

INFOWATCH

InfoWatch Device Monitor for Linux. Руководство по установке

04/06/2025

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 5

2 Комплект документов 6

3 Техническая поддержка пользователей 7

4 Аппаратно-программные требования 8

5 Установка Device Monitor 17

5.1 Состав дистрибутива 17

5.2 Схема развертывания Device Monitor 17

5.3 Подготовка окружения 20

5.3.1 Примеры установки дополнительных пакетов 24

Установка .NET на примере операционной системы Альт 24

Установка .NET на примере операционной системы Astra Linux 24

Установка .NET на примере операционной системы РЕД ОС 25

Установка conntrack и socat на примере операционной системы РЕД ОС 26

5.4 Новая установка 27

5.4.1 Шаги установки в режиме "Все-в-одном" 28

5.4.2 Шаги распределенной установки Device Monitor 32

5.4.3 Подготовка Сервера Device Monitor к миграции с ОС Windows на ОС семейства Linux 35

5.5 Настройка проверки сертификатов удаленных серверов 37

5.5.1 Чтобы настроить проверку сертификатов удаленных серверов при установлении SSL-сессии: 38

5.5.2 Чтобы установить сертификат службы XAPI Traffic Monitor: 38

5.5.3 Чтобы установить сертификат веб-сервера Traffic Monitor: 39

5.5.4 Чтобы установить сертификат службы EPEVENTS Платформы: 40

5.5.5 Просмотр логов 40

5.6 Установка Агентов Device Monitor 41

5.6.1 Локальная установка Агента на рабочей станции под управлением ОС Windows 45

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью MSI-пакета с последующим вводом параметров вручную: 45

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью MSI-пакета в тихом режиме: 46

5.6.2 Локальная установка Агента на рабочей станции под управлением ОС семейства Linux 49

5.6.3 Локальная установка Агента на рабочей станции под управлением Mac OS 51

5.6.4 Установка Агентов с помощью задачи распространения 53

6 Настройка сетевых правил доступа 55

7 Обновление Device Monitor 57
7.1 Обновление Сервера Device Monitor 57
7.2 Обновление Агентов Device Monitor 64
8 Удаление Device Monitor 66
8.1 Удаление Платформы и Сервера Device Monitor 66
8.2 Удаление Агентов Device Monitor 67
8.2.1 Локальное удаление Агента на рабочей станции под управлением ОС Windows 67
Удаление Агента с помощью инструмента "Программы и компоненты" 67
Удаление Агента с помощью Microsoft Program Install and Uninstall troubleshooter 68
Удаление Агента с помощью Windows Management Instrumentation (WMI) 68
Удаление Агента с помощью Windows Management Instrumentation (WMI) и утилиты PsExec 69
8.2.2 Локальное удаление Агента на рабочей станции под управлением ОС семейства Linux 69
Удаление с помощью скрипта 69
Удаление средствами ОС 70
8.2.3 Локальное удаление Агента на рабочей станции под управлением Mac OS 70

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

1 Аудитория

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

2 Комплект документов

В документацию входят:

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

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

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание установки, настройки, обновления и удаления системы InfoWatch Traffic Monitor.
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию системы InfoWatch Traffic Monitor (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, подготовка политик для обработки объектов).
- «InfoWatch Traffic Monitor. Справочник по конфигурационным файлам». Содержит пояснения к часто используемым конфигурационным файлам.

3 Техническая поддержка пользователей

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

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

Часы работы службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

4 Аппаратно-программные требования

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

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

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Сервер Device Monitor на Платформе				
Не менее 100 ГБ свободного пространства для установки. Также понадобится свободное пространство для анализа данных, объем зависит от нагрузки на сервер	От 4 ядер (частота - 3.1 ГГц, разрядность - 64 bit, с поддержкой инструкций SSE 4.2)	От 16 ГБ	ОС: • РЕД ОС 7.3.3; • РЕД ОС 8; • Astra Linux 1.7.5 в редакциях "Орел" и "Смоленск" • Astra Linux 1.8 в редакциях "Орел", "Воронеж" и "Смоленск" • Альт Сервер Виртуализаци	• 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:

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			и СП 10. • Альт Сервер Виртуализации 10.2. СУБД: PostgreSQL версии 11 и более поздних	• "Схема развертывания Device Monitor" • "Подготовка окружения"
Агент Device Monitor для рабочих станций				
Не менее 1 ГБ свободного пространства для установки. Также понадобится свободное пространство для временного хранения файлов, предназначенных для передачи на анализ	От 2 ядер	От 2.5 ГБ	ОС: • [1]Microsoft Windows 7 Service Pack 1; • Microsoft Windows 8 и 8.1; • Microsoft Windows 10; • Microsoft Windows 11; • [1]Microsoft Windows Server 2008 R2; • Microsoft Window	**Поддерживаемые версии ядра Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" и "Смоленск"** • 5.4.0-54-generic • 5.4.0-54-hardened • 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) • 5.10.0-1045-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) • 5.15.0-33-generic • 5.15.0-33-hardened • 5.15.0-70-generic

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			s Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Microsoft Windows Server 2022; • Astra Linux Special Edition 1.7 в редакциях "Орел" (x64), "Воронеж" (x64) и "Смоленск" (x64); • Astra Linux Special Edition	• 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) • 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) **Поддерживаемые версии ядра Astra Linux Special Edition 1.8 в редакциях "Орел", "Воронеж" и "Смоленск"** • 6.1.90-1-generic (начиная с версии 7.17) • 6.6.28-1-generic (начиная с версии 7.17) **Поддерживаемые версии ядра РЕД ОС 7.3** • 5.15.10-1 • 5.15.10-2 • 5.15.10-3 • 5.15.10-4 • 5.15.35-1 • 5.15.35-4 • 5.15.35-5

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			1.8.1.16 в редакциях "Орел" (x64), "Воронеж" (x64) и "Смоленск" (x64); • РЕД ОС 7.3; • РЕД ОС 8.0; • Альт Рабочая станция 10; • Альт Сервер 10.1 с профилем "Офисный сервер"; • Альт Сервер 10.1 СП (сертифицированный);	• 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) • 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) **Поддерживаемые версии ядра 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) **Поддерживаемые версии ядра Альт Рабочая станция 10** • 5.10.133-std-def-alt1 • 5.10.135-std-def-alt1

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			• macOS Sequoia 15.1; • macOS Sequoia 15.2; • macOS Sequoia 15.3.	• 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)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 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) • 5.15.94-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

