 2.2**
- **Data Analysis Service 1.6**

> **Примечание:**
>
> Для расчета аппаратных требований при совместной установке **учитывайте требования каждого продукта**. Для расчета требований под конкретный проект обратитесь к специалистам компании InfoWatch.

Подробнее о процессе установки см. *Установка Data Explorer*.

4.2 Типы обновления

Data Explorer 2.0 не поддерживает обновление.

4.3 Аппаратные требования

Минимальные системные требования, необходимые для установки:

Процессор	ОЗУ	Жесткий диск
Количество ядер – 4; Частота – 3.1 ГГц; Разрядность – 64 бит; Поддержка	16 ГБ	От 150 ГБ свободного места. Минимальное количество последовательных операций ввода-вывода – от 50 IOPS.

Процессор	ОЗУ	Жесткий диск
инструкций SSE 4.2.		

4.4 Программные требования

Для установки и работы Data Explorer требуется использовать следующее программное обеспечение:

Тип ПО	Варианты
Операционная система	• Astra Linux Special Edition "Смоленск", версии: • 1.7.5 • 1.8.0 • Astra Linux Special Edition "Орел" 1.7.5 • Astra Linux Special Edition "Воронеж" 1.7 • Red Hat Enterprise Linux, версии: • 7.9 • 8.9 • 8.10 • Oracle Linux, версии: • 7.9 • 8.4 • РЕД ОС, версии: • 7.3.3 • 8 • ОС Альт: • Сервер 10.2; • СП 10. **Важно!** Модули **Netfilter** и **NAT** должны быть загружены в ядро ОС.
Браузер	• Google Chrome; • Яндекс.Браузер. **Важно!** Для корректной работы рекомендуется использовать последние версии поддерживаемых браузеров.

Примечание:

Data Explorer использует PostgreSQL 16.4.
СУБД поставляется вместе с продуктом и не требует отдельной установки.

5 Подготовка сервера

Перед установкой Data Explorer обязательно подготовьте сервер:

1. Программа установки написана на языке Python версии 2.7, поэтому для установки Сервиса установите интерпретатор этого языка. Пакет с интерпретатором не входит в состав дистрибутива Сервиса.
2. Настройте правила POD сети или отключите межсетевой экран (подробнее см. статьи Базы знаний *Конфликты при взаимодействии службы firewalld и Kubernetes*, *Полное отключение межсетевого экрана*). В противном случае установка Сервиса будет невозможна.
3. Для корректной работы Сервиса настройте сетевые правила доступа (подробнее см. *Настройка сетевых правил доступа*).
4. Data Explorer использует компонент Kubernetes. Для корректной установки Сервиса и работы Kubernetes на сервере должен быть установлен пакет *conntrack*.
   Убедитесь, что пакет установлен.

   Для этого введите в командной строке:

   ```
   conntrack
   ```

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

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

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

Tables: conntrack, expect, dying, unconfirmed

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

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

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

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

Если модуль не установлен, установите его с помощью команды:

- **Для ОС Red Hat Enterpise Linux, Oracle Linux и РЕД ОС**

```
yum install conntrack
```

- **Для ОС Astra Linux и ОС Альт**

```
apt-get install conntrack
```

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

- **Для ОС Red Hat Enterpise Linux, Oracle Linux, РЕД ОС и ОС Альт**

```
rpm -Uhv ./<имя_пакета>
```

- **Для ОС Astra Linux**

```
dpkg -i ./<имя_пакета>
```

5. Если вы используете антивирус, настройте его для совместной работы с Data Explorer (см. статью Базы знаний *Настройка антивируса для продуктов Платформы*).
6. **На сервере под управлением Red Hat Enterprise Linux и РЕД ОС настройте SELinux.**

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

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

     ```
     dnf install container-selinux
     ```

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

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

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

     b. Перезагрузите сервер с помощью команды:

        ```
        reboot
        ```

     c. Проверьте статус системы SELinux с помощью команды:

        ```
        sestatus
        ```

7. Если вы устанавливаете Сервис на ОС Альт, установите пакеты:
   - **python-modules-json**
   - **python-modules-distutils**
   - **python-modules-sqlite3**

   > **Примечание:**
   >
   > Пакеты не входят в состав дистрибутива продукта.

Пакеты могут отсутствовать в репозиториях. В этом случае скачайте и установите требуемые пакеты вручную.

