

INFOWATCH

InfoWatch Device Monitor for Linux. Руководство по установке

17/09/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 5

2 Комплект документов 6

3 Техническая поддержка пользователей 7

4 Аппаратно-программные требования 8

4.1 Аппаратные требования 8

4.2 Программные требования 9

5 Установка Device Monitor 18

5.1 Состав дистрибутива 18

5.2 Схема развертывания Device Monitor 18

5.3 Подготовка окружения 22

5.3.1 Примеры установки дополнительных пакетов 30

Установка .NET на примере операционной системы Альт 30

Установка .NET на примере операционной системы Astra Linux 30

Установка .NET на примере операционной системы РЕД ОС 31

Установка conntrack, socat на примере операционной системы РЕД ОС 32

5.4 Новая установка 33

5.4.1 Установка в режиме "Все-в-одном" 34

5.4.2 Распределенная установка Device Monitor 39

5.4.3 Установка вспомогательного сервера 44

5.4.4 Подготовка Сервера Device Monitor к миграции с ОС Windows на ОС семейства Linux 46

5.5 Настройка проверки сертификатов удаленных серверов 47

5.5.1 Проверка сертификатов удаленных серверов при установлении SSL-сессии 48

5.5.2 Установка сертификата службы XAPI Traffic Monitor 49

5.5.3 Установка сертификата веб-сервера Traffic Monitor 50

5.5.4 Установка сертификата службы EPEVENTS Платформы 50

5.5.5 Просмотр логов 51

5.6 Установка Агентов Device Monitor 51

5.6.1 Способы установки Агента Device Monitor 52

5.6.2 Подготовка к установке 52

5.6.3 Локальная установка Агента на рабочей станции под управлением ОС Windows 57

Установка Агента Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью MSI-пакета с последующим вводом параметров вручную 57

Установка Агента Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью MSI-пакета в тихом режиме 58

5.6.4 Локальная установка Агента на рабочей станции под управлением ОС семейства Linux 62
Примеры команд для других ОС 65
Установка Агента на рабочую станцию под управлением МОС 66
5.6.5 Локальная установка Агента на рабочей станции под управлением Mac OS 67
5.6.6 Установка Агентов с помощью задачи распространения 68

6 Настройка сетевых правил доступа 70

7 Обновление Device Monitor 75

7.1 Обновление Сервера Device Monitor 75

7.2 Обновление Агентов Device Monitor 83

7.3 Обновление конфигурации на Агентах Device Monitor 85

8 Удаление Device Monitor 89

8.1 Удаление веб-интерфейса и Сервера Device Monitor 89

8.2 Удаление Агентов Device Monitor 90

8.2.1 Локальное удаление Агента на рабочей станции под управлением ОС Windows 91
Удаление Агента с помощью инструмента "Программы и компоненты" 91
Удаление Агента с помощью Microsoft Program Install and Uninstall troubleshooter 91
Удаление Агента с помощью Windows Management Instrumentation (WMI) 91
Удаление Агента с помощью Windows Management Instrumentation (WMI) и утилиты PsExec 92
8.2.2 Локальное удаление Агента на рабочей станции под управлением ОС семейства Linux 93
Удаление с помощью скрипта 93
Удаление средствами ОС 94
8.2.3 Локальное удаление Агента на рабочей станции под управлением Mac OS 94

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.

Кроме основных руководств для пользователей и администраторов Системы предусмотрена База знаний lk.infowatch.ru, которая включает материалы по устранению неисправностей и ответы на вопросы. В случае отсутствия доступа к Базе знаний, просьба обращаться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

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.

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

4 Аппаратно-программные требования

4.1 Аппаратные требования

Требования к аппаратной конфигурации сервера зависят от предполагаемой нагрузки на Систему и параметров сети, в которой происходит развертывание. Примерные минимальные аппаратные требования приведены в следующей таблице. Подробный расчет конфигурации настоятельно рекомендуется проводить с участием специалистов InfoWatch или компании-партнера, у которой вы приобретаете продукт.

Тип	Требования
Сервер Device Monitor	
Дисковая подсистема	Не менее 100 ГБ свободного пространства для установки. Также понадобится свободное пространство для анализа данных, объем зависит от нагрузки на сервер.
Процессор	От 4 ядер (частота – 3.1 ГГц, разрядность – 64 бит, с поддержкой инструкций SSE 4.2)
Оперативная память	От 16 ГБ
Консоль управления Device Monitor	
Дисковая подсистема	Не менее 100 ГБ свободного пространства для установки
Процессор	От 2 ядер (частота – 3.1 ГГц, разрядность – 64 бит, с поддержкой инструкций SSE 4.2)
Оперативная память	От 16 ГБ, дополнительно 1 ГБ на каждую вкладку браузера
Агент Device Monitor для рабочих станций	
Дисковая подсистема	Не менее 1 ГБ свободного пространства для установки. Также понадобится свободное пространство для временного хранения файлов, предназначенных для передачи на анализ.
Процессор	От 2-х ядер
Оперативная память	От 2.5 ГБ *

Примечание:

* При работе агентов с терминальной сессией:

- потребление ОЗУ на терминальном сервере может достигать краткосрочных пиков до 2,5 ГБ (примерно 850 МБ на одну рабочую сессию пользователя). Расчет ресурсов ОЗУ по среднему значению на всех пользователей может снизить потребление ресурсов до 600-700 МБ на одну сессию;
- потребление ОЗУ на рабочей станции пользователя может достигать 1 ГБ. Применение настроек по ограничению одновременного обновления конфигураций агентами может снизить потребление ресурсов до 500-700 МБ.

4.2 Программные требования

Требования к программному обеспечению представлены в таблице:

Программное обеспечение	Дополнительно
Сервер Device Monitor	
Операционная система *(установка сервера на хосте, режим Host)*: • РЕД ОС, версии: 7.3.3 – 7.3.6, 8.0.0 • Astra Linux Special Edition "Смоленск", версии: • 1.7.1.0 – 1.7.9.46 • 1.8.1.0 – 1.8.5.46 • Astra Linux Special Edition "Орел", версии: 1.7.1.0 – 1.7.9.46 • Astra Linux Special Edition "Воронеж", версии: 1.7.1.0 – 1.7.9.46 • Astra Linux Special Edition версии 1.8.5 сертифицированная • Альт, варианты: • СП Сервер 10.1.0 – 10.2.0 • Сервер 10.1.0 – 10.2.0 Вы можете установить сервер Device Monitor *с поддержкой контейнеризации (режим Container)* на любую ОС, где возможно установить `podman`. Установка сервера с поддержкой контейнеризации гарантируется на следующих **ОС**: • РЕД ОС, версии: 7.3.3 – 7.3.6, 8.0.0	• На сервере Traffic Monitor 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 • Если предполагается распространение агентов на рабочие станции под управлением ОС Windows, на сервере должен быть установлен Samba-клиент **Важно!** Для повышения производительности следуйте рекомендациям, представленным в статьях: • "Схема развертывания Device Monitor" • "Подготовка окружения"

Программное обеспечение	Дополнительно
• Astra Linux Special Edition "Смоленск", версии: • 1.7.1.0 – 1.7.9.46 • 1.8.1.0 – 1.8.5.46 • Astra Linux Special Edition "Орел", версии: 1.7.1.0 – 1.7.9.46 • Astra Linux Special Edition "Воронеж", версии: 1.7.1.0 – 1.7.9.46 • Astra Linux Special Edition версии 1.8.5 сертифицированная • Альт, варианты: • Сервер 10.1.0 – 10.2.0 • Рабочая станция 10.1.0 – 10.2.0 • СП Сервер 10.1.0 – 10.2.0 • СП Рабочая станция 10.1.0 – 10.2.0 • Red Hat Enterprise Linux, версии: 7.6 – 7.9, 8.4 – 8.10 • Oracle Linux, версии: 7.6 – 7.9, 8.4 – 8.10 • Мос.ОС Серверная Арбат 15.5 **СУБД** *(оба режима установки)*: PostgreSQL версии 11 и более поздних	
Веб-интерфейс на базе Платформы	
Операционная система: • Astra Linux Special Edition "Смоленск", версии: • 1.7.1.0 – 1.7.9.46 • 1.8.1.0 – 1.8.5.46 • Astra Linux Special Edition "Орел", версии: • 1.7.1.0 – 1.7.9.46 • Astra Linux Special Edition "Воронеж", версии: • 1.7.1.0 – 1.7.9.46 • Astra Linux Special Edition версии 1.8.5 сертифицированная • Red Hat Enterprise Linux, версии: • 7.6 – 7.9 • 8.4 – 8.10 • Oracle Linux, версии: • 7.6 – 7.9 • 8.4 – 8.10 • РЕД ОС, версии:	В браузере должна быть реализована аппаратная поддержка WebGL/WebGL2

<table>
<tr><th>Программное обеспечение</th><th>Дополнительно</th></tr>
<tr><td>

- 7.3.3 – 7.3.6
- 8.0.0
- ОС Альт:
- Сервер 10.1.0 – 10.2.0
- СП Сервер 10.1.0 – 10.2.0
- Рабочая станция 10.1.0 – 10.2.0
- СП Рабочая станция 10.1.0 – 10.2.0
- Мос.ОС Серверная Арбат 15.5

Браузер:

- Google Chrome
- Яндекс.Браузер

</td><td></td></tr>
<tr><th colspan="2">Агент Device Monitor для рабочих станций</th></tr>
<tr><td>

Операционная система:

- Microsoft Windows, версии:
  7 Service Pack 1[1], 8, 8.1, 10, 11
- Microsoft Windows Server, версии:
  2008 R2[1], 2012, 2012 R2, 2016,
  2019, 2022
- Astra Linux Special Edition в
  редакциях "Орел" (x64),
  "Воронеж" (x64) и "Смоленск" (x64),
  версии:
  1.7 (включая кумулятивное
  обновление 1.7.10), 1.8
- РЕД ОС, версии:
  7.3, 8.0
- Альт, варианты:
- Рабочая станция 10
- Рабочая станция 11.1 [2]
- Сервер 10.1 с профилем "Офисный
  сервер"
- СП Сервер 10.1
- МОС 12.0
- macOS Sequoia, версии:
  15 (все сборки)
- macOS Tahoe, версии:
  26 (все сборки)

Примечание:

[1] – Для ОС Microsoft Windows 7 Service Pack 1 и Microsoft Windows Server 2008 R2 требуется установка следующих исправлений от компании Microsoft: KB4474419, KB4490628.

</td><td>

Поддерживаемые версии ядер:

Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" 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
- 5.4.0-186.astra2+ci2 (начиная с версии 7.15.2)
- 5.4.0-218-generic (начиная с версии 7.18.4)
- 5.10.0-1045-generic
- 5.10.0-1045-hardened
- 5.10.142-1-generic
- 5.10.176-1-generic
- 5.10.216-1.astra2+ci2 (начиная с версии 7.15.2)
- 5.10.233-1-generic (начиная с версии 7.17.2)
- 5.10.239-1-generic (начиная с версии 7.18.4)
- 5.10.241-1-generic (начиная с версии 7.19.2)
- 5.10.248-1-generic (начиная с версии 7.19.4)
- 5.15.0-33-generic
- 5.15.0-33-hardened
- 5.15.0-70-generic
- 5.15.0-70-hardened
- 5.15.0-83-generic
- 5.15.0-111-generic (начиная с версии 7.15.1)
- 5.15.0-127-generic (начиная с версии 7.17.4)
- 5.15.0-142-generic (начиная с версии 7.18.4)
- 5.15.0-158-generic (начиная с версии 7.19.2)
- 5.15.0-170-generic (начиная с версии 7.19.4)

</td></tr>
</table>

Программное обеспечение	Дополнительно
Проверка на наличие данных исправлений на компьютере проводится Системой перед установкой и/или обновлением продукта. 2 – Для всех поддерживаемых ОС семейства Linux реализован перехват по протоколу X11 (X.Org). Для ОС Альт Рабочая станция 11.1 доступен также перехват по протоколу Wayland.	• 6.1.50-1-generic#astra2+ci6 (до версии 7.13.5) • 6.1.50-1-generic#astra4+ci68 (начиная с версии 7.13.6) • 6.1.90-1-generic (начиная с версии 7.15.1) • 6.1.124-1-generic (начиная с версии 7.17.2) • 6.1.141-1-generic (начиная с версии 7.18.4) • 6.1.152-1-generic (начиная с версии 7.19.2) • 6.1.161-1-generic (начиная с версии 7.19.4) **Astra Linux Special Edition 1.7.10** • 5.4.0-218-generic (начиная с версии 7.21.1 – 1.7.10.hotfix80) • 5.10.248-1-generic (начиная с версии 7.21.1 – 1.7.10.hotfix80) • 5.15.0-170-generic (начиная с версии 7.21.1 – 1.7.10.hotfix80) • 6.1.161-1-generic (начиная с версии 7.21.1 – 1.7.10.hotfix80) **Astra Linux Special Edition 1.8 в редакциях "Орел", "Воронеж" и "Смоленск"** • 6.1.90-1-generic (начиная с версии 7.17) • 6.1.124-1-generic (начиная с версии 7.17.5) • 6.1.141-1-generic (начиная с версии 7.17.10) • 6.1.152-1-generic (начиная с версии 7.18.8) • 6.1.158-1-generic (начиная с 7.19.5) • 6.1.166-1-generic (начиная с версии 7.20.8) • 6.6.28-1-generic (начиная с версии 7.17) • 6.12.11-1-generic (начиная с версии 7.17.5) • 6.12.34-1-generic (начиная с версии 7.17.10) • 6.12.47-1-generic (начиная с версии 7.18.8) • 6.12.60-1-generic (начиная с 7.19.5) • 6.12.77-1-generic (начиная с версии 7.20.8) **Astra Linux Special Edition 1.8.6** • 6.1.166-1-generic (начиная с версии 7.21.2 – 1.8.6hotfix42) • 6.1.166-1-generic (начиная с версии 7.21.2 – 1.8.6hotfix44) • 6.1.166-1-generic (начиная с версии 7.21.4 – 1.8.6hotfix46) • 6.12.77-1-generic (начиная с версии 7.21.2 – 1.8.6hotfix42) • 6.12.77-1-generic (начиная с версии 7.21.2 – 1.8.6hotfix44) • 6.12.77-1-generic (начиная с версии 7.21.4 – 1.8.6hotfix46) **РЕД ОС 7.3**

Программное обеспечение	Дополнительно
	• 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 • 5.15.161-1 (начиная с версии 7.14.1) • 5.15.178-1 (начиная с версии 7.18.6) • 6.1.20-2 • 6.1.44-1 • 6.1.52-1 • 6.1.85-1 (начиная с версии 7.13.4) • 6.1.94-1 (начиная с версии 7.14.1) • 6.1.110-1 (начиная с версии 7.14.5) • 6.1.128-2 (начиная с версии 7.16.4) • 6.1.143-1 (начиная с версии 7.17.10) • 6.1.148-1 (начиная с версии 7.18.4) • 6.1.158-1 (начиная с версии 7.18.8) • 6.1.162-1 (начиная с версии 7.19.4) • 6.1.170-1 (начиная с версии 7.20.3) • 6.1.173-1 (начиная с версии 7.20.5) • 6.1.175-1 (начиная с версии 7.20.5) • 6.1.180-1 (начиная с версии 7.21.2) **РЕД ОС 8.0** • 6.6.6-1 (начиная с версии 7.17.0) • 6.6.26-1 (начиная с версии 7.17.0) • 6.6.34-1 (начиная с версии 7.17.0) • 6.6.51-1 (начиная с версии 7.17.0) • 6.6.76-1 (начиная с версии 7.17.0) • 6.12.21-1 (начиная с версии 7.17.3) • 6.12.37-1 (начиная с версии 7.17.10) • 6.12.56-1 (начиная с версии 7.18.8) • 6.12.69-1 (начиная с версии 7.19.4) • 6.12.85-1 (начиная с версии 7.20.3) • 6.12.90-1 (начиная с версии 7.20.5) • 6.12.92-1 (начиная с версии 7.20.5) • 6.12.101-1 (начиная с версии 7.21.2) **Альт Рабочая станция 10**

Программное обеспечение	Дополнительно
	• 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 • 5.10.195-std-def-alt1 • 5.10.197-std-def-alt1 • 5.10.198-std-def-alt1 • 5.10.199-std-def-alt2 • 5.10.200-std-def-alt1 • 5.10.203-std-def-alt1 • 5.10.204-std-def-alt1 • 5.10.205-std-def-alt1 • 5.10.206-std-def-alt1 • 5.10.207-std-def-alt1 (начиная с версии 7.12.1) • 5.10.208-std-def-alt1 (начиная с версии 7.12.1) • 5.10.209-std-def-alt2 (начиная с версии 7.12.2) • 5.10.211-std-def-alt1 • 5.10.212-std-def-alt1 • 5.10.213-std-def-alt1 (начиная с версии 7.13.1) • 5.10.216-std-def-alt1 (начиная с версии 7.13.6) • 5.10.217-std-def-alt1 (начиная с версии 7.13.9) • 5.10.218-std-def-alt1 (начиная с версии 7.13.10) • 5.10.219-std-def-alt1 (начиная с версии 7.14.1) • 5.10.220-std-def-alt2 (начиная с версии 7.14.1) • 5.10.221-std-def-alt1 (начиная с версии 7.14.2) • 5.10.227-std-def-alt1 (начиная с версии 7.15.1) • 5.10.228-std-def-alt1 (начиная с версии 7.15.2) • 5.10.231-std-def-alt1 (начиная с версии 7.16.1) • 5.10.233-std-def-alt1 (начиная с версии 7.16.2) • 5.10.234-std-def-alt1 (начиная с версии 7.16.3) • 5.10.235-std-def-alt1 (начиная с версии 7.17.1) • 5.10.237-std-def-alt1 (начиная с версии 7.17.4) • 5.10.238-std-def-alt1 (начиная с версии 7.17.7) • 5.10.240-std-def-alt1 (начиная с версии 7.17.10)

