

INFOWATCH

InfoWatch Device Monitor for Linux. Руководство по установке

22/06/2023

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 4

2 Комплект документов 5

3 Техническая поддержка пользователей 6

4 Аппаратно-программные требования 7

5 Установка Device Monitor 11

5.1 Подготовка окружения 11

5.1.1 Установка .NET 11

5.1.2 Установка conntrack и socat 12

5.2 Установка Платформы и Веб-консоли Device Monitor 12

5.3 Установка Сервера Device Monitor 14

5.3.1 Установка Сервера с помощью параметров командной строки 16

5.4 Получение открытого ключа Платформы 17

5.5 Установка Агентов Device Monitor 18

5.5.1 Установка с помощью задачи распространения 18

5.5.2 Локальная установка 19

6 Обновление Device Monitor 21

6.1 Обновление Сервера Device Monitor 21

6.2 Обновление Агентов Device Monitor 21

7 Удаление Сервера Device Monitor 23

8 Удаление Агентов Device Monitor 24

В настоящем документе содержится инструкция по установке компонентов InfoWatch Device Monitor for Linux (далее Система или Device Monitor).

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 СУБД PostgreSQL.

2 Комплект документов

В документацию входят:

- «InfoWatch Device Monitor for Linux. Руководство по установке». Документ содержит описание процесса установки Сервера, Веб-консоли и Агентов, входящих в Систему.
- «InfoWatch Device Monitor for Linux. Руководство пользователя». Содержит описание работы в Веб-консоли для решения задач.

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 Аппаратно-программные требования

Требования к аппаратной конфигурации сервера определяются на основании предполагаемой нагрузки на Систему и параметров сети, в которой происходит развертывание, поэтому спецификация оборудования для каждого случая рассчитывается отдельно.

Примерные минимальные программно-аппаратные требования приведены в следующей таблице. Подробный расчет конфигурации настоятельно рекомендуется проводить с участием специалистов InfoWatch или компании-партнера, у которой вы приобретаете продукт.

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Сервер Device Monitor на Платформе				
Не менее 100 GB свободного пространства для установки. Также понадобится свободное пространство для анализа данных, объем зависит от нагрузки на сервер	От 4 ядер (частота - 3.1 ГГц, разрядность - 64 bit, с поддержкой инструкций SSE 4.2)	От 16 GB	ОС : РЕД ОС 7.3 СУБД: PostgreSQL версии 9.6 или 13	
Агент Device Monitor для рабочих станций				
Не менее 1 GB свободного пространства для установки. Также понадобится свободное пространство для временного хранения файлов, предназначенных для передачи на анализ	От 2 ядер	От 2.5 GB	ОС: • Astra Linux Special Edition "Смоленск" (x64) версии 1.6 с установленным обновлением безопасности Update 5 или 6; • Astra Linux Special Edition 1.7 в редакциях "Орел" и "Смоленск"; • Astra Linux Common Edition	**Поддерживаемые версии ядра Astra Linux Special Edition 1.7 в редакциях "Орел" и "Смоленск"** • 5.4.0-54-generic • 5.4.0-54-hardened • 5.4.0-81-generic • 5.4.0-81-hardened • 5.4.0-110-generic • 5.4.0-110-hardened • 5.10.0-1045-generic • 5.10.0-1045-hardened

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			"Орёл" (x64) версии 2.12; • РЕД ОС 7.3; • Альт Рабочая станция 10.	• 5.10.142-1-generic **Поддерживаемые версии ядра Astra Linux Common Edition "Орел" версии 2.12** • 4.9.135-1-generic • 4.15.3-1-generic • 4.15.3-1-hardened • 4.15.3-2-generic • 4.15.3-2-hardened • 4.15.3-3-generic • 4.15.3-3-hardened • 4.15.3-141-generic • 4.15.3-141-hardened • 4.19.0-1-generic • 5.2.13-050213-generic • 5.4.0-54-generic • 5.4.0-54-hardened • 5.4.0-71-generic • 5.4.0-71-hardened • 5.4.0-110-generic • 5.4.0-110-hardened • 5.10.0-1038.40-generic • 5.10.0-1038.40-hardened

