INFOWATCH

InfoWatch Device Control. Руководство по установке

21/01/2025

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

Настоящее руководство содержит сведения по установке, обновлению и удалению InfoWatch Device Control (далее также Система или Device Control) - программного обеспечения, позволяющего управлять правами доступа к съемным устройствам.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, работающих с Системой (выполняющих установку, обновление, удаление и т. п.).

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем семейств Linux и Microsoft Windows.

2 Комплект документов

В комплект документации по InfoWatch Device Control входят:

- «InfoWatch Device Control. Руководство по установке». Содержит описание установки, обновления и удаления InfoWatch Device Control.
- «InfoWatch Device Control. Руководство администратора». Содержит информацию по настройке и подготовке к работе InfoWatch Device Control.
- «InfoWatch Device Control. Руководство пользователя». Содержит описание работы с InfoWatch Device Control.

Сопутствующая документация по модулю InfoWatch Device Monitor for Linux включает в себя:

- «InfoWatch Device Monitor for Linux. Руководство по установке». Содержит описание установки, обновления и удаления модуля InfoWatch Device Monitor for Linux.
- «InfoWatch Device Monitor for Linux. Руководство пользователя». Содержит описание работы с InfoWatch Device Monitor for Linux.

3 Техническая поддержка пользователей

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

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

Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: 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

4.1.1 InfoWatch Device Monitor

Для работы **Device Control 1.1** необходим модуль **InfoWatch Device Monitor for Linux 7.16**, установленный с ним в одном кластере. При этом они могут быть установлены как на разных серверах, так и на одном.

> **Примечание:**
>
> Вы можете установить их в любом порядке, но в случае миграции правил рекомендуется устанавливать Device Monitor первым. Подробнее о миграции см. ниже.

Device Control осуществляет защиту от утечек, используя Агенты Device Monitor (начиная с версии 7.14), установленные на рабочих станциях компании.

Миграция правил контроля внешних устройств и белых списков из Device Monitor

С версии Device Monitor for Linux 7.15 работа с правилами контроля внешних устройств осуществляется в Device Control. При обновлении Device Monitor for Linux с версией 7.14 и ниже до версии 7.16, а также при миграции сервера Device Monitor for Windows на Device Monitor for Linux 7.16 вы можете перенести старые правила и белые списки в Систему. Для этого:

1. Произведите обновление/миграцию Device Monitor на старую базу данных.
   В процессе инсталлятор спросит вас, хотите ли вы перенести правила и белые списки в Device Control. Подробнее см. документацию для Device Monitor → Руководство по установке → Обновление Device Monitor.
2. Установите Device Control в кластер с Device Monitor.
   Правила контроля внешних устройств и белые списки появятся на вкладке **Правила** раздела **Устройства**. Подробнее см. *"InfoWatch Device Control. Руководство пользователя → Вкладка "Правила"*.

4.1.2 Центр расследований InfoWatch

Device Control является частью Центра расследований InfoWatch.

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

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

- Data Analysis Service 1.3.1

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

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

> **Важно!**
>
> При распределенной установке примите во внимание следующие ключевые аспекты:
>
> - Продукты в кластере должны быть установлены на одной версии Платформы. 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.
> - Device Control поддерживает установку только в режиме `central`. При этом Система поддерживает 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 **Device Control 1.1 совместно** с:

- **Activity Monitor 3.2**
- **Data Discovery 2.0**
- **Data Access Tracker 2.2**
- **Prediction 3.2**
- **Vision 3.4**
- **Data Analysis Service 1.3.1**

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 Device Control".

4.2 Типы обновления

Device Control 1.1 поддерживает только обновление с помощью сброса и переустановки на прошлые данные.

Подробнее о процессе обновления см. "Обновление Device Control".

4.3 Аппаратные требования

Нагрузка на аппаратное обеспечение рассчитывается, исходя из объема анализируемых данных. В таблице приведены системные требования к процессору, объему оперативной памяти и жесткого диска для установки и работы Device Control на отдельном сервере. Требования рассчитаны, исходя из средней активности пользователей в 250 событий в день.

