INFOWATCH

InfoWatch Data Discovery. Руководство по установке

12/01/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 5

2 Комплект документов 6

3 Техническая поддержка пользователей 7

4 Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования 8

4.1 Типы установки и совместимость с другими продуктами InfoWatch 8

4.2 Типы обновления 10

4.3 Экспорт данных в Traffic Monitor 10

4.4 Аппаратные и программные требования 10

4.4.1 Аппаратные требования 10

4.4.2 Программные требования 12

5 Подготовка сервера 13

5.1 Шаги по подготовке сервера: 13

6 Настройка сетевых правил доступа 15

7 Установка Data Discovery 18

7.1 Варианты запуска установки Data Discovery 19

7.2 Модуль контентного анализа 19

7.3 Установка Data Discovery в интерактивном режиме 19

7.4 Установка Data Discovery с указанием параметров в командной строке 24

7.5 Установка Модуля контентного анализа в интерактивном режиме 28

7.6 Установка Модуля контентного анализа с указанием параметров в командной строке 32

8 Установка лицензии и плагина Traffic Monitor 37

8.1 Экспорт данных в Traffic Monitor 37

8.2 Импорт данных из Traffic Monitor 37

9 Устранение неполадок 39

10 Обновление Data Discovery 40

10.1 Настройки и данные Системы 40
10.2 Варианты обновления Data Discovery 40
10.3 Обновление Data Discovery с помощью сброса установки (reset) 41
10.4 Переустановка Data Discovery в другой кластер 45
11 Удаление Data Discovery 47

Настоящее руководство содержит сведения по установке, обновлению и удалению InfoWatch Data Discovery (далее Система или Data Discovery) – программного обеспечения, предназначенного для поиска конфиденциальной информации на общих сетевых ресурсах, рабочих станциях, серверах и в хранилищах документов.

1 Аудитория

Данное руководство предназначено для инженеров внедрения и офицеров безопасности, которые будут работать с Системой и заниматься ее администрированием. Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и MS Windows.

2 Комплект документов

В документацию входят:

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

Сопутствующая документация по системе InfoWatch Traffic Monitor (далее Traffic Monitor) включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию системы InfoWatch Traffic Monitor (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, подготовка 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 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 РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

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

4.1 Типы установки и совместимость с другими продуктами InfoWatch

InfoWatch Data Discovery является частью Центра расследований InfoWatch.

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

- Activity Monitor 3.2
- Data Access Tracker 2.2
- Data Discovery 2.0
- Prediction 3.2
- Vision 3.4

Каждый продукт может быть установлен и работать отдельно, однако использование нескольких продуктов одновременно существенно повышает возможности офицера по обеспечению информационной безопасности компании.

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 Платформы и продукта 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. Если вы установите в кластер продукт на новой версии Платформы, для корректной работы вам будет необходимо обновить все 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.

- Для работы Data Discovery в режиме `office` необходимо, чтобы в кластере был экземпляр в режиме `central`.
- Data Access Tracker и Prediction поддерживают установку только в режиме `central`. При этом продукты поддерживают установку как на центральную, так и на офисные ноды 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.

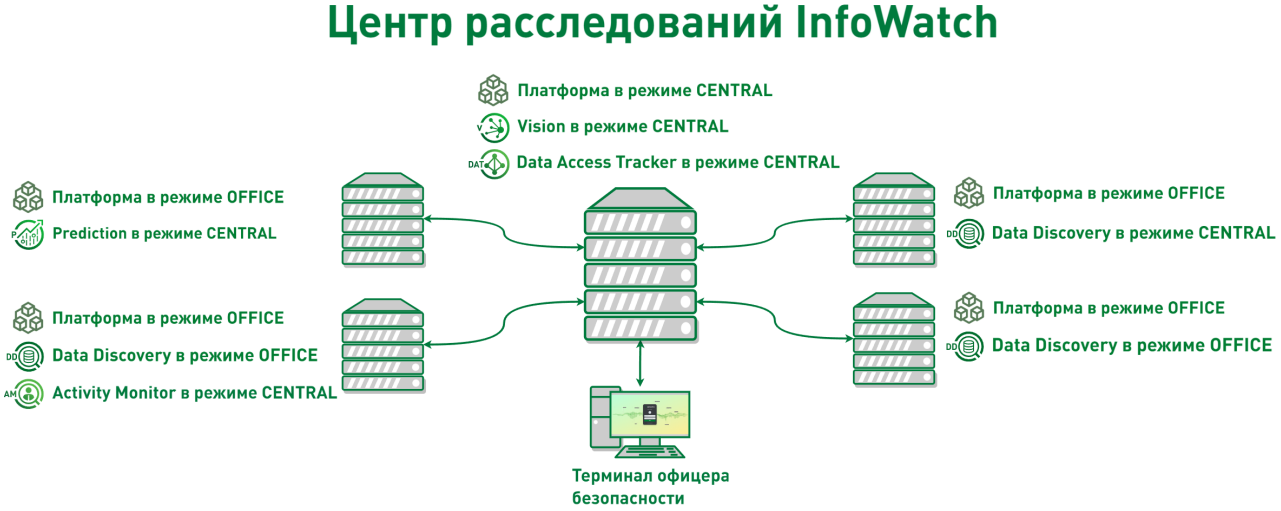
Вы можете установить **Data Discovery 2.0 совместно** с:

- **Activity Monitor 3.2**
- **Data Access Tracker 2.2**
- **Prediction 3.2**
- **Vision 3.4**

Примечание:

Для расчета аппаратных требований при совместной установке учитывайте требования каждого продукта. Для точного расчета требований под конкретный проект обратитесь в службу технической поддержки компании InfoWatch.

Ниже представлен **пример** распределенного кластера Центра расследований с совместными установками нескольких продуктов.



Подробнее о процессе установки см. "Установка Data Discovery".

4.2 Типы обновления

Data Discovery 2.0 поддерживает только обновление с помощью сброса и переустановки на прошлые данные.

Подробнее о процессе обновления см. "Обновление Data Discovery".

4.3 Экспорт данных в Traffic Monitor

Data Discovery имеет возможность экспорта данных в InfoWatch Traffic Monitor. Data Discovery взаимодействует с Traffic Monitor:

- версии 6.10.x (6.10.15 и выше);
- версии 7.x (7.1 и выше).

Для настройки см. статьи:

- "Установка лицензии и плагина Traffic Monitor";
- "InfoWatch Data Discovery. Руководство администратора", "Зоны и серверы".

4.4 Аппаратные и программные требования

4.4.1 Аппаратные требования

Аппаратные требования Data Discovery зависят от сетевого окружения и предполагаемой нагрузки. Ниже приведена примерная конфигурация сервера Data Discovery для обработки 50 хостов в одной задаче сканирования:

Компонент	Рекомендуемые требования
ЦПУ	8 ядер, 16 потоков Intel Xeon или аналог, с поддержкой инструкций SSE 4.2

Компонент	Рекомендуемые требования
ОЗУ	16 GB
Диск	• Дисковый массив: RAID 5 • Диски: 10K HDD • Объем дискового массива: 400 GB **Примечание**: Требуемый объем дискового массива зависит от количества и объема сканируемых файлов. **Важно!** Если использовать функциональность InfoWatch Data Analysis Service и/или Модуля контентного анализа, Data Discovery будет занимать дополнительный объем дискового пространства для хранения извлеченных текстовых контентов. Рекомендуем увеличить объем доступного дискового пространства на 40%, но учитывайте, что требуемое дополнительное пространство зависит от объема текстовых данных и особенностей документооборота компании
Сеть	1 Gbps LAN

Примечание:

При расчете аппаратных требований для совместной установки рекомендуется суммировать требования Data Discovery и требования других продуктов для каждого компонента.