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 5.10.0-1057-generic **Поддерживаемые версии ядра РЕД ОС 7.3** • 5.15.10-1 • 5.15.10-2 • 5.15.10-3 • 5.15.10-4 • 5.15.35-1 • 5.15.35-4 • 5.15.35-5 • 5.15.72-1 (начиная с версии 7.7.1) • 5.15.78-2 (начиная с версии 7.8) • 5.15.87-1 (начиная с версии 7.8.1) **Поддерживаемые версии ядра Альт Рабочая станция 10** • 5.10.133-std-def-alt1 • 5.10.135-std-def-alt1 • 5.10.136-std-def-alt1 • 5.10.163-std-def-alt1 • 5.10.164-std-def-alt1 • 5.10.165-std-def-alt1 • 5.10.168-std-def-alt1 • 5.10.170-std-def-alt1 • 5.10.172-std-def-alt1 • 5.10.174-std-def-alt1

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Веб-консоль Device Monitor				
	Дополнительно 1 ядро	1 GB на каждую вкладку браузера	Браузеры: • Google Chrome • Яндекс .Браузер	В браузере должна быть реализована аппаратная поддержка WebGL/WebGL2 Платформа версии 1.7 и выше

5 Установка Device Monitor

Рекомендуется соблюдать следующий порядок установки:

1. Подготовка окружения.
2. Установка Платформы и веб-консоли Device Monitor.
3. Установки Сервера Device Monitor.
4. Получение открытого ключа Платформы.
5. Установка Агентов Device Monitor.

5.1 Подготовка окружения

Для функционирования Сервера Device Monitor в среде операционной системы РЕД ОС необходимо подготовить окружение:

1. Установить Microsoft .NET 6 (https://dotnet.microsoft.com/) на этом компьютере.
2. Установить СУБД PostgresSQL на этом либо другом компьютере.
3. Установить пакеты `conntrack` (или `conntrack-tools`) и `socat.`
4. Настроить антивирус для совместной работы с Системой (см. статью Базы знаний "Настройка антивируса для Device Monitor Server на ОС Linux").

5.1.1 Установка .NET

Перед установкой .NET нужно:

1. Добавить ключ подписания пакета Microsoft в список доверенных ключей.
2. Добавить репозиторий пакетов Microsoft.

Для этого:

1. Откройте терминал и выполните следующие команды:
   `sudo rpm -Uvh https://packages.microsoft.com/config/centos/7/packages-microsoft-prod.rpm`
   При этом будет установлен ключ, и в каталоге `/etc/yum.repos.d` будет добавлен файл **microsoft-prod.repo** со следующим содержимым:
   ```
   packages-microsoft-com-prod]
   name=packages-microsoft-com-prod
   baseurl=https://packages.microsoft.com/centos/7/prod
   enabled=1
   gpgcheck=1
   gpgkey=https://packages.microsoft.com/keys/microsoft.asc
   sslverify=1
   ```
2. Установите непосредственно среду выполнения NET 6 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:
   `sudo yum install aspnetcore-runtime-6.0`
3. Проверьте установленный NET 6, выполнив команду:
   `dotnet --info`

```
[root@aspredos731dm yum.repos.d]# dotnet --info

Host (useful for support):
  Version: 6.0.5
  Commit:  70ae3df4a6

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 6.0.5 [/usr/share/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 6.0.5 [/usr/share/dotnet/shared/Microsoft.NETCore.App]

To install additional .NET runtimes or SDKs:
  https://aka.ms/dotnet-download
```

5.1.2 Установка conntrack и socat

Для корректной поддержки Kubernetes проверьте наличие установленных пакетов `conntrack` и `socat`.
Для этого:

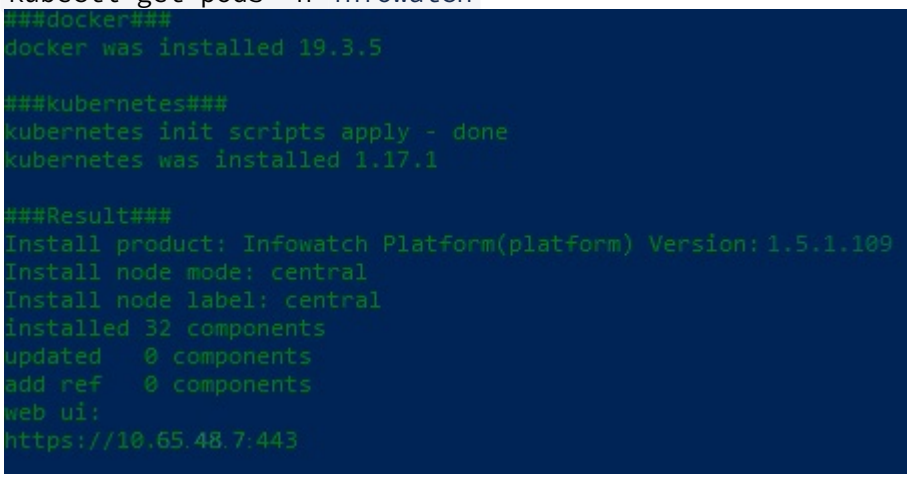
1. Введите в командной строке:
   `conntrack`
   В ответ будут выведены сведения о работе и актуальная версия этого пакета.
2. Если `conntrack` не установлен, следует установить его с помощью команды:
   `yum install conntrack`
3. Если пакет недоступен в репозитории, скачайте его, перейдите в директорию с пакетом и установите вручную с помощью команды вида:
   `rpm -Uhv ./<имя_пакета>`
4. Повторите описанные выше действия для установки пакета `socat`.