8. **Если вы устанавливаете Data Explorer на ОС Альт СП 10, выполните следующие действия:**

   a. В файле `/etc/apt/sources.list.d/altsp.list` раскомментируйте три последних строки, указывающие репозитории.

   Пример содержимого altsp.list с раскомментированными строками

   ```
   # update.altsp.su (IVK, Moscow)

   # ALT Certified 10
   #rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64
   classic gostcrypto
   #rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64-
   i586 classic
   #rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTLinux c10f/branch/noarch
   classic

   rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64
   classic gostcrypto
   rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64-
   i586 classic
   rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/noarch
   classic
   ```

   b. Обновите пакеты с помощью команды:

   ```
   apt-get update
   ```

   c. Установите требуемые пакеты с помощью команд:

   ```
   apt-get install python-modules-sqlite3
   apt-get install conntrack-tools
   ```

   d. Установите менеджер контейнеров Podman с помощью команды:

   ```
   apt-get install podman
   ```

   e. С помощью Podman загрузите образы:

   ```
   podman pull registry.altlinux.org/k8s-c10f2/kube-apiserver:v1.31.1
   podman pull registry.altlinux.org/k8s-c10f2/kube-controller-manager:v1.31.1
   podman pull registry.altlinux.org/k8s-c10f2/kube-scheduler:v1.31.1
   podman pull registry.altlinux.org/k8s-c10f2/kube-proxy:v1.31.1
   podman pull registry.altlinux.org/k8s-c10f2/pause:3.10
   podman pull registry.altlinux.org/k8s-c10f2/etcd:3.5.15-0
   ```

```
podman pull registry.altlinux.org/k8s-c10f2/coredns:v1.11.3
podman pull registry.k8s.io/pause:3.10
```

f. Установите Kubernetes с помощью команд:

```
apt-get install kubernetes-kubeadm kubernetes-kubelet kubernetes-crio cri-tools
systemctl enable --now crio kubelet
swapoff -a
```

g. Для корректного создания кластера отключите использование прокси-соединения:

```
unset http_proxy
unset https_proxy
```

h. Создайте кластер:

```
kubeadm init --pod-network-cidr=10.244.0.0/16 --kubernetes-version=1.31.1 --image-
repository=registry.altlinux.org/k8s-c10f2
```

i. После создания кластера на экран будет выведена инструкция. Выполните предложенные действия.

> **Примечание:**
>
> **Рекомендуется** выполнить действия из инструкции.
> Если вы не будете выполнять все действия из инструкции, чтобы продолжить установку продукта, выполните команду для настройки переменной окружения:
>
> ```
> export KUBECONFIG=/etc/kubernetes/admin.conf
> ```
>
> Команда позволит использовать `kubectl` в рамках текущей сессии подключения. При следующем подключении или перезагрузке выполните команду повторно.

j. Установите для Kubernetes сетевой провайдер Flannel, для этого загрузите образы:

```
podman pull registry.altlinux.org/k8s-c10f2/flannel:v0.25.7
podman pull registry.altlinux.org/k8s-c10f2/flannel-cni-plugin:v1.4.0-flannel1
```

k. Загрузите манифест Flannel:

```
wget https://github.com/flannel-io/flannel/releases/latest/download/kube-flannel.yml
```

l. Отредактируйте файл-манифест:

i. Строку `image: docker.io/flannel/flannel-cni-plugin:v1.1.2` замените на:

Строка для замены:

```
image: registry.altlinux.org/k8s-c10f2/flannel-cni-plugin:v1.4.0-flannel1
```

ii. Строки `image: docker.io/flannel/flannel:v0.22.0` замените на:

Строка для замены:

```
image: registry.altlinux.org/k8s-c10f2/flannel:v0.25.7
```

> **Примечание:**
>
> В конфигурационном файле две одинаковых строки вида image: `docker.io/flannel/flannel:v0.22.0`. Замените обе.
>
> В связи с периодическими обновлениями Flannel версии в заменяемых строках могут отличаться.

m. Откройте на редактирование конфигурацию CoreDNS:

```
kubectl edit cm -n kube-system coredns
```

n. Добавьте следующее содержимое:

```
     rewrite stop {
        name substring iwplatform cluster answer auto
     }
```