Количество сотрудников	Срок хранения в архиве	Ядер/потоков (ядер в VM)	ОЗУ, Гбайт	Жесткий диск, Гбайт
100	Хранение – 1 год	4/8 (8)	20	101
200		4/8 (8)	20	137
500		4/8 (8)	20	247
1000		8/16 (16)	32	430

Количество сотрудников	Срок хранения в архиве	Ядер/потоков (ядер в VM)	ОЗУ, Гбайт	Жесткий диск, Гбайт
3000		12/24 (24)	48	1164
6000		16/32 (32)	64	2264
10000		24/48 (48)	80	3764

4.4 Программные требования

Для установки и работы в Системе может быть использовано следующее программное обеспечение:

Тип ПО	Варианты
Операционная система	• РЕД ОС 7.3; • Astra Linux 1.7 "Смоленск"; • Альт Сервер Виртуализации 10. **Важно!** Модули **netfilter** и **nat** должны быть обязательно загружены в ядро ОС
Браузер	• Google Chrome; • Яндекс.Браузер. **Важно!** Для корректной работы рекомендуется использовать последние версии поддерживаемых браузеров

Примечание:

Device Control использует PostgreSQL 16.4. СУБД поставляется вместе с продуктом и не требует отдельной установки.

5 Подготовка сервера

Перед установкой Device Control выполните шаги по подготовке сервера.

5.1 Шаги по подготовке сервера:

1. Установите интерпретатор языка Python версии 2.7. Он необходим для установки Системы, так как программа установки написана на языке Python версии 2.7.

   > **Примечание:**
   >
   > Пакет с интерпретатором не входит в состав дистрибутива Device Control.

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. Если вы используете распределенную структуру, убедитесь, что:
   - **на всех нодах кластера** открыт UDP-порт 8472 или выполните команду:

     ```
     firewall-cmd --zone=public --add-port=8472/udp
     ```

   - **на ноде, где будет установлен Device Control**, открыт TCP-порт 6443 или выполните команду:

     ```
     firewall-cmd --zone=public --add-port=6443/tcp
     ```

4. Для корректной работы Device Control настройте сетевые правила доступа (подробнее см. "Настройка сетевых правил доступа").
5. Device Control использует компонент Kubernetes. Для корректной установки Системы 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.

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

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

Tables: conntrack, expect, dying, unconfirmed

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

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

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

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

Если пакет не установлен, установите его с помощью команды:

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

```
yum install conntrack
```

- **для ОС Astra Linux**

```
apt-get install conntrack
```

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

```
rpm -Uhv ./<имя_пакета>
```

- **для ОС Astra Linux**

  ```
  dpkg -i ./<имя_пакета>
  ```

- **socat** - аналогично пакету **conntrack** .

6. Если вы используете антивирус, настройте его для совместной работы с Системой (см. статью Базы знаний "Настройка антивируса для продуктов Платформы").
7. В окружении Red Hat Enterprise Linux и РЕД ОС обновите политики SELinux. Для этого скачайте и установите пакет **container-selinux**.
   Вы можете установить пакет, выполнив команду:

   ```
   yum install container-selinux
   ```

   Примечание:

   Пакет не входит в состав дистрибутива Device Control.

   Пакет может отсутствовать в репозиториях некоторых операционных систем. В этом случае загрузите пакет и установите модуль вручную.

8. Если установка производится на ОС Альт, установите пакеты:
   - **python-modules-json**;
   - **python-modules-distutils**;
   - **python-modules-sqlite3**.

   Примечание:

   Пакеты не входят в состав дистрибутива Device Control.

   Пакеты могут отсутствовать в репозиториях некоторых операционных систем. В этом случае загрузите и установите требуемые пакеты вручную.