Например: если для продукта требуется 24 GB оперативной памяти, то для совместного функционирования Data Discovery и этого продукта требуется 40 GB оперативной памяти.

Модуль контентного анализа, используемый для обнаружения объектов защиты в текстовых данных, вы можете установить на одном сервере с Data Discovery или отдельно.
Если вы будете использовать **Модуль контентного анализа на одном сервере с Data Discovery**:

- для сканирования хранилищ одной задачей с одним сканером добавьте к аппаратным требования Data Discovery **не менее**:
  - 2-х ядер ЦПУ;
  - 1 ГБ ОЗУ;
  - 50 ГБ дискового пространства.
- для сканирования файловых хранилищ с большим объемом данных одновременно двумя или более задачами сканирования, с одним сканером в каждой, добавьте **не менее**:
  - 4-х ядер ЦПУ;
  - 2 ГБ ОЗУ;
  - 50 ГБ дискового пространства.

При дополнительном увеличении предполагаемой нагрузки рекомендуем установить дополнительные Модули контентного анализа на отдельные серверы. Нагрузка между ними будет распределена равномерно.
Если вы будете использовать **Модуль контентного анализа на отдельном сервере**, обеспечьте **не менее**:

- 4-х ядер ЦПУ;

- 12 ГБ ОЗУ;
- 100 ГБ дискового пространства.

Важно!

Не рекомендуется устанавливать Data Discovery и Traffic Monitor на один сервер. Увеличение нагрузки от Traffic Monitor может привести к некорректной работе Data Discovery.

4.4.2 Программные требования

Для установки и работы Системы должно быть использовано следующее программное обеспечение:

Тип ПО	Варианты
Операционная система	• Astra Linux Special Edition 1.7 "Орел" версии 1.7.x, начиная с 1.7.5 • Astra Linux Special Edition 1.7 "Воронеж" версии 1.7.x, начиная с 1.7.0 (1.7.0-11.06.2021_12.40) • Astra Linux Special Edition 1.7 "Смоленск " версии 1.7.x, начиная с 1.7.0 • Red Hat Enterprise Linux: • версии 7.x (начиная с 7.7); • версии 8.x (начиная с 8.0); • Oracle Linux: • версии 7.x (начиная с 7.9); • версии 8.x (начиная с 8.4); • РЕД ОС: • версии 7.x.x (начиная с 7.3.1); • ОС Альт: • Рабочая Станция 10; • Сервер Виртуализации 10. **Важно**: Модули **Netfilter** и **NAT** должны быть загружены в ядро ОС
Браузер	• Google Chrome; • Яндекс.Браузер. **Важно**: В браузере должна быть реализована аппаратная поддержка WebGL/WebGL2

Примечание:

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

Модуль контентного анализа поддерживает установку на те же ОС, что и Data Discovery.

5 Подготовка сервера

Перед установкой Data Discovery выполните шаги по подготовке сервера.

5.1 Шаги по подготовке сервера:

1. Программа установки написана на языке Python версии 2.7. Установите интерпретатор языка Python версии 2.7. Пакет с интерпретатором не входит в состав дистрибутива продукта.
2. Настройте правила POD сети или отключите межсетевой экран (подробнее см. статьи Базы знаний "Конфликты при взаимодействии firewalld и Kubernetes ", "Полное отключение межсетевого экрана").
3. Для корректной работы продукта настройте сетевые правила доступа (подробнее см. "Настройка сетевых правил доступа").
4. Data Discovery использует Kubernetes. Для корректной работы Kubernetes установите пакеты:
   - **socat**;
   - **conntrack** или **conntrack-tools** (пакет необходимо установить, даже если **libnetfilter_conntrack** уже установлен).

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

5. Если вы используете антивирус, настройте его для совместной работы с Системой (см. статью Базы знаний "Настройка антивируса для продуктов Платформы").
6. Если в операционной системе используется SELinux, установите пакет **container-selinux**. Данный пакет необходим для корректной работы Data Discovery совместно с SELinux.

   > **Примечание:**
   >
   > Пакет не входит в состав дистрибутива продукта.
   >
   > Пакет может отсутствовать в репозиториях некоторых операционных систем. В этом случае загрузите и установите требуемый пакет вручную.

7. Если установка продукта проводится 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 загрузите и установите требуемые пакеты вручную.

8. Если вы устанавливаете продукт в ОС Astra Linux Special Edition, отключите настройку `astra-nochmodx-lock`.
   Выполните команду:

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

6 Настройка сетевых правил доступа

Для корректной работы должны быть разрешены соединения:

Доступ к веб-интерфейсу и SSH-консоли		
Рабочая станция Администратора → Сервер Data Discovery	TCP 22	Порт сервера Data Discovery. Используется для управления сервером Data Discovery с помощью протокола SSH
Соединение	Порт	Описание
Рабочая станция Офицера Безопасности → Центр расследований	TCP 443	Порт для подключения к веб-интерфейсу Центра расследований (центральная нода Платформы). Значение по умолчанию: **443**. Вы указываете значение во время установки Платформы. Чтобы изменить номер порта: 1. Произведите сброс установки Системы (см. "Устранение неполадок"). 2. Установите Систему повторно, указав новое значение.
Соединения с внешними системами		
Сервер Data Discovery → Сервер Traffic Monitor	TCP 9100	Порт сервера Traffic Monitor. Используется для передачи данных из Data Discovery в Traffic Monitor через XAPI
Сервер Data Discovery → LDAP-сервер	TCP 3268 TCP 389	Порты LDAP-сервера. Используются для интеграции Data Discovery с LDAP-каталогами
Сервер Data Discovery → LDAPS-сервер	TCP 3269 TCP 636	Порты LDAPS-сервера. Используются для интеграции Data Discovery с LDAPS-каталогами
Сервер Data Discovery → DNS-серверы	UDP 53	Порт DNS-сервера. Используется для разрешения DNS-запросов
Сервер Data Discovery → NTP-серверы	UDP 123	Порт NTP-сервера. Используется для синхронизации времени
Сервер Data Discovery → Почтовый сервер	Для протокола :	Порты почтового сервера. Указаны значения по умолчанию.