Программное обеспечение	Дополнительно
	• 5.10.241-std-def-alt1 (начиная с версии 7.18.3) • 5.10.242-std-def-alt1 (начиная с версии 7.18.4) • 5.10.244-std-def-alt1 (начиная с версии 7.18.4) • 5.10.245-std-def-alt1 (начиная с версии 7.19) • 5.10.246-std-def-alt1 (начиная с версии 7.18.8) • 5.10.247-std-def-alt2 (начиная с версии 7.19.3) • 5.10.248-un-def-alt1 (начиная с версии 7.19.4) • 5.10.250-std-def-alt1 (начиная с версии 7.19.4) • 5.10.252-std-def-alt1 (начиная с версии 7.19.5) • 5.10.253-std-def-alt1 (начиная с версии 7.20.3) • 5.10.256-std-def-alt1 (начиная с версии 7.20.4) • 5.10.257-std-def-alt1 (начиная с версии 7.20.6) • 5.10.258-std-def-alt1 (начиная с версии 7.20.7) • 5.10.260-std-def-alt1 (начиная с версии 7.20.8) • 5.10.262-std-def-alt1 (начиная с версии 7.21.2) • 5.10.264-std-def-alt1 (начиная с версии 7.21.2) • 5.10.268-std-def-alt1 (начиная с версии 7.21.4) • 5.15.94-un-def-alt1 • 5.15.109-un-def-alt1 • 6.1.29-un-def-alt1 • 6.1.32-un-def-alt1 • 6.1.42-un-def-alt1 • 6.1.49-un-def-alt1 (начиная с версии 7.13.2) • 6.1.67-un-def-alt0.c10f.1 (начиная с версии 7.12.4) • 6.1.75-un-def-alt1 (начиная с версии 7.12.2) • 6.1.77-un-def-alt1 (начиная с версии 7.12.2) • 6.1.78-un-def-alt1 (начиная с версии 7.12.4) • 6.1.79-un-def-alt1 (начиная с версии 7.12.5) • 6.1.80-un-def-alt1 • 6.1.81-un-def-alt1 • 6.1.82-un-def-alt1 (начиная с версии 7.13.1) • 6.1.83-un-def-alt1 (начиная с версии 7.13.2) • 6.1.84-un-def-alt1 (начиная с версии 7.13.4) • 6.1.85-un-def-alt1 (начиная с версии 7.13.4) • 6.1.90-un-def-alt1 (начиная с версии 7.13.8) • 6.1.94-un-def-alt1 (начиная с версии 7.14.1) • 6.1.96-un-def-alt1 (начиная с версии 7.14.1) • 6.1.99-un-def-alt1 (начиная с версии 7.14.2) • 6.1.112-un-def-alt1 (начиная с версии 7.15.0) • 6.1.113-un-def-alt1 (начиная с версии 7.15.1) • 6.1.115-un-def-alt1 (начиная с версии 7.15.2) • 6.1.119-un-def-alt1 (начиная с версии 7.16) • 6.1.121-un-def-alt1 (начиная с версии 7.16.1) • 6.1.123-un-def-alt1 (начиная с версии 7.16.1) • 6.1.124-un-def-alt1 (начиная с версии 7.16.2) • 6.1.127-un-def-alt1 (начиная с версии 7.16.3) • 6.1.128-un-def-alt1 (начиная с версии 7.16.3)

Программное обеспечение	Дополнительно
	• 6.1.129-un-def-alt1 (начиная с версии 7.16.4) • 6.1.130-un-def-alt1 (начиная с версии 7.17.1) • 6.1.131-un-def-alt1 (начиная с версии 7.17.1) • 6.1.132-un-def-alt1 (начиная с версии 7.17.2) • 6.1.140-un-def-alt1 (начиная с версии 7.17.4) • 6.1.141-un-def-alt1 (начиная с версии 7.17.7) • 6.1.144-un-def-alt1 (начиная с версии 7.17.10) • 6.1.146-un-def-alt1 (начиная с версии 7.17.10) • 6.1.147-un-def-alt1 (начиная с версии 7.18.1) • 6.1.148-un-def-alt1 (начиная с версии 7.18.3) • 6.1.151-un-def-alt1 (начиная с версии 7.18.4) • 6.1.153-un-def-alt1 (начиная с версии 7.18.4) • 6.1.157-un-def-alt1 (начиная с версии 7.18.6) • 6.1.158-un-def-alt1 (начиная с версии 7.18.8) • 6.1.159-un-def-alt1 (начиная с версии 7.19.2) • 6.1.159-un-def-alt1 (начиная с версии 7.19.2) • 6.1.160-un-def-alt1 (начиная с версии 7.19.4) • 6.1.161-un-def-alt1 (начиная с версии 7.19.4) • 6.1.163-un-def-alt1 (начиная с версии 7.19.4) • 6.1.166-un-def-alt1 (начиная с версии 7.19.5) • 6.1.167-un-def-alt1 (начиная с версии 7.19.7) • 6.1.168-un-def-alt1 (начиная с версии 7.19.7) • 6.1.169-un-def-alt1 (начиная с версии 7.20.3) • 6.1.173-un-def-alt1 (начиная с версии 7.20.4) • 6.1.174-un-def-alt1 (начиная с версии 7.20.6) • 6.1.175-un-def-alt1 (начиная с версии 7.20.7) • 6.1.177-un-def-alt1 (начиная с версии 7.20.8) • 6.1.180-un-def-alt1 (начиная с версии 7.21.2) • 6.1.182-un-def-alt1 (начиная с версии 7.21.2) • 6.1.186-un-def-alt1 (начиная с версии 7.21.4) **Альт Рабочая станция 11.1** • 6.12.41-6.12-alt1 • 6.12.59-6.12-alt1 • 6.12.74-6.12-alt1 • 6.12.85-6.12-alt1 (начиная с версии 7.20.3) • 6.12.94-6.12-alt1 (начиная с версии 7.20.7) • 6.12.96-6.12-alt1(начиная с версии 7.21.1) • 6.12.98-6.12-alt1 (начиная с версии 7.21.2) • 6.12.103-6.12-alt1 (начиная с версии 7.21.4) • 6.18.34-6.18-alt1 (начиная с версии 7.20.7) **МОС 12.0** • 5.4.150-generic-1rosa2021.1 (начиная с версии 7.21.0) • 5.10.244-generic-1rosa2021.1 (начиная с версии 7.21.0)

Программное обеспечение	Дополнительно
	• 5.10.260-generic-1rosa2021.1 (начиная с версии 7.21.1) • 5.15.193-generic-2rosa2021.1 (начиная с версии 7.21.0) • 5.15.211-generic-1rosa2021.1 (начиная с версии 7.21.1) • 5.16.19-generic-2rosa2021.1 (начиная с версии 7.21.0) • 5.17.11-generic-2rosa2021.1 (начиная с версии 7.21.0) • 6.1.152-generic-2rosa2021.1 (начиная с версии 7.21.0) • 6.6.126-generic-1rosa2021.1 (начиная с версии 7.21.0) • 6.6.144-generic-1rosa2021.1 (начиная с версии 7.21.1) • 6.12.47-generic-5rosa2021.1 (начиная с версии 7.21.0) • 6.12.74-generic-2rosa2021.1 (начиная с версии 7.21.0) • 6.12.91-generic-6rosa2021.1 (начиная с версии 7.21.0) • 6.12.91-generic-10rosa2021.1 (начиная с версии 7.21.1) • 6.12.91-generic-19rosa2021.1 (начиная с версии 7.21.1) • 6.12.91-generic-20rosa2021.1 (начиная с версии 7.21.1)

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 с Центром расследований.
3. Установка Сервера Device Monitor.
4. Настройка проверки сертификатов удаленных серверов.
5. Получение открытого ключа Платформы.
6. Установка Агентов Device Monitor.

5.1 Состав дистрибутива

Дистрибутив Device Monitor представляет собой архив `dmsl_setup_X.X.X.xxx.tar.gz`, где `X.X.X` – номер версии, `xxx` – номер сборки. В состав дистрибутива входят следующие компоненты:

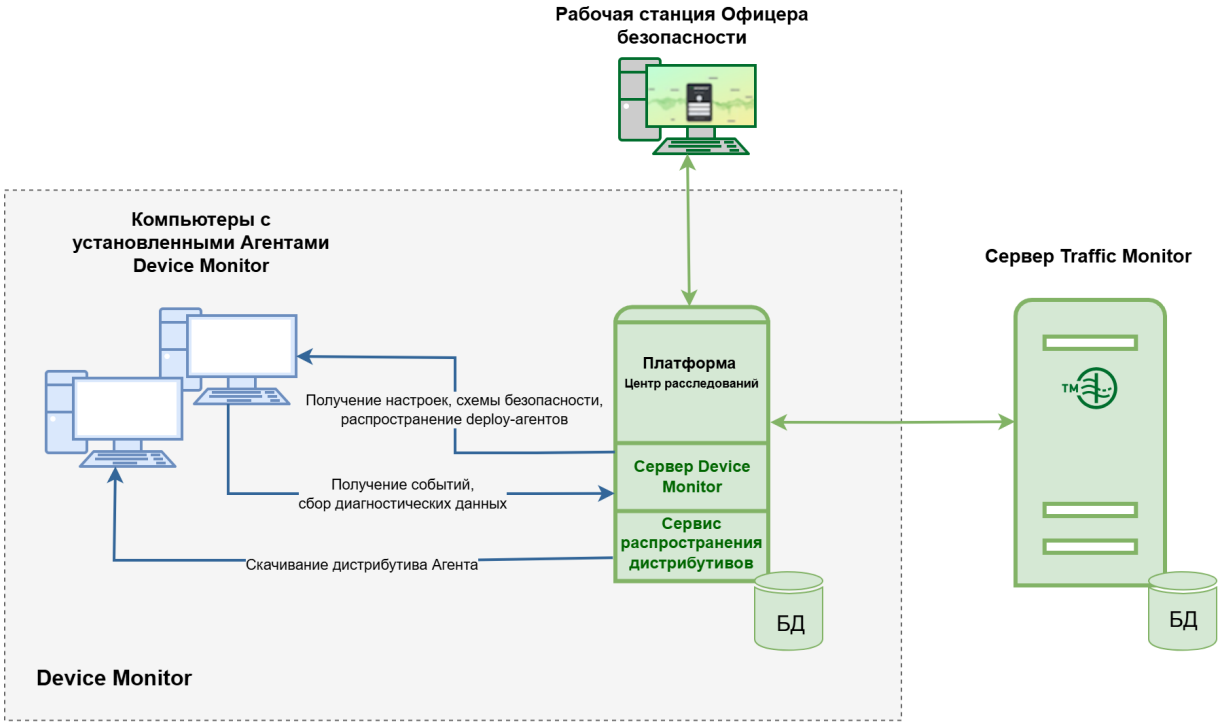
- `data/iwdms` – содержит архив с исполняемыми файлами Сервера Device Monitor и скрипт для его установки с поддержкой установки через параметры командной строки.
- `data/scripts/include` – содержит вспомогательные скрипты, необходимые для корректной работы `setup.sh` и `install_iwdms.sh`;
- `data/ui` – дистрибутив Платформы с веб-интерфейсом Центра расследований.
- `setup.sh` – скрипт, запускающий установщик Сервера Device Monitor в терминале Linux.

5.2 Схема развертывания Device Monitor

Компоненты, входящие в состав InfoWatch Device Monitor, перечислены в таблице:

Компонент	Назначение
Агент InfoWatch Device Monitor (Агент)	Сбор данных и контроль операций на рабочих станциях
Сервер InfoWatch Device Monitor (Сервер)	Распространение схемы безопасности на рабочие станции с Агентами, получение данных от Агентов и передача этих данных системе InfoWatch Traffic Monitor, распространение deploy-агентов на рабочие станции
InfoWatch Device Monitor Database (База данных)	Хранение событий и информации, необходимой для работы Device Monitor
Веб-интерфейс на базе Платформы	Управление модулями Device Monitor и Device Control
Сервис распространения дистрибутивов (Сервис распространения)	Хранение новой версии дистрибутива и доставка дистрибутива Агента Device Monitor на рабочие станции

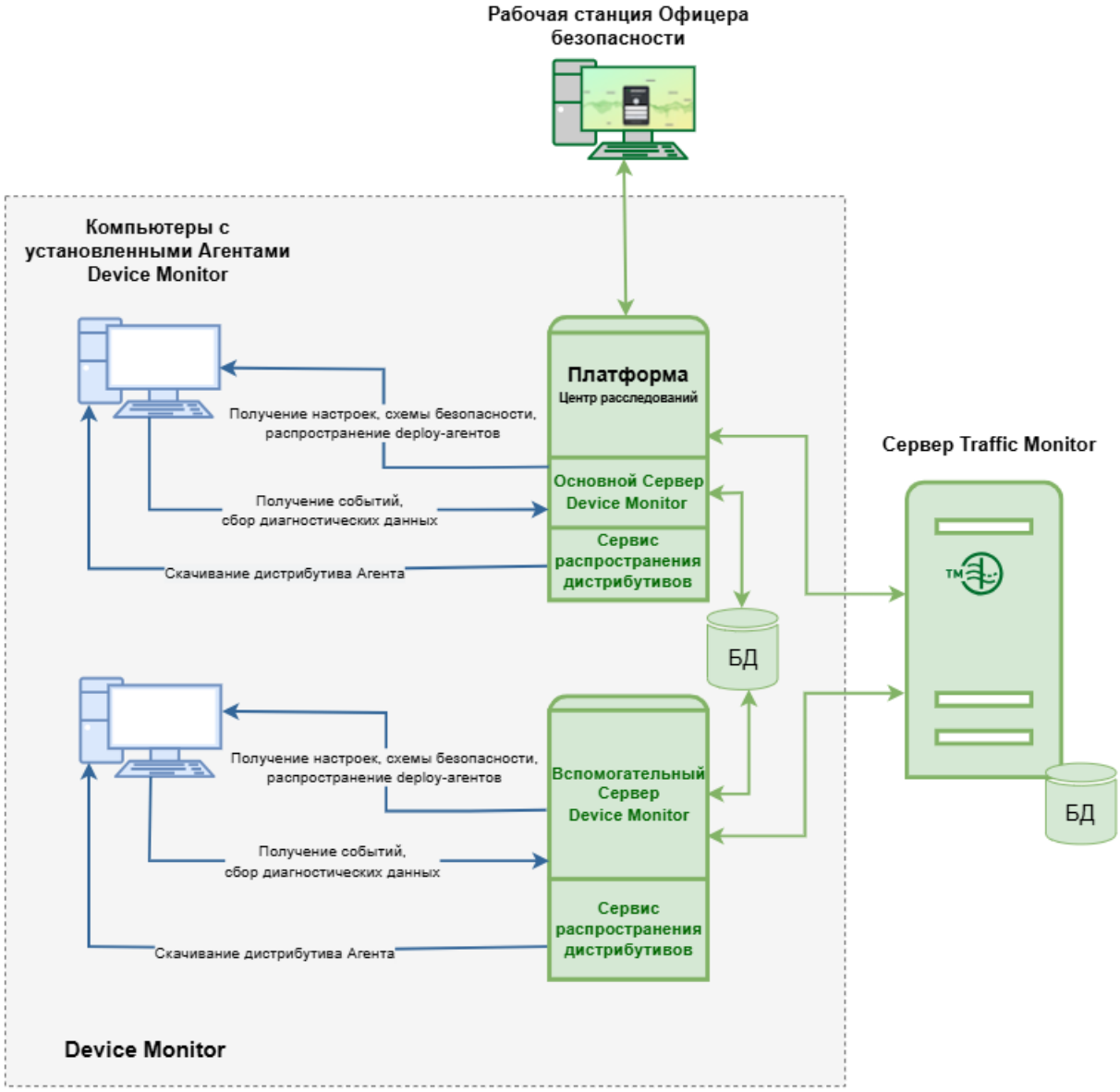
Офицер безопасности подключается со своей рабочей станции к веб-интерфейсу Центра расследований, где может настраивать схему безопасности и управлять модулями Device Monitor и Device Control. Взаимодействие компонентов Device Monitor показано на рисунке:



Для повышения производительности Device Monitor следуйте рекомендациям:

- Используйте несколько серверов Device Monitor. При этом:
  - одна схема Базы данных будет использоваться несколькими серверами для хранения и распространения общей схемы безопасности
  - Агент проверяет доступность всех серверов в пуле по сети, и подключается к одному из доступных
- Сервер и База данных могут находиться на одном компьютере. Однако для увеличения производительности рекомендуется размещать Базу данных и Сервер на разных компьютерах.

Схема с несколькими Серверами Device Monitor:



Порядок установки Системы:

1. Определите масштабы системы в инфраструктуре компании и с помощью специалистов компании InfoWatch согласуйте требования к системе в соответствии с масштабами.
2. Определите место и установите **Базу данных.** Она может быть расположена как отдельно, так и на одном компьютере с Сервером Device Monitor.
3. Основой для установки Device Monitor является Платформа. Инсталлятор содержит и Платформу, и компоненты продукта. Обе части являются обязательными для установки. Сначала установите центральную ноду **Платформы.** Она содержит веб-интерфейс **Центра расследований** для работы с продуктами и **Центра администрирования** для настройки Сервера Device Monitor. Здесь вы можете настраивать схему безопасности в соответствии с требованиями корпоративной политики безопасности**,** управлять Агентами**.**

4. Установите **основной сервер Device Monitor** на **Платформу**. При этом также:

- Укажите место расположения **Базы данных**
- установите **Сервис распространения дистрибутивов.** Сервис имеет хранилище с дистрибутивами Агентов для поддерживаемых ОС.
  Далее вы можете настраивать схему безопасности в соответствии с требованиями корпоративной политики безопасности, управлять Агентами.
- Если предполагается использовать более 500 Агентов на рабочих станциях, установите **вспомогательные серверы Device Monitor**.
- Установите Агенты на рабочие станции. Это можно сделать как локально на самой контролируемой рабочей станции, так и удаленно с помощью задачи распространения в веб-интерфейсе Центра расследований. Во втором случае **основной сервер** распространит deploy-агенты Device Monitor на **рабочие станции**, которые затем скачают дистрибутивы Агентов с ближайшего **сервиса распространения** из указанных точек публикации дистрибутивов. Скачивание дистрибутивов проходит несколькими рабочими станциями одновременно.

Порядок работы Системы:

1. После установки Агенты выполняют подключение к серверу Device Monitor по каналу с шифрованием трафика на основании общего для Агента и Сервера ключа шифрования.
2. Агенты получают настройки и схему безопасности.
3. Агенты собирают информацию о событиях, подпадающих под действие правил и политик схемы безопасности, теневые копии файлов и передают на сервер Device Monitor.
4. Сервер получает события и теневые копии и отправляет в Traffic Monitor или Activity Monitor.

Пример 1

Сотрудник, работающий на контролируемой рабочей станции, начинает переписку в мессенджере VK с внешним собеседником. При этом в Device Monitor настроено правило, позволяющее контролировать обмен сообщениями чата и любыми типами исходящих файлов в веб-версии VK. Обмен сообщениями отслеживается, теневые копии переданных файлов, если размер файла попадает в указанный диапазон, отправляются в Traffic Monitor для анализа.

Пример 2

В Device Monitor задано правило, отслеживающее печать текстовых файлов. В правиле указано, что при выполнении подобной операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к отправке документа на печать.
2. Если задание на печать сформировано успешно, то Агент Device Monitor генерирует событие и создает теневую копию документа, отправленного на печать.
3. В случае если создать теневую копию документа невозможно (например, при отсутствии свободного места на жестком диске), операция печати будет произведена без создания теневой копии, о чем будет указано в информации о событии.
4. Агент передает данные (событие и теневую копию документа) на Сервер Device Monitor. Если соединение с Сервером отсутствует, то данные сохраняются на контролируемом компьютере. После восстановления связи данные будут доставлены на Сервер.
5. Сервер отправляет данные в систему InfoWatch Traffic Monitor для анализа. Если соединение с сервером InfoWatch Traffic Monitor отсутствует, то данные сохраняются в

базе данных. После восстановления связи данные будут доставлены в систему InfoWatch Traffic Monitor.