9. Для установки и корректной работы Device Control 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
   ```

Дистрибутив Device Control представляет собой архив **`iw_devicecontrol_setup_1.1.X.xxx.tar. xz`**, где xxx — номер сборки. Архив содержит набор бинарных модулей образов контейнеров, необходимых для развертывания Device Control без доступа к сети Интернет. Архив также содержит программу установки.

Вы можете установить Device Control:

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

Важно!

Device Control должен быть установлен в одном кластере с Device Monitor.

Вы можете установить в кластере только один экземпляр Device Control и только в режиме `central`.

Для установки Device Control используйте командную строку.

6 Настройка сетевых правил доступа

Для корректной работы Device Control должны быть разрешены соединения:

Соединение	Порт	Описание
Рабочая станция Администратора → Сервер Device Control	TCP 22	Используется для управления сервером Device Control через SSH-консоль
Рабочая станция Офицера Безопасности → Центр расследований	TCP 443	Используется для доступа Офицера безопасности к веб-интерфейсу Центра расследований (центральная нода платформы).
Сервер Device Control → Сервер Device Monitor	TCP 15007	Доступ к API Device Monitor
Сервер Device Monitor → Сервер Device Control	TCP 17104	Взаимодействие сервера DM с сервером Device Control

7 Установка Device Control

> **Примечание:**
>
> Если вы устанавливаете Device Control на сервер, на котором уже установлен модуль InfoWatch Device Monitor, инсталлятор не запросит часть параметров, так как эти директории и настройки уже были указаны при первичной установке Платформы.

Чтобы установить Device Control:

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 Device Control (см. "Подготовка сервера").
3. Создайте целевую директорию на диске, например, `devicecontrol`:

   ```
   mkdir devicecontrol
   ```

4. Скопируйте архив **iw_devicecontrol_setup_1.1.X.xxx.tar.xz** в созданную директорию.
5. Перейдите в директорию, в которую был скопирован архив.
6. Распакуйте архив с дистрибутивом Device Control в созданную директорию:

   ```
   tar xvf iw_devicecontrol_setup_1.1.X.xxx.tar.xz
   ```

7. Запустите программу установки с помощью команды вида:

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

   > **Примечание:**
   >
   > Чтобы установить:
   >
   > - **на центральную ноду Платформы продукт в режиме central:**
   >
   >   ```
   >   ./setup.py install --nodemode=central --productmode=central
   >   ```
   >
   > - **на офисную ноду Платформы продукт в режиме central:**
   >
   >   ```
   >   ./setup.py install --nodemode=office --productmode=central
   >   ```
   >
   > Если вы не укажете режимы установки Платформы и продукта, инсталлятор по умолчанию выберет режим `central`.

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

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

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

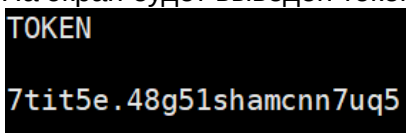
10. Если вы устанавливаете **центральную ноду Платформы** (`--nodemode=central`), введите IP-адрес сетевого интерфейса для взаимодействия с кластером в формате IPv4: "xxx.xxx.xxx.xxx" (по умолчанию: `0.0.0.0`) и нажмите **Enter**.
Если указать `0.0.0.0` , будут использованы все доступные сетевые интерфейсы.

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

11. Если вы устанавливаете **офисную ноду Платформы** (`--nodemode=office`):
    a. Укажите адрес центральной ноды Платформы в формате IP-адреса или доменного имени (например: `192.0.2.0` или `host.example.com`).
    b. Укажите токен для подключения к центральной ноде Платформы.
    Чтобы получить токен для подключения к центральной ноде Платформы:
        i. Подключитесь по ssh к консоли центральной ноды Платформы;
        ii. Выполните в терминале команду для получения токена:

```
kubeadm token list
```

        На экран будет выведен токен:



        Токен в нашем примере: `7tit5e.48g51shamcnn7uq5`
        iii. Укажите лейбл ноды (по умолчанию: `office`) и нажмите **Enter**.
        Лейбл может состоять из букв латинского алфавита и/или цифр. Длина лейбла не должна превышать 32 символа.
12. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию 80%) и нажмите **Enter**.
13. Укажите путь для размещения данных Clickhouse (по умолчанию `/opt/chdata`) и нажмите **Enter**.

14. Укажите путь для размещения данных PostgreSQL (по умолчанию `/opt/pgdata`) и нажмите **Enter**.
15. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
16. Укажите путь для хранения 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.