5.2 Установка Платформы и Веб-консоли Device Monitor

Чтобы установить Платформу и Веб-консоль Device Monitor:

1. Создайте директорию на жестком диске, например, dm:
   `mkdir dm`
2. Скопируйте архив **iw_devicemonitor_setup_xx.xx.xx.tar.xz** в созданную директорию.
3. Распакуйте архив с дистрибутивом продукта в созданную директорию:
   `tar xf iw_devicemonitor_setup_xx.xx.xx.tar.xz`
4. Запустите программу интерактивной установки продукта:
   `./setup.py install`
5. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
6. Введите "`y`", чтобы принять лицензионное соглашение, и нажмите **Enter**.
7. Введите IP-адрес рабочей станции формата IPv4: `"xxx.xxx.xxx.xxx"` и нажмите **Enter**.
8. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию 80%) и нажмите **Enter**.
9. Укажите путь для размещения данных Clickhouse (по умолчанию / `mnt/chdata`) и нажмите **Enter**.
10. Укажите путь для размещения данных Tarantool (по умолчанию `/mnt/trdata`) и нажмите **Enter**.

11. Укажите путь для размещения данных PostgreSQL (по умолчанию `/mnt/pgdata`) и нажмите **Enter**.
12. Укажите путь для хранения данных (по умолчанию `/mnt/dsdata`) и нажмите **Enter**.
13. Укажите порт подключения к веб-интерфейсу (по умолчанию `443`) и нажмите **Enter**.
14. Дождитесь окончания процесса установки. Программа установит компоненты продукта и требуемое окружение.
15. Убедитесь, что сервисы запущены. Для этого выполните команду:
    `kubectl get pods -n infowatch`



16. Выполните команду:
    `kubectl get configmap nginx-config -o yaml -n infowatch > n.yaml`
17. Отредактируйте `n.yaml` и внесите новый `server location` с указанным адресом для сервера DM (по умолчанию порт `15007`):

```
vi n.yaml
location /api_dm {
    rewrite /api_dm/(.+) /$1 break;
    proxy_pass https://SERVER_IP_ADRESS:15007;
    proxy_set_header Cookie $http_cookie;
}
```

> **Важно!**
>
> Формат `.yaml` не поддерживает табуляцию, поэтому убедитесь, что отступ в начале строк выставлен с помощью пробелов.

18. Выполните команды:

```
kubectl apply -f n.yaml
kubectl rollout restart deployment webgui-central -n infowatch
```

19. Введите в браузере полученный IP-адрес и порт (в нашем примере – `https://10.65.48.7:443`), чтобы начать эксплуатацию Системы.

> **Важно!**
>
> При редактирования файла `n.yaml` всегда необходимо выполнять шаги 17-19.

5.3 Установка Сервера Device Monitor

Дистрибутив Сервера Device Monitor для РЕД ОС состоит из двух файлов: **iwdms.zip** и **install.sh**. Скопируйте их на сервер РЕД ОС с предварительно настроенным окружением (подробнее см. "Подготовка окружения").

Шаги установки:

1. Перейдите в директорию, где содержатся указанные файлы и добавьте атрибут *исполняемый* для файла **install.sh** с помощью команды:
   `sudo chmod +x ./install.sh`
2. Запустите скрипт от пользователя **root** или с помощью команды:
   `sudo ./install.sh`
3. Скрипт работает в режиме диалога с пользователем. Введите "Y", чтобы продолжить установку. В этом случае:
   a. Будут установлены каталоги:
      - `/var/log/iwdms` – каталог логов выполнения сервера DM;
      - `/opt/iw/dmserver/bin` – каталог, в который помещаются файлы сервера DM;
      - `/opt/iw/dmserver/queue` – каталог файловой очереди;
      - `/opt/iw/dmserver/log` – символическая ссылка на каталог `/var/log/iwdms`.
   b. Будет добавлен пользователь **iwdms**. Пользователь добавляется с ключом `--system`, что позволяет запустить под этим пользователем службу, но не дает авторизоваться под ним в консоли управления. Пользователь **iwdms** будет также назначен владельцем вышеуказанных папок.
   c. Архив **iwdms.zip** будет распакован в требуемые каталоги.
   d. В каталоге systemd-служб `/etc/systemd/system` будет добавлен файл манифеста службы сервера DM – **iwdms.service**.
4. Дождитесь появления сообщения:
   ```
   Creating short link to log folder
   Extracting DM Server files
   IW DMS extracted.
   ```
5. Для продолжения установки запустите скрипт первичной настройки. Введите "Y", чтобы запустить скрипт:
   `Run primary configuration script? [Y/N]:`
   В случае отказа ("N") впоследствии скрипт можно запустить вручную от пользователя **root**, выполнив команды:
   ```
   cd /opt/iw/dmserver/bin/
   sudo ./firstconf.sh
   ```
6. Выберите язык устанавливаемого сервера. Это определит названия предустановленных групп, политик и правил. Для этого введите:
   - R – для работы в консоли управления на русском языке;
   - E – для работы в консоли управления на английском языке.
7. Ознакомьтесь с лицензионным соглашением и выберите необходимое действие. Для продолжения установки необходимо принять лицензионное соглашение. Введите требуемый символ:
   - L – показать лицензионное соглашение на выбранном ранее языке;
   - C – принять лицензионное соглашение и продолжить установку;
   - Q – выйти.
8. Укажите тип устанавливаемого сервера. Для этого введите:

- P – основной сервер;
- S – вспомогательный сервер.

9. При установке **основного** сервера укажите путь до PFX-файла ключа шифрования канала между сервером DM и агентами. Если путь не указывать, то будет использован путь, предложенный по умолчанию, – `/opt/iw/dmserver/ssl.pfx`
   Если вы устанавливаете **вспомогательный** сервер Device Monitor, далее выполните пункты 12-19. При установке **вспомогательных** серверов автоматически присваивается адрес Traffic Monitor, который был назначен основному серверу.
10. В случае отсутствия ключа его необходимо создать. Для этого в сообщении "`PFX file not exists. Create new? [Y/N]:`" введите:
    - Y – чтобы создать новый ключ;
    - N – чтобы скрипт заново запросил путь до PFX-файла. Если указать путь до существующего ключа, сервер проверит его корректность, и, если ключ подходит, скрипт продолжит свою работу.
11. Настройте взаимодействие с базой данных, Для этого введите:
    - N – чтобы создать новую базу данных;
    - U – чтобы настроить существующую базу данных.
12. Укажите имя или IP-адрес сервера, на котором располагается СУБД PostgreSQL. Нельзя выбрать СУБД, ранее используемую для установки Сервера Device Monitor на ОС Windows.
13. Укажите порт для настройки взаимодействия. Если порт не указан, будет использован порт по умолчанию – `5432`.
14. Введите имя базы данных. По умолчанию – `iwdm.`
15. Введите имя пользователя СУБД. По умолчанию – `postgres.`
16. Введите пароль.
17. Введите адрес InfoWatch Traffic Monitor (IWTM). Для этого используйте имя сервера или его IP-адрес.
18. Введите токен доступа к IWTM. После этого скрипт выполнит работу по созданию, заполнению и обновлению (при необходимости) базы данных.
19. Укажите путь до файла открытого ключа Платформы с установленной веб-консолью Device Monitor. Указанный файл будет скопирован в каталог Сервера в файл `/opt/iw/dmserver/bin/guard.pem`. Параметр можно оставить пустым. При этом будет отображен запрос на продолжение установки без указания ключа, но после завершения установки необходимо выполнить инструкцию "Получение открытого ключа Платформы".
20. Укажите, нужно ли установить сервис распространения дистрибутивов. Для этого введите:
    - Y – чтобы установить сервис. В этом случае точка распространения будет опубликована в таблице `PublicationPoint` связанной СУБД PostgreSQL и сможет распространять дистрибутивы агентов под РЕД ОС версии 7.3 (x64).
    - N – чтобы пропустить шаг. В этом случает установить сервис распространения позднее будет невозможно.

В случае возникновения ошибки будет выведена ссылка на журнал с детальным описанием ошибки: "`[ERR] Can't create/update database! Log: /var/log/iwdms/dbinstall.log`". Процесс установки при этом будет остановлен.