5.3 Подготовка окружения

Для функционирования Сервера Device Monitor необходимо подготовить окружение:

1. Введите в домен компьютер, на который будет установлен Сервер Device Monitor.
2. Удостоверьтесь, что для сервера задано FQDN-имя хоста. Для этого выполните команду:

   ```
   echo $HOSTNAME
   ```

   В результате должно быть выведено полное имя, например, `dmserv.company.ru`.
   Если выведено короткое имя, например, dmserv, то:

   a. Задайте полное имя хоста:
      - На компьютере под управлением ОС Astra Linux, Альт или Мос.ОС используйте команду:

        ```
        hostnamectl set-hostname <FQDN>
        ```

      - На компьютере под управлением РЕД ОС:
        i. Запустите утилиту `nmtui`:

           ```
           nmtui
           ```

        ii. В текстовом интерфейсе выберите `Set system hostname`.
        iii. В окне `Set Hostname` введите новое имя хоста и нажмите `OK`.
        iv. В окне `Set hostname to '<новое_имя>'` нажмите `OK`.
        v. Нажмите `Quit`.

   b. Перезагрузите сервер.
   c. Повторно выполните команду:

      ```
      echo $HOSTNAME
      ```

3. Установите Microsoft .NET 8 (https://dotnet.microsoft.com/) на этом компьютере. Примеры установки см. ниже.

   > **Примечание:**
   >
   > Если вы планируете устанавливать Сервер Device Monitor с поддержкой контейнеризации (подробнее см. "Установка "Все-в-одном""), то установка .NET 8 не требуется.

4. Дополните настройки подсистемы Inotify. Для этого:
   a. Откройте на редактирование конфигурационный файл `/etc/sysctl.conf`.
   b. Добавьте в конце файла строки:

```
fs.inotify.max_user_instances = 16384
fs.inotify.max_user_watches = 32768
fs.inotify.max_queued_events = 262144
```

Вы также можете задать максимальное количество открываемых файлов. Для этого укажите значение параметра `file-max`, например:

```
fs.file-max = 500000
```

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

```
sysctl -p
```

5. Если установка проводится на сервере под управлением Мос.ОС, убедитесь, что доступны официальные репозитории ОС: `software`, `update`, `oss-suse`.
6. Установите пакеты `conntrack` (или `conntrack-tools`) и `socat`. Пример установки пакетов см. ниже.
7. Если вы будете использовать опцию установки сервера с поддержкой контейнеризации, установите пакет `podman`.
Примеры для установки пакета podman на ОС Альт, ОС Astra Linux, РЕД ОС и Мос.ОС:

- **ОС Альт**:

```
apt-get install podman
```

- **ОС Astra Linux**:

```
apt install podman
```

- **РЕД ОС**:

```
sudo dnf install podman
```

Если пакет недоступен в репозитории, скачайте его на официальном сайте РЕД ОС. Перейдите в директорию с пакетом и установите его вручную с помощью команды вида:

```
rpm -Uhv ./<имя_пакета>
```

> **Важно!**
>
> Минимальная версия `podman` для РЕД ОС 4.9.
> Если устанавливаете пакет `podman` на РЕД ОС вручную, то установите также зависимые пакеты, необходимые для его работы.

- **Мос.ОС**:

```
zypper install podman
```

8. Настройте антивирус для совместной работы с Системой (см. статью Базы знаний "Настройка антивируса для Device Monitor Server на ОС Linux").
9. Настройте правила POD сети или отключите межсетевой экран (см. статьи Базы знаний "Конфликты при взаимодействии firewalld и Kubernetes", "Полное отключение межсетевого экрана").
10. Установите интерпретатор языка Python версии 3. Пакет с интерпретатором не входит в состав дистрибутива продукта.
11. **Если установка проводится на сервере под управлением RedOS, Мос.ОС, ОС Astra Linux:**

    Установите следующие пакеты:

    - **РЕД ОС**:

```
dnf install python3-pyyaml
dnf install python3-importlib-metadata
```

    - **ОС Astra Linux**:

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

    - **Мос.ОС**:

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

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

12. **Если установка проводится на сервере под управлением ОС Альт:**

    - Установите утилиту `unzip` аналогично установке `conntrack` и `socat`;
    - Установите следующие пакеты:

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

Примечание:

Пакеты могут отсутствовать в составе дистрибутива продукта и в репозиториях. В этом случае загрузите и установите требуемые пакеты вручную.

- Настройте соответствие алгоритмов шифрования Сервера Device Monitor и Сервера Traffic Monitor. Для этого измените файл `/etc/openssl/openssl.cnf` следующим образом:
  - Найдите в файле строки:

```
# Extra OBJECT IDENTIFIER info:
#oid_file       = $ENV::HOME/.oid
oid_section     = new_oids
```

  - После них добавьте строки:

```
# System default
openssl_conf = default_conf
```

  - 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
```

13. **Если установка проводится с использованием опции Host на сервере под управлением ОС Astra Linux 1.8:**

- Настройте соответствие алгоритмов шифрования Сервера Device Monitor и Сервера Traffic Monitor. Для этого измените файл `/etc/ssl/openssl.cnf` следующим образом:
  - Найдите в файле строки:

```
# Extra OBJECT IDENTIFIER info:
#oid_file       = $ENV::HOME/.oid
oid_section     = new_oids
```

  - После них добавьте строки:

```
# System default
openssl_conf = default_conf
```

- 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
```

14. **Если установка проводится с использованием опции Host на сервере под управлением РЕД ОС 8:**

    Установите пакет `openldap-compat`:

    ```
    dnf install openldap-compat
    ```

    Если вы установили пакет после установки сервера Device Monitor, перезапустите службу `webapi`:

    ```
    systemctl restart iwdms_webapi
    ```

15. **Если установка проводится на сервере под управлением Мос.ОС:**

    Установите пакеты `ethtool`, `app_armor`, `fuse-overlayfs` и `sysctl` с зависимостями:

    ```
    zypper install ethtool
    zypper install patterns-base-apparmor
    zypper install procps
    zypper install fuse-overlayfs
    ```

16. **Если планируется распространение Агентов на рабочие станции под управлением ОС Windows:**

    Установите Samba-клиент на сервер:

    - **РЕД ОС**:

      ```
      dnf install samba samba-client samba-common-tools
      ```

    - **ОС Astra Linux**:

      ```
      apt install samba samba-common smbclient
      ```

      В случае сервера под управлением ОС Astra Linux 1.7 и установки Samba-клиента из локального репозитория необходимо, чтобы пакеты `smbclient` и `samba-common` были версии 4.19.6 или более поздней.

- **ОС Альт**:

```
apt-get install samba samba-client smbclient
```

> **Примечание:**
>
> Если вы планируете устанавливать Сервер Device Monitor с поддержкой контейнеризации (подробнее см. "Установка "Все-в-одном""), то установка Samba-клиента на сервере не требуется.

17. Установите СУБД PostgreSQL.
Рекомендуется устанавливать СУБД на другом компьютере. Если необходимо получать события от небольшого количества Агентов, вы можете установить СУБД PostgreSQL совместно с Сервером Device Monitor.
Пример установки PostgreSQL 15 на РЕД ОС

    a. Обновите установленные в системе пакеты:

```
sudo dnf update
```

    b. Установите и инициализируйте СУБД, выполнив команды:

```
sudo dnf install postgresql
sudo dnf install postgresql15-server
sudo postgresql-15-setup initdb
sudo systemctl enable postgresql-15.service --now
```

    c. Убедитесь, что служба PostgreSQL запущена и имеет статус `active`:

```
sudo systemctl status postgresql-15.service
```

    Также информацию по установке PostgreSQL на РЕД ОС вы можете получить из официальной документации РЕД ОС.

> **Примечание:**
>
> Для обеспечения корректной и бесперебойной работы Сервера необходимо хранение файлов СУБД и теневых копий событий на разных физических дисках.
>
> Для работы с СУБД необходима роль с правами на создание базы данных.

18. Дополнительно настройте базу данных.

> **Важно!**

Названия файлов **`postgresql.conf`** и **`pg_hba.conf`** одинаковы для всех ОС, но пути к ним различаются. В статье в качестве примера приведены пути, используемые на РЕД ОС.

a. Откройте на редактирование файл `/var/lib/pgsql/15/data/postgresql.conf`.
b. Включите возможность экранирования специальных символов при вставке строк в таблицы БД. Для этого присвойте параметру `"standard_conforming_strings"` значение `on`.
c. Задайте параметры, оптимизирующие быстродействие. Для более точного подбора параметров используйте калькулятор PGTune.
    i. Присвойте параметру `"max_connections"` значение 250.
    ii. Настройте ротацию логов.
    iii. Укажите прочие параметры (потребление ресурсов памяти, настройки WAL, планирование запросов) согласно официальной документации PostgreSQL.
d. Если вы будете использовать опцию установки сервера с поддержкой контейнеризации и размещать базу данных на один сервер с Device Monitor: Найдите в файле строку:

```
# listen_addresses = 'localhost'
```

и замените ее на следующую:

```
listen_addresses = '*'
```

e. Откройте на редактирование файл `/var/lib/pgsql/15/data/pg_hba.conf`.
f. Если вы будете использовать опцию установки сервера с поддержкой контейнеризации и размещать базу данных на один сервер с Device Monitor, в качестве первой строки добавьте параметр:

```
host all all 0.0.0.0/0 md5
```

g. Если вы устанавливаете СУБД на отдельном от Device Monitor сервере, настройте доступ к СУБД в файле `pg_hba.conf` согласно официальной документации PostgreSQL.
h. Перезапустите службу PostgreSQL.
Пример команды для РЕД ОС:

```
sudo systemctl restart postgresql-15.service
```

i. Если вы планируете далее установить Систему с поддержкой контейнеризации и использовать ОС Oracle Linux, то после установки СУБД рекомендуется установить языковой пакет:

```
sudo dnf install langpacks-ru -y
```

19. Задайте пароль для пользователя `postgres`. Для этого:
    a. Авторизуйтесь от имени пользователя `postgres`:

```
su - postgres
```

b. Запустите программу `psql`:

```
psql
```

c. Введите команду задания пароля:

```
\password postgres
```

d. Дважды введите новый пароль.
e. Выйдите из программы `psql` и смените пользователя `postgres`:

```
\q
exit
```

20. Для успешного соединения Сервера Device Monitor с Сервером Traffic Monitor настройте проверку сертификата удаленного сервера (подробнее см. "Настройка проверки сертификатов удаленных серверов"). Также вы можете сделать это после установки.
21. **Если вы планируете использовать протокол Kerberos для получения информации о сотрудниках и компьютерах из MS Active Directory:**

- В случае установки Device Monitor с использованием опции *Host*:
  a. Убедитесь, что время Сервера Device Monitor совпадает с временем контроллером домена. Максимальное допустимое отклонение – 5 минут. Если необходимо, установите и настройте `chrony` или `ntpd`.
  b. Убедитесь, что в файле `/etc/resolv.conf`:
     - домен поиска указан корректно;
     - в качестве серверов DNS указаны DNS-серверы Active Directory.
  c. Установите пакеты `krb5-workstation`, `krb5-libs`, `cyrus-sasl-gssapi`. Вы также можете установить пакет `openldap-clients` для диагностики в случае ошибок подключения.
  d. Настройте конфигурационный файл протокола Kerberos `/etc/krb5.conf`. Соблюдайте регистр при указании адресов Realm.
- В случае установки Device Monitor с использованием опции *Container*:
  a. Установите пакет `openldap-clients` для диагностики в случае ошибок подключения.
  b. Настройте конфигурационный файл протокола Kerberos `/opt/iw/dmserver/etc/krb5.conf`. Соблюдайте регистр при указании адресов Realm.
     - Параметр `default_ccache_name` заполните следующим образом:

```
default_ccache_name = FILE:/tmp/krb5cc_%{uid}
```

> **Примечание:**
>
> Шаги могут быть выполнены также после установки Сервера Device Monitor.

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

5.3.1 Примеры установки дополнительных пакетов

Установка .NET на примере операционной системы Альт

1. Убедитесь, что репозитории Альт доступны, выполнив команду:

```
apt-repo list
```

2. Если репозитории недоступны (закомментированы), необходимо отредактировать файл `/etc/apt/sources.list`, раскомментировав в нем строки с адресами репозиториев.
3. Отредактируйте файл `/etc/apt/apt.conf`:
   a. Раскомментируйте все строки
   b. Укажите корректные имя пользователя и пароль доменной учетной записи.
4. Установите среду выполнения .NET 8 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:

```
apt-get install dotnet-aspnetcore-runtime-8.0
```

   В результате будет установлена среда выполнения .NET 8 с поддержкой ASP.NET Core.
5. Проверьте установленный .NET 8, выполнив команду:

```
dotnet --info
```

```
[root@altserver ~]# dotnet --info

Host:
  Version:      8.0.11
  Architecture: x64
  Commit:       8.0.11-alt
  RID:          linux-x64

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 8.0.11 [/usr/lib64/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 8.0.11 [/usr/lib64/dotnet/shared/Microsoft.NETCore.App]
```

Установка .NET на примере операционной системы Astra Linux

1. Убедитесь, что репозитории Astra Linux доступны, выполнив команду:

```
apt-get update
```

2. Если репозитории недоступны (закомментированы), необходимо отредактировать файл `/etc/apt/sources.list`, раскомментировав в нем строки с адресами репозиториев.

3. Отредактируйте файл `/etc/apt/apt.conf`:
    a. Раскомментируйте все строки.
    b. Укажите корректные имя пользователя и пароль доменной учетной записи.
4. Установите среду выполнения .NET 8 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:

```
apt install aspnetcore-runtime-8.0
```

В результате будет установлена среда выполнения .NET 8 с поддержкой ASP.NET Core.

> **Примечание:**
>
> Пакеты, необходимые для установки .NET 8, могут отсутствовать в репозиториях. В этом случае загрузите и установите требуемые пакеты вручную.
>
> Подробнее об установке .NET в ОС Astra Linux см. на официальном сайте "Astra Linux: Установка MS .Net Core и MS Visual Studio Code" и ".Net"

5. Проверьте установленный .NET 8, выполнив команду:

```
dotnet --info
```

```
root@astra-smolensk-1-8:~# dotnet --info

Host:
  Version:      8.0.0
  Architecture: x64
  Commit:       5535e31a71
  RID:          debian.12-x64

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 8.0.0 [/usr/share/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 8.0.0 [/usr/share/dotnet/shared/Microsoft.NETCore.App]
```

Установка .NET на примере операционной системы РЕД ОС

1. Убедитесь, что репозитории РЕД ОС доступны, выполнив команду:

```
dnf repoinfo
```

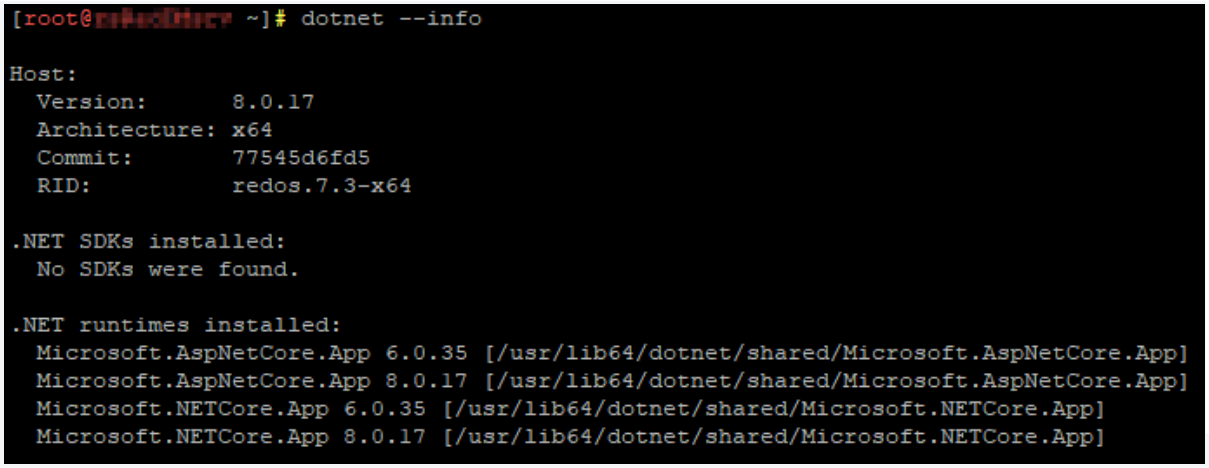
2. Установите среду выполнения .NET 8 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:

```
sudo dnf install aspnetcore-runtime-8.0
```

В некоторых дистрибутивах Linux имя пакета может быть `dotnet-aspnetcore-runtime-8.0`
В результате будет установлена среда выполнения .NET 8 с поддержкой ASP.NET Core.

3. Проверьте установленный .NET 8, выполнив команду:

```
dotnet --info
```



Если в процессе установки .NET возникли ошибки:

- Удалите из операционной системы все пакеты, связанные с .NET. Выполните команду:

```
sudo dnf remove 'dotnet*' 'aspnet*' 'netstandard*'
```

- Установите заново конкретную версию .NET, например:

```
sudo dnf install aspnetcore-runtime-8.0-8.0.17-1.el7
```

- Чтобы посмотреть список доступных версий, выполните:

```
dnf --showduplicates list aspnetcore-runtime-8.0
```

Установка `conntrack`, `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 dnf 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`.

5.4 Новая установка

Возможные режимы установки Device Monitor:

- Установка "**Все-в-одном**" предполагает размещение Сервера Device Monitor и Платформы с веб-интерфейсом Центра расследований и Центра администрирования на одном сервере.
- **Распределенная** установка Сервера Device Monitor на офисную ноду Платформы.

> **Важно!**
>
> При распределенной установке примите во внимание следующие ключевые аспекты:
>
> - Продукты в кластере должны быть установлены на одной версии Платформы. Если вы установите в кластер продукт на новой версии Платформы, для корректной работы вам будет необходимо обновить все продукты.
> - В одном кластере можно развернуть только одну центральную ноду Платформы и каждый продукт в режиме `central` только в единственном экземпляре.
> - Если в кластере уже установлен продукт в режиме `central`, еще одна установка этого продукта в режиме `central` в том же кластере будет прервана ошибкой.
> - Device Monitor поддерживает установку только в режиме `central`. При этом он поддерживает установку как на центральную, так и на офисные ноды Платформы.

Продукты в одном кластере имеют:

- доступ ко всей функциональности в в интерфейсе Центра расследований, едином для всех продуктов;
- общие настройки;
- общую ролевую модель;
- общий доступ к данным независимо от того, на каком из них выполнена интеграция с источником, а также доступ к обработанным данным.

> **Важно!**

При переходе с ОС Windows на Device Monitor for Linux вы можете сохранить данные, т.е. продолжить использовать ту же базу данных, которая использовалась с сервером Device Monitor for Windows. Во время миграции автоматически модифицируется структура и содержимое базы данных. Для корректной миграции:

- Убедитесь, что база данных готова к миграции; в противном случае подготовьте ее. Подробнее см. статью "Подготовка Сервера Device Monitor к миграции с ОС Windows на ОС семейства Linux".
- В ходе установки, на шаге настройки взаимодействия с БД, выберите **Update an existing database**.
- После установки убедитесь, что для базы данных установлена русская локаль (`ru_RU.utf8`). Подробнее см. статью Базы знаний "Проверка и изменение локали базы данных PostgreSQL".