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 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)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 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) • 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)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 6.1.140-un-def-alt1 (начиная с версии 7.17.4)
Веб-консоль Device Monitor				
	Дополнительно 1 ядро	1 ГБ на каждую вкладку браузера	Браузеры: • Google Chrome • Яндекс. Браузер	В браузере должна быть реализована аппаратная поддержка WebGL/ WebGL2 Платформа версии 1.7 и выше

Примечание:

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

Примечание:

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

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

5 Установка Device Monitor

Рекомендуется соблюдать следующий порядок установки:

1. Подготовка окружения.
2. Установка Платформы 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

В состав дистрибутива Device Monitor входят следующие компоненты:

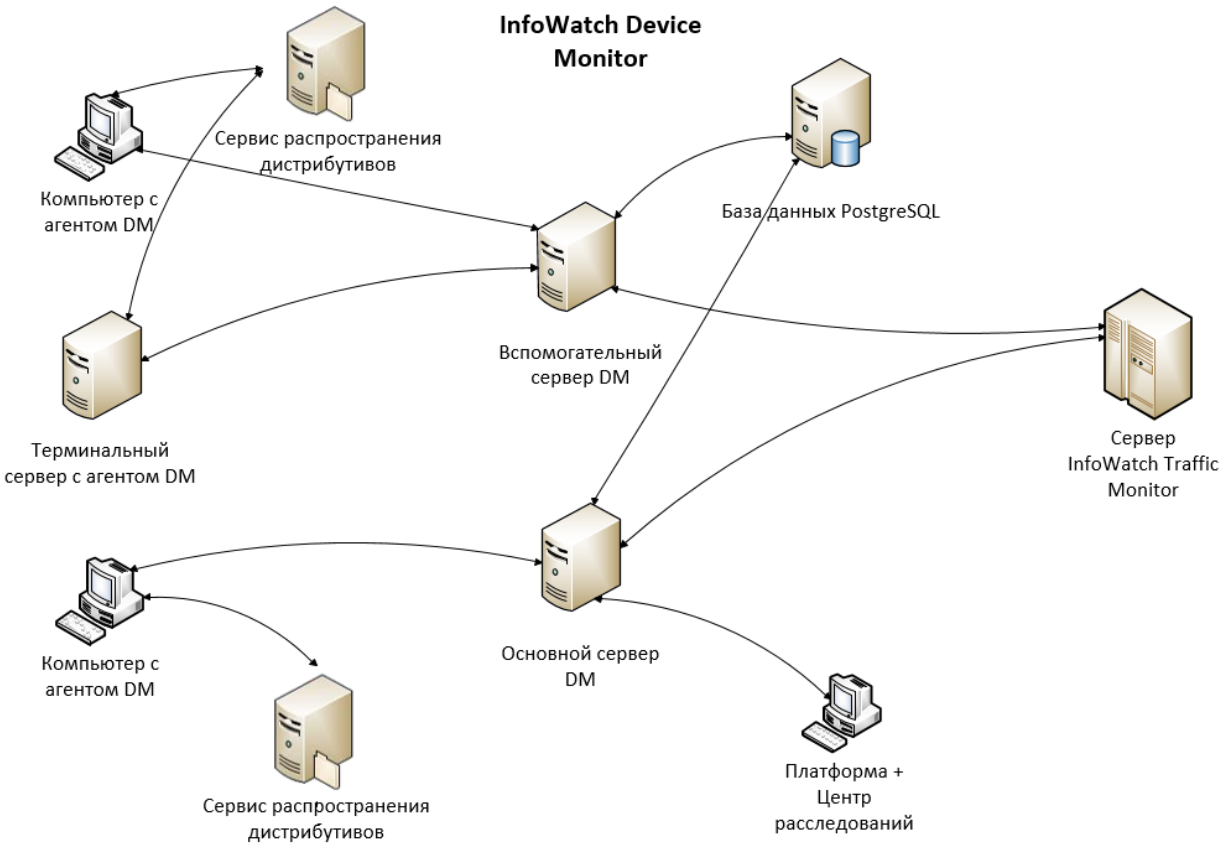
- `data/iwdms` – содержит архив с исполняемыми файлами Сервера Device Monitor и скрипт для его установки с поддержкой установки через параметры командной строки.
- `data/scripts/include` – содержит вспомогательные скрипты, необходимые для корректной работы `setup.sh` и `install_iwdms.sh`;
- `data/ui` – 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 следующей таблице:

Компонент	Назначение
InfoWatch Device Monitor Client (клиентское приложение InfoWatch Device Monitor, Агент)	Перехват действий сотрудников на контролируемых рабочих станциях
InfoWatch Device Monitor Server (сервер InfoWatch Device Monitor, Сервер)	Конфигурирование клиентских приложений, сбор данных от клиентских приложений и передача этих данных системе InfoWatch Traffic Monitor, распространение deploy-агентов на рабочие станции
InfoWatch Device Monitor Database (база данных)	Хранение информации, необходимой для работы Device Monitor
Центр расследований	Управление модулями Device Monitor и Device Control
Сервис распространения дистрибутивов (Сервис распространения)	Получение и хранение новой версии дистрибутива агента Device Monitor

Взаимодействие компонентов Device Monitor показано на рисунке:



Для повышения производительности Device Monitor следуйте рекомендациям:

- Используйте кластеризацию. При этом одна схема базы данных будет использоваться несколькими серверами для хранения и распространения общей схемы безопасности.
- Сервер и база данных могут находиться на одном компьютере. Однако для увеличения производительности рекомендуется размещать базу данных и сервер на разных компьютерах.
- Если используется виртуализация, размещайте диски виртуальных машин на разных дисковых полках.

Консоль управления может подключаться только к основному серверу. Используя Консоль управления можно управлять всеми серверами в кластере.

Система разворачивается и работает следующим образом:

1. Первой устанавливается центральная нода **Платформы** с веб-интерфейсом **Центра расследований**, где выполняется настройка схемы безопасности в соответствии с требованиями корпоративной политики безопасности**.**
2. **На Платформу** устанавливается **основной сервер Device Monitor**.
3. При установке основного сервера определяют используемый сервер **базы данных**: СУБД может располагаться как отдельно, так и на том же компьютере, что и основной сервер, а также создается **схема базы данных**, где будет храниться **схема безопасности** и другие параметры Device Monitor.
4. При необходимости, можно установить **вспомогательные серверы**, которые будут обеспечивать балансировку нагрузки.