Доступ к веб-интерфейсу и SSH-консоли		
Рабочая станция Администратора → Сервер Data Discovery	TCP 22	Порт сервера Data Discovery. Используется для управления сервером Data Discovery с помощью протокола SSH
Соединение	Порт	Описание
	• TLS - 465 • START TLS - 587	Используются для отправки почтовых уведомлений Prediction и Activity Monitor. Data Discovery использует почтовый сервер только для регулярной отправки отчетов
Подключение к ресурсам для сканирования (указаны протоколы или хранилища)		
Сервер Data Discovery → SMB	TCP 139, 445	Порт хоста с SMB-подключением. Для сканирования общих сетевых ресурсов и рабочих станций под управлением ОС MS Windows
Сервер Data Discovery → SSH	TCP 22	Порт хоста с SSH-подключением. Для сканирования серверов и рабочих станций под управлением ОС семейства Linux
Сервер Data Discovery → SharePoint	TCP 443	Порт хоста с SharePoint-подключением. Для сканирования библиотек документов в SharePoint Server 2016 по протоколу HTTPS
Сервер Data Discovery → FTP	TCP 21	Порт хоста с FTP-подключением. Для сканирования файловых ресурсов по протоколу FTP
Сервер Data Discovery → WebDAV (Nextcloud)	TCP 443	Порт хоста с WebDAV-подключением. Для сканирования хранилищ данных Nextcloud по протоколу WebDAV
Сервер Data Discovery → Alfresco	TCP 443	Порт хоста с системой Alfresco. Для сканирования серверов системы управления контентом Alfresco Community Edition по протоколам HTTP/HTTPS
Примечание: Для подключения к ресурсам сканирования указаны порты по умолчанию. Если в вашей сетевой инфраструктуре используются другие порты подключения, учитывайте это при создании задач сканирования и добавлении хостов		
Работа в кластере		

Доступ к веб-интерфейсу и SSH-консоли		
Рабочая станция Администратора → Сервер Data Discovery	TCP 22	Порт сервера Data Discovery. Используется для управления сервером Data Discovery с помощью протокола SSH
Соединение	Порт	Описание
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 Discovery

Дистрибутив представляет собой архив **`iw_discovery_setup_2.1.X.xxx.tar.xz`**, где `xxx` – номер сборки. Архив содержит полный набор бинарных модулей образов контейнеров, необходимых для развертывания Платформы и компонентов Data Discovery без доступа к Интернету (offline-установка), а также - программу установки.

Для установки Data Discovery используйте командную строку.

Вы можете установить Data Discovery:

- на отдельном сервере;
- в кластере из серверов Data Discovery;
- на сервере совместно с другими продуктами;
- в кластере с другими продуктами.

Важно!

Если вы устанавливаете Data Discovery в одном кластере с другими продуктами InfoWatch, 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 устанавливаемого продукта:

1. Распакуйте архив с дистрибутивом продукта. В нашем примере, в директорию `/ddiscovery`. Для этого перейдите в директорию и выполните команду:

   Пример для версии 2.0.0.15:

   ```
   tar -xvf iw_discovery_setup_2.1.0.15.tar.xz
   ```

2. Выполните команду:

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

Важно!

Все ноды кластера должны быть доступны друг для друга в сети. Для этого откройте 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>
```

7.1 Варианты запуска установки Data Discovery

Вы можете запустить установку Data Discovery:

- **в интерактивном режиме** - инсталлятор последовательно запросит параметры установки (см. "Установка Data Discovery в интерактивном режиме");
- **с указанием параметров** установки в команде запуска инсталлятора (см. "Установка Data Discovery с указанием параметров в командной строке").

В обоих вариантах запуска инсталлятор поддерживает и совместную установку с другими продуктами Центра расследований на одном сервере, и распределенную установку в кластере.

7.2 Модуль контентного анализа

Чтобы обнаруживать объекты защиты в просканированных текстовых файлах без отправки данных на анализ в Traffic Monitor, Data Discovery использует отдельный Модуль контентного анализа.

Модуль контентного анализа должен быть установлен в одном кластере с Data Discovery. Его можно установить на отдельный сервер или совместно с Data Discovery.

Вы можете запустить установку Модуля контентного анализа:

- **в интерактивном режиме** - инсталлятор последовательно запросит параметры установки (см. "Установка Модуля контентного анализа в интерактивном режиме");
- **с указанием параметров** установки в команде запуска инсталлятора (см. "Установка Модуля контентного анализа с указанием параметров в командной строке").

В обоих вариантах запуска инсталлятор поддерживает и совместную установку с другими продуктами Центра расследований на одном сервере, и распределенную установку в кластере.

7.3 Установка Data Discovery в интерактивном режиме

Примечание:

Если вы планируете совместную установку с Activity Monitor на одном сервере, установите его первым.

Если вы устанавливаете Data Discovery на сервер, на котором уже установлены другие продукты Центра расследований, инсталлятор не запросит часть параметров, так как эти директории и настройки уже были указаны при первичной установке Платформы.

Чтобы установить Data Discovery:

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям (см. "Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования").
2. Выполните шаги по подготовке сервера к установке Data Discovery (см. "Подготовка сервера").

3. Создайте новую директорию на сервере (например, `distr_discovery`):

```
mkdir distr_discovery
```

4. Скопируйте архив **`iw_discovery_setup_2.0.X.xxx.tar.xz`** в созданную директорию.
   В нашем примере будет использована версия `2.0.0.15`, соответственно, архив - `iw_discovery_setup_2.0.0.15.tar.xz`.
5. Перейдите в директорию, в которую был скопирован архив.
6. Распакуйте архив с дистрибутивом в эту директорию:

```
tar -xvf iw_discovery_setup_2.0.0.15.tar.xz
```

7. Запустите программу установки с помощью команды вида:

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

> **Примечание:**
>
> Чтобы установить:
>
> - **на центральную ноду Платформы продукт в режиме central:**
>
>   ```
>   ./setup.py install --nodemode=central --productmode=central
>   ```
>
> - **на центральную ноду Платформы продукт в режиме office:**
>
>   ```
>   ./setup.py install --nodemode=central --productmode=office
>   ```
>
> - **на офисную ноду Платформы продукт в режиме central:**
>
>   ```
>   ./setup.py install --nodemode=office --productmode=central
>   ```
>
> - **на офисную ноду Платформы продукт в режиме office:**
>
>   ```
>   ./setup.py install --nodemode=office --productmode=office
>   ```
>
> Если вы не укажете режимы установки Платформы и продукта, инсталлятор по умолчанию выберет режим `central`.
>
> Если вы устанавливаете Data Discovery на сервер первым и укажете только параметр `--nodemode`, инсталлятор использует такое же значение и для параметра `--productmode`.

> **Важно!**
>
> Во время установки могут быть недоступны продукты Платформы, установленные на сервере.

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

> **Примечание:**
>
> Если отклонить лицензионное соглашение, инсталлятор прервет процесс и завершит работу.

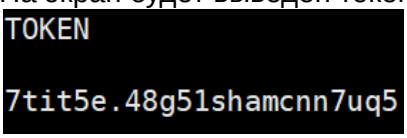
10. Если вы устанавливаете **центральную ноду Платформы** (`--nodemode=central`), введите IP-адрес сетевого интерфейса для взаимодействия с кластером в формате IPv4: "xxx.xxx.xxx.xxx" (по умолчанию: `0.0.0.0`) и нажмите **Enter**.
Если указать `0.0.0.0` , будут использованы все доступные сетевые интерфейсы.

> **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:

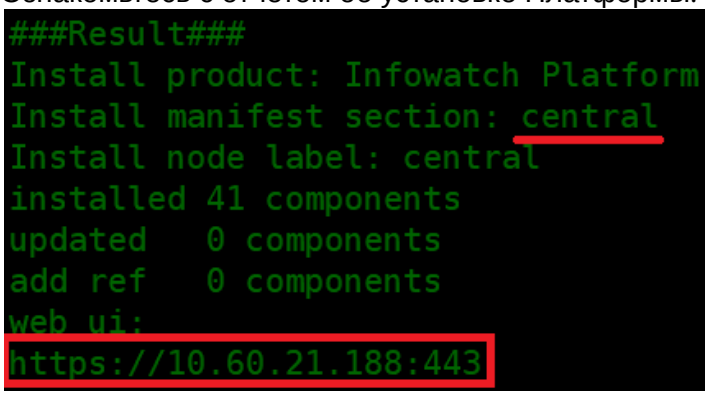
```
kubeadm token list
```

        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. Если вы устанавливаете **центральную ноду Платформы**, укажите порт подключения к веб-интерфейсу (по умолчанию: `443`) и нажмите **Enter**.
18. Дождитесь завершения установки Платформы.
19. Ознакомьтесь с отчетом об установке Платформы.



При установке центральной ноды Платформы в графе **`web ui`** указаны адрес и порт для подключения к веб-интерфейсу (в нашем примере – `https://10.60.21.188:443`).

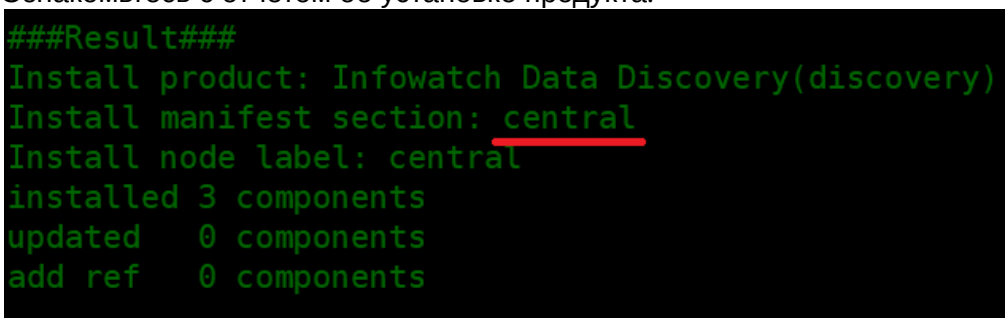
20. Укажите путь для хранилища просканированных файлов (по умолчанию: `/opt/disctps`) и нажмите **Enter**. Этот путь будет использоваться на всех серверах Data Discovery кластера.

> **Важно!**
>
> Директория для хранилища должна быть пустой.
>
> После установки в хранилище должны находиться только файлы и директории, которые были добавлены Data Discovery. Если вы добавите другие файлы или директории в хранилище, Data Discovery может работать некорректно.

> **Примечание:**
>
> Рекомендуется, чтобы хранилище сервера находилось в отдельном разделе или диске. О настройке хранилища сервера см. "InfoWatch Data Discovery. Руководство администратора", "Зоны и серверы".

21. Дождитесь завершения установки Data Discovery.

22. Ознакомьтесь с отчетом об установке продукта:



23. Чтобы вывести на экран информацию о Платформе и продуктах в кластере, выполните команду:

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

24. Убедитесь что все сервисы запущены, выполнив команду:

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

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

> **Примечание:**
>
> Чтобы увеличить скорость сканирования ресурсов, вы можете в ОС дополнить настройки подсистемы Inotify.
>
> Для этого:
>
> a. Откройте на редактирование конфигурационный файл `/etc/sysctl.conf`
> b. Добавьте в конце файла строки:
>
> ```
> fs.inotify.max_user_instances = 32768
> fs.inotify.max_user_watches = 32768
> fs.inotify.max_queued_events = 262144
> ```
>
> c. Сохраните изменения и закройте конфигурационный файл.
> d. Чтобы применить новые настройки подсистемы, выполните команду:
>
> ```
> sysctl -p
> ```

25. Для использования продукта подключитесь к веб-интерфейсу Центра расследований. Для этого введите в браузере адрес и порт центральной ноды Платформы.

7.4 Установка Data Discovery с указанием параметров в командной строке

> **Примечание:**
>
> Если вы планируете совместную установку с Activity Monitor на одном сервере, установите его первым.

Инсталлятор Data Discovery позволяет установить продукт с минимальным участием пользователя. Для этого запустите программу установки, указав в командной строке все требуемые параметры.

Перед запуском инсталлятора Data Discovery:

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям (см. "Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования").
2. Выполните шаги по подготовке сервера к установке Data Discovery (см. "Подготовка сервера").
3. Создайте новую директорию на диске (например, `distr_discovery`):

   ```
   mkdir distr_discovery
   ```

4. Скопируйте архив **`iw_discovery_setup_2.0.X.xxx.tar.xz`** в созданную директорию. В нашем примере будет использована версия `2.0.0.15`, соответственно, архив - `iw_discovery_setup_2.0.0.15.tar.xz`.
5. Перейдите в директорию, в которую был скопирован архив.
6. Распакуйте архив с дистрибутивом в эту директорию:

   ```
   tar -xvf iw_discovery_setup_2.0.0.15.tar.xz
   ```

Ознакомьтесь со списком ключей в таблице ниже, с их помощью вы можете указать инсталлятору параметры установки продукта. Указанные значения по умолчанию - значения, предлагаемые инсталлятором в интерактивном режиме.

> **Примечание:**
>
> Если вы не укажете режимы установки Платформы и продукта, инсталлятор использует значение `central`.

Ключ	Значение по умолчанию	Доступные значения	Описание
`--nodemode`	`central`	`central, office`	Режим установки Платформы
`--productmode`	`central`	`central, office`	Режим установки продукта
`--loc`	`ru`	`ru, en`	Локализация продукта, язык для предустановленных сущностей. Параметр **необязателен** для запуска инсталлятора
`--licagree`	`n`	`y, yes, n, no`	Принятие лицензионного соглашения
`--chmemsize`	`80%`	1-100% или числовое значение Если не указать %, указанное значение будет принято за объем в GB	Объем оперативной памяти, используемой для данных Clickhouse
`--chdbpath`	`/opt/chdata`		Путь для размещения данных ClickHouse
`--natspath`	`/opt/natsdata`		Путь для размещения данных NATS
`--pgdbpath`	`/opt/pgdata`		Путь для размещения файлов базы данных PostgreSQL
`--dsdatapath`	`/opt/dsdata`		Путь где будут располагаться бинарные данные
`--advertise`	`0.0.0.0`		IP-адрес сетевого интерфейса, на котором работает сервис `kubelet`. Указывайте при установке центральной ноды Платформы

Ключ	Значение по умолчанию	Доступные значения	Описание
`--guiport`	`443`		Порт подключения к веб-интерфейсу. Указывайте при установке центральной ноды Платформы
`--cluster`			Адрес центральной ноды Платформы в кластере. Указывайте при установке офисной ноды Платформы
`--clustertoken`			Токен для подключения к центральной ноде Платформы. Чтобы получить токен, в терминале центральной ноды Платформы выполните команду: `kubeadm token list` Указывайте при установке офисной ноды Платформы
`--nodelabel`	`office`		Лейбл ноды. Указывайте при установке офисной ноды Платформы
`--tpspath`	`/opt/disctps`		Укажите путь для хранилища просканированных файлов. Этот путь будет использоваться на всех серверах Data Discovery кластера. Указывайте при установке центральной ноды Data Discovery

Чтобы установить Data Discovery:

1. Запустите программу установки Data Discovery с указанием параметров.

Пример команды установки центральной Платформы и Data Discovery в режиме central:

```
./setup.py install --nodemode=central --productmode=central --licagree=yes --advertise=0.0.0.0 --chmemsize=80% --chdbpath=/opt/chdata --pgdbpath=/opt/pgdata --dsdatapath=/opt/dsdata --guiport=443 --natspath=/opt/natsdata --tpspath=/opt/disctps
```

Пример команды установки офисной Платформы и Data Discovery в режиме office:

```
./setup.py install --nodemode=office --productmode=office --licagree=yes --nodelabel=lv-426
 --cluster=10.60.21.188 --clustertoken=bvp2e1.e9zilgwg7v2urtsr --chdbpath=/opt/chdata --
chmemsize=80% --natspath=/opt/natsdata --pgdbpath=/opt/pgdata --dsdatapath=/opt/dsdata
```

2. Если вы указали все обязательные параметры, инсталлятор запустит установку.
   Если вы не указали часть параметров, инсталлятор запустит интерактивный режим и попросит задать значения.
3. Дождитесь завершения установки Data Discovery.
4. Чтобы вывести на экран информацию о Платформе и продуктах в кластере, выполните команду:

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

5. Убедитесь что все сервисы запущены, выполнив команду:

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

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

   Примечание:

   Чтобы увеличить скорость сканирования ресурсов, вы можете в ОС дополнить настройки подсистемы Inotify.

   Для этого:

   a. Откройте на редактирование конфигурационный файл `/etc/sysctl.conf`
   b. Добавьте в конце файла строки:

```
fs.inotify.max_user_instances = 32768
fs.inotify.max_user_watches = 32768
fs.inotify.max_queued_events = 262144
```

   c. Сохраните изменения и закройте конфигурационный файл.
   d. Чтобы применить новые настройки подсистемы, выполните команду:

```
sysctl -p
```

6. Для использования продукта подключитесь к веб-интерфейсу Центра расследований. Для этого введите в браузере адрес и порт центральной Платформы.

7.5 Установка Модуля контентного анализа в интерактивном режиме

> **Примечание:**
>
> Модуль контентного анализа обязательно должен быть установлен в одном кластере с Data Discovery.
>
> Если вы устанавливаете Модуль контентного анализа на сервер, на котором уже установлены продукты Центра расследований, инсталлятор не запросит часть параметров, так как эти директории и настройки уже были указаны при первичной установке Платформы.

Чтобы установить Модуль контентного анализа:

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям (см. "Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования").
2. Выполните шаги по подготовке сервера к установке Модуля контентного анализа (см. "Подготовка сервера").
3. Создайте новую директорию на сервере (например, `distr_cas`):

   ```
   mkdir distr_cas
   ```

4. Скопируйте архив **`iw_tm_setup_7.11.0.xxx.tar.xz`** в созданную директорию.
   В нашем примере будет использована версия `7.11.0.209`, соответственно, архив - `iw_tm_setup_7.11.0.209.tar.xz`.
5. Перейдите в директорию, в которую был скопирован архив.
6. Распакуйте архив с дистрибутивом в эту директорию:

   ```
   tar -xvf iw_tm_setup_7.11.0.209.tar.xz
   ```

7. Запустите программу установки с помощью команды вида:

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

   > **Примечание:**
   >
   > Чтобы установить:
   >
   > - **на центральную ноду Платформы модуль в режиме central:**
   >
   >   ```
   >   ./setup.py install --nodemode=central --productmode=central
   >   ```

- **на центральную ноду Платформы модуль в режиме office:**

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

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

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

- **на офисную ноду Платформы модуль в режиме office:**

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

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

Важно!

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

8. Ознакомьтесь с условиями лицензионного соглашения. Лицензионное соглашение содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
9. Чтобы принять лицензионное соглашение, введите " `y` " 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:

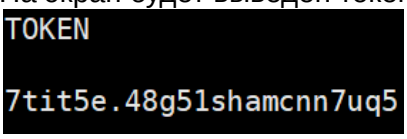
Здесь и далее для использования значений, предложенных по умолчанию, нажмите **Enter** без ввода значений.

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. Если вы устанавливаете **центральную ноду Платформы**, укажите порт подключения к веб-интерфейсу (по умолчанию: `443`) и нажмите **Enter**.
18. Дождитесь завершения установки Платформы.
19. Ознакомьтесь с отчетом об установке Платформы.
20. Модуль контентного анализа использует конфигурацию Traffic Monitor. Для загрузки конфигурации укажите адрес сервера с базой данных Traffic Monitor и нажмите **Enter**.

> **Важно!**
>
> Поддерживается взаимодействие **только с СУБД PostgreSQL**.
>
> Если вы используете **Traffic Monitor 7.10 или более ранние** версии, объекты защиты не должны содержать элементы технологии Автолингвист. Для работы модуля контентного анализа с конфигурациями этих версий Traffic Monitor, удалите из объектов защиты элементы технологии Автолингвист.

> **Примечание:**
>
> Если Traffic Monitor установлен на нескольких серверах или использует удаленную базу данных, укажите именно тот сервер, на котором развернута СУБД.
>
> Если в кластере будет несколько серверов с Модулем контентного анализа, у них должна быть одинаковая конфигурация.

21. Укажите порт для подключения к базе данных Traffic Monitor (по умолчанию: `5433`) и нажмите **Enter**.

22. Для доступа к базе данных укажите пароль пользователя `iwtm_linux`.

    > **Примечание:**
    >
    > Если вы не меняли имя пользователя и пароль при установке Traffic Monitor, укажите значение по умолчанию (см. "*InfoWatch Traffic Monitor. Руководство по установке*" статью "*Предустановленные серверные параметры*")