В случае успешной установки будет запущена служба сервера DM. Служба будет помечена как запускаемая автоматически. Запуск службы осуществляется под пользователем **iwdms**, созданным на этапе развертывания Системы при помощи скрипта **install.sh**. Чтобы проверить, запущена ли служба сервера DM, выполните команду:

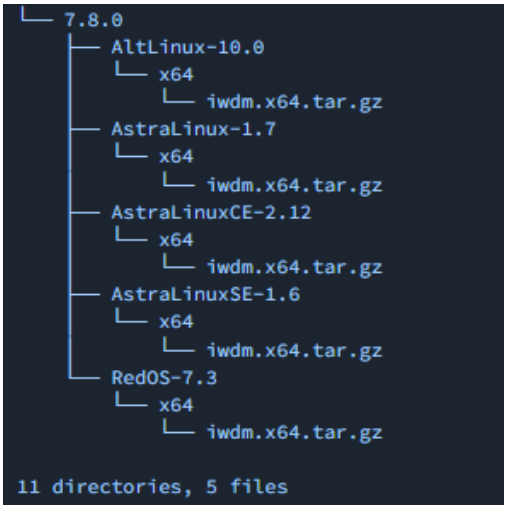
```
systemctl status iwdms
```

```
[root@aspredos731dm bin]# systemctl status iwdms
● iwdms.service - The InfoWatch Device Monitor Server service
     Loaded: loaded (/etc/systemd/system/iwdms.service; enabled; vendor preset: disabled)
     Active: active (running) since Mon 2022-05-23 18:58:24 MSK; 4min 16s ago
   Main PID: 3404 (dotnet)
      Tasks: 76 (limit: 9498)
     Memory: 92.0M
        CPU: 3.576s
     CGroup: /system.slice/iwdms.service
             ├─3404 /usr/bin/dotnet /opt/iw/dmserver/bin/InfoWatch.DeviceMonitor.Server.dll
             └─3464 dotnet /opt/iw/dmserver/bin/InfoWatch.DeviceMonitor.Server.WebApi.dll --Culture
```

При установке сервиса распространения будет автоматически создана структура папок для публикации. Чтобы посмотреть ее, выполните команду:

```
tree
```

Например, для версии 7.8 структура имеет следующий вид:



Диагностическую информацию по работе службы можно найти в логах сервера в каталоге `/opt/iw/dmserver/log`.

5.3.1 Установка Сервера с помощью параметров командной строки

Сервер Device Monitor может быть установлен с помощью параметров командной строки. Чтобы вызвать справку по параметрам, введите:

```
./install.sh --help
```

При этом на экран будет выведена справка по возможным параметрам:

```
This script must be run with super-user privileges.
Usage: ./install.sh [arguments] [additional arguments]
Arguments:
  f - [optional] Suppress installation prompt
  c - [optional] Run primary configuration script after extracting files.
      Values:
      1 - run /opt/iw/dmserver/bin/firstconf.sh and pass parameters from [additional
arguments]
      0 - not run /opt/iw/dmserver/bin/firstconf.sh. It's default value
Additional arguments:
  l - [optional] DM Server language. Values: 'r' for russian language or 'e' for english
language. Default value is 'e'
  t - [required] DM Server type. Values: 'p' for primary server or 's' for secondary
```

```
server
  k - [required] PFX file path. If the file does not exist, it will be created
  h - [required] PostgreSQL server name (only host name)
  p - [optional] PostgreSQL server communication port. Default value is '5432'
  n - [required] Create a new database or use an existing one. Values: '1' for new or '0'
for use existing one
  d - [required] Database name
  u - [required] Database user name
  z - [required] Database user password
  s - [required] Install DM Server in standalone mode. Values: '1' or '0'
  x - [required] IW Traffic Monitor address
  a - [required] IW Traffic Monitor auth token
  j - [required] Platform pubkey in PEM format
  w - [optional] Install IW IW Distribution Service. Values: '1' or '0'
```

Через командную строку можно задать все параметры, описанные выше, кроме дополнительного параметра "`s`", который нельзя указать в интерактивном режиме . Если указать этот параметр со значением "`1`", Сервер будет установлен в автономном режиме, т.е. не будет подключаться к Traffic Monitor.

В случае, если распаковка Сервера осуществляется отдельно от его настройки, то в скрипте настройки также можно вызвать справку по параметрам. Для этого необходимо перейти в каталог сервера и вызвать скрипт с параметром --help:

```
cd /opt/iw/dmserver/bin/
./firstconf.sh --help
```

Параметры скрипта настройки аналогичны дополнительным аргументам (Additional arguments) скрипта `install.h`.

