

INFOWATCH

InfoWatch Data Explorer. Руководство по установке

10/09/2026

© 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 11

5.1 Шаги по подготовке сервера: 11

6 Настройка сетевых правил доступа 20

7 Установка Data Explorer 21

8 Устранение неполадок 26

9 Обновление Data Explorer 27

9.1 Варианты обновления Data Explorer 27

9.2 Особенности обновления кластера Центра расследований 27

9.3 Обновление Data Explorer с помощью сброса установки (reset) 28

10 Удаление Data Explorer 32

В настоящем руководстве вы можете найти сведения по установке, обновлению 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, обновления 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 2.3**
- **Data Analysis Service 1.7**

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.

Data Explorer 2.1 реализован на базе Платформы версии 2.6.

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 2.1 совместно** с:

- **Data Discovery 2.3**
- **Data Analysis Service 1.7**

> **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 2.1 поддерживает только обновление с помощью сброса и переустановки на старые данные.

Подробнее о процессе обновления и поддерживаемых вариантах см. *Обновление Data Explorer*.

4.3 Аппаратные требования

Минимальные системные требования, необходимые для установки:

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

Процессор	ОЗУ	Жесткий диск
Поддержка 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: • 1.7.1.0 – 1.7.9.46 • 1.8.1.0 – 1.8.5.46 • Astra Linux Special Edition "Орел", версии: • 1.7.5.0 – 1.7.9.46 • Astra Linux Special Edition "Воронеж", версии: • 1.7.5.0 – 1.7.9.46 • Astra Linux Special Edition версии 1.8.5 сертифицированная • Red Hat Enterprise Linux, версии: • 7.9 • 8.4 – 8.10 • Oracle Linux, версии: • 7.9 • 8.4 – 8.10 • РЕД ОС, версии: • 7.3.3 – 7.3.6 • 8.0.0 • ОС Альт: • Сервер 10.1.0 – 10.2.2 • СП Сервер 10.1.0 – 10.2.2 **Примечание**: Вы можете установить Сервис на ОС Альт СП во внешний кластер kubernetes, развернутый до установки, или в кластер kubernetes, который создаст инсталлятор. • Мос.ОС Серверная Арбат 15.5 **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 или обновлением Data Explorer обязательно подготовьте сервер.

5.1 Шаги по подготовке сервера:

1. Программа установки написана на языке Python 3. Установите интерпретатор этого языка версии 3.6 или более поздней.
   Пакет с интерпретатором **не** входит в состав дистрибутива Data Explorer.
2. На некоторых дистрибутивах ОС не установлена часть стандартных модулей Python 3, в том числе `importlib-metadata` и `pyyaml`. Установите их с помощью следующих команд:

   - **для Red Hat Enterprise Linux, Oracle Linux и РЕД ОС**

     ```
     yum install python3-importlib-metadata
     yum install python3-pyyaml
     ```

   - **для ОС Astra Linux**

     ```
     apt-get install python3-importlib-metadata
     apt-get install python3-distutils
     apt-get install python3-mako
     apt-get install python3-yaml
     ```

   - **для ОС Альт**

     ```
     apt-get install python-modules-json
     apt-get install python-modules-distutils
     apt-get install python3-modules-sqlite3
     apt-get install python3-module-importlib-metadata
     apt-get install python3-module-yaml
     ```

   - **для Мос.ОС**

     ```
     zypper install python3-importlib-metadata
     zypper install python3-PyYAML
     ```

     > **Примечание:**
     >
     > Пакеты не входят в состав дистрибутива Data Explorer.
     >
     > Пакеты могут отсутствовать в репозиториях некоторых операционных систем. В этом случае загрузите и установите требуемые пакеты вручную.

