

INFOWATCH

InfoWatch Device Monitor for Linux. Руководство по установке

15/07/2024

© 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 Аппаратно-программные требования 8

5 Установка Device Monitor 15

5.1 Подготовка окружения 15

5.1.1 Установка .NET на примере операционной системы РЕД ОС 16

5.1.2 Установка conntrack и socat на примере операционной системы РЕД ОС 17

5.2 Установка Платформы и Веб-консоли Device Monitor 17

5.3 Установка Сервера Device Monitor 20

5.3.1 Установка Сервера с помощью параметров командной строки 22

5.4 Настройка проверки сертификатов удаленных серверов 24

5.4.1 Чтобы настроить проверку сертификатов удаленных серверов при установлении SSL-сессии: 24

5.4.2 Чтобы установить сертификат службы XAPI Traffic Monitor: 25

5.4.3 Чтобы установить сертификат веб-сервера Traffic Monitor Traffic Monitor: 26

5.4.4 Чтобы установить сертификат службы EPEVENTS Платформы: 26

5.4.5 Просмотр логов 27

5.5 Получение открытого ключа Платформы 27

5.6 Установка Агентов Device Monitor 28

5.6.1 Локальная установка Агентов 32

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью msi-пакета с последующим вводом параметров вручную: 32

5.6.2 Установка Агентов с помощью задачи распространения 34

6 Настройка сетевых правил доступа 36

7 Обновление Device Monitor 38

7.1 Обновление Сервера Device Monitor 38

7.2 Обновление Агентов Device Monitor 39

8 Удаление Device Monitor 41

8.1 Удаление Сервера Device Monitor 41

8.2 Удаление Агентов Device Monitor 41

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; • Astra Linux 1.7 "Смоленск"; • Альт Сервер Виртуализации 10. СУБД: PostgreSQL версии 11 и более поздние версии.	• На сервере ТМ должен быть включен автозапуск процесса **iw_xapi_xapi** • Наличие локального DNS для перевода доменных имен в адреса • Режим FIPS должен быть отключен • Должен поддерживаться протокол TLS 1.2
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: • [1]Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 и 8.1; • Microsoft Windows 10;	**Поддерживаемые версии ядра Astra Linux Special Edition "Смоленск" версии 1.6 (все пакеты безопасности)** • 4.15.3-1-generic

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			• Microsoft Windows 11; • [1]Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Astra Linux Special Edition "Смоленск" (x64) версии 1.6 с установленным обновлением безопасности Update 5, 6 или 12; • Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" и "Смоленск"; • Astra Linux Common Edition "Орёл" (x64) версии 2.12; • РЕД ОС 7.3;	• 4.15.3-1-hardened • 4.15.3-2-generic • 4.15.3-2-hardened • 4.15.3-154-generic • 4.15.3-154-hardened • 4.15.3-177-generic • 4.15.3-177-hardened • 5.4.0-110-generic • 5.4.0-110-hardened • 5.10.142-1-generic • 5.15.0-33-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

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			• Альт Рабочая станция 10.	• 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 • 5.10.0-1057-generic • 5.10.142-1-generic • 5.10.142-1-hardened • 5.15.0-33-generic • 5.15.0-33-hardened • 5.15.0-70-generic • 5.15.0-70-hardened **Поддерживаемые версии ядра Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" и "Смоленск"** • 5.4.0-54-generic • 5.4.0-54-hardened

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 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 • 5.10.142-1-generic • 5.15.0-33-generic • 5.15.0-70-generic • 6.1.50-1-generic (начиная с версии 7.11.2) **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) • 5.15.106-1 • 5.15.117-1 • 5.15.125-1 • 5.15.131-1

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 6.1.20-2 • 6.1.44-1 • 6.1.52-1 (начиная с версии 7.11.4) **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 • 5.10.176-std-def-alt1 • 5.10.177-std-def-alt1 • 5.10.179-std-def-alt1 • 5.10.182-std-def-alt1 • 5.10.185-std-def-alt1 • 5.10.186-std-def-alt1 • 5.10.191-std-def-alt1 • 5.10.194-std-def-alt1

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 5.10.198-std-def-alt1 (начиная с версии 7.11.2) • 5.10.199-std-def-alt2 (начиная с версии 7.11.2) • 5.15.94-un-def-alt1 • 5.15.109-un-def-alt1 • 6.1.29-un-def-alt1 (начиная с версии 7.11.2) • 6.1.32-un-def-alt1 • 6.1.42-un-def-alt1
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

Примечание:

[1] - для указанных ОС требуется установка следующих исправлений от компании Microsoft: KB4474419, KB4490628. Проверка на наличие данных исправлений на компьютере проводится Системой перед установкой и/или обновлением продукта.

Примечание:

Допустима установка в виртуальную среду: VMware, MS Hyper-V или других систем виртуализации.

Работа агентов Device Monitor поддержана в средах виртуализации Microsoft RDS, Citrix XenApp 6.0, 7.6, 7.13, 7.14 и 7.15 LTSR.

5 Установка Device Monitor

Рекомендуется соблюдать следующий порядок установки:

1. Подготовка окружения.
2. Установка Платформы и веб-консоли Device Monitor.
3. Установка Сервера Device Monitor.
4. Настройка проверки сертификатов удаленных серверов.
5. Получение открытого ключа Платформы.
6. Установка Агентов Device Monitor.