Пример:

Запуск скрипта настройки:

```
./install.sh -f -c 0
cd /opt/iw/dmserver/bin/
./firstconf.sh -l r -t p -k "/opt/iw/dmserver/key.pfx" -h dbserver -p 5432 -n 1 -d
iwdm7 -u postgres -z postgres -s 1 -x tm -a tmtoken
```

Запуск скрипта с параметрами:

```
./install.sh -f -c 1 -l r -t p -k "/opt/iw/dmserver/key.pfx" -h dbserver -p 5432 -n
1 -d iwdm7 -u postgres -z postgres -s 1 -x tm -a tmtoken
```

5.4 Получение открытого ключа Платформы

Открытый ключ Платформы необходим Серверу Device Monitor для проверки JWT-токенов, получаемых от DM WEB UI при вызовах DM WEB API. Если на Сервере отсутствует ключи или добавлен ключ, отличный от используемого в Платформе, на которую установлен DM WEB UI, то все запросы на DM WEB API будут возвращать ошибку авторизации.

Каталог размещения ключа на Сервере Device Monitor: `/opt/iw/dmserver/bin`. Выполните следующие действия в контексте суперпользователя – от имени **root** или через команду **sudo**:

1. Получите ключ в Платформе и сохраните его в `/opt/iw/dmserver/bin /guard.pem`. Для этого выполните команду:
   `kubectl get secret guardkeys-central -n infowatch -o 'go-template={{index .data "ec256-public.pem"}}' | base64 -d > /opt/iw/dmserver/bin/guard.pem`
   Ключ будет сохранен на диске в PEM-формате и иметь содержимое вида:

   ```
   -----BEGIN PUBLIC KEY-----
   MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEYD54V/vp+54P9DXarYqx4MPcm+HK
   RIQzNasYSoRQHQ/6S6Ps8tpMcT+KvIIC8W/e9k0W7Cm72M1P9jU7SLf/vg==
   -----END PUBLIC KEY-----
   ```

2. Служба Сервера Device Monitor исполняется от имени пользователя **iwdms**, поэтому необходимо назначить этого пользователя владельцем ключа. Выполните команду:
   `chown -f iwdms:iwdms /opt/iw/dmserver/bin/guard.pem`
3. Перезапустите службу `iwdms` для применения нового ключа:
   `systemctl restart iwdms`

5.5 Установка Агентов Device Monitor

Установка Агентов Device Monitor на рабочие станции может быть выполнена:

- с помощью задачи распространения в веб-консоли Device Monitor;
- локально на каждой контролируемой рабочей станции.

> **Важно!**
>
> Не допускается установка Агента InfoWatch Device Monitor и сервера Device Monitor на один компьютер, это может привести к неработоспособности сервера.

> **Важно!**
>
> При установке, обновлении и удалении Агента выполняется кратковременный разрыв всех сетевых соединений. Это связано с установкой компонентов контроля сетевого трафика, используемых в Device Monitor (IWPROXY и IWNBG). Кроме того, разрыв связан как с технологическими особенностями ОС при установке модулей, так и с принудительным перезапуском сетевых карт при установке модуля «прозрачная прокси».

5.5.1 Установка с помощью задачи распространения

Для установки Агентов Device Monitor с помощью задачи распространения необходимо наличие установленного сервиса распространения (подробнее см. "Установка Сервера Device Monitor", Шаг 19).

Для установки Агентов выполните шаги:

1. В разделе **Задачи** веб-консоли создайте задачу первичного распространения (см. "Задача первичного распространения и обновления").
2. Сформируйте список рабочих станций для установки Агентов (см. "Задача первичного распространения и обновления").

3. Запустите задачу, нажав .
4. Введите учетные данные пользователя, от имени которого запускается задача, и нажмите **Запустить**.
5. Дождитесь окончания выполнения задачи. В области **Выполнение задачи** будет отображен список рабочих станций с информацией об Агентах.

> **Примечание:**
>
> Если на рабочей станции используется антивирус, рекомендуется:
>
> - добавить файлы Агента в исключения антивируса (список файлов см. в статье "Список файлов Агента InfoWatch для добавления в исключения антивирусов");
> - исключить антивирус из перехвата (см. "InfoWatch Device Monitor for Linux. Руководство пользователя", "Исключение приложений из перехвата").