5. **Сервис распространения дистрибутивов** устанавливается вместе с **основным сервером Device Monitor** по умолчанию, имеет хранилище с дистрибутивами Агентов для используемых ОС и платформы. Сервис может быть установлен и со **вспомогательными серверами Device Monitor**.
6. С **основного сервера** на **рабочие станции** распространяются deploy-агенты (агентом распространения) Device Monitor, которые затем скачивают дистрибутивы Агентов с ближайшего **сервиса распространения** из указанных точек публикации дистрибутивов. Скачивание Агентов может происходить параллельно несколькими рабочими станциями одновременно.
7. Агенты выполняют подключение к серверу Device Monitor по зашифрованному каналу, с привязкой к серверу на основании ключа, используемого для шифрования трафика. Агенты Device Monitor обеспечивают реализацию схемы безопасности, а также получение теневых копий и их отправку на сервер Device Monitor.
8. Серверы Device Monitor получают из базы данных обновленные версии схемы безопасности и распространяют их на контролируемые рабочие станции. С контролируемых рабочих станций на сервер передается информация о событиях, подпадающих под действие правила схемы безопасности, а также теневые копии файлов. Информация о событиях передается в базу данных. Теневые копии передаются в систему InfoWatch Traffic Monitor.

Пример 1

1. Сотрудник, работающий на контролируемой рабочей станции, обращается к контролируемому периферийному устройству (например, дает команду распечатать документ через USB принтер).
2. Агент проверяет, имеет ли сотрудник право на работу с периферийным устройством. Если такого разрешения нет, то сотруднику будет отказано в доступе к устройству (в рассматриваемом случае документ не будет отправлен на печать).

Печать документов на локальных и сетевых принтерах отслеживается перехватчиком Print Monitor. Копия задания на печать передается в InfoWatch Traffic Monitor для анализа. Отправка документов на печать возможна при условии, что сотруднику разрешен доступ к принтеру (проверяется перехватчиком Device Monitor).

Пример 2

В Device Monitor задано правило, отслеживающее запись в PDF-файл на съемном устройстве. В правиле указано, что при выполнении этой операции должна создаваться теневая копия документа.

1. Сотрудник, работающий на контролируемой рабочей станции, выполняет действия, приводящие к записи в файл на съемном устройстве (например, копирует файл на USB Flash Drive).
2. Если операция записи в файл на съемном устройстве успешно завершена, то Агент InfoWatch Device Monitor генерирует событие и создает теневую копию файла.
3. Если создать теневую копию файла невозможно (например, при отсутствии свободного места на жестком диске), операция записи в файл на съемном устройстве будет произведена без создания теневой копии, о чем будет указано в информации о событии.
4. Агент передает данные (событие и теневую копию файла) на Сервер InfoWatch 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.

Попытки записи в файлы на съемных устройствах отслеживаются перехватчиком File Monitor. Полученные сведения передаются затем в InfoWatch Traffic Monitor для анализа. В то же время доступ к съемному устройству контролируется перехватчиком Device Monitor. Поэтому сотрудник может выполнять операцию записи в файл только на тех съемных устройствах, к которым у него есть доступ.

Пример 3

В Device Monitor задано правило, отслеживающее печать DOC-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 InfoWatch 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 InfoWatch 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. Ввести в домен компьютер, на который будет установлен Сервер Device Monitor.
2. Удостовериться, 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 или Альт 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. Установить Microsoft .NET 6 (https://dotnet.microsoft.com/) на этом компьютере.
4. Для повышения производительности увеличить максимальное число экземпляров подсистемы Inotify, которое может задать пользователь (`max_user_instances`), до 512.
5. Установить пакеты `conntrack` (или `conntrack-tools`) и `socat`.
6. Настроить антивирус для совместной работы с Системой (см. статью Базы знаний "Настройка антивируса для Device Monitor Server на ОС Linux").
7. Настроить правила POD сети или отключить межсетевой экран (см. статьи Базы знаний "Конфликты при взаимодействии firewalld и Kubernetes", "Полное отключение межсетевого экрана").
8. Установить интерпретатор языка Python версии 2.7. Пакет с интерпретатором не входит в состав дистрибутива продукта.
9. **Если установка проводится на ОС Альт:**

- Установить утилиту `unzip` аналогично установке `conntrack` и `socat`;
- Установить пакет с интерпретатором языка Python версии 2.7, а также следующие пакеты:
  - `python-modules-json`
  - `python-modules-distutils`
  - `python-modules-sqlite3`

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

- Настроить соответствие алгоритмов шифрования Сервера Device Monitor и Сервера Traffic Monitor. Для этого измените файл `/etc/openssl/openssl.cnf` следующим образом:
  - 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
```

10. 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
      ```

    - ОС Альт:

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

11. Установить 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 yum update
       ```

    b. Установите и инициализируйте СУБД, выполнив команды:

       ```
       sudo yum install postgresql
       sudo yum 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
       ```

    d. Задайте пароль для пользователя `postgres`. Для этого:

i. Авторизуйтесь пользователем `postgres`:

```
su - postgres
```

ii. Запустите программу `psql`:

```
psql
```

iii. Введите команду задания пароля:

```
\password postgres
```

iv. Дважды введите новый пароль.
v. Выйдите из программы **psql** и смените пользователя **postgres**:

```
\q
exit
```

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.

12. Подготовить СУБД:
    a. Выполните настройки в конфигурационном файле `postgresql.conf`. Для более точного подбора параметров используйте калькулятор PGTune.
        - Присвойте параметру `"max_connections"` значение 250.
        - Настройте ротацию логов.
        - Укажите прочие параметры, оптимизирующие быстродействие (потребление ресурсов памяти, настройки WAL, планирование запросов), согласно официальной документации PostgreSQL.
    b. Если вы устанавливаете СУБД на отдельном от Device Monitor сервере:
        i. Настройте доступ к СУБД в файле `pg_hba.conf` согласно официальной документации PostgreSQL.
        ii. Перезапустите службу **postgresql**.
        Пример команды для РЕД ОС:

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

13. 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.

14. 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:

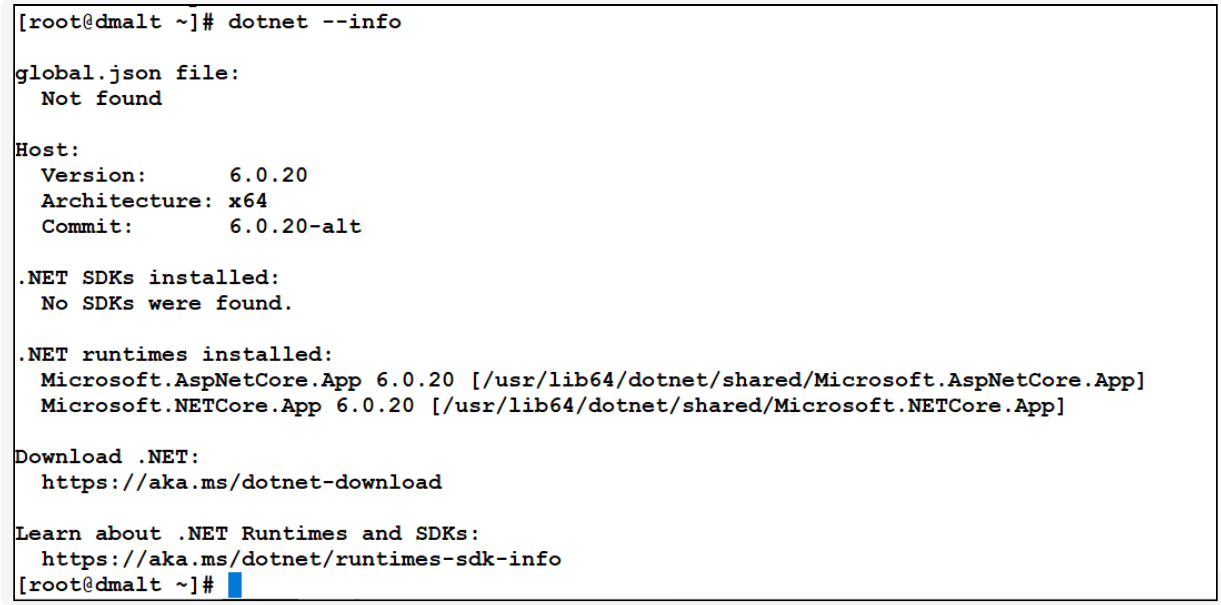
```
apt-repo list
```

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 6 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:

```
apt-get install dotnet-aspnetcore-runtime-6.0
```

   В результате будет установлена среда выполнения .NET 6 с поддержкой ASP.NET Core.
5. Проверьте установленный NET 6, выполнив команду:

```
dotnet --info
```



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 6 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:

```
apt install dotnet-aspnetcore-runtime-6.0
```

   В результате будет установлена среда выполнения .NET 6 с поддержкой ASP.NET Core.
5. Проверьте установленный NET 6, выполнив команду:

```
dotnet --info
```

```
root@dmAstra:~# dotnet --info

global.json file:
  Not found

Host:
  Version:      6.0.10
  Architecture: x64
  Commit:       5a400c212a

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 6.0.10 [/usr/lib/dotnet/dotnet6-6.0.110/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 6.0.10 [/usr/lib/dotnet/dotnet6-6.0.110/shared/Microsoft.NETCore.App]

Download .NET:
  https://aka.ms/dotnet-download

Learn about .NET Runtimes and SDKs:
  https://aka.ms/dotnet/runtimes-sdk-info
root@dmAstra:~#
```

Установка .NET на примере операционной системы РЕД ОС

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

```
dnf repoinfo
```

2. Установите среду выполнения NET 6 с необходимой поддержкой ASP.NET Core. Для этого в терминале выполните команду:

```
sudo yum install aspnetcore-runtime-6.0
```

   В некоторых дистрибутивах Linux имя пакета может быть `dotnet-aspnetcore-runtime-6.0`
   В результате будет установлена среда выполнения .NET 6 с поддержкой ASP.NET Core.

3. Проверьте установленный NET 6, выполнив команду:

```
dotnet --info
```



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

4. Удалите из операционной системы все пакеты, связанные с .NET, выполните команду:

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

5. Установите заново конкретную версию .NET, например:

```
sudo dnf install aspnetcore-runtime-6.0-6.0.5-1.el7
```

6. Чтобы посмотреть список доступных версий, выполните:

```
dnf --showduplicates list aspnetcore-runtime-6.0
```

Установка `conntrack` и `socat` на примере операционной системы РЕД ОС

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

1. Введите в командной строке:

```
conntrack
```

В ответ будут выведены сведения о работе и актуальная версия этого пакета.

2. Если `conntrack` не установлен, следует установить его с помощью команды:

```
sudo yum install conntrack
```

3. Если пакет недоступен в репозитории, скачайте его, перейдите в директорию с пакетом и установите вручную с помощью команды вида:

```
rpm -Uhv ./<имя_пакета>
```

4. Повторите описанные выше действия для установки пакета `socat` .

5.4 Новая установка

Основой для установки Device Monitor является Платформа. Инсталлятор каждого продукта содержит и Платформу, и продуктовые компоненты. Обе части обязательны к установке при развертывании продуктов.
И продуктовые компоненты, и Платформа поддерживают установку в двух режимах:

- **`central`** ;
- **`office`** .

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

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

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

- общий доступ к данным независимо от того, на каком из них выполнена интеграция с источником, а также доступ к обработанным данным.

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

Возможные режимы установки Device Monitor:

- Установка "**Все-в-одном**" предполагает размещение Платформы с веб-интерфейсом Центра расследований и Сервера Device Monitor на одном физическом сервере.

  > **Важно!**
  >
  > Если вы переходите на Device Monitor for Linux с ОС Windows и вам необходима миграция данных:
  >
  > - 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".
  > - На шаге 25 инструкции 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".

- **Распределенная** установка Сервера Device Monitor на офисную ноду Платформы на отдельном сервере.

5.4.1 Шаги установки в режиме "Все-в-одном"

Режим подходит для новой чистой установки Device Monitor, а также при переходе на Device Monitor for Linux с ОС Windows.

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям ("Аппаратно-программные требования").

   > **Примечание:**
   >
   > В ходе установки инсталлятор проверит наличие:
   > - не менее 100 ГБ на диске для директорий, которые будут указаны далее в пп. 15-18. Если директории для хранения данных находятся на разных дисках, то проверятся наличие 100 ГБ свободного места на каждом из них;
   > - не менее 20 ГБ на диске для директорий с образами;
   > - не менее 16 ГБ ОЗУ;
   > - не менее 4 ядер процессора;
   > - поддержки инструкции SSE 4.2;

- установленного пакета **`conntrack`**.

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_7.17.0.310.tar.gz -C /dmsl_distr
```

5. Перейдите в созданную директорию.
6. Добавьте файлу **setup.sh** атрибут "*исполняемый*":

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

7. Запустите скрипт **setup.sh**, который входит в состав дистрибутива:

```
./setup.sh
```

После этого будут доступны действия:
- **Install** – новая установка Платформы и Центра администрирования
- **Update** – обновление установленных компонентов
- **Utilities** – переход в меню утилит
- **Exit** – выход из программы

8. Выберите тип установки Install. Будет доступен список компонентов:
   - **DM Server Service, FrontEnd** – установка "все-в-одном" при отсутствии установленной Платформы либо другого Сервера Device Monitor
   - **Only FrontEnd** – установка только Платформы и веб-интерфейса Центра администрирования
   - **Only DM Server Service** – установка только Сервера Device Monitor
9. Выберите **DM Server Service, FrontEnd**. В этом случае 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 37-39.