5.1 Подготовка окружения

Для функционирования Сервера Device Monitor необходимо подготовить окружение:

1. Ввести в домен компьютер, на который будет установлен Сервер Device Monitor.
2. Установить Microsoft .NET 6 (https://dotnet.microsoft.com/) на этом компьютере.
3. Установить СУБД PostgreSQL на этом либо другом компьютере.
4. Установить пакеты `conntrack` (или `conntrack-tools`) и `socat`.
5. Настроить антивирус для совместной работы с Системой (см. статью Базы знаний "Настройка антивируса для Device Monitor Server на ОС Linux").
6. Настроить правила POD сети или отключить межсетевой экран (см. статьи Базы знаний "Конфликты при взаимодействии firewalld и Kubernetes", "Полное отключение межсетевого экрана").
7. Если установка проводится на ОС Альт:
   - Установить утилиту `unzip` аналогично установке `conntrack` и `socat`;
   - Установить пакет с интерпретатором языка Python версии 2.7, а также следующие пакеты:
     - `python-modules-json`
     - `python-modules-distutils`
     - `python-modules-sqlite3`

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

   - Настроить соответствие алгоритмов шифрования Сервера Device Monitor и Сервера Traffic Monitor. Для этого измените файл `/etc/openssl/openssl.cnf` следующим образом:
     a. После раздела `oid` добавьте раздел `System default`:
     ```
     # Extra OBJECT IDENTIFIER info:
     #oid_file       = $ENV::HOME/.oid
     oid_section     = new_oids

     # System default
     openssl_conf = default_conf
     ```
     b. В конец файла добавьте следующие строки:

```
[default_conf]
ssl_conf = ssl_sect

[ssl_sect]
system_default = system_default_sect

[system_default_sect]
MinProtocol = TLSv1.2
CipherString = DEFAULT:@SECLEVEL=1
```

Важно!

Для успешного соединения Сервера Device Monitor с Сервером Traffic Monitor необходимо до или после установки настроить проверку сертификата удаленного сервера (подробнее см. "Настройка проверки сертификатов удаленных серверов").

5.1.1 Установка .NET на примере операционной системы РЕД ОС

1. Убедитесь, что репозитории РЕД ОС доступны, выполнив команду:
   `dnf repoinfo`
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`
   В некоторых дистрибутивах Linux имя пакета может быть `dotnet-aspnetcore-runtime-6.0`
   В результате будет установлена среда выполнения .NET 6 с поддержкой ASP.NET Core.
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
```

В процессе установки .NET могут возникнуть ошибки. В этом случае:

1. Удалите из операционной системы все пакеты, связанные с .NET, выполните команду:
   `sudo dnf remove 'dotnet*' 'aspnet*' 'netstandard*'`
2. Установите заново конкретную версию .NET, например:
   `sudo dnf install aspnetcore-runtime-6.0-6.0.5-1.el7`
3. Чтобы посмотреть список доступных версий, выполните:
   `dnf --showduplicates list aspnetcore-runtime-6.0`

5.1.2 Установка conntrack и socat на примере операционной системы РЕД ОС

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:
   `sudo 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`.

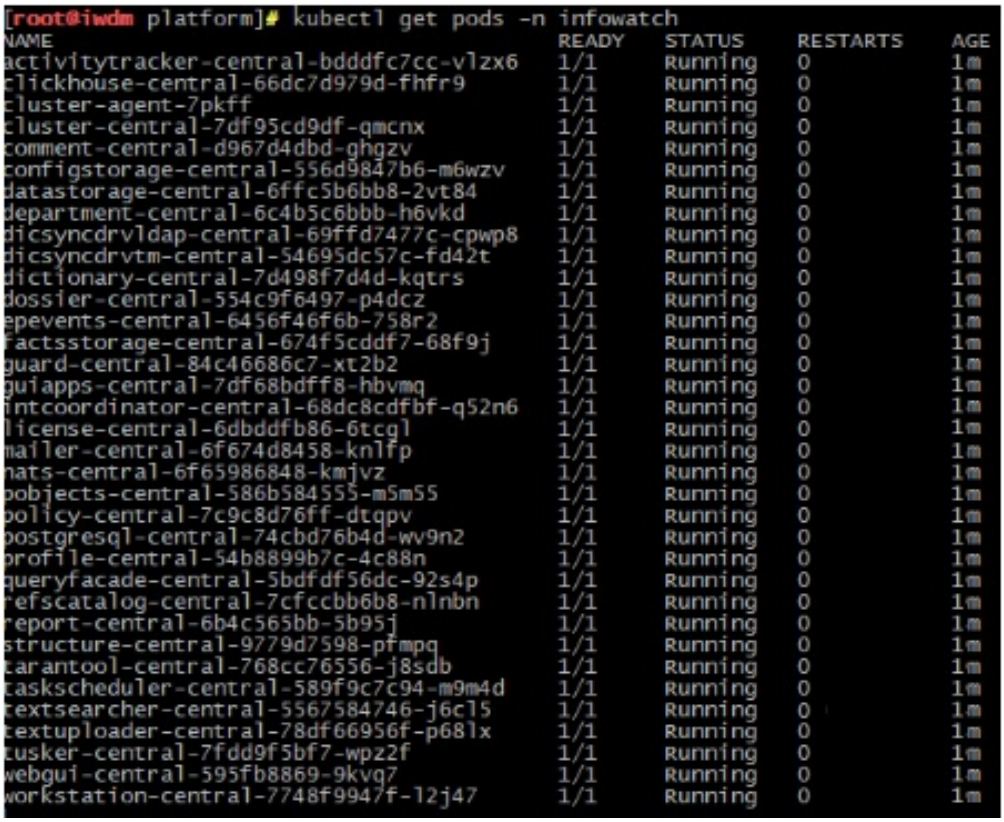
5.2 Установка Платформы и Веб-консоли Device Monitor

Важно!

Не поддерживается совместная установка на одном сервере InfoWatch Device Monitor с другими продуктами InfoWatch на Платформе.

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 xvf 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 сервера в формате 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. После окончания установки компонентов продукта и окружения убедитесь, что сервисы запущены. Для этого выполните команду:
    `kubectl get pods -n infowatch`



15. Выполните команду:
    `kubectl get configmap nginx-config -o yaml -n infowatch > n.yaml`
16. 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.

17. Выполните команды:
    ```
    kubectl apply -f n.yaml
    kubectl rollout restart deployment webgui-central -n infowatch
    ```
18. 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 16-18.

5.3 Установка Сервера Device Monitor

Далее будет рассмотрена установка Сервера Device Monitor на операционной системе РЕД ОС.

Дистрибутив Сервера Device Monitor состоит из двух файлов: **iwdms.zip** и **install.sh**. Скопируйте их на сервер с 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 каталог 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, на следующем шаге введите **N**. 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.

> **Важно!**
>
> Для успешного соединения Сервера Device Monitor с Сервером Traffic Monitor необходимо настроить проверку сертификата удаленного сервера (подробнее см. "Настройка проверки сертификатов удаленных серверов")

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 на рабочие станции, кроме рабочих станций под управлением ОС Windows;

- 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 /opt/iw/iwdistribution/
```