3. **На сервере под управлением Мос.ОС:**

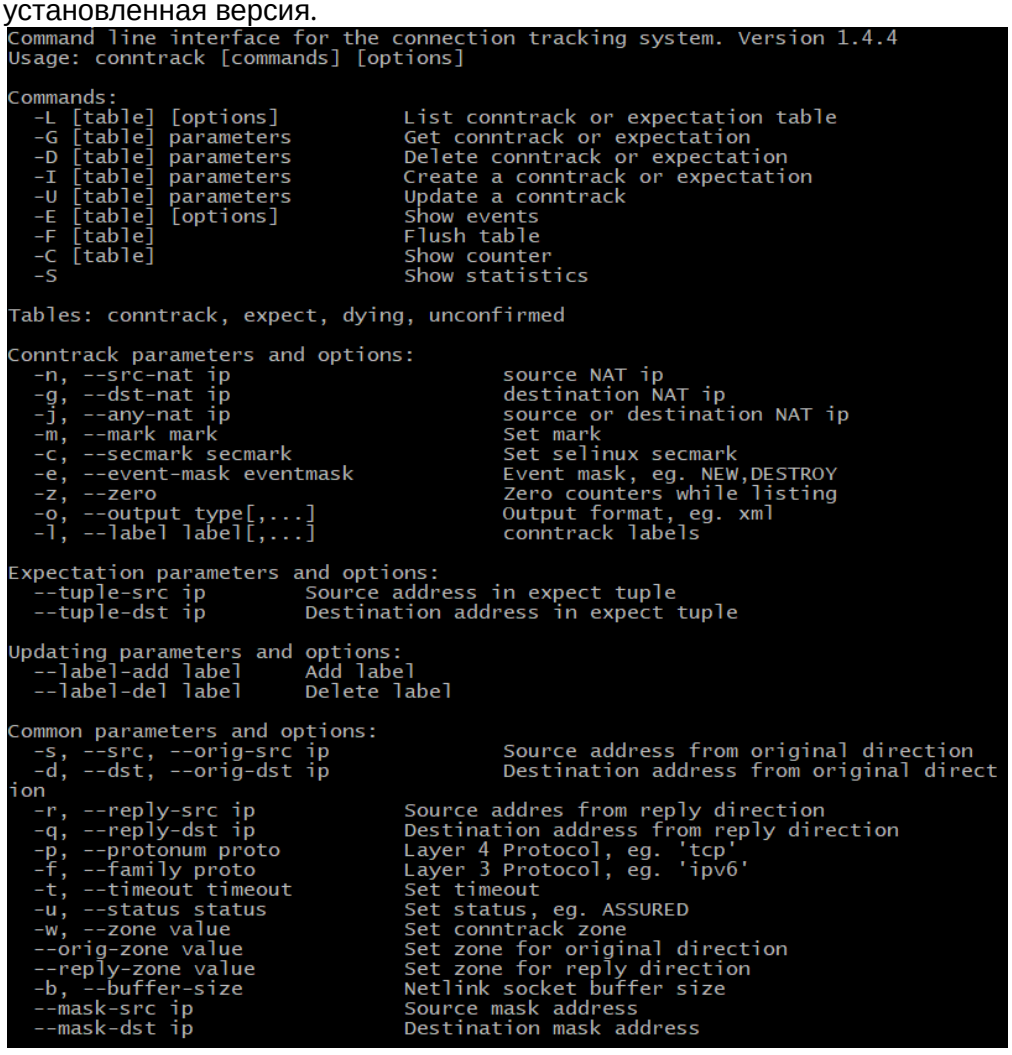
   Убедитесь, что доступны официальные репозитории ОС:

- `software`
- `update`
- `oss`

4. 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.
5. Для корректной работы Сервиса настройте сетевые правила доступа (подробнее см. *Настройка сетевых правил доступа*).
6. Data Explorer использует компонент Kubernetes. Для корректной установки Модуля и работы Kubernetes на сервере должны быть установлены следующие пакеты:
   - `conntrack` или `conntrack-tools` (пакет необходимо установить, даже если `libnetfilter_conntrack` уже установлен).
     Убедитесь, что пакет установлен. Для этого введите в командной строке:

     ```
     conntrack
     ```

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



     Если пакет не установлен, установите его с помощью команды:

- **для Red Hat Enterprise Linux, Oracle Linux и РЕД ОС**

  ```
  yum install conntrack
  ```

- **для ОС Astra Linux**

  ```
  apt-get install conntrack
  ```

- **для ОС Альт**

  ```
  apt-get install conntrack-tools
  ```

- **для Мос.ОС**

  ```
  zypper install conntrack-tools
  ```

Если пакет недоступен в репозитории, скачайте его самостоятельно, например, из официального репозитория РЕД ОС. Затем перейдите в директорию с пакетом и установите его вручную с помощью команды вида:

- **для Red Hat Enterprise Linux, Oracle Linux, РЕД ОС и ОС Альт**

  ```
  rpm -Uhv ./<имя_пакета>
  ```

- **для ОС Astra Linux**

  ```
  dpkg -i ./<имя_пакета>
  ```

- **для Мос.ОС**

  ```
  zypper install <имя_пакета>
  ```

- `socat` – аналогично пакету `conntrack`.