Вид конфигурационного файла после редактирования:

```
Corefile: |
  .:53 {
      log
      errors
      health {
         lameduck 5s
      }
      rewrite stop {
         name substring iwplatform cluster answer auto
      }
      ready
      kubernetes cluster.local in-addr.arpa ip6.arpa {
         pods insecure
         fallthrough in-addr.arpa ip6.arpa
```

```
            ttl 30
        }
        prometheus :9153
        forward . /etc/resolv.conf {
            max_concurrent 1000
        }
        cache 30
        loop
        reload
        loadbalance
    }
```

o. Сохраните изменения и закройте редактор.
p. Примените изменения в манифесте и запустите Flannel с помощью команды:

```
kubectl apply -f kube-flannel.yml
```

q. Дождитесь запуска всех подов.
Вы можете проверить их статусы с помощью команды:

```
kubectl get pods -A
```

Все поды должны быть в статусе `Running`.
r. Смените директорию для временных файлов:

```
export TMPDIR=/var/tmp
```

9. Для установки и корректной работы Data Explorer в ОС Astra Linux Special Edition убедитесь, что настройка безопасности *astra-nochmodx-lock* отключена.
Вы можете отключить эту настройку с помощью команды:

```
astra-nochmodx-lock disable
```

10. Убедитесь, что на сервере установлены актуальные дата и время.

Дистрибутив Data Explorer представляет собой архив **`iw_dataexplorer_setup_2.0.X.xxx.tar.xz`**, где xxx — номер сборки. Архив содержит набор бинарных модулей образов контейнеров, необходимых для развертывания Data Explorer без доступа к сети Интернет. Архив также содержит программу установки.

Вы можете установить Data Explorer:

- на сервере совместно с другими продуктами;
- в кластере с другими продуктами.

> **Важно!**
>
> Data Explorer должен быть установлен в одном кластере с Data Discovery и Data Analysis Service.

Вы можете установить в кластере только один экземпляр Data Explorer и только в режиме `central`.

Важно!

Если вы устанавливаете Data Explorer в одном кластере с другими продуктами InfoWatch, то убедитесь, что версия Платформы совпадает у всех продуктов. В противном случае продукты, установленные на старой версии Платформы, необходимо обновить.

Чтобы узнать версию Платформы устанавливаемого продукта:

1. Распакуйте архив с дистрибутивом Data Explorer. Для этого перейдите в директорию с архивом и выполните команду:

   ```
   tar xvf iw_dataexplorer_setup_2.0.X.xxx.tar.xz
   ```

2. Выполните команду:

   ```
   cat platform/setup.yaml | grep version
   ```

Важно!

Необходимо, чтобы все ноды кластера были доступны друг для друга в сети. Для этого должны быть открыты необходимые порты (см. *Настройка сетевых правил доступа*).
Также перед установкой убедитесь, что:

- настроено разрешение имен нод средствами DNS
  или
- в файле `/etc/hosts` каждой ноды определено соответствие между адресами и именами нод.

Для проверки доступности нод выполните команду между нодами кластера:

```
ping <имя ноды>
```

Для установки Data Explorer используйте командную строку.

6 Настройка сетевых правил доступа

Для корректной работы Data Explorer должны быть разрешены соединения:

Соединение	Порт	Описание
Доступ к веб-интерфейсу и SSH-консоли		
Рабочая станция Офицера Безопасности → Центр расследований	TCP 443	Используется для доступа Офицера безопасности к веб-интерфейсу Центра расследований (центральная нода платформы).
Работа в кластере		
Сервер Платформы в режиме `office` → Сервер Платформы в режиме `central`	TCP 6443 TCP 2379, 2380 TCP 10251, 10252, 10255	Порты сервера Платформы в режиме `central`. Используются для взаимодействия Платформы в режиме `office` с Платформой в режиме `central`
Сервер Платформы в режиме `central` → Сервер Платформы в режиме `office`	TCP 10251, 10255 TCP 30000–32767	Порты сервера Платформы в режиме `office`. Используются для взаимодействия Платформы в режиме `central` с Платформой в режиме `office`
Сервер Платформы в режиме `central` ← → Сервер Платформы в режиме `office`	UDP 8472 TCP 10250	Используются для туннелирования трафика между узлами кластера
Сервер Платформы в режиме `central` ← → Сервер Платформы в режиме `office`	TCP 10256	Порт должен быть доступен на всех нодах кластера. Используется для проверки состояния компонента `kube-proxy`

7 Установка Data Explorer

> **Примечание:**
>
> Если вы устанавливаете Data Explorer на сервер, на котором уже установлены другие платформенные продукты, инсталлятор не запросит часть параметров, так как эти директории и настройки уже были указаны при первичной установке Платформы.