Например, для версии 7.8 структура имеет следующий вид:

```
└── 7.8.0
    ├── AltLinux-10.0
    │   └── x64
    │       └── iwdm.x64.tar.gz
    ├── AstraLinux-1.7
    │   └── x64
    │       └── iwdm.x64.tar.gz
    ├── AstraLinuxCE-2.12
    │   └── x64
    │       └── iwdm.x64.tar.gz
    ├── AstraLinuxSE-1.6
    │   └── x64
    │       └── iwdm.x64.tar.gz
    └── RedOS-7.3
        └── x64
            └── iwdm.x64.tar.gz

11 directories, 5 files
```

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.sh`.

> **Пример:**
>
> **Установка с параметрами из скрипта настройки `firstconf.sh`:**
>
> ```
> ./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
> ```
>
> **Запуск скрипта настройки с дополнительными параметрами, вводимыми вручную:**
>
> ```
> ./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
> ```

5.4 Настройка проверки сертификатов удаленных серверов

На сервере Device Monitor для повышения безопасности реализована возможность проверки сертификатов удаленных серверов. Данная проверка позволяет установить подлинность удаленного сервера при подключении к нему.

Device Monitor осуществляет проверку следующих сертификатов:

- сертификата службы XAPI – при подключении к серверу Traffic Monitor для отправки событий
- сертификата веб-сервера Traffic Monitor (сертификат TMConfig) – при подключении к серверу Traffic Monitor для синхронизации политик защиты данных
- сертификата службы EPEVENTS – при подключении к серверу Платформы для отправки событий

Чтобы успешно подключиться к удаленному серверу для отправки событий:

1. Настройте проверку сертификатов на сервере Device Monitor;
2. На сервере Device Monitor установите корневой сертификат удаленного сервера в хранилище корневых сертификатов уровня "локальный компьютер".

Чтобы успешно подключиться к серверу Traffic Monitor для синхронизации политик защиты данных:

1. Настройте проверку сертификатов на сервере Device Monitor;
2. В центре сертификации вашей компании выпустите сертификат X.509 для веб-сервера Traffic Monitor;
3. Настройте работу веб-сервера Traffic Monitor с выпущенным сертификатом;
4. Установите корневой сертификат веб-сервера Traffic Monitor в хранилище корневых сертификатов уровня "локальный компьютер" на сервере Device Monitor.

> **Важно!**
>
> Если вы не выполните шаги 2-4, то необходимо отключить проверку сертификата веб-сервера Traffic Monitor. Соединение с сервером Traffic Monitor будет защищено протоколом TLS, но сервер Device Monitor не сможет удостовериться, что он подключился к нужному серверу Traffic Monitor.

5.4.1 Чтобы настроить проверку сертификатов удаленных серверов при установлении SSL-сессии:

Установите значение `True` или `False` для следующих полей таблицы Settings в базе данных сервера Device Monitor:

- `IGNORE_SSLERR_TMXAPI_CONNECTION` – игнорировать проверку сертификата службы XAPI Traffic Monitor;
- `IGNORE_SSLERR_TMCONFIG_CONNECTION` – игнорировать проверку сертификата TMConfig Traffic Monitor;
- `IGNORE_SSLERR_PLATFORM_CONNECTION` – игнорировать проверку сертификата службы EPEVENTS Платформы.

При значении `False` проверка сертификата будет выполняться.

Значение поля `IGNORE_SSLERR_TMXAPI_CONNECTION` по умолчанию:

- при первичной установке сервера Device Monitor – `False`, т.е. проверка сертификата службы XAPI Traffic Monitor включена;
- при обновлении сервера Device Monitor версии 7.9 и ниже – `True`, т.е. проверка выключена;
- при обновлении сервера Device Monitor версии 7.10 и выше – значение остается равным тому, что было до обновления.

Значение поля `IGNORE_SSLERR_TMCONFIG_CONNECTION` по умолчанию:

- при первичной установке сервера Device Monitor – `False`, т.е. проверка сертификата веб-сервера Traffic Monitor включена;
- при обновлении сервера Device Monitor – `True`, т.е. проверка выключена.