7. Если вы используете антивирус, настройте его для совместной работы с Data Explorer (см. статью Базы знаний *Настройка антивируса для продуктов Платформы*).
8. **На сервере под управлением Мос.ОС:**

   Установите пакеты `ethtool`, `app_armor` и `sysctl` с зависимостями:

   ```
   zypper install ethtool
   zypper install patterns-base-apparmor
   zypper install procps
   zypper install libprocps7
   ```

9. **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:

  ```
  yum 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
  ```

10. **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 python3-module-yaml
apt-get install python3-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
```

f. Для присвоения имени образу выполните команду:

```
podman tag registry.altlinux.org/k8s-c10f2/pause:3.10 registry.k8s.io/pause:3.10
```

g. Установите Kubernetes с помощью команд:

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

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

```
unset http_proxy
```

```
unset https_proxy
```

i. Создайте кластер:

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

j. 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.

k. 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
```

l. Загрузите манифест Flannel:

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

m. 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.

n. Откройте на редактирование конфигурацию CoreDNS:

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

o. 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
  }
```

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

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

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

```
kubectl get pods -A
```

Все поды должны быть в статусе `Running`.

s. Смените директорию для временных файлов:

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

11. 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
```

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

Дистрибутив Data Explorer представляет собой архив **`iw_dataexplorer_setup_2.1.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_2.1.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*).
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 .1.X.xxx .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_2.1.X.xxx.tar.xz
   ```

7. **Для установки Data Explorer на ОС Альт СП 10 во внешний кластер kubernetes:**

   Вы должны использовать Kubernetes из репозиториев ОС.
   Для этого:

   a. Выполните действия для ОС Альт СП 10 из статьи *Подготовка сервера*.
   Если вы уже выполнили подготовку, пропустите этот шаг.
   b. Выполните команду:

   ```
   kubectl taint nodes <hostname_ноды> node-role.kubernetes.io/control-plane:NoSchedule
   -
   ```

   c. На следующем шаге при запуске инсталлятора дополнительно укажите опцию **`--externalK8S=True`**
8. 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.

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

Примечание:

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

11. 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:

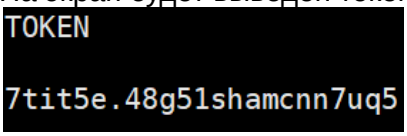
Здесь и далее для использования значений, предложенных по умолчанию, нажмите **Enter** без ввода значений.

12. 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.

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



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

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

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

25. 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: 2.6.0.374 Node: my-server(central) Mode:
central DbState: commited
```

26. Если до установки Data Explorer в кластере был установлен Device Monitor, обновите конфигурационный файл `n.yaml`:
    a. Подключитесь к центральной ноде Платформы.
    b. Если Device Monitor установлен на офисной ноде Платформы, скопируйте на центральную его дистрибутив и распакуйте.
    c. На центральной ноде Платформы перейдите в папку, где распакован дистрибутив Device Monitor.
    d. Запустите скрипт **setup.sh**, выполнив команду:

    ```
    ./setup.sh
    ```

    e. Выберите в меню пункт **Utilities**.
    f. Выберите **Fix n.yaml file**.
    g. Введите IP-адрес сервера Device Monitor и дождитесь окончания процесса.

    > **Примечание:**
    >
    > Если вы обновляете несколько продуктов в кластере, обновите `n.yaml` только после обновления последнего продукта.

Чтобы начать работу в Data Explorer:

1. Установите в кластере Data Discovery и Data Analysis Service, если они еще не установлены. Подробнее см. *InfoWatch Data Discovery. Руководство по установке* и *InfoWatch 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. *InfoWatch 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. *InfoWatch 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 Обновление Data Explorer

Data Explorer поддерживает обновление с версии **2.0**.

Обновление Data Explorer производится вручную, с помощью командной строки.

Для обновления Data Explorer используется архив `iw_dataexplorer_setup_x.x.x.xx.tar.xz`, где x.x.x.xx – номер версии. Архив входит в состав дистрибутива. Архив содержит полный набор бинарных модулей образов контейнеров, необходимых для развертывания Системы без доступа к сети Интернет. Также архив содержит программу обновления.

> **Важно!**
>
> Для успешного обновления Data Explorer необходимо не менее 100 Гбайт свободного места на жестком диске.