   Будут предложены режимы установки Платформы с веб-интерфейсом Центра расследований:
   - **Central** – предназначен для установки на основную ноду или в случае отсутствия уже установленного Центра расследований.
   - **Office** – предназначен для распределенной установки.
10. Выберите режим **Central**. Начнется процесс установки Платформы

11. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
12. Введите **y**, чтобы принять лицензионное соглашение, и нажмите **Enter**.
13. Введите IP-адрес сервера в формате IPv4: `"xxx.xxx.xxx.xxx"` и нажмите **Enter**.
14. Выделите объем оперативной памяти для размещения данных ClickHouse (по умолчанию 80%) и нажмите **Enter**.
15. Укажите путь для размещения данных ClickHouse (по умолчанию: `/opt/chdata`) и нажмите **Enter**.
16. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/opt/pgdata`) и нажмите **Enter**.
17. Укажите путь для размещения данных NATS (по умолчанию: `/opt/natsdata`) и нажмите **Enter**.
18. Укажите путь для хранения данных (по умолчанию `/opt/dsdata`) и нажмите **Enter**.
19. Укажите порт подключения к веб-интерфейсу (по умолчанию `443`) и нажмите **Enter**.
20. 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 Центре администрирования
    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**
21. Выберите язык устанавливаемого сервера и нажмите **Enter**. Это определит названия предустановленных групп, политик и правил.
22. Ознакомьтесь с лицензионным соглашением и выберите необходимое действие. Для продолжения установки необходимо принять лицензионное соглашение. Выберите **Accept and continue** и нажмите **Enter**
23. Далее можно выбрать, какой тип сервера необходимо установить: **Primary** (основной) или **Secondary** (второстепенный).
24. Если вы устанавливаете Систему впервые или переходите с Device Monitor, установленном на ОС Windows, выберите **Primary**. Для установки второстепенного сервера выполните шаги 27-31 и далее начиная с шага 35.
25. Настройте взаимодействие с Базой данных:
    - **Create 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**.
26. 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.
27. Укажите порт для настройки взаимодействия. Если порт не указан, будет использован порт по умолчанию – `5432`.

28. Введите имя базы данных. По умолчанию – `iwdm`.
29. Введите имя пользователя СУБД. По умолчанию – `postgres`.
30. Введите пароль.
31. Если на шаге 24 вы выбрали **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`
32. Введите адрес InfoWatch Traffic Monitor (IWTM). Для этого используйте имя сервера или его IP-адрес.
    Если взаимодействие с Traffic Monitor не планируется, то введите любое не существующее в вашей сети имя сервера.

    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).

33. Введите токен доступа к IWTM. 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").
    Если взаимодействие с Traffic Monitor не планируется, то введите любое значение токена.
34. Укажите **Yes**, чтобы установить сервис распространения дистрибутивов. В этом случае точка распространения сможет распространять дистрибутивы агентов на рабочие станции;
35. 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.
36. 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**

37. Если вы далее будете устанавливать другой продукт InfoWatch, то необходимо прописать в файл **n.yaml** настройки, получить открытый ключ службы **nguard** Платформы и сохранить его в каталог Сервера. Введите IP-адрес Сервера Device Monitor, а затем запустите скрипт установки:

```
./setup.sh
```

38. Выберите в меню пункт **Utilities**. Раздел содержит утилиты:
    a. **Fix n.yaml file** – 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 прописать в **n.yaml** необходимые настройки. Это действие следует производить после установки любого продукта в Центр расследований;
    b. **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;
    c. **Show IWDM Service version** - утилита показывает версию установленного сервера;
    d. **Export ssl key** – утилита позволяет экспортировать ключ защиты канала "агент-сервер".
39. Выберите **Fix n.yaml file**. Дождитесь окончания процесса.
40. Запустите скрипт установки:

```
./setup.sh
```

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

```
systemctl restart iwdms
```

Распределенная установка используется в случаях, если в организация использует также и другие продукты InfoWatch или имеет филиальную структуру с центральным офисом и филиалами. В этом случае необходимо дополнительно установить один или несколько Серверов Device Monitor на другие компьютеры с офисными ноды Платформы с другими установленными продуктами InfoWatch.

5.4.2 Шаги распределенной установки Device Monitor

1. Проверьте, соответствует ли сервер аппаратным и программным требованиям ("Аппаратно-программные требования").

> **Примечание:**
>
> В ходе установки инсталлятор проверит наличие:

- не менее 100 ГБ на диске для директорий, которые будут указаны далее на шаге 16. Если директории для хранения данных находятся на разных дисках, то проверятся наличие 100 ГБ свободного места на каждом из них;
- не менее 20 ГБ на диске для директорий с образами;
- не менее 16 ГБ ОЗУ;
- не менее 4 ядер процессора;
- поддержки инструкции SSE 4.2;
- установленного пакета **`conntrack`**.