Значение поля `IGNORE_SSLERR_PLATFORM_CONNECTION` по умолчанию:

- при первичной установке сервера Device Monitor – `True`, т.е. проверка сертификата службы EPEVENTS Платформы выключена;
- при обновлении сервера Device Monitor версии 7.9 и ниже – `True`, т.е. проверка выключена;
- при обновлении сервера Device Monitor версии 7.10 и выше – значение остается равным тому, что было до обновления.

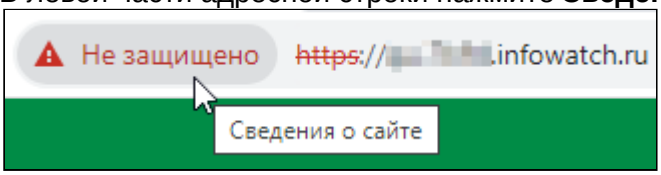
Если значения параметров `IGNORE_SSLERR_TMXAPI_CONNECTION`, `IGNORE_SSLERR_TMCONFIG_CONNECTION` и `IGNORE_SSLERR_PLATFORM_CONNECTION` были изменены, то чтобы правила проверки сертификатов удаленных серверов вступили в силу, перезапустите службу сервера Device Monitor.

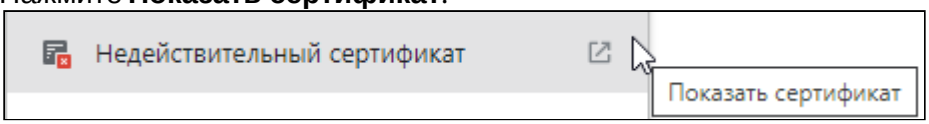
5.4.2 Чтобы установить сертификат службы XAPI Traffic Monitor:

1. На сервере Traffic Monitor откройте файл `/opt/iw/tm5/etc/xapi.conf`.
2. В секции **ThriftServers** -> **xapi** найдите параметр `TrustedCertificatesPath`.
   В значении данного параметра указаны путь к файлу корневого сертификата и его имя. Если указан относительный путь, то его необходимо рассматривать от каталога `/opt/iw/tm5`.
   Значение параметра `TrustedCertificatesPath` по умолчанию: `/opt/iw/tm5/etc/cert/trusted_certificates`.
3. Скопируйте корневой сертификат на компьютер, где установлен или будет установлен сервер Device Monitor.
4. Перейдите в директорию, куда был скопирован корневой сертификат.
5. Переименуйте корневой сертификат в `tmca.crt`.
6. Введите команды в зависимости от операционной системы, в среде которой производится установка корневого сертификата:
   - Для операционной системы РЕД ОС:
     ```
     sudo cp tmca.crt /etc/pki/ca-trust/source/anchors/
     sudo update-ca-trust force-enable
     sudo update-ca-trust extract
     ```
   - Для операционной системы Альт:
     ```
     su -
     cp tmca.crt /etc/pki/ca-trust/source/anchors/
     update-ca-trust
     ```
   - Для операционной системы Astra Linux:
     ```
     sudo cp tmca.crt /usr/local/share/ca-certificates/tmca.crt
     sudo update-ca-certificates
     ```

Выполнение команд может занять некоторое время.

5.4.3 Чтобы установить сертификат веб-сервера Traffic Monitor Traffic Monitor:

1. Откройте Консоль управления Traffic Monitor в браузере.
2. Экспортируйте сертификат веб-сервера Traffic Monitor из браузера, в нашем примере Google Chrome. Для этого:
   a. В левой части адресной строки нажмите **Сведения о сайте** .
   

   b. Нажмите **Показать сертификат**.
   

   c. В Инструменте просмотра сертификатов откройте вкладку *Подробнее*.
   d. Нажмите **Экспорт**.
   e. Нажмите **Сохранить**.
3. Скопируйте корневой сертификат на компьютер, где установлен или будет установлен сервер Device Monitor.
4. Перейдите в директорию, куда был скопирован корневой сертификат.
5. Выполните шаг 6 инструкции по установке сертификата службы XAPI Traffic Monitor, описанной выше, используя вместо `tmca.crt` имя скопированного ранее корневого сертификата веб-сервера Traffic Monitor.

5.4.4 Чтобы установить сертификат службы EPEVENTS Платформы:

1. На сервере Платформы получите корневой сертификат `plca.crt` с помощью команды:
   ```
   kubectl get secret -n infowatch epeventskeys-central -o 'go-template={{index .data "tls.crt"}}' | base64 -d > plca.crt
   ```
   Если сервер Платформы не является центральным в кластере, то команда будет иметь вид:
   ```
   kubectl get secret -n infowatch epeventskeys-<node label> -o 'go-template={{index .data "tls.crt"}}' | base64 -d > plca.crt
   ```
   где `<node label>` – это имя серверной ноды.
2. Скопируйте корневой сертификат на компьютер, где установлен или будет установлен сервер Device Monitor.
3. Перейдите в директорию, куда был скопирован корневой сертификат.
4. Выполните шаг 6 инструкции по установке сертификата службы XAPI Traffic Monitor, описанной выше, используя вместо `tmca.crt` имя скопированного ранее корневого сертификата Платформы.

Выполнение команд может занять некоторое время.