```
###Result###
Install product: Infowatch Platform(platform)
Install manifest section: central
Install node label: central
installed 41 components
updated   0 components
add ref   0 components
web ui:
https://10.60.25.59:443
```

    При установке центральной ноды Платформы в графе **`web ui`** указаны адрес и порт для подключения к веб-интерфейсу (в нашем примере – `https://10.60.25.59:443`).
20. Дождитесь окончания процесса установки. Программа установит компоненты Device Control и требуемое окружение.
21. Ознакомьтесь с отчетом об установке Device Control:

```
###Result###
Install product: Device Control(devicecontrol)
Install manifest section: central
Install node label: central
installed 1 components
updated   0 components
add ref   0 components
```

22. Убедитесь, что сервисы запустились, выполнив команду.

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

    Каждый сервис должен иметь статус `Running`.
23. Чтобы вывести на экран информацию о Платформе, выполните команду:

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

24. Если Device Monitor был установлен до Device Control, обновите конфигурационный файл `n.yaml`:
    a. На сервере, где установлен Device Monitor, перейдите в директорию, куда был распакован дистрибутив Device Monitor.
    b. Запустите скрипт **setup.sh**, выполнив команду:

    ```
    ./setup.sh
    ```

    c. Выберите в меню пункт **Utilities**.
    d. Выберите **Fix n.yaml file**. Дождитесь окончания процесса.

Важно!

После добавления в кластер любого продукта Центра Расследования, необходимо выполнять шаг 24.

Чтобы начать работу в Device Control:

1. Установите Device Monitor, если он еще не установлен. Подробнее см. "*Документация для InfoWatch Device Monitor (Linux). InfoWatch Device Monitor for Linux. Руководство по установке*".
2. Настройте передачу событий из Device Monitor в Платформу, см. "*Документация для InfoWatch Device Monitor (Linux). InfoWatch Device Monitor for Linux. Руководство пользователя → Настройка Device Monitor → Серверы DM*".
3. В базе данных Device Monitor включите настройку для отправки событий контроля устройств в Платформу. Вы можете это сделать, например, с помощью следующей команды:

   ```
   UPDATE public."Settings" SET "Value"='True' WHERE "Name"='SEND_DEVICE_EVT_TO_PLATFORM';
   ```

4. Убедитесь, что в Device Monitor в разделе **Настройки → Настройки продукта → Агенты** для настройки **Логировать события от перехватчика устройств и облачных хранилищ** выбрано значение **Логировать всегда**. Подробнее см. "*Документация для InfoWatch Device Monitor (Linux). InfoWatch Device Monitor for Linux. Руководство пользователя → Настройка Device Monitor → Агенты*".
5. 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 Системы, то достаточно обновить страницу в браузере.

8 Устранение неполадок

Во время установки Системы возможны сбои: прерывания работы программы установки, отключение электричества и т.д. В этом случае Система будет установлена некорректно. Для решения этой проблемы, а также при обновлении на новую версию с удалением старой версии, следует сбросить установку. После сброса все данные сохранятся в Системе, а установку необходимо произвести заново (см. "Установка Device Control"). В процессе установки на вопрос об удалении существующих данных выберите ответ **Нет**.

Чтобы сбросить установку:

1. Если неполадки возникли в процессе установки, то перейдите в директорию, где распакован дистрибутив продукта. В ином случае, если осуществляется обновление Системы, перейдите в директорию, где установлена Система.
2. Выполните команду:
   `./setup.py reset`

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 Device Control повторно установите и другие продукты в кластере.

9 Обновление Device Control

Обновление Device Control производится вручную, с помощью командной строки.

Для обновления Системы используется архив `iw_devicecontrol_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.

9.1 Варианты обновления Device Control

Device Control 1.1 поддерживает только обновление с помощью сброса текущей установки и переустановки на старые данные.

На время обновления Система будет недоступна во всем кластере. Если до обновления Device Control и другие продукты были установлены в разных кластерах, то объединение их в общий кластер после обновления не поддерживается.

Чтобы **обновить распределенный кластер** продуктов Платформы:

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

> **Важно!**
>
> Если вы обновляете Device Control 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 Device Control (см. "Установка Device Control", шаг 6). В нашем примере, в директорию `devicecontrol`.
> 2. Выполните команду:
>   `cat devicecontrol/platform/setup.yaml | grep version`

9.2 Обновление Device Control 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 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 Device Control:

1. Выполните шаги по подготовке сервера к установке Device Control (см. "Подготовка сервера").
2. Создайте новую директорию на сервере (например, `devicecontrol`):

   ```
   mkdir devicecontrol
   ```

3. Скопируйте архив **`iw_devicecontrol_setup_1.1.X.xxx.tar.xz`** в созданную директорию. В нашем примере будет использована версия `1.1.0.15`, соответственно, архив - `iw_devicecontrol_setup_1.1.0.15.tar.xz`.
4. Перейдите в директорию, в которую был скопирован архив.
5. Распакуйте архив с дистрибутивом в эту директорию:

   ```
   tar -xvf iw_devicecontrol_setup_1.1.0.15.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 Device Control 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 Device Control, 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:
    a. Скопируйте на другой раздел или на новый сервер директории с данными, которые были указаны при установке.