5.4.1 Установка в режиме "Все-в-одном"

Режим подходит для установки веб-интерфейса, Сервера Device Monitor и базы данных на одном сервере, а также при переходе на Device Monitor for Linux с ОС Windows.

Чтобы установить Device Monitor в режиме "все-в-одном":

1. Убедитесь, что сервер соответствует аппаратным и программным требованиям ("Аппаратно-программные требования").
2. Выполните шаги по подготовке сервера к установке Device Monitor (см. "Подготовка окружения").
3. Скопируйте архив с дистрибутивом Сервера Device Monitor на жесткий диск.
4. Создайте директорию и распакуйте в нее содержимое архива. В примере архив будет распакован в директорию `/dmsl_distr` :

```
mkdir -p /dmsl_distr && tar xvf dmsl_setup_7.21.0.310.tar.gz -C /dmsl_distr
```

5. Перейдите в созданную директорию.
6. Запустите скрипт **setup.sh**, который входит в состав дистрибутива:

```
./setup.sh
```

> **Примечание:**
>
> В случае ошибки доступа при запуске скрипта, сделайте файл исполняемым, используя команду:
>
> ```
> chmod +x ./setup.sh
> ```
>
> Затем запустите скрипт.

После этого будут доступны действия:

- **Install** – новая установка
- **Update** – обновление установленных компонентов

- **Utilities** – переход в меню утилит
- **Exit** – выход из программы

7. Выберите тип установки **Install**. Будет доступен список компонентов:
   - **DM Server Service, Front End** – установка "все-в-одном", т.е. установка Сервера Device Monitor и компонента Front End

     > **Примечание:**
     >
     > Компонент Front End необходим для работы Центра администрирования и его необходимо устанавливать, даже если на сервере уже установлен какой-либо продукт на базе Платформы.

   - **Front End only** – установка только Платформы и веб-интерфейса
   - **DM Server Service only** – установка только Сервера Device Monitor
8. Чтобы установить "все-в-одном", выберите **DM Server Service, Front End**.
9. Выберите опцию установки сервера Device Monitor:
   - **Host**, чтобы установить сервер на хосте, или
   - **Container (podman)**, чтобы установить сервер с поддержкой контейнеризации.
10. Будут предложены режимы установки Платформы с веб-интерфейсом Центра расследований и Центра администрирования:
    - **Central** – предназначен для установки на основную ноду или в случае отсутствия уже установленного веб-интерфейса.
    - **Office** – предназначен для распределенной установки.
11. Выберите режим **Central**.
12. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
13. Введите **y**, чтобы принять лицензионное соглашение, и нажмите **Enter**.
14. Введите IP-адрес сервера в формате IPv4: `"xxx.xxx.xxx.xxx"` и нажмите **Enter**.
15. Выделите объем оперативной памяти для размещения данных ClickHouse (по умолчанию 80%) и нажмите **Enter**.
16. Укажите путь для размещения данных ClickHouse (по умолчанию: `/opt/chdata`) и нажмите **Enter**.
17. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/opt/pgdata`) и нажмите **Enter**.
18. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
19. Укажите путь для хранения данных (по умолчанию `/opt/dsdata`) и нажмите **Enter**.
20. Укажите путь для временного хранения событий Traffic Monitor перед их загрузкой в Платформу (по умолчанию: `/opt/factsldrtmdata`) и нажмите **Enter**.
21. Укажите порт подключения к веб-интерфейсу (по умолчанию `443`) и нажмите **Enter**.
22. Дождитесь окончания процесса установки Платформы. Далее будет произведена установка Сервера Device Monitor. При этом:
    a. Будут созданы каталоги:
       - `/var/log/iwdms` – каталог логов выполнения сервера Device Monitor
       - `/opt/iw/dmserver/bin` – каталог с файлами сервера Device Monitor
       - `/opt/iw/dmserver/queue` – каталог файловой очереди
       - `/opt/iw/dmserver/log` – символическая ссылка на каталог `/var/log/iwdms`

b. Добавлен пользователь **iwdms** с ключом `--system`, что позволяет запустить под этим пользователем службу, но не дает авторизоваться под этим пользователем в Центра расследований
c. Распакован zip-файл из `data/iwdms` инсталляционного пакета в требуемые каталоги. Для вышеуказанных папок в качестве владельца буден назначен пользователь **iwdms**
d. В каталоге systemd служб `/etc/systemd/system` будет добавлен файл манифеста службы Сервера Device Monitor **iwdms.service**, а также службы синхронизации с Active Directory – **iwdms_ldap.service**

23. Выберите язык устанавливаемого сервера и нажмите **Enter**. Это определит названия предустановленных групп, политик и правил.
24. Ознакомьтесь с лицензионным соглашением и выберите необходимое действие. Для продолжения установки необходимо принять лицензионное соглашение. Выберите **Accept and continue** и нажмите **Enter**
25. Выберите, какой тип сервера необходимо установить: **Primary** (основной) или **Secondary** (второстепенный).
Если вы устанавливаете Систему впервые или переходите с Device Monitor, установленном на ОС Windows, выберите **Primary**.
26. Настройте взаимодействие с базой данных:
    - **Create a new database** – чтобы создать новую базу данных. Используйте этот вариант **для чистой установки**;
    - **Update an existing database** – чтобы настроить существующую базу данных. Используйте этот вариант **для установки с миграцией данных**.
27. Укажите имя или IP-адрес сервера, на котором располагается СУБД PostgreSQL. Если вы устанавливаете Device Monitor с миграцией данных, используйте СУБД PostgreSQL, ранее используемую для установки Сервера Device Monitor на ОС Windows.
Если ранее вы выбрали опцию установки **Container (podman)** и разместили базу данных на одном сервере с Device Monitor, то введите адрес сетевого интерфейса этого сервера. Предварительно настройте базу данных (подробнее см. "Подготовка окружения").

    > **Важно!**
    >
    > При выбранной опции установки **Container (podman)** нельзя вводить в качестве IP-адреса `localhost` и `127.0.0.1`.

28. Укажите порт для настройки взаимодействия. Если порт не указан, будет использован порт по умолчанию – `5432`.
29. Введите имя базы данных. По умолчанию – `iwdm`.
30. Введите имя пользователя СУБД. По умолчанию – `postgres`.
31. Введите пароль.
32. Выберите **Yes**, чтобы установить сервис распространения дистрибутивов. В этом случае точка распространения сможет распространять дистрибутивы агентов на рабочие станции. Если вы ранее выбрали опцию установки сервера **Container (podman)**, то сервис распространения дистрибутивов будет также установлен с поддержкой контейнеризации.
33. Если ранее вы выбрали **Primary** (основной сервер), то укажите путь до PFX-файла ключа шифрования канала между Сервером Device Monitor и агентами. Если путь не указывать, то будет использован путь, предложенный по умолчанию, – `/opt/iw/dmserver/ssl.pfx`.

34. Если вы устанавливаете Сервер на новую БД, то ключ шифрования необходимо создать. Выберите **Yes**.
35. Далее можно выбрать тип развертывания:
    a. **Interact with Traffic Monitor** – с возможностью отправки событий в Traffic Monitor;
    b. **Operate autonomously** – работать автономно, без интеграции с Traffic Monitor.

> **Важно!**
>
> При выборе автономного режима работы в политиках по умолчанию не будут созданы предустановленные правила.

> **Примечание:**
>
> После установки вы можете переключить автономный режим в веб-интерфейсе в разделе **Настройки → Серверы Device Monitor**.

36. Если на предыдущем шаге вы выбрали **Interact with Traffic Monitor**, то введите имя сервера или его IP-адрес.

> **Важно!**
>
> Имя сервера может содержать латинские буквы от «a» до «z» (без учета регистра), цифры от «0» до «9» и знак дефиса "-". Оно не должно состоять только из цифр. Рекомендуется использовать имя сервера, начинающееся с буквы.

> **Примечание:**
>
> Если после установки необходимо изменить адрес InfoWatch Traffic Monitor, вы можете сделать это в базе данных сервера Device Monitor:
>
> - поле `TRAFFIC_MONITOR_POLICY_SERVER_ADDRESS` таблицы Settings – содержит адрес сервера Traffic Monitor, который используется всеми серверами пула Device Monitor – основным и вспомогательными – для получения политики Traffic Monitor и ее распространения на агенты;
> - поле `TmAddress` таблицы ServerOption – содержит адрес сервера Traffic Monitor, на который отправляются события из Device Monitor. В этой таблице поле `TmAddress` может присутствовать несколько раз (по количеству серверов в пуле).

37. Если запрошен токен доступа к Traffic Monitor, введите его значение.
Для успешного соединения Сервера Device Monitor с Сервером Traffic Monitor необходимо настроить проверку сертификата удаленного сервера (подробнее см. далее в разделе "Настройка проверки сертификатов удаленных серверов").
38. Если вы выбрали **Update an existing database**, то запускается проверка на наличие неподдерживаемых для настройки правил в новой версии Device Monitor. В случае, если обнаружено неподдерживаемые правила, то миграция завершится с ошибкой. В этом случае рекомендуем обратиться в службу технической поддержки InfoWatch.

39. Если вы выбрали **Update an existing database** и планируете использовать модуль Device Control, правила и белые списки, выберите **Using Device Control is required, migrate rules and white lists**. Подождите, пока правила Device Control и белые списки будут мигрированы на новую версию. Если использование Device Control не планируется, выберите **Using Device Control is not required, delete rules and white lists**.
40. Введите IP-адрес Сервера Device Monitor.
41. При первичной установке Сервера Device Monitor и базы данных доступна загрузка пользовательского файла конфигурации с политиками и настройками по умолчанию. Чтобы загрузить файл, введите путь до него, например, `/root/configuration.zip`. В этом случае все существующие настройки и элементы конфигурации будут заменены на импортированные.
    Чтобы пропустить этот шаг, нажмите **Enter**.

    > **Важно!**
    >
    > Файл конфигурации должен быть расположен на локальном диске или внешнем носителе. Не поддерживается загрузка файла из сетевой папки.

42. Дождитесь окончания установки.
    Если вы устанавливаете "все-в-одном" и ранее выбрали опцию установки **DM Server Service**, **Front End**, то будут автоматически:
    - получен и записан в Device Monitor открытый ключ службы **guard** Платформы, необходимый для корректного взаимодействия веб-интерфейса с Сервером;
    - исправлен файл **n.yaml**.

    > **Важно!**
    >
    > Любой продукт, который будет установлен в Центре расследований после Device Monitor, сгенерирует новый файл **n.yaml**, и из него будет удалена секция, которая необходима для корректного взаимодействия веб-интерфейса с Сервером. Чтобы восстановить **n.yaml**, выполните шаги 43a-43d.

43. Если вы устанавливаете веб-интерфейс на базе Платформы и Сервер Device Monitor по очереди, используя опции установки **Front End only** и **DM Server Service only**, то действия с ключом службы **guard** Платформы и файлом **n.yaml** из предыдущего шага не будут выполнены автоматически. После установки Платформы и Сервера осуществите их с помощью инсталлятора. Для этого:
    a. Запустите скрипт установки:

    ```
    ./setup.sh
    ```

    b. Выберите в меню пункт **Utilities**. Раздел содержит утилиты:
        i. **Fix n.yaml file** – утилита для автоматического внесения в **n.yaml** необходимых настроек. Выберите этот пункт, если на текущем компьютере установлена Платформа с веб-интерфейсом Центра расследований и основной сервер Device Monitor. Это действие также следует производить после установки любого продукта в Центр расследований;
        ii. **Save platform guard public key to IWDM Service** – если на текущем компьютере установлен Device Monitor в роли **основного** сервера, а также

Платформа (в любом из режимов central или office), то с помощью запуска этой утилиты можно автоматически получить открытый ключ службы **guard** Платформы и сохранить его в каталог сервера;

iii. **Show IWDM Service version** – утилита показывает версию установленного сервера;

iv. **Export ssl key** – утилита позволяет экспортировать ключ защиты канала "агент-сервер".

c. Выберите **Fix n.yaml file**.

d. Введите IP-адрес Сервера Device Monitor и дождитесь окончания процесса.

e. Запустите скрипт установки:

```
./setup.sh
```

f. Выберите в меню пункт **Utilities** и далее **Save platform guard public key to IWDM Service**. Дождитесь окончания процесса.

g. Перезапустите службу **iwdms**:

```
systemctl restart iwdms
```

Важно!

Для подключения к веб-интерфейсу Центра расследований **всегда** используйте адрес или имя сервера, на котором установлена **Платформа в режиме** `central`

5.4.2 Распределенная установка Device Monitor

Распределенная установка нужна, когда организация использует также и другие продукты InfoWatch и/или имеет структуру с центральным офисом и филиалами. В этом случае можно установить один или несколько Серверов Device Monitor на компьютеры с офисными нодами Платформы, где могут быть установлены и другие продукты InfoWatch.

Чтобы установить основной сервер Device Monitor в режиме распределенной установки:

1. Убедитесь, что сервер соответствует аппаратным и программным требованиям ("Аппаратно-программные требования").
2. Выполните шаги по подготовке сервера к установке Device Monitor (см. "Подготовка окружения").
3. Скопируйте архив с дистрибутивом Сервера Device Monitor на жесткий диск другого компьютера.
4. Создайте директорию и распакуйте в нее содержимое архива. В примере архив будет распакован в директорию `/dmsl_distr`:

```
mkdir -p /dmsl_distr && tar xvf dmsl_setup_7.21.0.310.tar.gz -C /dmsl_distr
```

5. Перейдите в созданную директорию.
6. Запустите скрипт **setup.sh**, который входит в состав дистрибутива:

```
./setup.sh
```

Примечание:

В случае ошибки доступа при запуске скрипта, сделайте файл исполняемым, используя команду:

```
chmod +x ./setup.sh
```

Затем запустите скрипт.

7. Выберите тип установки **Install**. Будет доступен список компонентов:
   - **DM Server Service, Front End** – установка "все-в-одном", т.е. установка Сервера Device Monitor и компонента Front End

     Примечание:

     Компонент Front End необходим для работы Центра администрирования и его необходимо устанавливать, даже если на сервере уже установлен какой-либо продукт на базе Платформы.

   - **Front End only** – установка только Платформы и веб-интерфейса
   - **DM Server Service only** – установка только Сервера Device Monitor
8. Выберите **DM Server Service, Front End**.
9. Выберите опцию установки сервера Device Monitor:
   - **Host**, чтобы установить сервер на хосте, или
   - **Container (podman)**, чтобы установить сервер с поддержкой контейнеризации.
10. Будут предложены режимы установки Платформы с веб-интерфейсом Центра расследований и Центра администрирования:
    - **Central** – предназначен для установки на основную ноду или в случае отсутствия уже установленного веб-интерфейса.
    - **Office** – предназначен для распределенной установки.
11. Выберите режим **Office**.
12. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
13. Введите **y**, чтобы принять лицензионное соглашение, и нажмите **Enter**.
14. Введите IP-адрес центральной ноды Платформы, установленной ранее.
15. Получите токен центральной ноды. Для этого на сервере с центральной нодой выполните команду:

```
kubeadm token list
```

16. Скопируйте полученный токен.
17. Введите полученный токен на офисной ноде Платформы и нажмите **Enter**.
18. Укажите лейбл для офисной ноды Платформы.

19. Выделите объем оперативной памяти для размещения данных ClickHouse (по умолчанию 80%) и нажмите **Enter**.
20. Укажите путь для размещения данных ClickHouse (по умолчанию: `/opt/chdata`) и нажмите **Enter**.
21. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/opt/pgdata`) и нажмите **Enter**.
22. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
23. Укажите путь для хранения данных (по умолчанию `/opt/dsdata`) и нажмите **Enter**.
24. Укажите путь для временного хранения событий Traffic Monitor перед их загрузкой в Платформу (по умолчанию: `/opt/factsldrtmdata`) и нажмите **Enter**.
25. Дождитесь окончания процесса установки офисной ноды Платформы. Далее будет произведена установка Сервера Device Monitor. При этом:
    a. Будут созданы каталоги:
        - `/var/log/iwdms` – каталог логов выполнения сервера Device Monitor
        - `/opt/iw/dmserver/bin` – каталог с файлами сервера Device Monitor
        - `/opt/iw/dmserver/queue` – каталог файловой очереди
        - `/opt/iw/dmserver/log` – символическая ссылка на каталог `/var/log/iwdms`
    b. Добавлен пользователь **iwdms** с ключом `--system`, что позволяет запустить под этим пользователем службу, но не дает авторизоваться под этим пользователем в Центра расследований
    c. Распакован zip-файл из `data/iwdms` инсталляционного пакета в требуемые каталоги. Для вышеуказанных папок в качестве владельца буден назначен пользователь **iwdms**
    d. В каталоге systemd служб `/etc/systemd/system` будет добавлен файл манифеста службы Сервера Device Monitor **iwdms.service**, а также службы синхронизации с Active Directory – **iwdms_ldap.service**
26. Выберите язык устанавливаемого сервера и нажмите **Enter**. Это определит названия предустановленных групп, политик и правил.
27. Ознакомьтесь с лицензионным соглашением и выберите необходимое действие. Для продолжения установки необходимо принять лицензионное соглашение. Выберите **Accept and continue** и нажмите **Enter**
28. Выберите основной (**Primary**) тип сервера для установки.
29. Настройте взаимодействие с базой данных:
    - **Create a new database** – чтобы создать новую базу данных. Используйте этот вариант **для чистой установки**;
    - **Update an existing database** – чтобы настроить существующую базу данных. Используйте этот вариант **для установки с миграцией данных**.
30. Укажите имя или IP-адрес сервера, на котором располагается СУБД PostgreSQL. Если вы устанавливаете Device Monitor с миграцией данных, используйте СУБД PostgreSQL, ранее используемую для установки Сервера Device Monitor на ОС Windows.
    Если ранее вы выбрали опцию установки **Container (podman)** и разместили базу данных на одном сервере с Device Monitor, то введите адрес сетевого интерфейса этого сервера. Предварительно настройте базу данных (подробнее см. "Подготовка окружения").

    Важно!

При выбранной опции установки **Container (podman)** нельзя вводить в качестве IP-адреса `localhost` и `127.0.0.1`.