5.4.5 **Просмотр логов**

Если сервер Device Monitor не сможет проверить сертификат, в логах появится ошибка с указанием сертификата и его статуса:

`Can't validate TmXapi certificate. Chain error: Certificate thumbprint: <thumbprint> Subject: CN=XAPI, OU=TD, O=InfoWatch, S=Moscow, C=RU`

> `UntrustedRoot Цепочка сертификатов обработана, но обработка прервана на корневом сертификате, у которого отсутствует отношение доверия с поставщиком доверия.`

`Certificate thumbprint: <thumbprint> Subject: CN=XAPI, OU=TD, O=InfoWatch, L=Moscow, S=Moscow, C=RU`

> `UntrustedRoot Цепочка сертификатов обработана, но обработка прервана на корневом сертификате, у которого отсутствует отношение доверия с поставщиком доверия.`

Интервал между отправкой сообщений об ошибках в лог определяется значениями полей `WRITE_SSLVERIFY_TMXAPI_LOG_INTERVAL`, `WRITE_SSLVERIFY_TMCONFIG_LOG_INTERVAL` и `WRITE_SSLVERIFY_PLATFORM_LOG_INTERVAL` таблицы Settings базы данных сервера Device Monitor. По умолчанию эти значения равны 3600 секунд. Если сертификат удаленного сервера повторно не пройдет проверку и с момента последней отправки сообщения об ошибке прошло меньше указанного времени, то новое сообщение об ошибке отправлено не будет.

Чтобы просмотреть логи:

1. Перейдите в каталог `/opt/iw/dmserver/log` .
2. Откройте файл `iwdms-<date>.txt`, где `<date>` – это дата в формате YYYYMMDD .

5.5 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`.
   a. Если используется система управления контейнерами Kubernetes (K8s), то 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`
   b. Если используется Docker (docker compose), то выполните команду:
   `curl http://<host>:13374/v1/pubkey > /opt/iw/dmserver/bin/guard.pem`
   где `<host>` - адрес компьютера с Платформой.
   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-----
```

Пример:

Если необходимо установить Сервер Device Monitor на тот же сервер, где установлена Платформа, то команда будет иметь следующий вид:

```
curl http://localhost:13374/v1/pubkey > /opt/iw/dmserver/bin/guard.pem
```

В случае, когда Сервер Device Monitor устанавливается "с нуля", файл ключа лучше сохранить по пути, отличному от `/opt/iw/dmserver/bin/guard.pem`. При установке будет запрошен путь к сохраненному ключу, и далее установщик сам скопирует его в необходимое местоположение.

Команда ниже позволит сохранить файл по пути `/tmp/guard.pem`:

```
curl http://localhost:13374/v1/pubkey > /tmp/guard.pem
```

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`

5.6 Установка Агентов Device Monitor

Агент Device Monitor и Сервер Device Monitor необходимо устанавливать в одном часовом поясе. Это обеспечит отображение корректного времени перехвата события.

Важно!

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

Агенты InfoWatch Device Monitor могут быть установлены на рабочие станции одним из следующих способов:

- Локальная установка. Выполняется при помощи универсальной программы установки непосредственно на каждом компьютере.
- Установка с помощью задачи распространения. Выполняется в веб-консоли InfoWatch Device Monitor.

Чтобы успешно установить или обновить Агент InfoWatch Device Monitor, следуйте рекомендациям:

1. Исключите параллельное использование сторонних DLP-систем;
2. Добавьте в исключения антивируса процессы Агента InfoWatch Device Monitor (список файлов см. в статье "Список файлов Агента InfoWatch для добавления в исключения антивирусов");
3. Отключите самозащиту антивируса;
4. По возможности отключите или удалите антивирус на время установки, обновления и удаления Агента InfoWatch Device Monitor;
5. Если на рабочих станциях используется VMWare Horizon VDI 8.0.0-16530, то необходимо отключить компонент ftapihook654.dll версии 3.2.4.1. (подробнее см. "Проблема совместимости с VmWare Horizon VDI")

6. Обеспечьте доступ к портам, необходимым для работы Агента InfoWatch Device Monitor (список портов см. в "*Infowatch Traffic Monitor. Руководство администратора*", раздел "Настройка Сервера InfoWatch Device Monitor");
7. Для быстрого получения FQDN имени рабочей станции под управлением ОС семейства Linux, перед установкой Агента убедитесь, что следующие параметры настроены:
   a. Файл `/etc/hostname` содержит:
      - имя хоста, например, `computer-20`;
        или
      - FQDN имя, например, `computer-20.corp.ad`
   b. В файле `/etc/hosts` определено соответствие между именем хоста, FQDN именем и IP-адресом:
      - если на рабочей станции определено имя хоста и у рабочей станции есть FQDN имя, то файл должен содержать следующую строку:
        `127.0.1.1 <FQDN name> <hostname>`

        где `<FQDN name>` – FQDN имя;
        `<hostname>` – имя хоста.
        Например, для имени хоста `computer-20` и FQDN имени `computer-20.corp.ad` строка будет выглядеть следующим образом:
        `127.0.1.1 computer-20.corp.ad computer-20`
      - если у рабочей станции нет FQDN имени, то файл должен содержать следующую строку:
        `127.0.1.1 <hostname>`
      - если в файле `/etc/hostname` указано FQDN имя, то файл должен содержать следующую строку:
        `127.0.1.1 computer-20.corp.ad`

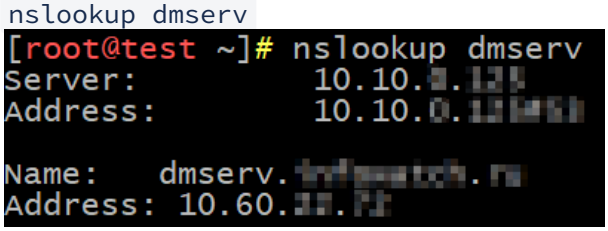
        > **Примечание:**
        >
        > Значение IP-адреса в строке может быть равно 127.0.1.1 или 127.0.0.1.

        > **Примечание:**
        >
        > Перечисленные параметры также могут быть настроены с помощью стороннего ПО, например, программы "Ввод в домен".

        Для исключения ошибок при добавлении хоста в Active Directory к имени хоста предъявляются следующие требования:
        - разрешены символы латинского алфавита (A-Z,a-z), цифры (0-9) и дефис;
        - длина имени должна быть не более 15 символов.
8. Для соединения между сервером InfoWatch Device Monitor и рабочей станцией, на которую устанавливается Агент InfoWatch Device Monitor, необходимо, чтобы их доменные имена корректно преобразовывались (резолвились) DNS-сервером в IP-адреса. Убедитесь в этом с помощью команды:
   `nslookup <имя_хоста>`
   В результате будет выведено сообщение, содержащее адрес DNS-сервера, FQDN имя рабочей станции и ее адрес.

Пример:

`nslookup dmserv`



Если в результате выполнения данной команды для сервера InfoWatch Device Monitor, выведена ошибка `server can't find dmserv: SERVFAIL` , то соединение не будет установлено.

> **Примечание:**
>
> Также для установления соединения Агента InfoWatch Device Monitor с сервером InfoWatch Device Monitor вы можете добавить следующую строку в файл `/etc/hosts` на рабочей станции, на которую устанавливается Агент:
> `<IP_адрес_сервера_Device_Monitor> <имя_сервера_Device_Monitor>`

При возникновении трудностей с настройкой сетевых параметров обратитесь к системному администратору.

9. Если не требуется использовать компонент контроля сетевых соединений, отключите его при создании дистрибутива Агента InfoWatch Device Monitor;
10. Установите Агенты InfoWatch Device Monitor сначала на тестовые машины или небольшую группу рабочих станций;
    Если на тестовой группе в течение 2-3 дней не возникало ошибок, снижения производительности, зависания приложений, продолжайте установку на рабочие станции.

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

> **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».

> **Важно!**
>
> В процессе установки Агента будут закрыты (если они были запущены) программы Mozilla Firefox и Mozilla Thunderbird.

Примечание:

Перед установкой Агента на рабочей станции с ОС Windows 7 Service Pack 1 или Windows Server 2008 R2 следует установить пакеты исправлений Windows для указанных ОС (подробнее см. в статье "Аппаратные и программные требования").

Примечание:

Перед установкой Агента Device Monitor на рабочую станцию под управлением ОС Astra Linux версий 1.6 или 2.12 проверьте наличие установленной библиотеки `libxcb-res0`:

```
dpkg -s libxcb-res0
```

При необходимости установите ее:

```
sudo apt-get install libxcb-res0
```

Примечание:

При установке Агента на ОС Windows 7 и Windows 2008 R2 Server следует учесть, что:

Если Агент устанавливается впервые, компонент Контроль сетевых соединений не будет установлен. При необходимости, данный компонент возможно установить вручную, используя командную строку.

Примечание:

Запуск Агента InfoWatch Device Monitor осуществляется автоматически сразу после установки. До перезагрузки компьютера функционал Агента ограничен только:
- перехватом трафика, проходящего через proxy-сервер,
- сетевым перехватом (при установке Агента на ОС Windows 8 и более поздние,
- перехватом копирования на внешние носители.

Чтобы ограничить доступ к данным Device Monitor, при установке Агента на ОС семейства Linux создаются следующие учетные записи в операционной системе:

- *iwdm* – используется основной службой Device Monitor;
- *iwdeployagent* – используется службой распространения агентов Device Monitor;
- *iwregistry* – в настоящий момент не используется.

При удалении Агента InfoWatch Device Monitor указанные учетные записи будут удалены автоматически.

Важно!

Не допускается самостоятельное удаление или изменение перечисленных выше учетных записей, так как это приведет к неработоспособности Агента InfoWatch Device Monitor.

5.6.1 Локальная установка Агентов

> **Важно!**
>
> Настоятельно не рекомендуется устанавливать Агенты InfoWatch Device Monitor на компьютеры с одинаковыми именами. Такие компьютеры будут зарегистрированы как один компьютер и, соответственно, на них будет распространяться одна политика, будет вестись единая регистрация событий и т.д.

Получите и запишите на внешний носитель актуальный пакет для установки Агента. Установку на компьютере может выполнять пользователь, имеющий на нем права локального администратора.

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью msi-пакета с последующим вводом параметров вручную:

1. **Запуск мастера установки**
   Вставьте внешний носитель с дистрибутивом Агента в компьютер. Затем откройте каталог `Client`. В данном каталоге найдите и запустите пакет установки для требуемой платформы для развёртывания в соответствии с заданными при формировании пакетов параметрами, например, `InfoWatch.DeviceMonitor.Client.7.11.0.x64.msi.`
   В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor Client. Нажмите на кнопку **Далее**, чтобы перейти к следующему окну мастера установки.
2. **Выбор каталога для установки**
   Укажите путь к каталогу, в который будет установлен **Агент**.

   > **Важно!**
   >
   > Путь к каталогу может содержать следующие символы: 0-9,a-z,A-Z, ":", ".", "_", "-", "\", " ". При наличии в пути других символов, установка Агента будет некорректной.

   Нажмите кнопку **Далее**.
3. **Настройка параметров**
   Укажите параметры соединения с Сервером InfoWatch Device Monitor:
   - **Сервер**. Имя сервера InfoWatch Device Monitor.
   - **Порт**. Номер порта, используемого для соединения между Агентом и Сервером InfoWatch Device Monitor (по умолчанию задан порт 15101).

   Нажмите кнопку **Далее**.
4. **Завершение установки**
   После перехода к окну **Подтверждение установки**, нажмите кнопку **Далее,** чтобы начать установку Агента. Следуйте дальнейшим указаниям мастера для завершения установки. По окончании установки перезагрузите компьютер.

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС семейства Linux:

Важно!

Для установки Агента на компьютере под управлением ОС Astra Linux 1.6 **обязательно** установите обновление безопасности ОС Astra Linux Special Edition 1.6 Update 6 (20200722SE16) (см. официальную инструкцию);

Важно!

Для установки Агента на компьютере под управлением ОС Альт Рабочая Станция 10 убедитесь, что выделены права на исполнение su. Для компьютеров под управлением других ОС семейства Linux необходимы привилегии sudoers.

Примечание:

Если на компьютере установлена кастомизированная версия системы SeLinux, корректная установка Агента не гарантируется.

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 текущую версию ядра Astra Linux (например, **4.15.3-2-generic**):
      `uname -r`
      ii. 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.**
      iii. Удалите такие пакеты при наличии:
      `apt-get purge linux-image-4.15.3-1`
      iv. 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 поставляется в составе дистрибутива. 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 7.3.1;
      - `Setup.AltLinux-10.0-iwdm.x64.x.x.x.xx.tar.gz` - для Альт Рабочая станция 10.

      x.x.x.xx - номер сборки.
      Далее мы рассмотрим пример установки и удаления Агента на РЕД ОС 7.3. Установка и удаление на других поддерживаемых ОС аналогичны.

В нашем примере:
`Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`

c. 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`
Пример команды для Агента на Alt Linux:
`tar -xvzf Setup.AltLinux-10.0-iwdm.x64.7.11.0.126.tar.gz`
В результате будут созданы файлы `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<версия_агента>.deb`.

2. **Установка Агента InfoWatch Device Monitor:**
   a. Перейдите в директорию, в которую распаковано содержимое архива **`Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`**.