> **Важно!**
>
> В одном кластере может быть только один экземпляр Data Explorer.

Чтобы установить Data Explorer:

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям (см. *Типы установки, совместимость с другими продуктами, аппаратные и программные требования*).

   > **Примечание:**
   >
   > В ходе установки инсталлятор проверит наличие:
   >
   > - не менее 100 ГБ на диске для директорий размещения данных ClickHouse, PostgreSQL, NATS и бинарных данных. Эти директории необходимо указать при выполнении инструкций по установке. Если директории находятся на разных дисках, то проверятся наличие 100 ГБ свободного места на каждом из них;
   > - не менее 20 ГБ на диске для директорий с образами;
   > - не менее 8 ГБ ОЗУ;
   > - не менее 2 ядер процессора;
   > - поддержки инструкции SSE 4.2;
   > - установленного пакета `conntrack.`

2. Выполните шаги по подготовке сервера к установке Data Explorer (см. *Подготовка сервера*).
3. Создайте новую директорию на диске (например, `dataexplorer`):

   ```
   mkdir dataexplorer
   ```

4. Скопируйте архив `iw_dataexplorer_setup_2 .0.0.60 .tar.xz` в созданную директорию.
5. Перейдите в директорию, в которую был скопирован архив.
6. Распакуйте архив с дистрибутивом продукта в эту директорию:

   ```
   tar xvf iw_dataexplorer_setup_2.0.X.xxx.tar.xz
   ```

7. Запустите программу установки продукта:

```
./setup.py install --nodemode=<режим_установки_Платформы> --productmode=central
```

Примечание:

Чтобы установить:

- **на центральную ноду Платформы продукт в режиме central:**

```
./setup.py install --nodemode=central --productmode=central
```

- **на офисную ноду Платформы продукт в режиме central:**

```
./setup.py install --nodemode=office --productmode=central
```

Если вы не укажете режимы установки Платформы и продукта, инсталлятор по умолчанию выберет режим `central`.

Важно!

Во время установки могут быть недоступны продукты Платформы, установленные на сервере.

8. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
9. Введите "**y**", чтобы принять лицензионное соглашение, и нажмите **Enter**.

Примечание:

Если отклонить лицензионное соглашение, инсталлятор прервет процесс и завершит работу.

10. Если вы устанавливаете **центральную ноду Платформы** (`--nodemode=central`), 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**.
Если указать `0.0.0.0`, будут использованы все доступные сетевые интерфейсы.

Примечание:

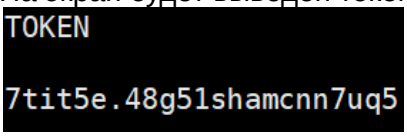
Здесь и далее для использования значений, предложенных по умолчанию, нажмите **Enter** без ввода значений.

11. Если вы устанавливаете **офисную ноду Платформы** (`--nodemode=office`):
    a. Укажите адрес центральной ноды Платформы в формате IP-адреса или доменного имени (например: `192.0.2.0` или `host.example.com`).

b. Укажите токен для подключения к центральной ноде Платформы.
Чтобы получить токен для подключения к центральной ноде Платформы:
   i. Подключитесь по ssh к консоли центральной ноды Платформы;
   ii. Выполните в терминале команду для получения токена:

```
kubeadm token list
```

На экран будет выведен токен:



Токен в нашем примере: `7tit5e.48g51shamcnn7uq5`

   iii. Укажите лейбл ноды (по умолчанию: `office`) и нажмите **Enter**.
Лейбл может состоять из букв латинского алфавита и/или цифр. Длина лейбла не должна превышать 32 символа.

12. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию: `80%`) и нажмите **Enter**.
13. Укажите путь для размещения данных Clickhouse (по умолчанию: `/opt/chdata`) и нажмите **Enter**.
14. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/opt/pgdata`) и нажмите **Enter**.
15. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
16. Укажите путь для размещения бинарных данных (по умолчанию: `/opt/dsdata`) и нажмите **Enter**.
17. Укажите путь для временного хранения событий Traffic Monitor перед их загрузкой в Платформу (по умолчанию: `/opt/factsldrtmdata`) и нажмите **Enter**.
18. Если вы устанавливаете **центральную ноду Платформы**, укажите порт подключения к веб-интерфейсу (по умолчанию: `443`) и нажмите **Enter**.
19. Дождитесь завершения установки Платформы.
20. Ознакомьтесь с отчетом об установке Платформы.