31. Укажите порт для настройки взаимодействия. Если порт не указан, будет использован порт по умолчанию – `5432`.
32. Введите имя базы данных. По умолчанию – `iwdm`.
33. Введите имя пользователя СУБД. По умолчанию – `postgres`.
34. Введите пароль.
35. Выберите **Yes**, чтобы установить сервис распространения дистрибутивов. В этом случае точка распространения сможет распространять дистрибутивы агентов на рабочие станции. Если вы ранее выбрали опцию установки сервера **Container (podman)**, то сервис распространения дистрибутивов будет также установлен с поддержкой контейнеризации.
36. Укажите путь до PFX-файла ключа шифрования канала между Сервером Device Monitor и агентами. Если путь не указывать, то будет использован путь, предложенный по умолчанию, – `/opt/iw/dmserver/ssl.pfx`
37. Если вы устанавливаете Сервер на новую БД, то ключ шифрования необходимо создать. Выберите **Yes**.
38. Далее можно выбрать тип развертывания:
    a. **Interact with Traffic Monitor** – с возможностью отправки событий в Traffic Monitor;
    b. **Operate autonomously** – работать автономно, без интеграции с Traffic Monitor.

Важно!

При выборе автономного режима работы в политиках по умолчанию не будут созданы предустановленные правила.

Примечание:

После установки вы можете переключить автономный режим в веб-интерфейсе в разделе **Настройки → Серверы Device Monitor**.

39. Если на предыдущем шаге вы выбрали **Interact with Traffic Monitor**, то введите имя сервера или его IP-адрес.

Важно!

Имя сервера может содержать латинские буквы от «a» до «z» (без учета регистра), цифры от «0» до «9» и знак дефиса "-". Оно не должно состоять только из цифр. Рекомендуется использовать имя сервера, начинающееся с буквы.

Примечание:

Если после установки необходимо изменить адрес InfoWatch Traffic Monitor, вы можете сделать это в базе данных сервера Device Monitor:

- поле `TRAFFIC_MONITOR_POLICY_SERVER_ADDRESS` таблицы Settings – содержит адрес сервера Traffic Monitor, который используется всеми серверами пула Device Monitor – основным и вспомогательными – для получения политики Traffic Monitor и ее распространения на агенты;
- поле `TmAddress` таблицы ServerOption – содержит адрес сервера Traffic Monitor, на который отправляются события из Device Monitor. В этой таблице поле `TmAddress` может присутствовать несколько раз (по количеству серверов в пуле).

40. Если запрошен токен доступа к Traffic Monitor, введите его значение.
Для успешного соединения Сервера Device Monitor с Сервером Traffic Monitor необходимо настроить проверку сертификата удаленного сервера (подробнее см. далее в разделе "Настройка проверки сертификатов удаленных серверов").
41. Если вы выбрали **Update an existing database**, то запускается проверка на наличие неподдерживаемых для настройки правил в новой версии Device Monitor. В случае, если обнаружено неподдерживаемые правила, то миграция завершится с ошибкой. В этом случае рекомендуем обратиться в службу технической поддержки InfoWatch.
42. Если вы выбрали **Update an existing database** и планируете использовать модуль Device Control, правила и белые списки, выберите **Using Device Control is required, migrate rules and white lists**. Подождите, пока правила Device Control и белые списки будут мигрированы на новую версию. Если использование Device Control не планируется, выберите **Using Device Control is not required, delete rules and white lists**.
43. Введите IP-адрес Сервера Device Monitor.
44. При первичной установке Сервера Device Monitor и базы данных доступна загрузка пользовательского файла конфигурации с политиками и настройками по умолчанию. Чтобы загрузить файл, введите путь до него, например, `/root/configuration.zip`. В этом случае все существующие настройки и элементы конфигурации будут заменены на импортированные.
Чтобы пропустить этот шаг, нажмите **Enter**.

> **Важно!**
>
> Файл конфигурации должен быть расположен на локальном диске или внешнем носителе. Не поддерживается загрузка файла из сетевой папки.

45. Дождитесь окончания установки.
Если вы устанавливаете "все-в-одном" на офисную ноду Платформы и выбрали опцию установки **DM Server Service, Front End**, то будут автоматически:
    - получен и записан в Device Monitor открытый ключ службы **guard** Платформы, необходимый для корректного взаимодействия веб-интерфейса с Сервером;
    - исправлен файл **n.yaml**.

> **Важно!**
>
> Любой продукт, который будет установлен в Центре расследований после Device Monitor, сгенерирует новый файл **n.yaml**, и из него будет удалена секция, которая необходима для корректного взаимодействия веб-интерфейса с Сервером. Чтобы восстановить **n.yaml**, выполните шаги 46a-46d.

46. Если вы устанавливаете веб-интерфейс на базе Платформы и Сервер Device Monitor по очереди, используя опции установки **Front End only** и **DM Server Service only**, то действия с ключом службы **guard** Платформы и файлом **n.yaml** из предыдущего шага не будут выполнены автоматически. После установки осуществите их с помощью инсталлятора. Для этого:
    a. Запустите скрипт установки:

    ```
    ./setup.sh
    ```

    b. Выберите в меню пункт **Utilities**.
    c. Выберите **Fix n.yaml file**.
    d. Введите IP-адрес Сервера Device Monitor и дождитесь окончания процесса.
    e. Запустите скрипт установки:

    ```
    ./setup.sh
    ```

    f. Выберите в меню пункт **Utilities** и далее **Save platform guard public key to IWDM Service**. Дождитесь окончания процесса.
    g. Перезапустите службу **iwdms**:

    ```
    systemctl restart iwdms
    ```

5.4.3 Установка вспомогательного сервера

Независимо от режима установки, в дополнение к основному серверу вы можете установить один или несколько вспомогательных серверов.

Чтобы установить вспомогательный сервер Device Monitor:

1. Убедитесь, что сервер соответствует аппаратным и программным требованиям ("Аппаратно-программные требования").
2. Выполните шаги по подготовке сервера к установке Device Monitor (см. "Подготовка окружения").
3. Скопируйте архив с дистрибутивом Сервера Device Monitor на жесткий диск.
4. Создайте директорию и распакуйте в нее содержимое архива. В примере архив будет распакован в директорию `/dmsl_distr`:

    ```
    mkdir -p /dmsl_distr && tar xvf dmsl_setup_7.21.0.310.tar.gz -C /dmsl_distr
    ```

5. Перейдите в созданную директорию.
6. Запустите скрипт **setup.sh**, который входит в состав дистрибутива:

    ```
    ./setup.sh
    ```

    Примечание:

В случае ошибки доступа при запуске скрипта, сделайте файл исполняемым, используя команду:

```
chmod +x ./setup.sh
```

Затем запустите скрипт.

7. Выберите **Install**.
8. Выберите **DM Server Service only**.
9. Выберите опцию установки сервера Device Monitor:
   - **Host**, чтобы установить сервер на хосте, или
   - **Container (podman)**, чтобы установить сервер с поддержкой контейнеризации.
10. Выберите язык устанавливаемого сервера и нажмите **Enter**. Это определит названия предустановленных групп, политик и правил.
11. Ознакомьтесь с лицензионным соглашением и выберите необходимое действие. Для продолжения установки необходимо принять лицензионное соглашение. Выберите **Accept and continue** и нажмите **Enter**
12. Выберите вспомогательный (**Secondary**) тип сервера для установки.
13. Укажите имя или IP-адрес сервера, на котором располагается СУБД PostgreSQL. Здесь и далее указывайте те же параметры СУБД, которые вы указали при установке основного сервера.
14. Укажите порт для настройки взаимодействия. Если порт не указан, будет использован порт по умолчанию – `5432`.
15. Введите имя базы данных. По умолчанию – `iwdm`.
16. Введите имя пользователя СУБД. По умолчанию – `postgres`.
17. Введите пароль.
18. Выберите **Yes**, чтобы установить сервис распространения дистрибутивов. В этом случае точка распространения сможет распространять дистрибутивы агентов на рабочие станции. Если вы ранее выбрали опцию установки сервера **Container (podman)**, то сервис распространения дистрибутивов будет также установлен с поддержкой контейнеризации.
19. Дождитесь окончания установки.

В случае успешной установки будет запущена служба Сервера Device Monitor. Служба будет помечена как запускаемая автоматически. Чтобы проверить, запущена ли служба сервера Device Monitor, выполните команду:

```
systemctl status iwdms
```

Далее перейдите в Центр расследований. Для подключения к веб-интерфейсу Центра расследований **всегда** используйте адрес или имя сервера, на котором установлена **Платформа в режиме `central`**. Если продукт в режиме `central` установлен на офисной ноде Платформы, для работы все равно используйте центральную ноду Платформы (`central`).

5.4.4 Подготовка Сервера Device Monitor к миграции с ОС Windows на ОС семейства Linux

Если при переходе с ОС Windows на Device Monitor for Linux вам необходима миграция данных, выполните шаги:

> **Важно!**
>
> Не удаляйте основной сервер Device Monitor до проверки поддержки миграции.

1. Обновите Device Monitor, установленный на ОС Windows, на версию 7.21 (подробнее см. "Документация для модуля InfoWatch Device Monitor, установленного на ОС MS Windows", статья "Обновление серверной части InfoWatch Device Monitor").
2. Проверьте, что База данных создана и установлена **с поддержкой русской локали**. Это необходимо для корректной работы веб-интерфейса и поиска объектов с использованием кириллицы в нем. Чтобы проверить локаль, выполните команду:

   ```
   psql -l
   ```

   Локаль указана в столбцах `LC_COLLATE` и `LC_CTYPE` строки искомой Базы данных, например:

   ```
                       Список баз данных
      Имя    | Владелец  | Кодировка   | LC_COLLATE   |  LC_CTYPE    |     Права доступа
   ----------+-----------+-------------+--------------+--------------+-----------------------
    iwdms     | postgres  | UTF8        | ru_RU.UTF-8  | ru_RU.UTF-8  |
   ```

3. Убедитесь, что База данных поддерживает миграцию, т.е. не содержит правил, которые не поддерживаются в новой версии. Для этого:
   a. В дистрибутиве по пути `7.21.x\DM for Windows\Utils` скопируйте архив `CheckMigration.zip`.
   b. Распакуйте архив.
   c. В файле run.bat укажите параметры доступа к Базе данных. При этом добавьте строку, если она отсутствует, и укажите актуальные значения `IP`, `PORT`, `DB_NAME`, `USER_NAME`, `PASSWORD`:

      ```
      "CheckMigration.exe" --Server <IP>:<PORT> --DBName <DB_NAME> --User <USER_NAME> --
      Password "<PASSWORD>" --Culture "ru-RU"
      ```

      Пример:

      ```
      "CheckMigration.exe" --Server 10.20.30.40:1234 --DBName iwdms --User postgres --
      Password "pass123" --Culture "ru-RU"
      ```

   d. Запустите файл `run.bat` с компьютера, где установлен основной сервер Device Monitor.

e. Дождитесь сообщения о готовности к миграции: *The database is ready for migration*.
f. Если утилита выведет список правил, которые не поддерживаются в новой версии, то необходимо удалить эти правила.
g. Если после проверки появилась ошибка о том, что База данных установлена с поддержкой неправильной локали, то выполните п. 2 по ее проверке и убедитесь, что установлена русская локаль. В ином случае смените ее (подробнее о смене локали см. статью Базы знаний "Проверка и изменение локали базы данных PostgreSQL").

4. Удалите все Серверы Device Monitor, оставив Базу данных и сохранив секретный ключ сервера. Для этого воспользуйтесь инструкцией для вашей версии продукта.

Неподдерживаемые в новой версии правила:

- Контроль мессенджеров: MMP, Facebook, Skype
- Контроль копирования с/на CD/DVD
- Контроль приложений: запрет запуска, использования буфера обмена, печати

Неподдерживаемые настройки:

- параметров AD и параметров серверов, подключение к которым разрешено
- автоматического обновление Агентов
- ключа формирования кодов

Не поддерживается миграция настройки подключения для получения управляющих команд от Activity Monitor

5.5 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.

Traffic Monitorосуществляет 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 Traffic 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.

5.5.1 Проверка сертификатов удаленных серверов при установлении SSL-сессии

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.

5.5.2 Установка сертификата службы XAPI Traffic Monitor

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. Если вы будете использовать или установили сервер Device Monitor в окружении Docker, скопируйте его в директорию `/opt/iw/dmserver/cert`. Не перемещайте файл сертификата в другие директории в течение всего времени работы и функционирования сервера Device Monitor.
4. Перейдите в директорию, куда был скопирован корневой сертификат. При использовании Docker – в директорию `/opt/iw/dmserver/cert`.
5. Переименуйте корневой сертификат в `tmca.crt`.
6. Введите команды в зависимости от операционной системы и использования контейнеризации, 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
     sudo update-ca-trust extract
     ```

   - Для операционной системы РЕД ОС с использованием Docker:

     ```
     sudo cp tmca.crt /opt/iw/dmserver/cert
     ```

   - Для операционной системы Альт:

     ```
     su -
     cp tmca.crt /etc/pki/ca-trust/source/anchors/
     update-ca-trust
     ```

   - Для операционной системы Альт с использованием Docker:

     ```
     su -
     cp tmca.crt /opt/iw/dmserver/cert
     ```

   - Для операционной системы Astra Linux:

     ```
     sudo cp tmca.crt /usr/local/share/ca-certificates/tmca.crt
     sudo update-ca-certificates
     ```

   - Для операционной системы Astra Linux с использованием Docker:

```
sudo cp tmca.crt /opt/iw/dmserver/cert/tmca.crt
```

Выполнение команд может занять некоторое время.

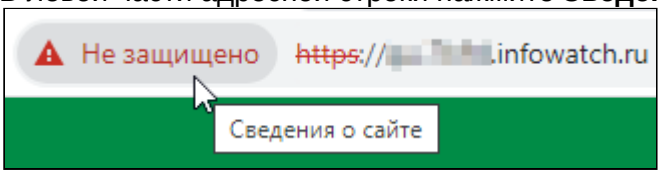
7. Перезапустите службу сервера `iwdms`:

```
systemctl restart iwdms
```

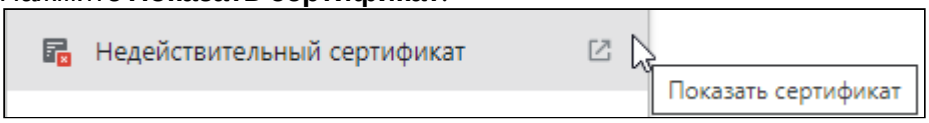
5.5.3 Установка сертификата веб-сервера Traffic Monitor

Чтобы установить сертификат веб-сервера 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.

5.5.4 Установка сертификата службы EPEVENTS Платформы

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.

5.5.5 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`.

5.6 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 Device Monitor и сервера Device Monitor на один компьютер, это может привести к неработоспособности сервера.

5.6.1 Способы установки Агента Device Monitor

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:
  - Локальная установка Агента на рабочей станции под управлением ОС Windows
  - Локальная установка Агента на рабочей станции под управлением ОС семейства Linux
  - Локальная установка Агента на рабочей станции под управлением Mac OS
- Установка с помощью задачи распространения. Выполняется в веб-консоли InfoWatch Device Monitor.

> **Примечание:**
>
> Не поддерживается установка Агента на рабочие станции под управлением МОС с помощью задачи распространения.

5.6.2 Подготовка к установке

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

1. Исключите параллельное использование сторонних DLP-систем;
2. **Для установки на ОС MS Windows добавьте в исключения антивируса следующие файлы Агента InfoWatch Device Monitor:**
   - `%SystemRoot%\SysWOW64\iwprn_x86.dll`
   - `%SystemRoot%\System32\iwprn.dll`
   - `%SystemRoot%\System32\tm.dll`
   - `%SystemRoot%\System32\Drivers\IWDMDV.SYS`
   - `%SystemRoot%\System32\Drivers\IWDMFS.SYS`
   - `%SystemRoot%\System32\Drivers\IWDMH.SYS`
   - `%SystemRoot%\System32\Drivers\IWDMSHC.SYS`
   - `%SystemRoot%\System32\Drivers\IWDMWFP.SYS`
   - `%SystemRoot%\System32\Drivers\IwNNwF.SYS`
   - `%SystemRoot%\System32\IWDeployAgent.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\7z.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\rmtdiag.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwscrctl.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwshcs.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwdmc.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\IWProxy\IWProxy.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\IWProxy\SystemCertificate\updroots.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\DM.Client.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\Client.RebootReminder.exe`
   - `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwmediarec.exe`

- `%ProgramFiles%\Infowatch\DeviceMonitor\Client\iwdmifilter.exe`

  где `%ProgramFiles%\Infowatch\DeviceMonitor\Client\` – **путь установки Агента по умолчанию**. Если вы будете использовать различные пути при установке различных групп рабочих станций, учтите все их все.

Также **рекомендуется** добавить в исключения:

- **Папку установки Агента**. По умолчанию: `C:\Program Files\Infowatch\DeviceMonitor\Client\`
- **Папку хранения теневых копий**: `_IWEVT_{3FF1ABF9-77EE-411c-A698-ECA23E44A3BF}_`. Это позволит снизить нагрузку. Папка может располагаться на любом томе, который имеет достаточно свободного места.

3. **Для установки на ОС семейства Linux добавьте в исключения антивируса следующие файлы Агента InfoWatch Device Monitor:**

   Все файлы в папках и их подпапках:

   - **`/sys/module/iwdmfsshc/`**
   - **`/sys/module/iwdmnfredir/`**
   - **`/opt/iw/dmagent/`**
   - **`/opt/iw/deployagent/`**
   - **`/opt/iw/share/config`**

   Также **рекомендуется** настроить исключения по процессам. Исключите процессы со следующими путями (включая дочерние процессы):

   - **`/sys/module/iwdmfsshc/*`**
   - **`/sys/module/iwdmnfredir/*`**
   - **`/opt/iw/dmagent/*`**
   - **`/opt/iw/deployagent/*`**
   - **`/opt/iw/share/config/*`**

4. Отключите самозащиту антивируса;
5. По возможности отключите или удалите антивирус на время установки, обновления и удаления Агента InfoWatch Device Monitor;
6. 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")
7. **На рабочих станциях под управлением ОС Astra Linux на время удаленной установки Агентов отключите часть настроек ОС.**

   Для этого:

   a. Отключите блокировку интерпретаторов, кроме bash, с помощью команды:

   ```
   sudo astra-interpreters-lock disable
   ```

   b. Отключите блокировку интерпретатора bash с помощью команды:

   ```
   sudo astra-bash-lock disable
   ```

   c. Отключите запрет установки бита исполнения с помощью команды:

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

> **Примечание:**
>
> После установки Агентов Device Monitor, вы можете вернуть измененные настройки к исходным значениям, для этого выполните те же команды, заменив в них `disable` на `enable`.
>
> Подробнее о настройках безопасности ОС Astra Linux см. документацию на официальном сайте.

8. 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");
9. **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:

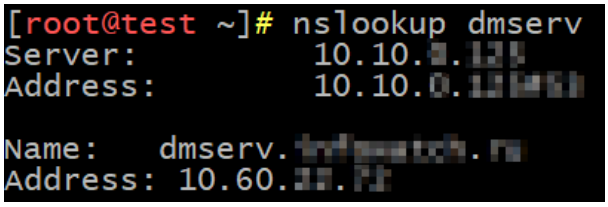
- разрешены символы латинского алфавита (`A` - `Z` , `a` - `z`), цифры (`0` - `9`) и дефис;
- длина имени должна быть не более 15 символов.

10. 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.