   b. Для установки Агента 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`
   Пример команды для Агента на Alt Linux:
   `su -c "./install.sh dm-server:15101"`
   Продукт будет установлен в директорию `/opt/iw/dmagent`.
   c. Проверить статус сервисов можно командой:
   `sudo systemctl status iwdm*`
   Пример команды для Агента на Alt Linux:
   `su - -c "systemctl status iwdm*"`

5.6.2 Установка Агентов с помощью задачи распространения

Для установки Агентов Device Monitor на рабочие станции с помощью задачи распространения в веб-консоли Device Monitor необходимо наличие установленного сервиса распространения (подробнее см. "Установка Сервера Device Monitor", Шаг 19).

> **Важно!**
>
> Не допускается установка Агентов InfoWatch Device Monitor через задачу распространения на рабочие станции под управлением ОС Windows.

Для установки Агентов на рабочие станции под управлением ОС Linux 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.
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:

Рекомендуется добавить файлы Агента в исключения антивируса. Список файлов см. в статье "Список файлов Агента InfoWatch для добавления в исключения антивирусов".

Примечание:

Если на компьютере установлена кастомизированная версия системы SeLinux, корректная установка Агента не гарантируется.

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».

6 Настройка сетевых правил доступа

Для корректной работы Системы должны быть разрешены соединения:

<table>
<tr><th rowspan="2">Компонент Системы, для работы которого необходимо соединение</th><th colspan="2">Взаимодействие между компонентами</th><th rowspan="2">Порт</th><th colspan="2" rowspan="2">Назначение порта</th></tr>
<tr><th>Источник</th><th>Получатель</th></tr>
<tr><td rowspan="8">Сервер Device Monitor (DM)</td><td>Платформа</td><td>Сервер DM</td><td>TCP 15007</td><td colspan="2">Взаимодействие Платформы с Сервером DM</td></tr>
<tr><td>Агент DM</td><td>Сервер DM</td><td>TCP 15004</td><td rowspan="4">Защищенное соединение Сервера DM с Агентами</td><td>Передача теневых копий (шифрованный канал)</td></tr>
<tr><td>Агент DM</td><td>Сервер DM</td><td rowspan="2">UDP 15100</td><td rowspan="2">Уведомление Агентов</td></tr>
<tr><td>Сервер DM</td><td>Агент DM</td></tr>
<tr><td>Агент DM</td><td>Сервер DM</td><td>TCP 15101</td><td>Передача теневых копий</td></tr>
<tr><td>Агент DM</td><td>Сервер DM</td><td>TCP 15200</td><td colspan="2">Инициация загрузки дистрибутива Агента с Сервера DM на рабочую станцию</td></tr>
<tr><td>Сервер DM</td><td>Агент DM</td><td>TCP 15505</td><td colspan="2">Установка и удаление Агента</td></tr>
<tr><td>Рабочая станция Офицера безопасности</td><td>Платформа</td><td>TCP 443</td><td colspan="2">Взаимодействие Офицера безопасности с Веб-консолью Сервера DM</td></tr>
<tr><td>Агент DM на ОС семейства Linux</td><td>Сервер DM</td><td>Рабочая станция сотрудника</td><td>TCP 22</td><td colspan="2">Установка Агента</td></tr>
</table>

Примечание:

Если в процессе установки были назначены порты, отличные от указанных в таблице:

- используйте те порты, что были назначены, вместо указанных в таблице;

или

- измените их на порты из таблицы:

    a. Остановите службу Сервера DM с помощью команды:
    `systemctl stop iwdms`
    b. Чтобы изменить порты соединения Сервера DM с Агентами, в таблице `ServerOption` базы данных Сервера DM отредактируйте параметры:
        - `NotificationPort` (UDP 15100);
        - `ClientFacadePort` (TCP 15101);
        - `SSLPort` (TCP 15004).
    c. Включите службу Сервера DM с помощью команды:
    `systemctl start iwdms`

7 Обновление Device Monitor

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

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

7.1 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. Не удаляйте данные БД. Для этого на шаге 5 инструкции (см. "Удаление Сервера Device Monitor") введите **N**.
3. Закройте порты для входящих соединений Сервера Device Monitor, чтобы не получать события от Агента Device Monitor до завершения обновления. По умолчанию это порты:
   - 15004/TCP;
   - 15101/TCP.
4. 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.
   f. Очистите кеш браузера.
5. Установите новую версию Сервера Device Monitor на существующую БД (подробнее см. "Установка Сервера Device Monitor"). При этом:
   a. шаги 9-10 не выполняются, так как PFX-файл ключа шифрования канала между Сервером Device Monitor и агентами сохраняется в БД при удалении старой версии.
   b. на шаге 11 введите **U** и далее укажите параметры для доступа к существующей БД.
   c. на шаге 19 укажите старый путь до файла открытого ключа, потому что при обновлении открытый ключ Платформы не будет изменен.
6. Скопируйте сохраненный на шаге 1 файл ключа в директорию `/opt/iw/dmserver/bin/`.
7. Чтобы Сервер Device Monitor смог распознать настройки и обработать неотправленные события Сервера, установленного ранее, необходимо вручную внести правки в БД. Для этого:

a. Остановите службу Сервера Device Monitor, выполнив команду:
`systemctl stop iwdms`
b. Подключитесь к БД Сервера Device Monitor с помощью любого удобного инструмента.
c. Выполните запрос:
`select * from "Server"`
Результат может выглядеть следующим образом:

```
1  select * from "Server";
```

Data Output | Explain | Messages | Notifications

	Id [PK] integer	Obsolete integer	Address character varying (128)	IsPrimary integer	Uid bytea
1	2	0	qa-95af	1	[binary data]
2	1	1	qa-95af	1	[binary data]

В данном случае обе записи соответствуют старой и новой установкам на одном физическом сервере, т.к. у них совпадают адреса. Флаг `Obsolete=1` означает, что этот экземпляр сервера выведен из эксплуатации или удален.
d. Измените флаг `Obsolete` для обеих записей, последовательно выполнив запросы:
```
update "Server" set "Obsolete"=1 where "Id"=2;
update "Server" set "Obsolete"=0 where "Id"=1;
```
e. Запустите службу Сервера Device Monitor, выполнив команду:
`systemctl start iwdms`
После этого на Сервер Device Monitor будут загружены все настройки, установленные в процессе работы в старой версии, и осуществлена доставка неотправленных событий.

8. Откройте порты для входящих соединений, которые были закрыты на шаге 3.

7.2 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 на рабочей станции под управлением ОС Windows до новой версии:

1. Удалите Агента старой версии (см. "Удаление Агентов Device Monitor");
2. Установите Агента новой версии (см. "Локальная установка Агентов").

Чтобы локально обновить Агенты на рабочей станции под управлением ОС семейства Linux 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*`

При обновлении Агентов Device Monitor до новой версии следует действовать следующим образом:

1. Произвести обновление на группе не более 10 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
2. Произвести обновление на группе не более 50 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
3. Произвести обновление на группе не более 500 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
4. Произвести обновление на группе не более 1000 компьютеров. Удостовериться, что в течение 2-3 дней на компьютерах не возникало ошибок, снижения производительности, зависания приложений.
5. Произвести обновление на оставшихся компьютерах до полного завершения процесса обновления.

Примечание:

При обновлении Агента на ОС Windows 7 и Windows 2008 R2 Server следует учесть, что если компонент **Контроль сетевых соединений** был установлен ранее, то при обновлении Агента он будет удален. При необходимости данный компонент можно установить вручную, используя командную строку.

Важно!

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

После обновления Агента обязательно перезагрузите рабочую станцию, чтобы использовать новый механизм перехвата для приложений, запущенных до обновления.

8 Удаление Device Monitor

В этом разделе:

1. Удаление Сервера Device Monitor
2. Удаление Агентов Device Monitor

8.1 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**. Если ввести **N**, то каталог с теневыми копиями событий будет сохранен, т.к. в нем могут быть еще не отправленные в Traffic Monitor или Activity Monitor события.
8. Дождитесь окончания процесса удаления, который включает в себя:
   - удаление СУБД. Если в п. 5 вы ввели **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.

8.2 Удаление Агентов Device Monitor

Удаление Агентов Device Monitor производится локально на рабочих станциях.

Чтобы удалить Агент InfoWatch Device Monitor на ОС Windows:

1. На рабочей станции, где установлен Агент, перейдите в оснастку **Добавить или удалить программы** (**Add or remove programs**).
2. Выберите **InfoWatch Device Monitor Client** и нажмите **Удалить** (**Remove**).
3. Дождитесь завершения процесса и перезагрузите рабочую станцию.

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

1. Перейдите в директорию, в которую было распаковано содержимое архива с установщиком.
2. Запустите скрипт удаления, выполнив команду:
   `sudo ./remove.sh`
   Пример команды для Агента на Alt Linux:
   `su -c "./remove.sh"`
   Будут удалены и Агент Device Moinitor, и Агент распространения.
3. Перезагрузите рабочую станцию.

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.