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_7.17.0.310.tar.gz -C /dmsl_distr
```

5. Перейдите в созданную директорию.
6. Добавьте файлу **setup.sh** атрибут "*исполняемый*":

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

7. Запустите скрипт **setup.sh**, который входит в состав дистрибутива:

```
./setup.sh
```

8. Выберите тип установки **Install**. Будет доступен список компонентов:
9. Выберите **DM Server Service, FrontEnd**. В этом случае 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`**:
>
> a. Запустите скрипт установки:
>
> ```
> ./setup.sh
> ```
>
> b. Выберите в меню пункт **Utilities**.
> c. Выберите **Fix n.yaml file**. Дождитесь окончания процесса.

Будут предложены режимы установки Платформы с веб-интерфейсом Центра расследований:
    - **Central** – предназначен для установки на основную ноду или в случае отсутствия уже установленного Центра расследований.
    - **Office** – предназначен для распределенной установки.
10. Выберите **Office**.
11. Введите IP-адрес центральной ноды Платформы, установленной ранее.
12. Получите токен центральной ноды. Для этого на сервере с центральной нодой выполните команду:

    ```
    kubeadm token list
    ```

13. Скопируйте полученный токен. Начнется установка Платформы.
14. Введите полученный токен на ноде офисной Платформы.
15. Укажите лейбл для офисной ноды Платформы
16. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
17. Введите **y**, чтобы принять лицензионное соглашение, и нажмите **Enter**.
18. Введите IP-адрес сервера в формате IPv4: `"xxx.xxx.xxx.xxx"` и нажмите **Enter**.
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 порт подключения к веб-интерфейсу (по умолчанию `443`) 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 Центре администрирования
    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. Далее можно выбрать, какой тип сервера необходимо установить: Основной (**Primary**) или Второстепенный (**Secondary**).
29. Если вы выбрали основной сервер (**Primary**), 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`
30. Если вы устанавливаете Сервер на новую БД, то ключ шифрования необходимо создать. Выберите **Yes**.

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, введя в браузере IP-адрес центральной ноды Платформы.

5.4.3 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 7.17 (подробнее см. "Документация для модуля InfoWatch Device Monitor, установленного на ОС MS Windows", статья "Обновление серверной части InfoWatch Device Monitor")
2. Убедитесь, что База данных поддерживает миграцию, т.е. не содержит правил, которые не поддерживаются в новой версии. Для этого:
    a. В дистрибутиве по пути `7.17.x\DM for Windows\Utils` скопируйте архив `CheckMigration_x64.zip`.
    b. Распакуйте архив.
    c. В файле `run.bat` укажите параметры доступа к Базе данных.
    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*. Если утилита выведет список правил, которые не поддерживаются в новой версии, то необходимо:
        - удалить эти правила
          или
        - в текущей Консоли Офицера безопасности настроить параметры так, чтобы поддержка осуществлялась.

3. Проверьте, что и указанная в параметрах СУБД PostgreSQL для сервера Device Monitor на ОС Windows, и СУБД PostgreSQL сервера Device Monitor, установленного на ОС Linux, созданы и установлены **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  |
   ```

4. Если установлена английская локаль, то выполните действия, чтобы установить русскую:
   a. 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"
      ```

   b. Запустите файл `run.bat` с компьютера, где установлен основной Сервер Device Monitor.
5. 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:

- Автоматическое создание снимков экрана для списков приложений и ресурсов
- Контроль ввода текста с клавиатуры для списка ресурсов
- Контроль активности сотрудника по сбору статистики действий: пользователя, с файлами, отправки на печать
- Контроль звукового окружения
- Контроль мессенджеров: MMP, Facebook
- Контроль копирования с/на CD/DVD
- Запрет создания снимков экрана для всех приложений или списков приложений
- Контроль файловых операций при теневом копировании файлов, передаваемых в приложениях

- Контроль приложений: запрет запуска, использования буфера обмена, печати
- Запись видео экрана рабочей станции по триггеру

Неподдерживаемые настройки:

- параметров AD и параметров серверов, подключение к которым разрешено
- автоматического обновление Агентов
- отправки событий с Агента в Activity Monitor
- ключа формирования кодов
- подключения для получения управляющих команд от Activity Monitor
- перехвата звукового окружения

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 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 Чтобы установить сертификат службы XAPI Traffic Monitor:

1. На сервере Traffic Monitor откройте файл `/opt/iw/tm5/etc/xapi.conf`.
2. В секции **ThriftServers** -> **xapi** найдите параметр `TrustedCertificatesPath`.
   В значении данного параметра указаны путь к файлу корневого сертификата и его имя. Если указан относительный путь, то его необходимо рассматривать от каталога `/opt/iw/tm5`.
   Значение параметра `TrustedCertificatesPath` по умолчанию: `/opt/iw/tm5/etc/cert/trusted_certificates`.
3. Скопируйте корневой сертификат на компьютер, где установлен или будет установлен сервер Device Monitor.

4. Перейдите в директорию, куда был скопирован корневой сертификат.
5. Переименуйте корневой сертификат в `tmca.crt`.
6. Введите команды в зависимости от операционной системы, в среде которой производится установка корневого сертификата:
   - Для операционной системы РЕД ОС:

     ```
     sudo cp tmca.crt /etc/pki/ca-trust/source/anchors/
     sudo update-ca-trust force-enable
     sudo update-ca-trust extract
     ```

   - Для операционной системы Альт:

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

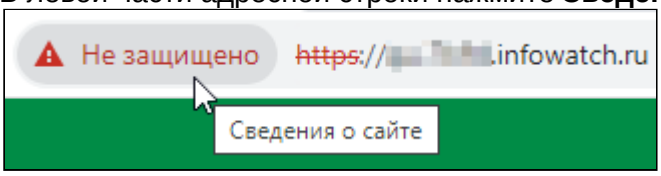
   - Для операционной системы Astra Linux:

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

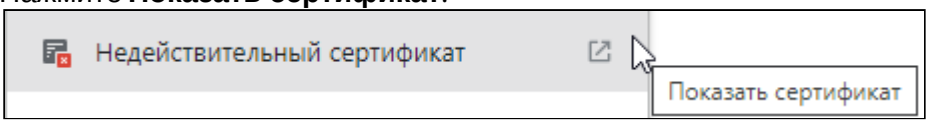
     Выполнение команд может занять некоторое время.

5.5.3 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 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.

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.

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

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

7. 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");
8. **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:

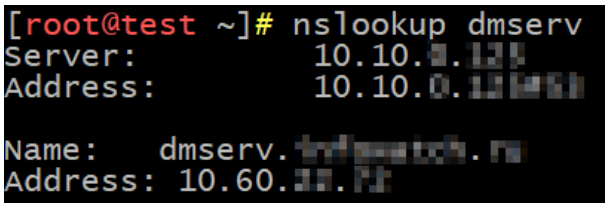
- разрешены символы латинского алфавита (A-Z,a-z), цифры (0-9) и дефис;
- длина имени должна быть не более 15 символов.

9. 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.

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

Примечание:

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.

Примечание:

Запуск Агента InfoWatch Device Monitor осуществляется автоматически сразу после установки. До перезагрузки компьютера функционал Агента ограничен только:

- перехватом трафика, проходящего через proxy-сервер,
- сетевым перехватом (при установке Агента на ОС Windows 8 и более поздние),
- перехватом копирования на внешние носители.