11. Если не требуется использовать компонент контроля сетевых соединений, отключите его при создании дистрибутива Агента InfoWatch Device Monitor;

12. 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!

Обратите внимание, что в процессе установки Агента:

- Выключение питания компьютера может привести к ошибкам, ведущим к нестабильной работе операционной системы. Особенность также относится к процессу удаления 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». Особенность также относится к процессам удаления и обновления Агента.
- Будут закрыты (если они были запущены) программы Mozilla Firefox и Mozilla Thunderbird.

Если на рабочей станции организовано подключение к корпоративной сети удаленно (через VPN-агент), добавьте VPN-агент в исключения из перехвата (в том числе сетевого).

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.

При включенном протоколе Secure Boot загрузка модуля режима ядра не гарантируется.

Важно!

Если вы устанавливаете Агента на рабочую станцию под управлением ОС Windows 7 Service Pack 1 или Windows 2008 R2 Server:

- Установите пакеты исправлений Windows для указанных ОС. См. в статье "Аппаратные и программные требования".
- Учтите, что если Агент устанавливается впервые, компонент *Контроль сетевых соединений* не будет установлен. При необходимости, данный компонент возможно установить вручную, используя командную строку.

Важно!

На ОС семейства **Linux** не допускается самостоятельное удаление или изменение перечисленных ниже учетных записей, так как это приведет к неработоспособности Агента InfoWatch Device Monitor:

- `iwdm` – используется основной службой Device Monitor;

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

Учетные записи создаются в операционной системе при установке Агента для ограничения доступа к данным Device Monitor. При удалении Агента указанные учетные записи будут удалены автоматически.

5.6.3 Локальная установка Агента на рабочей станции под управлением ОС Windows

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 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 развертывания в соответствии с заданными при формировании пакетов параметрами, например, `InfoWatch.DeviceMonitor.Client.7.21.0.x64.msi`.

   Примечание:

   Начиная с **Device Monitor 7.18.5**, **при первичной установке Агента** инсталлятор проверяет, получен ли список приложений, которые должны быть исключены из перехвата. Если список исключений не получен, установка этого Агента будет остановлена. В этом случае в лог будет добавлена запись `CustomAction GetExclusionsFromServerWithCheck returned actual error`.

   Отключение этой проверки доступно только при установке с помощью командной строки.

   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 Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью MSI-пакета в тихом режиме

Для минимизации участия в процессе установки вы можете установить Агента в тихом режиме.

Перед запуском инсталлятора:

1. Вставьте внешний носитель с дистрибутивом Агента в компьютер.
2. Запустите командную строку (`cmd.exe`) от имени Администратора.
3. Перейдите в каталог, где находится дистрибутив Агента, выполнив команду:

```
cd <путь_до_дистрибутива>
```

Ознакомьтесь со списком ключей в таблице ниже, с их помощью вы можете указать инсталлятору параметры установки продукта.

Ключ	Описание
`/quiet`	Запуск установки без отображения пользовательского интерфейса
`/i <имя_пакета_установки>`	Запуск установки продукта с помощью указанного файла
`PREDEFINED_CLIENTDIR`	Директория для установки продукта Значение по умолчанию: `"%ProgramFiles%\Infowatch\DeviceMonitor\Client"` **Важно!**

Ключ	Описание
	Путь к каталогу может содержать следующие символы: `0-9` , `a-z` , `A-Z` ,"`:`","`.`","`_`","`-`","`\`","` `" При наличии в пути других символов, установка Агента будет некорректной.
`UNINSTALL_PASSWORD_SHA1_HASH`	Хеш-значение пароля деинсталляции в шестнадцатеричном формате, вычисленное по алгоритму SHA-1. Если задать данный параметр, то удалить Агента Device Monitor можно будет только введя правильный пароль. **Важно!** Хеш-значение пароля необходимо вычислять для кодировки Юникод UTF-16LE. Указывайте хеш-значение, используя только заглавные буквы и цифры.
`IWPROXYDN`	Строка с доменным именем корневого сертификата proxy-сервера на рабочей станции, который используется для выпуска сертификатов при перехвате защищенного трафика. Имя должно соответствовать стандарту X.509 и содержать поле CN (Common Name). Поля внутри имени должны быть разделены запятой Значение по умолчанию: `"CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow"`
`SHOW_USER_NOTIFICATION`	Показывать пользователю уведомление о необходимости перезагрузить компьютер. Возможные значения: • `"#x01000000"` (по умолчанию) – показывать • `"#x00000000"` – не показывать
`WAITING_REBOOT_PERIOD`	Время ожидания перезагрузки рабочей станции до момента, когда Агент начнет показывать пользователю уведомление о необходимости перезагрузить компьютер. Указывается в часах Значение по умолчанию: `"0"`
`REBOOT_NOTIFICATION_PERIOD`	Время до принудительной перезагрузки, в течении которого Агент показывает пользователю уведомление о необходимости перезагрузить компьютер. Указывается в часах. Возможные значения: • целые числа от 0 до 1000;

Ключ	Описание
	• `"-1"` (по умолчанию), чтобы показывать уведомление бесконечно и не перезагружать компьютер принудительно.
`REBOOT_NOTIFICATION_RATE`	Частота, с которой Агент показывает пользователю уведомление о необходимости перезагрузить компьютер. Указывается в минутах. **Примечание:** Если параметр не задан, уведомление показывается каждые 10 минут
`REBOOT_NOTIFY_MESSAGE`	Текст уведомления о необходимости перезагрузить компьютер. Сообщение может содержать не более 255 символов Текст по умолчанию: `"Необходимо как можно скорее перезагрузить компьютер"`
`FORCE_REBOOT`	Отправить финальное уведомление перед принудительной перезагрузкой. Возможные значения: • `"0"` (по умолчанию) – показывать финальное уведомление • `"1"` – не показывать финальное уведомление **Важно!** После финального уведомления у сотрудника будет 5 минут на завершение своих операций. Если для параметра задано значение `"1"`, то принудительная перезагрузка (если она предусмотрена параметром `REBOOT_NOTIFICATION_PERIOD`) будет осуществлена неожиданно для сотрудника
`HIDE_CLIENT`	Скрывать присутствие Агента Device Monitor от пользователя рабочей станции. Возможные значения: • `"#x01000000"` – скрывать Агента • `"#x00000000"` (по умолчанию) – не скрывать Агента **Важно!** Неуведомление об использовании перехватчиков может входить в конфликт с действующим законодательством вашей страны. **Важно!** Уведомление о необходимости перезагрузить компьютер не будет показано, если для данного параметра задано значение `"#x01000000"` – скрывать Агента.
`NOIWPROXY`	Не устанавливать компонент перехвата сетевого трафика. Возможные значения:

Ключ	Описание
	• `"0"` (по умолчанию) – установить компонент • `"1"` – не устанавливать компонент
`NOIWNBG`	Не устанавливать компонент контроля сетевых соединений. Возможные значения: • `"0"` (по умолчанию) – установить компонент • `"1"` – не устанавливать компонент
`SRVPOOL`	Список серверов Device Monitor, с которыми может соединяться Агент. Список задается в следующем виде: `<Сервер>[;<Сервер>[;<Сервер>[{*};{*}...]]]` где `<Сервер>` = `<DNS имя сервера>:<номер порта>` Пример значения параметра: `"dmserver:15101;"` Если Агент не сможет соединиться с первым по списку сервером, то он будет пытаться соединиться со следующим по списку и так далее. После соединения с сервером Агент будет привязан к нему.
`EXCL_REQUIRED`	Начиная с **Device Monitor 7.18.5**, **при первичной установке Агента** инсталлятор проверяет, получен ли список приложений, которые должны быть исключены из перехвата. Если список исключений не получен, установка этого Агента будет остановлена. В этом случае в лог будет добавлена запись `CustomAction GetExclusionsFromServerWithCheck returned actual error`. Если вы хотите отключить проверку, добавьте в команду запуска опцию `EXCL_REQUIRED = 0`.
`/lvp <имя_лог_файла>`	Записывать данные в указанный лог-файл

Чтобы установить Агента InfoWatch Device Monitor:

1. В командной строке запустите программу установки Агента с указанием параметров.
   Пример команды установки:

```
%windir%\system32\msiexec.exe /quiet /i
InfoWatch.DeviceMonitor.Client.x64.ru.7.21.0.192.msi PREDEFINED_CLIENTDIR="%ProgramFiles%
\Infowatch\DeviceMonitor\Client" IWPROXYDN="CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO
InfoWatch,OU=TechDep,ST=Moscow" SHOW_USER_NOTIFICATION="#x01000000"
WAITING_REBOOT_PERIOD="48" REBOOT_NOTIFICATION_PERIOD="10" REBOOT_NOTIFICATION_RATE="1"
HIDE_CLIENT="#x00000000" FORCE_REBOOT="0" NOIWPROXY="0" NOIWNBG="0"
SRVPOOL="dmserver:15101;" /lvp InfoWatch.DeviceMonitor.Client.x64.ru.7.21.0.192.log
```

2. Дождитесь завершения установки.
3. Перезагрузите компьютер.

5.6.4 Локальная установка Агента на рабочей станции под управлением ОС семейства Linux

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.

Примечание:

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

1. **Подготовка к установке:**
   a. Убедитесь, что пользователь, от имени которого будет произведена установка, имеет необходимые права:
      - на компьютере под управлением ОС Альт Рабочая Станция – права на исполнение `su`;
      - на компьютере под управлением других ОС семейства Linux – привилегии `sudoers`.
   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.AstraLinux-1.7-iwdm.x86_64.x.x.x.xx.tar.gz` – для Astra Linux Special Edition 1.7;
      - `Setup.AstraLinux-1.8-iwdm.x86_64.x.x.x.xx.tar.gz` – для Astra Linux Special Edition 1.8;
      - `Setup.RedOS-7.3-iwdm.x86_64.x.x.x.xx.tar.gz` – для РЕД ОС 7.3.1;
      - `Setup.RedOS-8.0-iwdm.x86_64.x.x.x.xx.tar.gz` – для РЕД ОС 8.0;
      - `Setup.AltLinux-10.0-iwdm.x86_64.x.x.x.xx.tar.gz` – для Альт Рабочая станция 10;
      - `Setup.AltLinux-11.0-iwdm.x86_64.x.x.x.xx.tar.gz` – для Альт Рабочая станция 11;
      - `Setup.Rosa-12.5.1-iwdm.x86_64.x.x.x.xx.tar.gz` – для МОС.

      где `x.x.x.xx` – номер сборки.
      Далее мы рассмотрим пример установки Агента на РЕД ОС 7.3. Установка на ОС Альт, Astra Linux и РЕД ОС 8.0 аналогична. Примеры команд для Альт и Astra Linux приведены ниже.
      Для установки Агента на рабочую станцию под управлением МОС см. отдельную инструкцию.
   c. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки:

```
sudo tar -xvzf Setup.RedOS-7.3-iwdm.x86_64.x.x.x.xx.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.x86_64.x.x.x.xx.tar.gz`**.
   b. Для установки Агента запустите скрипт, выполнив команду:
      - Для обычной установки (при этом будет установлен компонент перехвата сетевого трафика):

```
sudo ./install.sh <сервер>:<порт> [-g '<Proxy_DN>']
```

где `<сервер>` - IP-адрес или доменное имя Сервера InfoWatch Device Monitor, `<порт>` - порт подключения к Серверу InfoWatch Device Monitor, `[-g '<Proxy_DN>']` – опциональный параметр для явного указания DN (Issuer Distinguished Name). Используйте его, если хотите задать DN для сертификата прокси.
Имя `<Proxy_DN>` должно содержать поле CN (Common Name). Поля внутри имени должны быть разделены запятой.

> **Примечание:**
>
> Значение DN по умолчанию: `' CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow'`
> Если вы не используете параметр **`-g`** или укажете значение по умолчанию, то DN в сгенерированном сертификате соединения будет иметь вид:
>
> `CN = IWDMProxy(<machine_uuid>)`
> `OU = Infowatch TechDep`
> `O = Infowatch`
> `L = Moscow`
> `ST = RU`
> `C = RU`
>
> где `<machine_uuid>` – это идентификатор рабочей станции, созданный Агентом.

В нашем примере команда будет следующей:

```
sudo ./install.sh dm-server:15101
```

Продукт будет установлен в директорию `/opt/iw/dmagent`.

> **Примечание:**

Начиная с **Device Monitor 7.18.5**, **при первичной установке Агента** инсталлятор проверяет, получен ли список приложений, которые должны быть исключены из перехвата. Если список исключений не получен, установка этого Агента будет остановлена. В этом случае будет выведено сообщение об ошибке вида:

```
D: Exit status: 0
[infowatch-agent-install] postinst: ERROR: exclusions not received (rc=255); abort install (exit 2)
```

Если вы хотите отключить проверку, добавьте в команду запуска опцию `IW_EXCL_REQUIRED=0`.

Пример команды установки Агента без проверки списка исключений:

```
sudo IW_EXCL_REQUIRED=0 ./install.sh dm-server:15101
```

Примечание:

Для вывода справки, выполните команду:

```
sudo ./install.sh -h
```

- Для установки без компонента перехвата сетевого трафика:

```
sudo IWDM_NO_PROXY=1 ./install.sh <сервер>:<порт>
```

c. Проверить статус сервисов можно командой:

```
sudo systemctl status "iwdm*"
```

Примечание:

Если вы выбрали не устанавливать компонент перехвата сетевого трафика, то:

- Сервис `iwdmproxy` не будет запущен.
- В директории `/opt/iw/dmagent/etc/iwdmproxy` будет создан файл `no_proxy`.
- При обновлении Агента компонент перехвата сетевого трафика также не будет установлен.

d. Перезагрузите рабочую станцию с помощью команды:

```
reboot
```

Примеры команд для других ОС

ОС Astra Linux:

1. Распаковка архива:

```
sudo tar -xvzf Setup.AstraLinux-1.7-iwdm.x86_64.x.x.x.xx.tar.gz
```

2. Запуск установки:

```
sudo ./install.sh dm-server:15101
```

Пример команды установки Агента без проверки списка исключений:

```
sudo IW_EXCL_REQUIRED=0 ./install.sh dm-server:15101
```

В случае установки без компонента перехвата сетевого трафика:

```
sudo IWDM_NO_PROXY=1 ./install.sh dm-server:15101
```

3. Проверка статуса сервисов:

```
sudo systemctl status "iwdm*"
```

ОС Альт:

1. Распаковка архива:

```
tar -xvzf Setup.AltLinux-10.0-iwdm.x86_64.x.x.x.xx.tar.gz
```

2. Запуск установки:

```
su -c "./install.sh dm-server:15101"
```

Пример команды установки Агента без проверки списка исключений:

```
su -c "IW_EXCL_REQUIRED=0 ./install.sh dm-server:15101"
```

В случае установки без компонента перехвата сетевого трафика:

```
su -c "IWDM_NO_PROXY=1 ./install.sh dm-server:15101"
```

3. Проверка статуса сервисов:

```
su - -c 'systemctl status "iwdm*"'
```

Установка Агента на рабочую станцию под управлением МОС

1. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки:

```
sudo tar -xvzf Setup.Rosa-12.5.1-iwdm.x86_64.x.x.x.xx.tar.gz
```

В результате будет создана директория `/depends` и файлы `iwdm-<версия_агента>.rpm`, `iwfiles.sign`, `iwfiles.digests`.

2. Для установки Агента установите RPM-пакет, выполнив команду:

```
rpm -i iwdm-<версия_агента>.rpm
```

Продукт будет установлен в директорию `/opt/iw/dmagent`.

3. Запустите скрипт `/opt/iw/dmagent/bin/first_run.sh`:

```
/opt/iw/dmagent/bin/first_run.sh <сервер>:<порт>
```

где `<сервер>` – IP-адрес Сервера InfoWatch Device Monitor,
`<порт>` – порт подключения к Серверу InfoWatch Device Monitor.
В нашем примере команда будет следующей:

```
/opt/iw/dmagent/bin/first_run.sh dm-server:15101
```

4. Проверить статус сервисов можно командой:

```
sudo systemctl status "iwdm*"
```

5. Перезагрузите рабочую станцию с помощью команды:

```
reboot
```

5.6.5 Локальная установка Агента на рабочей станции под управлением Mac OS

> **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.

> **Важно!**
>
> Не допускается установка через SSH-подключение.

1. **Подготовка к установке:**
   a. Убедитесь, что пользователь, от имени которого будет произведена установка, имеет привилегии `sudoers`.
   b. Скопируйте на компьютер архив, в котором содержатся пакет и скрипты для установки и удаления Агента Device Monitor.
   В нашем примере – `Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz`, где `x.x.x.xx` – номер сборки.
   c. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки:

   ```
   sudo tar -xvzf Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz
   ```

   В результате будут созданы файлы `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<версия_агента>.pkg`.
2. **Установка Агента InfoWatch Device Monitor:**
   a. Перейдите в директорию, в которую распаковано содержимое архива **`Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz`**.
   b. Для установки Агента запустите скрипт, выполнив команду:

   ```
   sudo ./install.sh <сервер>:<порт>
   ```

   В команде выше:
   `<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
   ```

   c. При установке скрипт вносит изменения в настройки доверительных сертификатов системы. После запуска скрипта операционная система запросит разрешение на это действие в отдельном окне. Для подтверждения введите

пароль вашей учетной записи.
Дождитесь окончания установки. Продукт будет установлен в директорию `/opt/iw/dmagent`.

d. Проверьте статусы сервисов с помощью команд:

```
sudo launchctl print system/com.infowatch.iwdmproxy | grep state
```

```
sudo launchctl print system/com.infowatch.iwdmc | grep state
```

e. Перезагрузите рабочую станцию с помощью команды:

```
reboot
```

5.6.6 Установка Агентов с помощью задачи распространения

> **Примечание:**
>
> Установка Агента с помощью задачи распространения возможна только на рабочих станциях под управлением ОС Windows, Astra Linux, Альт или РЕД ОС.

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 "Все-в-одном"", Шаг 34).

Перед установкой Агентов:

- Рекомендуется добавить файлы Агента в исключения антивируса. Список файлов см. в статье Базы знаний "Список файлов Агента InfoWatch для добавления в исключения антивирусов".
- Для распространения Агентов на рабочие станции под управлением:
  - ОС **Astra Linux Special Edition** версий **1.7** и **1.8:**
    Для пользователя, от имени которого будет произведена установка Агента, настройте максимальный уровень мандатного доступа. Например, чтобы повысить уровень доступа для пользователя `root`, используйте команду:

    ```
    sudo pdpl-user -i 63 root
    ```

  - ОС **Альт Рабочая станция 10**:
    Для пользователя, от имении которого будет выполняться запуск задачи:
    1. Вручную включите доступ на рабочую станцию по SSH, выполнив команду:

       ```
       service sshd start
       ```

    2. В файле `/etc/openssh/sshd_config` раскомментируйте строку `PermitRootLogin`.
    3. Добавите пользователя в группу `/etc/sudoers`.

Для установки Агентов:

1. В разделе **Задачи** веб-консоли создайте задачу первичного распространения. См. "InfoWatch Device Monitor for Linux. Руководство пользователя", статья "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.
6. Для корректной работы функциональности на рабочей станции под управлением ОС семейства Linux перезагрузите компьютер после установки Агента.