9.1 Варианты обновления Data Explorer

Data Explorer 2.1 поддерживает только Обновление Data Explorer с помощью сброса установки (reset).

Чтобы **обновить распределенный кластер** Центра расследований с несколькими установленными продуктами:

1. **Обновите центральную ноду** кластера и все установленные на ней продукты.
2. **Обновите офисные ноды** и все установленные на них продукты.

9.2 Особенности обновления кластера Центра расследований

Перед обновлением кластера рекомендуем ознакомиться с инструкциями всех установленных продуктов. Если в кластере установлено несколько продуктов, перед обновлением учтите особенности обновления каждого из них.

Особенности и рекомендации для обновления распределенного кластера Центра расследований:

- Перед обновлением рекомендуем выключить Систему и выполнить ее резервное копирование;
- Для планирования обновления ознакомьтесь с составом кластера. Чтобы отобразить информацию о Платформе и установленных продуктах, перейдите в директорию с инсталлятором и выполните команду:

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

- Если вы обновляете Data Explorer в одном кластере с другими продуктами InfoWatch, то убедитесь, что **версия Платформы совпадает у всех продуктов на всех нодах**. В противном случае продукты, установленные на старой версии Платформы, необходимо обновить;
  Чтобы узнать версию Платформы Сервиса:

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

Пример для версии 2.1.0.98:

```
tar -xvf iw_dataexplorer_setup_2.1.0.98.tar.xz
```

2. Выполните команду:

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

- В кластере с **Prediction**, на время любого обновления **остановите расчет рейтинга** (подробнее см. *InfoWatch Prediction. Руководство по установке. Обновление Prediction*);
- Если вы обновляете продукты с помощью сброса установки (`reset`):
  - До сброса установки запомните или сохраните пути хранения данных. Получить список папок можно, выполнив команду:

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

  - В кластере с **Data Discovery**:
    - На время любого обновления остановите все задачи сканирования в интерфейсе Data Discovery;
    - Чтобы сохранить настройки зон и серверов в новой версии, перед сбросом установки подключитесь к ноде, на которой Data Discovery установлен в режиме `central` и **остановите сервис Discoperator** с помощью команды:

```
kubectl scale --replicas=0 deployment discoperator-<лейбл_ноды> -n infowatch
```

Пример для Data Discovery в режиме central на офисной ноде с лейблом lv426:

```
kubectl scale --replicas=0 deployment discoperator-lv426 -n infowatch
```

  - В кластере с **Data Analysis Service** для переноса настроек, перед обновлением запустите скрипт миграции переменных. Подробнее см. *InfoWatch Data Analysis Service. Руководство по установке, конфигурированию и администрированию. Обновление Data Analysis Service*.

9.3 Обновление Data Explorer с помощью сброса установки (reset)

Важно!

Чтобы обновить весь распределенный кластер продуктов на Платформе с помощью сброса (reset) установки, действуйте в следующей последовательности:

1. Выполните **сброс на офисных** нодах с продуктами в режиме `office` .
2. Выполните **сброс на офисных** нодах с продуктами в режиме `central` .
3. Выполните **сброс центральной** ноды.
4. **Установите центральную** ноду кластера.
5. **Установите офисные** ноды с продуктами в режиме `central` .

6. **Установите офисные** ноды с продуктами в режиме `office`.

В рамках обновления кластера выполняйте сброс установки только один раз для каждой ноды.

Обновление с помощью сброса установки состоит из следующих шагов:

1. Сброс установки **с помощью нового инсталлятора**. При сбросе данные Системы не будут удалены.
2. Установка новых версий Платформы и модуля с указанием уже имеющихся папок с данными.

Примечание:

Если вы используете удаленное подключение по протоколу SSH, чтобы избежать проблем в случае разрыва соединения с сервером, рекомендуем использовать утилиту Screen. При отключении от утилиты запущенные в ней процессы не прервутся, что позволит безопасно продолжить обновление.