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

- `iwdm` – используется основной службой Device Monitor;

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

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

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

5.6.1 Локальная установка 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 InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью MSI-пакета с последующим вводом параметров вручную:

1. **Запуск мастера установки**
   Вставьте внешний носитель с дистрибутивом Агента в компьютер. Затем откройте каталог `Client`. В данном каталоге найдите и запустите пакет установки для требуемой платформы для развертывания в соответствии с заданными при формировании пакетов параметрами, например, `InfoWatch.DeviceMonitor.Client.7.17.0.x64.msi`.
   В результате на экран будет выведено окно приветствия мастера установки InfoWatch Device Monitor Client. Нажмите на кнопку **Далее**, чтобы перейти к следующему окну мастера установки.
2. **Выбор каталога для установки**
   Укажите путь к каталогу, в который будет установлен **Агент**.

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

   Нажмите кнопку **Далее**.

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

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

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС 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!
	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.

Ключ	Описание
	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; • `"-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:**

Ключ	Описание
	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: • `"0"` (по умолчанию) – установить компонент • `"1"` – не устанавливать компонент
`NOIWNBG`	Не устанавливать компонент контроля периметра сети. Возможные значения: • `"0"` (по умолчанию) – установить компонент • `"1"` – не устанавливать компонент

Ключ	Описание
`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.
`/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.7.17.0.192.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.7.17.0.192.log
   ```
2. Дождитесь завершения установки.
3. Перезагрузите компьютер.

5.6.2 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 10 - 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.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.7;
        - `Setup.AstraLinux-1.8-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.8;
        - `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz` - для РЕД ОС 7.3.1;
        - `Setup.RedOS-8.0-iwdm.x64.x.x.x.xx.tar.gz` - для РЕД ОС 8.0;
        - `Setup.AltLinux-10.0-iwdm.x64.x.x.x.xx.tar.gz` - для Альт Рабочая станция 10.

        где `x.x.x.xx` - номер сборки.
        Далее мы рассмотрим пример установки Агента на РЕД ОС 7.3. Установка на других поддерживаемых ОС аналогична. Примеры команд для них приведены ниже.
    c. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки:
    ```
    sudo tar -xvzf Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz
    ```
    В результате будут созданы файлы `install.sh`, `remove.sh`, `upgrade.sh`, `iwdm_<версия_агента>.deb`.
2. **Установка Агента InfoWatch Device Monitor:**
    a. Перейдите в директорию, в которую распаковано содержимое архива **`Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`**.
    b. Для установки Агента запустите скрипт, выполнив команду:
        - Для обычной установки (при этом будет установлен компонент перехвата сетевого трафика):
        ```
        sudo ./install.sh <сервер>:<порт>
        ```
        где `<сервер>` - ip-адрес или доменное имя Сервера InfoWatch Device Monitor, `<порт>` - порт подключения к Серверу InfoWatch Device Monitor.
        В нашем примере команда будет следующей:
        ```
        sudo ./install.sh dm-server:15101
        ```
        Продукт будет установлен в директорию `/opt/iw/dmagent`.
        - 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:

1. **ОС Astra Linux:**
   a. Распаковка архива:
   `sudo tar -xvzf Setup.AstraLinux-1.7-iwdm.x64.x.x.x.xx.tar.gz`
   b. Запуск установки:
   `sudo ./install.sh dm-server:15101`
   В случае установки без компонента перехвата сетевого трафика:
   `sudo IWDM_NO_PROXY=1 ./install.sh dm-server:15101`
   c. Проверка статуса сервисов:
   `sudo systemctl status "iwdm*"`
2. **ОС Альт:**
   a. Распаковка архива:
   ```
   tar -xvzf Setup.AltLinux-10.0-iwdm.x64.x.x.x.xx.tar.gz
   ```
   b. Запуск установки:
   ```
   su -c "./install.sh dm-server:15101"
   ```
   В случае установки без компонента перехвата сетевого трафика:
   ```
   su -c "IWDM_NO_PROXY=1 ./install.sh dm-server:15101"
   ```
   c. Проверка статуса сервисов:
   `su - -c 'systemctl status "iwdm*"'`

5.6.3 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
```

5.6.4 Установка Агентов с помощью задачи распространения

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

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 "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 → 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!

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:

Компонент Системы, для работы которого необходимо соединение	Взаимодействие между компонентами		Порт	Назначение порта	
	Источник	**Получатель**			
Сервер Device Monitor (DM)	Платформа	Сервер DM	TCP 15007	Взаимодействие Платформы с Сервером DM	
	Сервер DM	Сервер БД	TCP 5432	Взаимодействие Сервера DM с базой данных	
	Агент DM	Сервер DM	TCP 15004	Защищенное соединение Сервера DM с Агентами	Передача теневых копий (шифрованный канал)
	Агент DM	Сервер DM	UDP 15100		Уведомление Агентов
	Сервер DM	Агент DM			
	Агент DM	Сервер DM	TCP 15101		Передача теневых копий
	Агент DM	Сервер DM	TCP 15200	Инициация загрузки дистрибутива Агента с Сервера DM на рабочую станцию	
	Сервер DM	Агент DM	TCP 15505	Установка и удаление Агента	
	Рабочая станция Офицера безопасности	Платформа	TCP 443	Взаимодействие Офицера безопасности с Веб-консолью Сервера DM	
Агент DM на ОС семейства Linux	Сервер DM	Рабочая станция сотрудника	TCP 22	Установка Агента	

Примечание:

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

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

или

- измените их на порты из таблицы:

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

7 Обновление Device Monitor

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

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

7.1 Обновление Сервера Device Monitor

Важно!

Обновление с версий **7.15** и **7.16** поддерживается только **со сбросом** установки компонента **FrontEnd**.

С версии **7.17.x** вы можете использовать **прямое** обновление.