Важно!

Раздел **Задачи** будет отключен в последующих версиях. Управление установкой, обновлением и удалением доступно в новом разделе с расширенными возможностями контроля и приоритизации. См. "InfoWatch Device Monitor for Linux. Руководство пользователя", статья "Политики распространения".

Важно!

Учтите, что:

- Не допускается установка Агента InfoWatch Device Monitor и сервера Device Monitor на один компьютер, т.к. это может привести к неработоспособности сервера.
- 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*.
- Если на компьютере установлена кастомизированная версия системы SELinux, корректная установка Агента не гарантируется.

6 Настройка сетевых правил доступа

Для корректной работы Системы должны быть разрешены соединения:

Направление соединения	Порт	Назначение порта
Порты, необходимые для установки сервера и агентов Device Monitor:		
Сервер Device Monitor → Сервер СУБД	Порт СУБД PostgresSQL	Взаимодействие Сервера Device Monitor с СУБД PostgresSQL (по умолчанию TCP 5432)
Сервер Device Monitor → Агент Device Monitor (Linux)	TCP 22	Установка Агента Device Monitor на рабочую станцию под управлением ОС семейства Linux
Сервер Device Monitor → Агент Device Monitor (Windows)	TCP 135	Установка Агента на рабочую станцию Device Monitor под управлением ОС семейства Windows **Примечание:** * Порт TCP 593 может быть задействова

Направление соединения	Порт	Назначение порта
	UDP 137	н неявно, согласно настройкам ОС сервера Device Monitor, с которого выполняется развертывание агента распространения при первичной установке.
	UDP 138	
	TCP 139	
	TCP 593 *	
	TCP 445	
Агент Device Monitor (Windows) → Сервер Device Monitor	TCP 445	
Сервер Device Monitor → Агент Device Monitor (Linux\Windows)	TCP 15505	Связь со службой Deploy Agent (установка, обновление, удаление агента)
Агент Device Monitor → Сервер Device Monitor (сервис распространения дистрибутивов)	TCP 15200	Инициация загрузки дистрибутива Агента с Сервера Device Monitor на рабочую станцию
Порты, необходимые для работы сервера и агентов Device Monitor:		
Рабочая станция Администратора → Сервер Device Monitor	TCP 22	Подключение к серверу Device Monitor по SSH-протоколу
Рабочая станция Офицера безопасности → Центральная нода Платформы	TCP 443	Веб-консоль Центра расследований для управления

Направление соединения	Порт	Назначение порта
		Device Monitor
Сервер Device Monitor → Сервер Traffic Monitor	TCP 443	Получение политик защиты данных на агентах от Traffic Monitor
Сервер Device Monitor → Сервер Active Directory	TCP 389 TCP 636 TCP 3268	Синхронизация с Active Directory
Сервер Device Monitor → Сервер Traffic Monitor	TCP 9100	Передача теневых копий в Traffic Monitor
Агент Device Monitor → Сервер Activity Monitor	TCP 11008	Передача событий статистики активности с агента Device Monitor напрямую в Activity Monitor. Требуется выполнить настройку прямой отправки событий в Activity Monitor
Агент Device Monitor → Сервер Device Monitor	TCP 15101	Инициализация защищённого соединения

Направление соединения	Порт	Назначение порта
	TCP 15004	Передача теневых копий по шифрованному соединению
Агент Device Monitor → Сервер Device Monitor Сервер Device Monitor → Агент Device Monitor	UDP 15100	Внутренний протокол Device Monitor (передача статусов, уведомлений об изменении настроек и т.д.)
Сервер Device Monitor → Агент Device Monitor	TCP 15506	Управление Агентом Device Monitor (включение, выключение, сбор диагностической информации)
Платформа → основной Сервер Device Monitor	TCP 15507	Взаимодействие Платформы с основным Сервером Device Monitor (с установленной службой WebAPI)
Сервер Device Monitor → Сервер Activity Monitor	TCP 17104	Передача теневых копий в Activity Monitor (скриншоты, keylogger,

Направление соединения	Порт	Назначение порта
		события подключения устройств). Также через этот порт передаётся статистика активности для агентов версии 7.15 и ниже, либо при отсутствии настройки прямой отправки Событий в Activity Monitor

Примечание:

Если в процессе установки были назначены порты, отличные от указанных в таблице, то необходимо использовать их. Если далее вы хотите использовать стандартные порты из таблицы:

a. Остановите службу Сервера Device Monitor с помощью команды:

```
systemctl stop iwdms
```

b. Чтобы изменить порты соединения Сервера Device Monitor с Агентами, в таблице `ServerOption` базы данных Сервера Device Monitor отредактируйте параметры:
   - `NotificationPort` (UDP 15100);
   - `ClientFacadePort` (TCP 15101);
   - `SSLPort` (TCP 15004).

c. Включите службу Сервера Device Monitor 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

> **Примечание:**
>
> Начиная с версии 7.19, вы можете обновить конфигурации некоторых технологий, не обновляя Агенты (см. подробнее Обновление конфигурации на Агентах Device Monitor).

7.1 Обновление Сервера Device Monitor

> **Важно!**
>
> Обновление до версии **7.21** поддерживается только **со сбросом** установки компонента **Front End**.
>
> Для обновления кластера из нескольких серверов сначала обновите по инструкции основной (**Primary**) сервер Device Monitor, а затем второстепенные (**Secondary**) серверы.
>
> Убедитесь, что для базы данных, с которой взаимодействует сервер Device Monitor, установлена русская локаль (`ru_RU.utf8`). Подробнее см. статью Базы знаний "Проверка и изменение локали базы данных PostgreSQL".

В статье представлены:

- Обновление со сбросом установки
- Обновление со сбросом при распределенной установке
- Переход на версию Сервера с поддержкой контейнеризации

Обновление Сервера Device Monitor со сбросом установки

Чтобы обновить Сервер Device Monitor:

1. Выполните шаги по подготовке сервера к обновлению Device Monitor.

   > **Важно!**
   >
   > Обязательно установите интерпретатор языка Python версии 3 и дополнительные пакеты к нему, в том числе `importlib-metadata` и `pyyaml` .
   > Также убедитесь, что версия dotnet актуальна.
   > Подробнее см. "Подготовка окружения".

2. Скопируйте архив с дистрибутивом Сервера Device Monitor на жесткий диск.
3. Создайте каталог и распакуйте в него содержимое архива. В примере архив будет распакован в каталог `/tmp/dmsl_distr` :

```
mkdir -p /tmp/dmsl_distr && tar xvf dmsl_setup_7.21.0.402.tar.gz -C /tmp/dmsl_distr
```

4. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.21. В примере файл будет извлечен в каталог `/tmp/iwdm` :

```
mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.21.0.402.tar.xz -C /tmp/iwdm
```

5. Перейдите в каталог `/tmp/iwdm` и выполните сброс установки Платформы. Если у вас установлены несколько продуктов InfoWatch на разных серверах, то выполните команду сначала на **офисной** ноде Платформы, затем на **центральной** ноде:

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

   Дождитесь окончания процесса.
6. Перезагрузите сервер с помощью команды:

```
reboot
```

   Если у вас были установлены несколько продуктов InfoWatch, перезагрузите все серверы.
7. Чтобы освободить место на диске, вы можете удалить папку `/tmp/iwdm` .
8. Если вы обновляетесь с переходом на другой сервер или на новую ОС, скопируйте на другой раздел или на новый сервер каталоги с данными, которые были указаны при установке.

   > **Примечание:**
   >
   > По умолчанию каталоги расположены по пути `/opt` .
   > В версиях **Device Monitor ниже 7.16** каталоги по умолчанию располагались по пути `/mnt` .
   > Обязательно копируйте каталоги с сохранением прав и владельцев. Для копирования используйте стандартные средства, например, утилиту `rsync` .

9. Убедитесь, что в разделе с папкой `/var/lib/containerd` доступно не менее 30 ГБ дискового пространства.
   Чтобы проверить доступное дисковое пространство, используйте команду:

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

   > **Примечание:**

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

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

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

10. Перейдите в каталог `/tmp/dmsl_distr`.
11. Убедитесь, что сервер соответствует аппаратным и программным требованиям ("Аппаратно-программные требования").
12. Запустите скрипт **setup.sh**:

```
./setup.sh
```

Примечание:

В случае ошибки доступа при запуске скрипта, сделайте файл исполняемым, используя команду:

```
chmod +x ./setup.sh
```

Затем запустите скрипт.

13. Выберите **Update**.
14. Выберите опцию для обновления со сбросом – **Update all after you reset DM Front End: install DM Front End and update DM Server Service**.
Будет установлен компонент DM Front End на базе Платформы и обновлен Сервер Device Monitor.
15. Выберите режим установки Платформы – **Central** (или **Office** при распределенной установке).
16. Далее следуйте шагам по установке Платформы из инструкции "Новая установка".
Когда инсталлятор потребует указать директории для размещения данных, указывайте директории с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?»
17. Дождитесь окончания установки DM Front End и обновления Сервера Device Monitor.
Автоматически будут произведены следующие действия:
    - получен и записан в Device Monitor открытый ключ службы **guard** Платформы, необходимый для корректного взаимодействия веб-интерфейса с Сервером;
    - исправлен файл **n.yaml**.

Важно!

Любой продукт, который будет установлен в Центре расследований после Device Monitor, сгенерирует новый файл **n.yaml**, и из него будет удалена секция, которая необходима для корректного взаимодействия веб-интерфейса с Сервером. Чтобы восстановить **n.yaml**, выполните шаги 18a-18c.

18. Если вы устанавливаете веб-интерфейс на базе Платформы и обновляете Сервер Device Monitor по отдельности, используя опцию установки **DM Front End only** и опцию обновления **DM Server Service only**, то действия с ключом службы **guard** Платформы и файлом **n.yaml** из предыдущего шага не будут выполнены автоматически. После установки Платформы и обновления Сервера осуществите их с помощью инсталлятора. Для этого:
    a. Запустите скрипт установки:

    ```
    ./setup.sh
    ```

    b. Выберите **Utilities** и выполните пункт **Fix n.yaml file**.
    c. Укажите IP-адрес компьютера, на котором был установлен Сервер Device Monitor. Если он был установлен на текущем компьютере, нажмите **Enter**. Дождитесь окончания процесса.
    d. Запустите скрипт установки:

    ```
    ./setup.sh
    ```

    e. Выберите в меню пункт **Utilities** и далее **Save platform guard public key to IWDM Service**. Дождитесь окончания процесса.
    f. Перезапустите службу **iwdms**:

    ```
    systemctl restart iwdms
    ```

19. Обновите все установленные второстепенные (**Secondary**) Серверы Device Monitor, выполнив на каждом из них следующие шаги:
    a. Запустите скрипт **setup.sh**:

    ```
    ./setup.sh
    ```

    b. Выберите **Update**.
    c. Выберите **DM Server Service only**.
    d. Дождитесь окончания процесса обновления.

Чтобы проверить корректность обновления, перейдите в веб-интерфейс Центра расследований и проверьте доступность раздела **Настройки** → **Device Monitor** → **Серверы**.

Если перед обновлением вы выключали отправку уведомлений в Telegram, включите ее снова.

Обновление со сбросом при распределенной установке

Исходные условия:

- Device Control версии 1.4 и Activity Monitor версии 3.5 установлены на центральной ноде Платформы.

- Сервер Device Monitor версии 7.20 установлен (в режиме `central`) на офисной ноде Платформы.

Чтобы обновить Сервер Device Monitor:

1. На офисной ноде Платформы выполните шаги по подготовке сервера к обновлению Device Monitor (см. "Подготовка окружения", убедитесь, что версия dotnet актуальна).
2. Скопируйте на офисную ноду архив с дистрибутивом Сервера Device Monitor.
3. Создайте каталог и распакуйте в него содержимое архива. В примере архив будет распакован в каталог `/tmp/dmsl_distr`:

   ```
   mkdir -p /tmp/dmsl_distr && tar xvf dmsl_setup_7.21.0.402.tar.gz -C /tmp/dmsl_distr
   ```

4. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.21. В примере файл будет извлечен в каталог `/tmp/iwdm`:

   ```
   mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.21.0.402.tar.xz -C /tmp/iwdm
   ```

5. Перейдите в каталог `/tmp/iwdm` и выполните сброс установки Платформы:

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

6. Перезагрузите текущий сервер с помощью команды:

   ```
   reboot
   ```

7. Чтобы освободить место на диске, вы можете удалить папку `/tmp/iwdm`.
8. Если вы обновляетесь с переходом на другой сервер или на новую ОС, скопируйте на другой раздел или на новый сервер каталоги с данными, которые были указаны при установке.

   > **Примечание:**
   >
   > По умолчанию каталоги расположены по пути `/opt`.
   > В версиях **Device Monitor ниже 7.16** каталоги по умолчанию располагались по пути `/mnt`.
   > Обязательно копируйте каталоги с сохранением прав и владельцев. Для копирования используйте стандартные средства, например, утилиту `rsync`.

9. На центральной ноде Платформы распакуйте архив с дистрибутивом Device Control версии 1.5 и выполните команду:

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

Важно!

Так как на сервере установлен также и Activity Monitor, то его установка будет сброшена в результате сброса установки Платформы. При сбросе установки на центральной ноде продукты на офисных нодах перестанут функционировать.

10. Перезагрузите текущий сервер с помощью команды:

```
reboot
```

11. На центральной ноде Платформы установите Activity Monitor версии 3.6 из его же установочного файла с помощью команды:

```
./setup.py install
```

Выполните шаги по установке из инструкции из руководства "Activity Monitor. Руководство по установке", статья "Установка Activity Monitor". Когда инсталлятор потребует указать каталоги для размещения данных, указывайте каталоги с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?»

12. Затем на центральной ноде Платформы установите Device Control версии 1.5 из его установочного файла. Запустить установку вы можете с помощью команды вида:

```
./setup.py install --dmip=<IP_адрес_сервера_Device_Monitor>
```

Далее выполните шаги по установке Device Control.
Точную команду запуска установки Device Control и описание дальнейших шагов вы можете найти в "InfoWatch Device Control. Руководство по установке", статья "Установка Device Control".

13. Убедитесь, что сервер, на котором вы обновляете Device Monitor, соответствует аппаратным и программным требованиям (см. "Аппаратно-программные требования").
14. Убедитесь, что в разделе с папкой `/var/lib/containerd` доступно не менее 30 ГБ дискового пространства.
Чтобы проверить доступное дисковое пространство, используйте команду:

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

15. На офисной ноде Платформы перейдите в каталог, где находится скрипт установки Device Monitor **setup.sh**, и запустите его:

```
./setup.sh
```

Примечание:

В случае ошибки доступа при запуске скрипта, сделайте файл исполняемым, используя команду:

```
chmod +x ./setup.sh
```

Затем запустите скрипт.

16. Выберите **Update**.
17. Выберите опцию для обновления со сбросом – **Update all after you reset DM Front End: install DM Front End and update DM Server Service**.
    Будет установлен компонент DM Front End на базе Платформы и обновлен Сервер Device Monitor.
18. Выберите режим установки Платформы – **Office** (или **Central**, если Device Monitor установлен на центральной ноде).
19. Далее следуйте шагам по установке Платформы из инструкции "Новая установка".
    Когда инсталлятор потребует указать директории для размещения данных, указывайте директории с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?»
20. Дождитесь окончания установки DM Front End и обновления Сервера Device Monitor.
    Автоматически будут произведены следующие действия:
    - получен и записан в Device Monitor открытый ключ службы **guard** Платформы, необходимый для корректного взаимодействия веб-интерфейса с Сервером;
    - исправлен файл **n.yaml**.

    Важно!

    Любой продукт, который будет установлен в Центре расследований после Device Monitor, сгенерирует новый файл **n.yaml**, и из него будет удалена секция, которая необходима для корректного взаимодействия веб-интерфейса с Сервером. Чтобы восстановить **n.yaml**, выполните шаги 21a-21c.

21. Если вы устанавливаете веб-интерфейс на базе Платформы и обновляете Сервер Device Monitor по отдельности, используя опцию установки **DM Front End only** и опцию обновления **DM Server Service only**, то действия с ключом службы **guard** Платформы и файлом **n.yaml** из предыдущего шага не будут выполнены автоматически. После установки Платформы и обновления Сервера осуществите их с помощью инсталлятора. Для этого:
    a. Запустите скрипт установки:

    ```
    ./setup.sh
    ```

    b. Выберите **Utilities** и выполните пункт **Fix n.yaml file**.
    c. Укажите IP-адрес компьютера, на котором был установлен Сервер Device Monitor. Если он был установлен на текущем компьютере, нажмите **Enter**. Дождитесь окончания процесса.
    d. Запустите скрипт установки:

```
./setup.sh
```

e. Выберите в меню пункт **Utilities** и далее **Save platform guard public key to IWDM Service**. Дождитесь окончания процесса.
f. Перезапустите службу **iwdms**:

```
systemctl restart iwdms
```

22. Обновите все установленные второстепенные (**Secondary**) Серверы Device Monitor, выполнив на каждом из них следующие шаги:
    a. Запустите скрипт **setup.sh**:

```
./setup.sh
```

    b. Выберите **Update**.
    c. Выберите **DM Server Service only**.
    d. Дождитесь окончания процесса обновления.
23. Чтобы вывести на экран информацию о Платформе и продуктах в кластере, в директории, где распакован дистрибутив Device Monitor Frontend, выполните команду:

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

24. Если перед обновлением вы выключали отправку уведомлений в Telegram, включите ее снова.

Переход на версию Сервера с поддержкой контейнеризации

Чтобы перейти на версию Сервера Device Monitor с поддержкой контейнеризации:

1. Удалите старые версии Платформы и Сервера согласно статье "Удаление веб-интерфейса и Сервера Device Monitor".

> **Важно!**
>
> Если вы хотите переустановить Сервер на старые данные, не удаляйте Базу данных!

2. Если вы хотите перейти на другой сервер или на новую ОС, скопируйте на другой раздел или на новый сервер каталоги с данными, которые были указаны при установке.

> **Примечание:**
>
> По умолчанию каталоги расположены по пути `/opt`.
> В версиях **Device Monitor ниже 7.16** каталоги по умолчанию располагались по пути `/mnt`.
> Обязательно копируйте каталоги с сохранением прав и владельцев. Для копирования используйте стандартные средства, например, утилиту `rsync`.

3. Установите Сервер Device Monitor согласно статье "Установка "Все-в-одном"".
   Когда инсталлятор потребует указать директории для размещения данных, указывайте директории с данными прошлой версии и выбирайте «**n**» при ответе на вопрос «Очищать ли папки перед установкой?»
   При выборе варианта установки укажите опцию **Container (podman)**.
   Для установки на старые данные, в процессе установки укажите существующую Базу данных.