21. Дождитесь окончания процесса установки Data Explorer.
22. Ознакомьтесь с отчетом об установке.
23. Убедитесь, что все сервисы запущены, выполнив команду:

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

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

24. Чтобы вывести на экран информацию о Платформе, выполните команду:

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

Вывод команды должен содержать строку `DbState: commited`. Например:

```
platform Title: Infowatch Platform Version: 2.4.1.374 Node: my-server(central) Mode:
central DbState: commited
```

Чтобы начать работу в Data Explorer:

1. Установите в кластере Data Discovery и Data Analysis Service, если они еще не установлены. Подробнее см. *Data Discovery. Руководство по установке* и *Data Analysis Service. Руководство по установке, конфигурированию и администрированию*.
   При этом в Data Analysis Service обязательно должен быть включен модуль протокластеризации. Чтобы использовать функциональность поиска сущностей, также необходимо включить модуль распознавания именованных сущностей Data Analysis Service.
2. Настройте Data Analysis Service на обработку контентов, получаемых от Data Discovery. Подробнее см. *Data Analysis Service. Руководство по установке, конфигурированию и администрированию*. *Включение технологий Data Analysis Service в продуктах Платформы*.
3. Подключитесь к веб-интерфейсу Центра расследований. Для этого введите в браузере адрес и порт центральной ноды Платформы.
   Если веб-консоль уже была открыта до установки Модуля, то достаточно обновить страницу в браузере.
4. Data Explorer работает с документами, отсканированными Data Discovery. Чтобы они обрабатывались и отображались в Data Explorer, в задачах сканирования выбирайте режим **Определять похожие файлы**. Подробнее см. *Data Discovery. Руководство пользователя. Задача сканирования*.

8 Устранение неполадок

Во время установки Модуля возможны сбои: прерывания работы программы установки, отключение электричества и т.д. В этом случае Модуль будет установлен некорректно. В случае возникновения подобной ситуации следует сбросить установку. После сброса все данные сохранятся на сервере, а установку необходимо произвести заново (см. *Установка Data Explorer*). В процессе установки на вопрос об удалении существующих данных выберите ответ **Нет**.

Чтобы сбросить установку:

1. Запомните или сохраните пути к текущим директориям хранения данных. Получить список директорий можно, выполнив команду:

   ```
   cat /var/lib/iwplatform/data/volumes.txt
   ```

2. Запомните или сохраните лейблы нод. Чтобы посмотреть список лейблов в кластере, выполните команду:

   ```
   kubectl get node -n infowatch -o jsonpath="{range .items[*]}
   {.metadata.annotations.flannel\.alpha\.coreos\.com/public\-ip}
   {.metadata.labels.kubernetes\.io/hostname} {.metadata.labels.iwnode}{'\n'}{end}"
   ```

3. Перейдите в директорию, в которую был распакован архив с дистрибутивом при установке.
4. Выполните команду:

   ```
   ./setup.py reset
   ```

5. После сброса при установке присвойте нодам кластера те же лейблы, которые были до начала процедуры сброса.

Важно!

При сбросе установки Модуля автоматически производится сброс всех других продуктов Платформы, установленных на сервере.

Если произведен сброс установки на центральной ноде Платформы, станут недоступны компоненты всех продуктов в кластере. В этом случае выполните сброс на каждой офисной ноде.

После установки Data Explorer повторно установите и другие продукты в кластере.

9 Удаление Data Explorer

Чтобы удалить Data Explorer:

1. Перейдите в директорию на сервере, в которую был распакован архив с дистрибутивом при установке Data Explorer.
2. Выполните команду:

```
./setup.py remove
```

3. Дождитесь завершения удаления. Программа удалит компоненты Data Explorer. Данные Data Explorer удалены не будут. При необходимости вы можете удалить данные вручную из директорий, указанных при установке.

Примечание:

В случае распределенной установки, если Data Explorer установлен на офисной ноде и на ней отсутствуют другие продукты, то после удаления Data Explorer также рекомендуется удалить компоненты платформы. Для этого после выполнения команды `./setup.py remove`, также выполните команду:

```
./setup.py reset
```

Если Data Explorer установлен на центральной ноде или если на офисной ноде вместе с ним также установлены другие продукты, выполнять команду `./setup.py reset` категорически не рекомендуется.

Чтобы узнать, какие продукты установлены в кластере, вы можете перейти в директорию с инсталлятором и выполнить команду:

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