23. Дождитесь завершения установки Модуля контентного анализа.
24. Чтобы вывести на экран информацию о Платформе и продуктах в кластере, выполните команду:

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

25. Убедитесь что все сервисы запущены, выполнив команду:

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

    Команда выведет список сервисов. Каждый сервис должен иметь статус `Running`.
26. Для работы Data Discovery с Модулем контентного анализа необходимы объекты защиты. Чтобы добавить их в Центр расследований, создайте и запустите интеграцию с Traffic Monitor (подробнее см. "*InfoWatch Data Discovery. Руководство администратора*", статью "*Интеграция с InfoWatch Traffic Monitor*"). Рекомендуется добавлять объекты защиты из той же конфигурации Traffic Monitor, которая использована при установке Модуля контентного анализа.

После установки в **Настройках** Центра расследований в разделе **Зоны и серверы**:

- добавится сервер с ролью **Контентный анализ** - если Модуль контентного анализа установлен отдельно от Data Discovery;
- существующему серверу добавится роль **Контентный анализ** - если Модуль контентного анализа установлен на один сервер с Data Discovery.

> **Примечание:**
>
> **Удаление компонентов Модуля контентного анализа выполняется аналогично продуктам на Платформе:**
>
> 1. Перейдите в директорию на сервере, в которую был распакован архив с дистрибутивом.
> 2. Выполните команду:
>
>    ```
>    ./setup.py remove
>    ```

7.6 Установка Модуля контентного анализа с указанием параметров в командной строке

> **Примечание:**
>
> Модуль контентного анализа обязательно должен быть установлен в одном кластере с Data Discovery.
>
> Если вы устанавливаете Модуль контентного анализа на сервер, на котором уже установлены продукты Центра расследований, инсталлятор не запросит часть параметров, так как эти директории и настройки уже были указаны при первичной установке Платформы.

Инсталлятор Модуля контентного анализа позволяет установить продукт с минимальным участием пользователя. Для этого запустите программу установки, указав в командной строке все требуемые параметры.

Перед запуском инсталлятора Модуля контентного анализа:

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям (см. "Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования").
2. Выполните шаги по подготовке сервера к установке Модуля контентного анализа (см. "Подготовка сервера").
3. Создайте новую директорию на сервере (например, `distr_cas`):

   ```
   mkdir distr_cas
   ```

4. Скопируйте архив **`iw_tm_setup_7.11.0.xxx.tar.xz`** в созданную директорию.
   В нашем примере будет использована версия `7.11.0.209`, соответственно, архив - `iw_tm_setup_7.11.0.209.tar.xz`.
5. Перейдите в директорию, в которую был скопирован архив.
6. Распакуйте архив с дистрибутивом в эту директорию:

   ```
   tar -xvf iw_tm_setup_7.11.0.209.tar.xz
   ```

Ознакомьтесь со списком ключей в таблице ниже, с их помощью вы можете указать инсталлятору параметры установки продукта. Указанные значения по умолчанию - значения, предлагаемые инсталлятором в интерактивном режиме.

> **Примечание:**
>
> Если вы не укажете режимы установки Платформы и продукта, инсталлятор использует значение `central`.

Ключ	Значение по умолчанию	Доступные значения	Описание
`--nodemode`	`central`	`central, office`	Режим установки Платформы
`--productmode`	`central`	`central, office`	Режим установки модуля
`--loc`	`ru`	`ru, en`	Локализация продукта, язык для предустановленных сущностей. Параметр **необязателен** для запуска инсталлятора
`--licagree`	`n`	`y, yes, n, no`	Принятие лицензионного соглашения
`--chmemsize`	`80%`	1-100% или числовое значение Если не указать %, указанное значение будет принято за объем в GB	Объем оперативной памяти, используемой для данных Clickhouse
`--chdbpath`	`/opt/chdata`		Путь для размещения данных ClickHouse
`--natspath`	`/opt/natsdata`		Путь для размещения данных NATS
`--pgdbpath`	`/opt/pgdata`		Путь для размещения файлов базы данных PostgreSQL
`--dsdatapath`	`/opt/dsdata`		Путь где будут располагаться бинарные данные
`--advertise`	`0.0.0.0`		IP-адрес сетевого интерфейса, на котором работает сервис `kubelet`. Указывайте при установке центральной ноды Платформы
`--guiport`	`443`		Порт подключения к веб-интерфейсу. Указывайте при установке центральной ноды Платформы
`--cluster`			Адрес центральной ноды Платформы в кластере. Указывайте при установке офисной ноды Платформы

Ключ	Значение по умолчанию	Доступные значения	Описание
`--clustertoken`			Токен для подключения к центральной ноде Платформы. Чтобы получить токен, в терминале центральной ноды Платформы выполните команду: `kubeadm token list` Указывайте при установке офисной ноды Платформы
`--nodelabel`	`office`		Лейбл ноды. Указывайте при установке офисной ноды Платформы
`--tm-db-host`			Адрес сервера с базой данных Traffic Monitor. Поддерживается взаимодействие только с СУБД PostgreSQL. Если в кластере будет несколько серверов с Модулем контентного анализа, у них должна быть одинаковая конфигурация. Если вы используете **Traffic Monitor 7.10 или более ранние** версии, объекты защиты не должны содержать элементы технологии Автолингвист. Для работы модуля контентного анализа с конфигурациями этих версий Traffic Monitor, удалите из объектов защиты элементы технологии Автолингвист.
`--tm-db-port`	`5443`		Порт для подключения к базе данных Traffic Monitor
`--tm-db-pass-iwtm-linux`			Пароль пользователя `iwtm_linux` для доступа к базе данных

Чтобы установить Модуль контентного анализа:

1. Запустите программу установки с указанием параметров.

Пример команды установки центральной Платформы и модуля в режиме central:

```
./setup.py install --nodemode=central --productmode=central --licagree=yes --advertise=0.0.0.0 --chmemsize=80% --chdbpath=/opt/chdata --pgdbpath=/opt/pgdata --dsdatapath=/opt/dsdata --guiport=443 --natspath=/opt/natsdata --tm-db-host=10.60.22.33 --tm-db-port=5443 --tm-db-pass-iwtm-linux=xxXX1234
```

Пример команды установки офисной Платформы и модуля в режиме office:

```
./setup.py install --nodemode=office --productmode=office --licagree=yes --nodelabel=lv-426 --cluster=10.60.21.188 --clustertoken=bvp2e1.e9zilgwg7v2urtsr --chdbpath=/opt/chdata --chmemsize=80% --natspath=/opt/natsdata --pgdbpath=/opt/pgdata --dsdatapath=/opt/dsdata --tm-db-host=10.60.22.33 --tm-db-port=5443 --tm-db-pass-iwtm-linux=xxXX1234
```

2. Если вы указали все обязательные параметры, инсталлятор запустит установку.
   Если вы не указали часть параметров, инсталлятор запустит интерактивный режим и попросит задать значения.
3. Дождитесь завершения установки Модуля контентного анализа.
4. Чтобы вывести на экран информацию о Платформе и продуктах в кластере, выполните команду:

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

5. Убедитесь что все сервисы запущены, выполнив команду:

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

   Команда выведет список сервисов. Каждый сервис должен иметь статус `Running`.
6. Для работы Data Discovery с Модулем контентного анализа необходимы объекты защиты. Чтобы добавить их в Центр расследований, создайте и запустите интеграцию с Traffic Monitor (подробнее см. "*InfoWatch Data Discovery. Руководство администратора*", статью "*Интеграция с InfoWatch Traffic Monitor*"). Рекомендуется добавлять объекты защиты из той же конфигурации Traffic Monitor, которая использована при установке Модуля контентного анализа.

После установки в **Настройках** Центра расследований в разделе **Зоны и серверы**:

- добавится сервер с ролью **Контентный анализ** - если Модуль контентного анализа установлен отдельно от Data Discovery;
- существующему серверу добавится роль **Контентный анализ** - если Модуль контентного анализа установлен на один сервер с Data Discovery.

Примечание:

Удаление компонентов Модуля контентного анализа выполняется аналогично продуктам на Платформе:

1. Перейдите в директорию на сервере, в которую был распакован архив с дистрибутивом.

2. Выполните команду:

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

8 Установка лицензии и плагина Traffic Monitor

8.1 Экспорт данных в Traffic Monitor

Data Discovery позволяет экспортировать копии файлов для анализа в Traffic Monitor. Для этого в Traffic Monitor необходимы **плагин и лицензия на модуль перехвата**.

Чтобы добавить лицензию:

1. Войдите под учетной записью Офицера безопасности в Консоль управления сервера Traffic Monitor.
2. Перейдите в раздел **Управление** -> **Лицензии**.
3. В области **Лицензии** нажмите .
4. Добавьте полученный от сотрудников Технической поддержки InfoWatch файл лицензии **tm_license_yyyy_mm_dd.license**, используя Проводник.

После успешного добавления лицензии информация о ней будет доступна в разделе **Управление** -> **Лицензии**.

Для экспорта данных используйте **предустановленный плагин** в Консоли управления Traffic Monitor:

- "InfoWatch Crawler" для Traffic Monitor версии 7.3 и ниже;
- "InfoWatch Data Discovery" для Traffic Monitor версии выше 7.3.

Плагин отображается, только если в Traffic Monitor установлена действующая лицензия.

Информация о плагине будет доступна в разделе **Управление → Плагины** в Консоли управления Traffic Monitor. Для последующей отправки данных в Traffic Monitor необходим токен, который создается автоматически и доступен в разделе **Управление → Плагины → Токены**.

Подробнее о настройке экспорта данных см. "InfoWatch Data Discovery. Руководство администратора", "Зоны и серверы".

8.2 Импорт данных из Traffic Monitor

Для получения данных из Traffic Monitor в веб-интерфейсе Центра расследований необходимо настроить интеграцию (подробнее см. "*InfoWatch Data Discovery. Руководство администратора*", статья "Интеграция с InfoWatch Traffic Monitor"). Для этого в Traffic Monitor должны быть добавлены **лицензия на экспорт данных и плагин Центра расследований**. Токен для интеграции создается автоматически после добавления плагина. Токен доступен в разделе **Управление** > **Плагины** Консоли Управления Traffic Monitor, на вкладке **Токены** плагина **InfoWatch Investigation Centre**.

> **Примечание:**
>
> Data Discovery не использует данные по событиям Traffic Monitor. Функциональность могут использовать другие продукты, установленные в кластере Центра расследований.

В **Traffic Monitor 7.10 и более новых** версиях бессрочная лицензия на экспорт данных в Центр расследований и плагин **InfoWatch Investigation Centre** предустановлены.

В **Traffic Monitor 7.9 и более ранних** версиях добавьте лицензию на экспорт данных и плагин вручную, как описано ниже.

Чтобы добавить лицензию вручную:

1. Войдите под учетной записью Офицера безопасности в Консоль управления сервера Traffic Monitor.
2. Перейдите в раздел **Управление** > **Лицензии**.
3. В области **Лицензии** нажмите .
4. Добавьте полученный от сотрудников Технической поддержки InfoWatch файл лицензии **tm_license_yyyy_mm_dd.license**, используя Проводник.

После успешного добавления лицензии информация о ней будет доступна в разделе **Управление** > **Лицензии**.

Важно!

Для экспорта данных в Центр расследований в лицензии для Traffic Monitor должны быть указаны:

- компания, выпускающая лицензию - **IW**;
- система-получатель данных - **Platform**.

Чтобы добавить плагин вручную:

1. Войдите под учетной записью Офицера безопасности в Консоль управления сервера Traffic Monitor.
2. Перейдите в раздел **Управление** > **Плагины**.
3. В области **Плагины** нажмите .
4. В открывшемся окне нажмите **Выбрать файл**.
5. Добавьте архив с файлом плагина, используя Проводник.
   Плагин представляет собой zip-архив `platform/tmplugin/platform.zip`. Папка с плагином расположена в директории, куда был распакован архив дистрибутива.

После успешного добавления плагина информация о нем будет доступна в разделе **Управление** > **Плагины**.

Как загрузить плагин и лицензию в Traffic Monitor одним архивом, см. статью базы знаний "Как привязать плагин к лицензии".

9 Устранение неполадок

Во время установки возможны сбои: прерывания работы программы установки, отключение электричества и т.д. В таком случае Система будет установлена некорректно. В случае возникновения подобной ситуации следует запустить функционал сброса.

Чтобы сбросить установку:

1. Остановите все задачи сканирования в веб-интерфейсе Data Discovery.
2. Перейдите в директорию, в которую был распакован архив с дистрибутивом при установке.
3. Выполните команду:

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

Сброс установки не удалит результаты работы Системы. Вы сможете их использовать после повторной установки.

Важно!

При сбросе установки Системы 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 Discovery повторно установите и другие продукты в кластере.

10 Обновление Data Discovery

Data Discovery поддерживает обновление с версий:

- **1.8.0**;
- **1.9.0**;
- **1.9.1**;
- **1.10.0**;
- **1.10.1**.

> **Примечание:**
>
> Для обновления с более ранних версий, сначала обновите Data Discovery до версий **1.8.0**, **1.9.x** или **1.10.X**.

Дистрибутив представляет собой архив `iw_discovery_setup_2.0.X.xxx.tar.xz`, где `xxx` – номер сборки. Этот архив содержит полный набор бинарных модулей образов контейнеров, необходимых для развертывания Платформы и компонентов Data Discovery без доступа к Интернету (offline-установка). Кроме этого, данный архив содержит программу обновления.

Для обновления Data Discovery используйте командную строку.

10.1 Настройки и данные Системы

- **Задачи сканирования**:
  - Обработка ресурсов в рамках задач сканирования продолжится с того места, где она закончилась до обновления Системы.

    > **Важно!**
    >
    > Перед обновлением остановите все задачи сканирования в интерфейсе Data Discovery. Запустите задачи вручную, когда обновление будет завершено на всех серверах кластера.

- **Конфигурационные файлы**:
  - Если проводится обновление с помощью сброса текущей установки, в некоторых конфигурационных файлах могут быть установлены значения по умолчанию. Если вы редактировали конфигурационные файлы Системы, проверьте значения в файлах после обновления.

10.2 Варианты обновления Data Discovery

> **Важно!**

В случае совместной установки Data Discovery с Prediction, необходимо остановить расчет данных Prediction на время обновления Data Discovery. Подробную информацию см. в статье в Базе знаний "Обязательные действия для обновления продуктов на Платформе, которые установлены совместно с Prediction".

Data Discovery 2.0 поддерживает только обновление с помощью сброса текущей установки и переустановки на старые данные.

Примечание:

Если Data Discovery и другие продукты установлены в разных кластерах, вы можете обновить продукты в другом кластере и установить в него новую версию Data Discovery (подробнее см. "Переустановка Data Discovery в другой кластер").

Важно!

Если вы обновляете Data Discovery в одном кластере с другими продуктами InfoWatch, 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 обновляемого продукта:

1. Распакуйте архив с дистрибутивом продукта. В нашем примере, в директорию `/ddiscovery`. Для этого перейдите в директорию и выполните команду:

   Пример для версии 2.0.0.77:

   ```
   tar -xvf iw_discovery_setup_2.0.0.77.tar.xz
   ```

2. Выполните команду:

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

10.3 Обновление Data Discovery с помощью сброса установки (reset)

Важно!

Чтобы обновить весь распределенный кластер Центра расследований 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 продукта 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 Discovery:

1. **Остановите все задачи** сканирования в веб-интерфейсе Data Discovery.
2. Выполните шаги по подготовке сервера к обновлению (см. "Подготовка сервера").
3. Создайте новую директорию на диске (например, `distr_discovery`):

```
mkdir distr_discovery
```

4. Скопируйте архив `iw_discovery_setup_2.0.X.xxx.tar.xz` в созданную директорию.
   В нашем примере будет использована версия `2.0.0.15`, соответственно, архив - `iw_discovery_setup_2.0.0.15.tar.xz`.
5. Перейдите в директорию, в которую был скопирован архив.
6. Распакуйте архив с дистрибутивом в эту директорию:

```
tar -xvf iw_discovery_setup_2.0.0.15.tar.xz
```

7. Если Data Discovery и Prediction установлены совместно или планируется совместно их использовать, остановите расчет данных Prediction на время обновления Data Discovery (подробнее см. "Обязательные действия для обновления продуктов на Платформе, которые установлены совместно с Prediction").
8. 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}"
```

9. Чтобы в новой версии сохранить настройки зон и серверов, перед сбросом установки подключитесь к ноде, на которой установлен Data Discovery 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
```

10. 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
```

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

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

> **Важно!**
>
> Если на сервере установлены другие продукты на базе Платформы, установки этих продуктов будут сброшены. При сбросе установки на центральной ноде продукты на офисных нодах перестанут функционировать.
>
> После установки новой версии Data Discovery 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 Discovery, 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**.