7.2 Обновление Агентов Device Monitor

Обновление Агентов Device Monitor может быть выполнено:

- на рабочих станциях под управлением **ОС Windows**:
  - локально на каждой контролируемой рабочей станции.
- на рабочих станциях под управлением **ОС семейства Linux**:
  - с помощью задачи распространения в веб-консоли Device Monitor (см. "Задача первичного распространения и обновления");
  - локально на каждой контролируемой рабочей станции.

Обновление Агентов Device Monitor на рабочих станциях под управлением **macOS** не поддерживается. Чтобы перейти на новую версию, необходимо удалить Агент текущей версии и выполнить установку более поздней версии.

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.

Важно!

После обновления необходима перезагрука рабочей станции Агента.

Без перезагрузки возможна некорректная работа:

- контроля буфера обмена, облачных хранилищ, съемных устройств, терминальных сессий, сетевых ресурсов, файлов в приложениях, FTP, мессенджеров;
- блокировки по результатам анализа в Traffic Monitor:
  - передачи веб-почты, почты по протоколам POP, SMTP, IMAP, Outlook, а также сырых HTTP-запросов (Post, Files);

- копирования с/на съемные, сетевые, терминальные устройства, через FTP-протокол, в облачное хранилище;
- печати.

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 Агента на рабочей станции под управлением ОС Windows").

Чтобы локально обновить Агенты на рабочей станции под управлением ОС семейства Linux до новой версии:

1. Выполните *Шаг 1* инструкции по локальной установке (см. "Локальная установка Агента на рабочей станции под управлением ОС семейства Linux").
2. Перейдите в директорию, в которую было распаковано содержимое архива.
3. Запустите скрипт обновления, выполнив команду:

```
sudo ./upgrade.sh [-g '<Proxy_DN>']
```

где `[-g '<Proxy_DN>']` – опциональный параметр для явного указания DN (Issuer Distinguished Name). Используйте его, если хотите задать DN для сертификата прокси. Имя `<Proxy_DN>` должно содержать поле CN (Common Name). Поля внутри имени должны быть разделены запятой.

Примечание:

Значение DN по умолчанию: `' CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow'`
Если вы не используете параметр **`-g`** или укажете значение по умолчанию, то DN в сгенерированном сертификате соединения будет иметь вид:

```
CN = IWDMProxy(<machine_uuid>)
OU = Infowatch TechDep
O = Infowatch
L = Moscow
ST = RU
C = RU
```

где `<machine_uuid>` – это идентификатор рабочей станции, созданный Агентом.

Примечание:

Для вывода справки, выполните команду:

```
sudo ./upgrade.sh -h
```

4. Дождитесь окончания обновления. Проверить статус выполнения можно, выполнив команду:

```
sudo systemctl status "iwdm*"
```

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.

Важно!

Агенты версии 7.13 и более ранних, не поддерживающие новые политики, не будут функционировать до обновления на версию 7.14 и выше. На агенты старых версий не приходят обновления конфигурации.

7.3 Обновление конфигурации на Агентах Device Monitor

Чтобы передать дополнительные настройки технологий перехвата на Агенты без их обновления, используйте утилиту `AgentConfigurationUploader`.

Важно!

Вы можете применить утилиту только для обновления конфигурации контроля мессенджера Telegram. Для ее использования обновите Агенты до версии 7.19 или более поздней (подробнее см. Обновление Агентов Device Monitor).

Запускать `AgentConfigurationUploader.dll` необходимо в директории, где установлен сервер Device Monitor.

Чтобы добавить конфигурацию на Агент, в терминале введите следующую команду:

Команда добавления конфигурации на все Агенты

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString “Server=<Server_name>;
Port=<Port>; Database=<Database_name>; User Id=<User_name>; Password=<Database_password>; “ --ObjectType
```

```
All --Name <Configuration_name> --Description “<Description>” --Format <File_format> --ConfigFile
“<File_path>”
```

где `<Server_name>` – имя сервера, на котором располагается СУБД,

`<Port>` – порт настройки взаимодействия СУБД и Сервера (по умолчанию 5432),

`<Database_name>` – имя базы данных,

`<User_name>` – имя пользователя СУБД,

`<Database_password>` – пароль СУБД,

`<Configuration_name>` – имя конфигурации,

`<Description>` – описание вносимых изменений (любая текстовая информация),

`<File_format>` – формат файла конфигурации,

`<File_path>` – путь к файлу конфигурации. При указании только имени файла путь по умолчанию берется из директории запуска команды.

Пример команды

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString "Server=localhost;
Port=5432; Database=dmdevel; User Id=postgres; Password=pwd; " --ObjectType All --Name telegram --
Description "конфигурация" --Format gz --ConfigFile "D:\\Temp\\tg.gz"
```

Команда добавления конфигурации на определенный Агент

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString “Server=<Server_name>;
Port=<Port>; Database=<Database_name>; User Id=<User_name>; Password=<Database_password>; “ --ObjectType
Workstation --ObjectId “<Workstation_Id>” --Name <Configuration_name> --Description “<Description>” --
Format <File_format> --ConfigFile “<File_path>”
```

где `<Server_name>` – имя сервера, на котором располагается СУБД,

`<Port>` – порт настройки взаимодействия СУБД и Сервера (по умолчанию 5432),

`<Database_name>` – имя базы данных,

`<User_name>` – имя пользователя СУБД,

`<Database_password>` – пароль СУБД,

`<Workstation_Id>` – уникальный идентификатор компьютера с Агентом. Чтобы его узнать:

1. Перейдите в раздел **Группы > Компьютеры**;
2. Откройте консоль разработчика, нажав **F12**;
3. В ней перейдите в **Сеть > Ответ**, дополнительно выбрав **Fetch/XHR**;
4. В столбце **Имя** выберите рабочую станцию;
5. В запросе **GetWorkstation** найдите параметр `id` нужного компьютера и скопируйте его значение

`<Configuration_name>` – имя конфигурации,

`<Description>` – описание вносимых изменений (любая текстовая информация),

`<File_format>` – формат файла конфигурации,

`<File_path>` – путь к файлу конфигурации. При указании только имени файла путь по умолчанию берется из директории запуска команды.

Пример команды

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString "Server=localhost;
Port=5432; Database=dmdevel; User Id=postgres; Password=pwd; " --ObjectType Workstation --ObjectId
"C6D169D8-AA30-4090-8E81-2734D27A700B" --Name telegram --Description "конфигурация" --Format gz --
ConfigFile "D:\\Temp\\tg.gz"
```

> **Примечание:**
>
> Команда добавляет новую конфигурацию, если ее не было ранее, или обновляет существующую.

Чтобы удалить конфигурацию, введите следующую команду:

Команда удаления конфигурации на всех Агентах

```
dotnet AgentConfigurationUploader.dll remove --DbType PostgreSql --ConnectionString “Server=<Server_name>;
Port=<Port>; Database=<Database_name>; User Id=<User_name>; Password=<Database_password>; “ --ObjectType
All --Name <Configuration_name>
```

где `<Server_name>` – имя сервера, на котором располагается СУБД,

`<Port>` – порт настройки взаимодействия СУБД и Сервера (по умолчанию 5432),

`<Database_name>` – имя базы данных,

`<User_name>` – имя пользователя СУБД,

`<Database_password>` – пароль СУБД,

`<Configuration_name>` – имя конфигурации.

Пример команды

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString "Server=localhost;
Port=5432; Database=dmdevel; User Id=postgres; Password=pwd; " --ObjectType All --Name telegram
```

Команда удаления конфигурации на определенном Агенте

```
dotnet AgentConfigurationUploader.dll remove --DbType PostgreSql --ConnectionString “Server=<Server_name>;
Port=<Port>; Database=<Database_name>; User Id=<User_name>; Password=<Database_password>; “ --ObjectType
Workstation --ObjectId “<Workstation_Id>” --Name <Configuration_name>
```

где `<Server_name>` – имя сервера, на котором располагается СУБД,

`<Port>` – порт настройки взаимодействия СУБД и Сервера (по умолчанию 5432),

`<Database_name>` – имя базы данных,

`<User_name>` – имя пользователя СУБД,

`<Database_password>` – пароль СУБД,

`<Workstation_Id>` – уникальный идентификатор компьютера с Агентом. Чтобы его узнать:

1. Перейдите в раздел **Группы > Компьютеры**;
2. Откройте консоль разработчика, нажав **F12**;

3. В ней перейдите в **Сеть > Ответ**, дополнительно выбрав **Fetch/XHR**;
4. В столбце **Имя** выберите рабочую станцию;
5. В запросе **GetWorkstation** найдите параметр `id` нужного компьютера и скопируйте его значение

`<Configuration_name>` – имя конфигурации.

Пример команды

```
dotnet AgentConfigurationUploader.dll add --DbType PostgreSql --ConnectionString "Server=localhost;
Port=5432; Database=dmdevel; User Id=postgres; Password=pwd; " --ObjectType Workstation --ObjectId
"C6D169D8-AA30-4090-8E81-2734D27A700B" --Name telegram
```

8 Удаление Device Monitor

В этом разделе:

1. Удаление веб-интерфейса и Сервера Device Monitor
2. Удаление Агентов Device Monitor

8.1 Удаление веб-интерфейса и Сервера Device Monitor

Чтобы удалить веб-интерфейс Device Monitor:

1. Перейдите в директорию на сервере, в которую был распакован архив с дистрибутивом при установке.
2. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.21:

```
tar xvf data/ui/iw_devicemonitor_setup_7.21.0.310.tar.xz
```

3. Выполните команду:

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

4. Дождитесь завершения удаления. Программа удалит веб-интерфейс Device Monitor.

Удаление Сервера Device Monitor осуществляется с помощью скрипта remove.sh, который располагается в той же директории.

Чтобы удалить Сервер Device Monitor:

1. Запустите скрипт удаления от имени суперпользователя **`root`**:

```
sudo ./remove.sh
```

> **Примечание:**
>
> В случае ошибки доступа при запуске скрипта, сделайте файл исполняемым, используя команду:
>
> ```
> chmod +x ./remove.sh
> ```
>
> Затем запустите скрипт.

2. Подтвердите запрос на удаление, нажав **Y**.
3. Дождитесь остановки службы сервера и определения его типа.

```
Stopping the service iwdms...
Service iwdms stopped
Server role: primary
```

4. Если сервер основной, то подтвердите последующее удаление БД. Нажмите **Y** и введите пароль пользователя БД для подтверждения удаления.
5. Если требуется удалить каталог с файлами журнала (логами), нажмите **Y**.
6. Если требуется удалить каталог файловой очереди, нажмите **Y**. Если ввести **N**, то каталог с теневыми копиями событий будет сохранен, так как в нем могут быть еще не отправленные в Traffic Monitor или Activity Monitor события.
7. Дождитесь окончания процесса удаления, который включает в себя:
    - удаление СУБД. Если на шаге 5 вы ввели **N**, то сервер будет помечен как *устаревший*.
    - удаление каталогов сервера;
    - удаление службы сервера;
    - удаление пользователя *iwdms;*
    - удаление сервиса распространения, если он был установлен.
8. 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.

Важно!

В случае распределенной установки, если продукт установлен на офисной ноде и на данной ноде отсутствуют другие продукты, то после удаления продукта на ноде также рекомендуется удалить элементы платформы. Для этого после выполнения команды `./setup.py remove`, также выполните команду `./setup.py reset`.

Если продукт установлен на центральной ноде или если на офисной ноде также установлены другие продукты, выполнять `./setup.py reset` категорически не рекомендуется.

8.2 Удаление Агентов Device Monitor

В настоящей статье перечислены возможные способы удаления Агента InfoWatch Device Monitor. Удаление Агентов производится локально на рабочих станциях:

- Локальное удаление Агента на рабочей станции под управлением ОС Windows
- Локальное удаление Агента на рабочей станции под управлением ОС семейства Linux
- Локальное удаление Агента на рабочей станции под управлением Mac OS

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.

8.2.1 Локальное удаление Агента на рабочей станции под управлением ОС Windows

В данном подразделе описаны способы локального удаления Агентов InfoWatch Device Monitor на рабочих станциях под управлением ОС Windows:

- Удаление Агента с помощью инструмента "Программы и компоненты"
- Удаление Агента с помощью Microsoft Program Install and Uninstall troubleshooter
- Удаление Агента с помощью Windows Management Instrumentation (WMI)
- Удаление Агента с помощью Windows Management Instrumentation (WMI) и утилиты PsExec

Удаление Агента с помощью инструмента "Программы и компоненты"

Если Агент установлен не в скрытом режиме, то вы можете удалить его следующим способом:

1. Введите **панель управления** в поле поиска на панели задач, а затем в списке результатов выберите **Панель управления**.
2. Выберите **Программы** > **Программы и компоненты**.
3. Выберите в списке **InfoWatch Device Monitor Client**.
4. Щелкните по выбранной строке правой кнопкой и выберите **Удалить**. Затем следуйте инструкциям на экране.

Удаление Агента с помощью Microsoft Program Install and Uninstall troubleshooter

Вы можете использовать данный способ вне зависимости от того, находится Агент в скрытом режиме или нет, но только если не установлен пароль деинсталляции (пароль защиты от удаления). Рекомендуется использовать способ, когда:

- Не удается удалить Агент с помощью перечисленных ранее способов;
- Агент и его части могли остаться в реестре и/или на диске;
- Не получается повторно установить Агент на рабочую станцию.

Чтобы удалить Агент:

1. Скачайте утилиту **Microsoft Program Install and Uninstall troubleshooter** с официального сайта.
2. Запустите утилиту на рабочей станции, где необходимо удалить Агент.
3. Выберите **Удаление** – **InfoWatch Device Monitor Client**.
4. Дождитесь окончания удаления и перезагрузите компьютер.

Удаление Агента с помощью Windows Management Instrumentation (WMI)

Вы можете удалить Агент с помощью Windows Management Instrumentation (WMI). Для этого:

1. Запустите командную строку (`cmd.exe`) от имени администратора.
2. Запустите удаление Агента одним из следующих способов в зависимости от наличия пароля деинсталляции:
    - Если пароль не установлен, выполните команду:

```
wmic product where "Name like '%%Device Monitor client%%'" call uninstall
```

> **Примечание:**
>
> Чтобы запустить процесс удаления в тихом режиме, добавьте к команде параметр `/nointeractive`.
>
> Если пароль все же установлен, то будет предложено ввести его.

- Если пароль установлен:
  a. Узнайте идентификатор Агента с помощью команды:

```
wmic product where "Name like '%%Device Monitor client%%'" get
IdentifyingNumber
```

  b. Выполните команду удаления Агента:

```
msiexec /x {<IdentifyingNumber>} /qn /lvp c:\Windows\dm.log
UNINSTALL_PASSWORD=<пароль>
```

  где `<IdentifyingNumber>` – идентификатор Агента;
  "`/qn`" – параметр, скрывающий графический интерфейс `msiexec`. Если вы хотите наблюдать за процессом удаления, вместо этого используйте параметр "`/q`";
  "`/lvp c:\Windows\dm.log`" – необязательный параметр ведения журнала удаления Агента. Файл "`c:\Windows\dm.log`" приведен в качестве примера, вы можете указать любой другой.

3. Дождитесь окончания удаления, после чего будет сформирован лог-файл с подробной информацией. В случае успешного удаления Агента в лог-файле появится запись вида: *Удаление завершено с состоянием: 0*.
4. Перезагрузите рабочую станцию.

Удаление Агента с помощью Windows Management Instrumentation (WMI) и утилиты PsExec

Данный способ повторяет предыдущий (см. "Удаление Агента с помощью Windows Management Instrumentation (WMI)"), но использует утилиту **PsExec** и позволяет удалить Агент в случае, когда пароль деинсталляции утерян:

1. Скачайте утилиту PsExec с официального сайта.
2. Поместите скачанный файл в директорию `C:\Windows\`.
3. Запустите командную строку (`cmd.exe`) от имени администратора.
4. Узнайте идентификатор Агента с помощью команды:

```
wmic product where "Name like '%%Device Monitor client%%'" get IdentifyingNumber
```

5. Выполните команду удаления Агента:

```
PsExec.exe -i -s msiexec.exe /X {<IdentifyingNumber>} /q /lvp c:\Windows\dm.log
```

где `<IdentifyingNumber>` – идентификатор Агента;
" `/q` " – параметр, запускающий команду в тихом режиме, без взаимодействия с пользователем;
" `/lvp c:\Windows\dm.log` " – необязательный параметр ведения журнала удаления Агента. Файл " `c:\Windows\dm.log` " приведен в качестве примера, вы можете указать любой другой.

6. Дождитесь окончания удаления, после чего будет сформирован лог-файл с подробной информацией. В случае успешного удаления Агента в лог-файле появится запись вида: *Удаление завершено с состоянием: 0*.
7. Перезагрузите рабочую станцию.

8.2.2 Локальное удаление Агента на рабочей станции под управлением ОС семейства Linux

Вы можете локально удалить Агент на рабочей станции под управлением ОС семейства Linux следующими способами:

- Удаление с помощью скрипта
- Удаление средствами ОС

> **Примечание:**
>
> Удаление Агента на рабочих станциях под управлением МОС возможно только средствами ОС.

Удаление с помощью скрипта

Чтобы удалить Агент:

1. Убедитесь, что на рабочей станции есть архив, в котором содержатся пакет и скрипты для установки и удаления Агента. Архив поставляется в составе дистрибутива. Название архива может отличаться в зависимости от используемой ОС, подробнее см. "Локальная установка Агента на рабочей станции под управлением ОС семейства Linux".
   При необходимости скопируйте архив на рабочую станцию и распакуйте его содержимое.

   > **Примечание:**
   >
   > На рабочей станции архив может находиться в директории `/tmp/iwdmupload/`. Также его можно найти на сервере Device Monitor в директории `/opt/iw/iwdistribution/bin/SetupPackages`.

2. Перейдите в директорию, в которую было распаковано содержимое архива.
3. Запустите скрипт:

```
sudo ./remove.sh
```

Пример команды для Агента на ОС Альт:

```
su -c "./remove.sh"
```

В результате будут удалены и Агент Device Monitor, и Агент распространения.

Удаление средствами ОС

Если не удается удалить Агент с помощью скрипта, вы можете удалить его, выполнив следующие команды:

- На ОС Astra Linux:

```
dpkg --purge iwdm
dpkg --purge iwdeployagent
```

- На РЕД ОС и Альт:

```
rpm -e iwdm
rpm -e iwdeployagent
```

- На МОС:

```
rpm -e iwdm
```

8.2.3 Локальное удаление Агента на рабочей станции под управлением Mac OS

Вы можете локально удалить Агент на рабочей станции под управлением Mac OS с помощью скрипта. Для этого:

1. Убедитесь, что на рабочей станции есть архив, в котором содержатся пакет и скрипты для установки и удаления Агента.
   При необходимости скопируйте архив на рабочую станцию и распакуйте его содержимое.
   В нашем примере – `Setup.MacOS-15-iwdm.x86_64.x.x.x.xx.tar.gz`, где `x.x.x.xx` – номер сборки.
2. Перейдите в директорию, в которую было распаковано содержимое архива.
3. Запустите скрипт:

```
sudo ./remove.sh
```

4. Перезагрузите рабочую станцию с помощью команды:

```
reboot
```