Чтобы обновить Data Explorer с помощью сброса установки:

1. Выполните шаги по подготовке сервера к обновлению (см. "Подготовка сервера").
2. Создайте новую директорию на диске (например, `DE`):

```
mkdir DE
```

3. Скопируйте архив `iw_dataexplorer_setup_x.x.x.xx.tar.xz` в созданную директорию.
   В нашем примере будет использована версия `2.1.0.60`, ей соответствует архив `iw_dataexplorer_setup_2 .1.0.60 .tar.xz`.
4. Перейдите в директорию, в которую был скопирован архив.
5. Распакуйте архив с дистрибутивом Data Explorer в эту директорию:

```
tar -xvf iw_dataexplorer_setup_2.1.0.60.tar.xz
```

6. После сброса при установке новой версии присвойте нодам кластера те же лейблы, которые были до обновления.
   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}"
```

7. До сброса установки запомните или сохраните пути к текущим директориям хранения данных. Получить список директорий можно, выполнив команду:

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

8. Выполните **сброс** текущей установки **с помощью инсталлятора новой версии**:

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

Важно!

Если на сервере установлены другие продукты Платформы, установки этих продуктов будут сброшены в результате сброса установки Платформы. При сбросе установки на центральной ноде продукты на офисных нодах перестанут функционировать.

После установки новой версии Data Explorer повторно установите продукты Платформы, указав директории с имеющимися данными.

Если на этом сервере вы **уже обновили другой продукт** до совместимой версии, **не выполняйте повторный сброс** при обновлении Data Explorer, так как требуемая версия Платформы уже установлена.

Если продукт установлен **на офисной ноде в режиме central**, после сброса установки у добавленных ролей пользователя будет **сброшен доступ к продуктам**.

9. Дождитесь окончания процесса сброса установки Платформы и продукта.
10. Перезагрузите сервер с помощью команды:

```
reboot
```

11. Если вы обновляетесь с переходом на другой сервер или на новую ОС, скопируйте на другой раздел или на новый сервер директории с данными, которые были указаны при установке.
Обязательно копируйте директории с сохранением прав и владельцев. Для копирования используйте стандартные средства, например утилиту `rsync`.
12. Убедитесь, что в разделе с директорией `/var/lib/containerd` доступно не менее 30 ГБ дискового пространства.
Чтобы проверить доступное дисковое пространство, используйте команду:

```
df -h /var/lib/containerd
```

Примечание:

Чтобы освободить дисковое пространство, вы можете удалить директорию с образами контейнеров прошлых версий `/var/lib/containerd`. Для этого выполните команду:

```
rm -rf /var/lib/containerd
```

Данная команда удаляет все образы контейнеров. Не используйте ее, если на сервер уже установлены новые версии Data Explorer или других продуктов InfoWatch.

13. Удалите данные прошлой версии из директорий, указанных ранее при установке.
14. Установите новую версию Data Explorer (см. *Установка Data Explorer*).

15. Если до сброса на сервере были установлены и другие продукты, установите версии продуктов, совместимые с Data Explorer (см. *Типы установки, совместимость с другими продуктами, аппаратные и программные требования*).
16. Если Data Explorer установлен в распределенном кластере, обновите Платформу и продукты на других серверах кластера до версий, совместимых с Data Explorer.
17. Если Device Monitor был обновлен в кластере до Data Explorer, обновите конфигурационный файл `n.yaml`:
    a. Подключитесь к центральной ноде Платформы.
    b. Если Device Monitor установлен на офисной ноде Платформы, скопируйте на центральную его дистрибутив и распакуйте.
    c. На центральной ноде Платформы перейдите в папку, где распакован дистрибутив Device Monitor.
    d. Запустите скрипт **setup.sh**, выполнив команду:

    ```
    ./setup.sh
    ```

    e. Выберите в меню пункт **Utilities**.
    f. Выберите **Fix n.yaml file**.
    g. Введите IP-адрес сервера Device Monitor и дождитесь окончания процесса.

    > **Примечание:**
    >
    > Если вы обновляете несколько продуктов в кластере, обновите **`n.yaml`** только после обновления последнего продукта.

18. Очистите кеш браузера, в котором работали до обновления продукта. Веб-интерфейс Центра расследований доступен по адресу центральной ноды Платформы.

> **Важно!**
>
> Если Data Explorer установлен **на офисной ноде Платформы в режиме central**, то в результате сброса прошлой установки у добавленных ролей пользователя будет **сброшен доступ к продуктам**. После завершения обновления перейдите в **Настройки** и заново настройте доступ к продуктам в этих ролях (о ролях см. *InfoWatch Data Explorer. Руководство администратора,* статью *Роли*).
>
> После обновления у добавленных ролей пользователя не будет доступа к созданию и отправке уведомлений. Чтобы добавить эту возможность, включите роли функцию *Отправка и получение уведомлений*.

10 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
```