> **Примечание:**
>
> Если на компьютере установлена кастомизированная версия системы SeLinux, корректная установка Агента не гарантируется.

5.5.2 Локальная установка

> **Важно!**
>
> Если на компьютере под управлением ОС Astra Linux 1.6 установлен Агент InfoWatch Device Monitor версии ниже 7.0, для установки Агента новой версии **обязательно** выполните следующие действия:
>
> 1. Удалите Агент InfoWatch Device Monitor.
> 2. Установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 6 (20200722SE16) (см. официальную инструкцию).
> 3. Установите новую версию Агента InfoWatch Device Monitor.

1. **Подготовка к установке:**
   a. Если на компьютере под управлением ОС Astra Linux 1.6 ранее было установлено обновление безопасности (например, Update 5):
      i. Узнайте номер установленного обновления безопасности Astra Linux: `cat /etc/astra?update?version`
      ii. Узнайте текущую версию ядра Astra Linux (например, **4.15.3-2-generic**): `uname -r`
      iii. Проверьте, что директория */boot* не содержит старых пакетов ядра с более ранней версией, чем в предыдущем шаге (например, **initrd.img-4.15.3-1-generic** или **initrd.img-4.15.3-1-hardened**).
      iv. Удалите такие пакеты при наличии: `apt-get purge linux-image-4.15.3-1`

v. Удалите неиспользуемые Системой пакеты:
`apt-get autoremove`
`apt-get autoclean`

b. Скопируйте на компьютер архив, в котором содержатся пакет и скрипты для установки и удаления Агента Device Monitor. Архив расположен на сервере Device Monitor в папке `/opt/iw/dmserver/bin/SetupPackages/`. Название архива может отличаться в зависимости от используемой ОС:
   - `Setup.AstraLinuxSE-1.6-iwdm.x64.x.x.x.xx.tar.gz` – для Astra Linux Special Edition 1.6;
   - `Setup.AstraLinuxCE-2.12-iwdm.x64.x.x.x.xx.tar.gz` – для Astra Linux Common Edition 2.12;
   - `Setup.AstraLinux-1.7-iwdm.x64.x.x.x.xx.tar.gz` – для Astra Linux Special Edition 1.7;
   - `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz` – для РЕД ОС 7.3;
   - `Setup.AltLinux-10.0-iwdm.x64.x.x.x.xx.tar.gz` – для Альт Рабочая станция 10.

   где x.x.x.xx - номер сборки.
   Далее мы рассмотрим пример установки и удаления Агента на РЕД ОС 7.3. Установка и удаление продукта на других поддерживаемых ОС аналогичны. В нашем примере:
   `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`

c. На целевом компьютере перейдите в директорию, в которую скопирован архив, и введите команду для распаковки:
`sudo tar -xvzf Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`
В результате будут созданы файлы `install.sh`, `remove.sh`, `upgrade.sh`, `iwdm_<версия_агента>.rpm`.

2. **Установка Агента InfoWatch Device Monitor:**

a. Выполните *Шаг 1* инструкции по локальной установке (см. "Установка Агентов Device Monitor").

b. Перейдите в директорию, в которую распаковано содержимое архива `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`.

c. Запустите скрипт, выполнив команду:
`sudo ./install.sh <сервер>:<порт>`
где `<сервер>` – IP-адрес или доменное имя Сервера Infowatch Device Monitor, `<порт>` – порт подключения к Серверу Infowatch Device Monitor.
В нашем примере команда будет следующей:
`sudo ./install.sh dm-server:15101`
Продукт будет установлен в директорию `/opt/iw/dmagent`.

d. Проверьте статус сервисов, выполнив команду:
`sudo systemctl status iwdm*`

6 Обновление Device Monitor

Обновление Device Monitor выполняется в том же порядке, что и установка:

1. Обновление Сервера Device Monitor
2. Обновление Агентов Device Monitor

6.1 Обновление Сервера Device Monitor

> **Важно!**
>
> При обновлении Сервера Device Monitor все неотправленные в Traffic Monitor события будут утеряны. Проверьте успешную отправку событий на Сервер Traffic Monitor.