    Примечание:

    В **Device Control 1.0** директории по умолчанию расположены по пути `/mnt`.
    В **Device Control 1.1.0 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`.
12. 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
```

13. Установите новую версию Device Control (см. "Установка Device Control").

Важно!

Если до сброса установки на этом сервере был установлен Activity Monitor, сначала установите его, а затем Device Control.

Если вы обновляете Device Control после Device Monitor, обязательно обновите конфигурационный файл `n.yaml`. Подробнее см. шаг 24 "Установки Device Control".

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 1.0**, учитывайте, что с версии 1.1.0 пути установки по умолчанию изменились. Если ранее вы использовали пути по умолчанию, при установке Device Control 1.1.0 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.

14. Если до сброса на сервере были установлены и другие продукты, установите версии продуктов, совместимые с Device Control (см. "Аппаратные и программные требования").
15. Если Device Control установлен в распределенном кластере, обновите Платформу и продукты на других серверах кластера до версий, совместимых с Device Control.
16. **Если после обновления вам необходимо освободить место на диске, вы можете удалить неиспользуемые контейнеры.**

    Для этого выполните следующие шаги:

    a. Добавьте в файл `/etc/crictl.yaml` (при необходимости создайте его) строки:

    ```
    runtime-endpoint: unix:///run/containerd/containerd.sock
    image-endpoint: unix:///run/containerd/containerd.sock
    timeout: 5
    pull-image-on-create: false
    disable-pull-on-run: false
    ```

    b. Выполните команды:

    i. Для удаления контейнеров Платформы (где x.x.x.x – установленная версия Платформы):

    ```
    crictl rmi $(crictl image | awk '($2 !~ /\<x.x.x.x\>|\<latest\>/ && $1 ~ /
    docker.infowatch.ru\/platform-core-release/ && $1 !~ /flannel/) {print $3}')
    ```

    ii. Для удаления контейнеров Device Control (где x.x.x.x – установленная версия Device Control):

    ```
    crictl rmi $(crictl image | awk '($2 !~ /\<x.x.x.x\>|\<latest\>/ && $1 ~ /
    docker.infowatch.ru\/dctrl/) {print $3}')
    ```

    Данные команды удаляют контейнеры всех версий кроме указанной. Не удаляйте контейнеры установленной версии Device Control и Платформы!

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

Важно!

Если Device Control 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 Device Control. Руководство администратора*" статью "Роли").

10 Удаление Device Control

Чтобы удалить Device Control:

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

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

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

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