12. Дождитесь окончания процесса сброса установки Платформы и продукта.
13. Если вы обновляетесь с переходом на другой сервер или на новую ОС:
    a. Скопируйте на другой раздел или на новый сервер директории с данными, которые были указаны при установке.

> **Примечание:**
>
> В **Data Discovery 1.10 и более ранних** директории по умолчанию расположены по пути `/mnt`.
> В **Data Discovery 2.0 и более новых** - по умолчанию по пути `/opt`.
> Обязательно копируйте директории с сохранением прав и владельцев. Для копирования используйте стандартные средства, например утилиту `rsync`.

b. После сброса текущей установки скопируйте со старого сервера на новый файл с паролями базы данных `/var/lib/iwplatform/` **`dbadmin.yaml`**.

14. 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
```

15. Перезагрузите сервер с помощью команды:

```
reboot
```

16. Установите новую версию Data Discovery (см. "Установка Data Discovery").

> **Важно!**
>
> Если до сброса установки на этом сервере был установлен Activity Monitor, сначала установите его, а затем Data Discovery.
>
> Когда инсталлятор потребует указать директории для размещения данных, указывайте директории с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?».
>
> Если вы обновляетесь **с версии 1.10 и более ранних**, учитывайте, что в версии 2.0 пути установки по умолчанию изменились. Если ранее вы использовали пути по умолчанию, при установке Data Discovery 2.0 и более новых по умолчанию инсталлятор не обнаружит данные прошлой версии и создаст директории по пути `/opt`. Поэтому переместите данные в `/opt` или укажите старые директории при установке новой версии.
>
> На всех нодах кластера с Data Discovery должен быть одинаковый путь к хранилищу просканированных файлов (по умолчанию: `/opt/`**`disctps`**).

17. Если до сброса на сервере были установлены и другие продукты, установите версии продуктов, совместимые с Data Discovery 2.0 (см. "Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования").
18. Если Data Discovery установлен в распределенном кластере, обновите Платформу и продукты на других серверах кластера до версий, совместимых с Data Discovery 2.0.
19. Если после обновления вам необходимо освободить место на диске, вы можете удалить неиспользуемые контейнеры docker или containerd. Подробнее, см. в статье "Как удалить неиспользуемые контейнеры docker и containerd?".
20. Очистите кеш браузера, в котором работали до обновления продукта.
Веб-интерфейс Центра расследований доступен по адресу центральной ноды Платформы.

> **Важно!**
>
> Если Data Discovery установлен **на офисной ноде в режиме central**, в результате сброса прошлой установки у добавленных ролей пользователя **сброшен доступ к продуктам**. После обновления перейдите в **Настройки** и заново настройте доступ к продуктам в этих ролях (о ролях см. "*InfoWatch Data Discovery. Руководство администратора*" статью "*Роли*").

10.4 Переустановка Data Discovery в другой кластер

Если Data Discovery и другие продукты установлены в разных кластерах, вы можете установить новую версию Data Discovery в кластер к другому продукту. В результате вы сможете работать с Data Discovery и другими продуктами в одном веб-интерфейсе Центра расследований, а продукты будут иметь общие интеграции и возможность обмена данными.

Важно!

Учитывайте, что при переустановке Data Discovery в другой кластер **не будут перенесены**:

- пользователи;
- роли;
- интеграции;
- расписания запуска задач сканирования.

В результате в новом кластере Центра расследований останутся только пользователи, роли и интеграции, которые были до добавления Data Discovery.

После переустановки **настройте заново расписания** запуска задач сканирования.

Чтобы переустановить Data Discovery в другой кластер:

1. В кластере, в который хотите установить новую версию Data Discovery, обновите продукты до версий, совместимых с Data Discovery 2.0 (см. "Типы установки и обновления, совместимость с другими продуктами, аппаратные и программные требования").
2. На сервере Data Discovery выполните шаги по подготовке сервера к обновлению (см. "Подготовка сервера").
3. Создайте новую директорию на диске (например, `distr_discovery`):

   ```
   mkdir distr_discovery
   ```

4. Скопируйте архив **`iw_discovery_setup_2.0.X.xxx.tar.xz`** в созданную директорию. В нашем примере будет использована версия `2.0.0.15`, соответственно, архив - `iw_discovery_setup_2.0.0.15.tar.xz`.
5. Перейдите в директорию, в которую был скопирован архив.
6. Распакуйте архив с дистрибутивом в эту директорию:

   ```
   tar -xvf iw_discovery_setup_2.0.0.15.tar.xz
   ```

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

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

8. Дождитесь завершения процесса сброса установки Платформы и продукта.

9. 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
   ```

10. Перезагрузите сервер с помощью команды:

    ```
    reboot
    ```

11. Установите **офисную ноду Платформы с новой версией Data Discovery** (см. "Установка Data Discovery").

    Важно!

    Используйте команду для установки на офисную ноду Платформы

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

    Когда инсталлятор запросит, укажите адрес и токен центральной Платформы нового кластера.

    Когда инсталлятор потребует указать директории для размещения данных, указывайте директории с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?».

    Если вы обновляетесь **с версии 1.10 и более ранних**, учитывайте, что в версии 2.0 пути установки по умолчанию изменились. Если ранее вы использовали пути по умолчанию, при установке Data Discovery 2.0 и более новых по умолчанию инсталлятор не обнаружит данные прошлой версии и создаст директории по пути `/opt`. Поэтому переместите данные в `/opt` или укажите старые директории при установке новой версии.

    На всех нодах кластера с Data Discovery должен быть одинаковый путь к хранилищу просканированных файлов (по умолчанию: `/opt/disctps`).

12. Если после обновления вам необходимо освободить место на диске, вы можете удалить неиспользуемые контейнеры docker или containerd. Подробнее, см. в статье "Как удалить неиспользуемые контейнеры docker и containerd?".
13. Очистите кеш браузера, в котором работали до обновления продукта.
    Веб-интерфейс Центра расследований доступен по адресу центральной ноды Платформы.

11 Удаление Data Discovery

Чтобы удалить Data Discovery:

1. **Остановите все задачи** сканирования в веб-интерфейсе Data Discovery.
2. Перейдите в директорию на сервере, в которую был распакован архив с дистрибутивом при установке Data Discovery.
3. Выполните команду:

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

4. Дождитесь завершения удаления. Программа удалит компоненты Системы. Данные Data Discovery удалены не будут. При необходимости вы можете удалить данные вручную из директорий, указанных при установке.
5. Удалите оставшиеся на сервере внутренние пароли продукта и связанные данные с помощью команд:

```
kubectl delete daemonsets -l product=discovery -n infowatch
kubectl delete deployments -l product=discovery -n infowatch
kubectl delete configmaps -l product=discovery -n infowatch
kubectl delete secrets -l product=discovery -n infowatch
```

Примечание:

Если вы удалили Data Discovery, установленный в режиме central, компоненты Data Discovery, установленные в режиме office на других нодах, не будут удалены автоматически. Удалите их вручную.