Чтобы обновить Сервер:

1. Сохраните файл открытого ключа Платформы на жестком диске. Путь до файла `/opt/iw/dmserver/bin/guard.pem`.
2. Удалите старую версию Сервера Device Monitor (подробнее см. "Удаление Сервера Device Monitor"). Не удаляйте данные БД. Для этого на шаге 5 введите **N**.
3. Обновите Платформу на новую версию:
   a. Создайте директорию на жестком диске, например, `dm`:
   `mkdir dm`
   b. Скачайте архив с новой версией дистрибутива.
   c. Распакуйте архив с дистрибутивом продукта в созданную директорию:
   `tar xf iw_devicemonitor_setup_xx.xx.xx.tar.xz`
   d. Запустите скрипт обновления:
   `./setup.py update`
   e. Дождитесь окончания обновления.
4. Скопируйте сохраненный на шаге 1 файл ключа в директорию `/opt/iw/dmserver/bin/`.
5. Установите новую версию Сервера Device Monitor на существующую БД (подробнее см. "Установка Сервера Device Monitor"). Для этого на шаге 11 введите **U** и далее все данные сохраненной БД. При обновлении открытый ключ Платформы не меняется, поэтому на шаге 19 укажите старый путь до файла открытого ключа.

6.2 Обновление Агентов Device Monitor

Обновление Агентов Device Monitor на рабочих станциях может быть выполнено:

- с помощью задачи распространения в веб-консоли Device Monitor (см. "Задача первичного распространения и обновления");
- локально на каждой контролируемой рабочей станции.

Чтобы локально обновить Агенты до новой версии:

1. Выполните *Шаг 1* инструкции по локальной установке (см. "Установка Агентов Device Monitor").
2. Перейдите в директорию, в которую было распаковано содержимое архива.
3. Запустите скрипт обновления, выполнив команду:
   `sudo ./upgrade.sh`

4. Дождитесь окончания обновления. Проверить статус выполнения можно, выполнив команду:
   `sudo systemctl status iwdm*`

Важно!

Если остановленный агент был обновлен, то после завершения обновления он будет запущен.

Для корректной блокировки съемных устройств после обновления Агента на ОС семейства Linux обязательно перезагрузите рабочую станцию.

7 Удаление Сервера Device Monitor

Удаление Сервера Device Monitor осуществляется с помощью скрипта **remove.sh**, который располагается в каталоге `/opt/iw/dmserver/bin/`.

Чтобы удалить Сервер Device Monitor:

1. По умолчанию файл скрипта не помечен как исполняемый. Чтобы сделать его исполняемым, перейдите в указанный каталог и добавьте ему атрибут "*исполняемый*", используя команды:
   ```
   cd /opt/iw/dmserver/bin/
   sudo chmod +x ./remove.sh
   ```
2. Скрипт должен выполняться от имени суперпользователя **root**. Запустите скрипт удаления:
   ```
   sudo ./remove.sh
   ```
3. Подтвердите запрос на удаление, нажав **Y**. При этом можно выбрать:
   - Y – чтобы продолжить удаление;
   - N – чтобы прервать удаление.
4. Дождитесь остановки службы сервера и определения его типа.
   ```
   Stopping the service iwdms...
   Service iwdms stopped
   Server role: primary
   ```
5. Если сервер основной, то подтвердите последующее удаление БД. Нажмите **Y** и введите пароль пользователя БД для подтверждения удаления.
6. Если требуется удалить каталог с файлами журнала (логами), нажмите **Y**.
7. Если требуется удалить каталог файловой очереди, нажмите **Y**.
8. Дождитесь окончания процесса удаления, который включает в себя:
   - удаление СУБД. Если в п. 5 вы указали **N**, то сервер будет помечен как "устаревший";
   - удаление каталогов сервера;
   - удаление службы сервера;
   - удаление пользователя *iwdms*.
9. В процессе удаления возможно появление ошибок. Например, в случаях, когда сервер был не полностью сконфигурирован, БД оказалась недоступной на момент удаления или возникли ошибки при определении типа сервера. В этом случае в консоли вы увидите текст ошибки и вопрос, нужно ли продолжить удаление только файлов сервера Device Monitor.

8 Удаление Агентов Device Monitor

Удаление Агентов Device Monitor производится локально на рабочих станциях.

Чтобы удалить Агент InfoWatch Device Monitor на ОС Astra Linux, РЕД ОС и Альт Рабочая станция:

1. Выполните *Шаг 1* инструкции по локальной установке (см. "Установка Агентов Device Monitor").
2. Перейдите в директорию, в которую было распаковано содержимое архива.
3. Запустите скрипт удаления, выполнив команду:
   `sudo ./remove.sh`
   Будут удалены и Агент Device Moinitor, и Агент распространения.

Важно!

Выключение питания компьютера в процессе установки/удаления Агента может привести к ошибкам, ведущим к нестабильной работе операционной системы.

В случае возникновения трудностей при удалении Агента рекомендуем обратиться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

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