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
- Прямое обновление Сервера Device Monitor (с версии 7.17.x)

Обновление Сервера Device Monitor со сбросом установки

Чтобы обновить Сервер Device Monitor:

1. Скопируйте архив с дистрибутивом Сервера Device Monitor на жесткий диск.
2. 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_7.17.0.296.tar.gz -C /tmp/dmsl_distr
   ```

3. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.17. В примере файл будет извлечен в каталог `/tmp/iwdm` :

   ```
   mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.17.0.296.tar.xz -C /tmp/iwdm
   ```

4. 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.
5. Перезагрузите сервер с помощью команды:

```
reboot
```

Если у вас были установлены несколько продуктов InfoWatch, перезагрузите все серверы.

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

      > **Примечание:**
      >
      > В **Device Monitor 7.15 и более ранних** каталоги по умолчанию расположены по пути **`/mnt`**.
      > В **Device Monitor 7.16** – по умолчанию по пути **`/opt`**.
      > Обязательно копируйте каталоги с сохранением прав и владельцев. Для копирования используйте стандартные средства, например, утилиту **`rsync`**.

   b. После сброса текущей установки скопируйте со старого сервера на новый файл с паролями базы данных `/var/lib/iwplatform/` **`dbadmin.yaml`**.
8. Вы можете удалить старые образы контейнеров с помощью команды:

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

9. Перейдите в каталог `/tmp/dmsl_distr.`
10. Добавьте файлу **setup.sh** атрибут "*исполняемый* ":

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

11. Установите Платформу с Центром администрирования в режиме **Central** (или **Office** при распределенной установке):
    a. Запустите скрипт **setup.sh** :

```
./setup.sh
```

    b. Выберите **Install**.
    c. Выберите компонент **Only FrontEnd**.
    d. Выберите режим **Central** (или **Office** при распределенной установке) и далее следуйте шагам 8-16, описанным в инструкции по установке "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?»
12. Обновите Сервер Device Monitor:
    a. Запустите скрипт **setup.sh**:

```
./setup.sh
```

b. Выберите **Update**. Будет определена версия установленного Сервера Device Monitor.
c. Для начала обновления выберите **Yes** и дождитесь окончания процесса.

13. Далее необходимо прописать в файл **n.yaml** настройки. Запустите скрипт установки:

```
./setup.sh
```

a. Выберите **Utilities** и выполните пункт **Fix n.yaml file**.
b. Укажите IP-адрес компьютера, на котором был установлен Сервер Device Monitor. Если он был установлен на текущем компьютере, нажмите **Enter** . Дождитесь окончания процесса.
c. Затем необходимо получить открытый ключ службы **nguard** Платформы и сохранить его в каталог Сервера. Запустите скрипт установки:

```
./setup.sh
```

d. Выберите **Utilities** и выполните пункт **Save platform guard public key to IWDM Service**. Дождитесь окончания процесса.

14. Перезапустите службу Сервера Device Monitor :

```
systemctl restart iwdms
```

15. Обновите все установленные второстепенные (**Secondary**) Серверы Device Monitor, выполнив шаг 8 инструкции.

Чтобы проверить корректность обновления, перейдите в веб-интерфейс Центра расследований и проверьте доступность раздела **Настройки > Сервер DM**.

Обновление со сбросом при распределенной установке

> **Примечание:**
>
> В инструкции для примера указаны версии продуктов, совместимые с Device Monitor 7.15, однако действия актуальны и для Device Monitor 7.16, и для совместимых с ним версий продуктов.

Исходные условия:

- Device Control версии 1.0 и Activity Monitor версии 3.1 установлены на центральной ноде Платформы.
- Сервер Device Monitor версии 7.15 установлен (в режиме `central`) на офисной ноде Платформы.

1. Скопируйте на офисную ноду архив с дистрибутивом Сервера Device Monitor.
2. 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_7.17.0.296.tar.gz -C /tmp/dmsl_distr
```

3. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.17. В примере файл будет извлечен в каталог `/tmp/iwdm` :

```
mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.17.0.296.tar.xz -C /tmp/iwdm
```

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

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

5. Перезагрузите текущий сервер с помощью команды:

```
reboot
```

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

> **Примечание:**
>
> В **Device Monitor 7.15 и более ранних** каталоги по умолчанию расположены по пути **`/mnt`** .
> В **Device Monitor 7.16** – по умолчанию по пути **`/opt`** .
> Обязательно копируйте каталоги с сохранением прав и владельцев. Для копирования используйте стандартные средства, например, утилиту **`rsync`** .

   b. После сброса текущей установки скопируйте со старого сервера на новый файл с паролями базы данных `/var/lib/iwplatform/` **`dbadmin.yaml`** .
8. На центральной ноде Платформы распакуйте архив с дистрибутивом Device Control версии 1.1 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.

9. Перезагрузите текущий сервер с помощью команды:

```
reboot
```

10. На центральной ноде Платформы установите Activity Monitor версии 3.2 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?»

11. Затем на центральной ноде Платформы установите Device Control версии 1.1 из его же установочного файла с помощью команды:

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

Выполните шаги по установке из инструкции из руководства "Device Control. Руководство по установке", статья "Установка Device Control".

12. На офисной ноде Платформы перейдите в каталог, где находится скрипт **setup.sh**, и добавьте ему атрибут " *исполняемый* ":

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

13. Выберите **Install**, а затем **Only FrontEnd**, и выполните шаги из инструкции по установке в статье "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?»
14. На офисной ноде Платформы запустите обновление Сервера Device Monitor, выполнив команду:

```
/setup.sh
```

15. Выберите **Update**.
16. Выберите компонент **Only IWDM Service** и выполните шаги из инструкции по установке в статье "Новая установка".
Если вы обновляетесь **с версии 7.15**, учитывайте, что с версии **7.16** пути установки по

умолчанию изменились. Если ранее вы использовали пути по умолчанию, при установке Device Monitor 7.16 и более новых по умолчанию установщик не обнаружит данные прошлой версии и создаст каталоги по пути `/opt`. Поэтому переместите данные в `/opt` или укажите старые каталоги при установке новой версии.

17. Далее необходимо прописать в файл **n.yaml** настройки. Запустите скрипт установки:

```
/setup.sh
```

18. Выберите **Utilities** и выполните пункты **Fix n.yaml file**.
19. Затем необходимо получить открытый ключ службы **nguard** Платформы и сохранить его в каталог Сервера. Запустите скрипт установки:

```
./setup.sh
```

20. Выберите **Utilities** и выполните пункт **Save platform guard public key to IWDM Service**.
21. Перезапустите службу Сервера Device Monitor:

```
systemctl restart iwdms
```

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

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

Прямое обновление Сервера Device Monitor (с версии 7.17.x)

Важно!

Прямое обновление с версии **7.17.1 не поддерживается**. Чтобы перейти с версии 7.17.1 на 7.17.y:

1. В дистрибутиве 7.17.1 перейдите в папку **`iwdm`**.
2. Для удаления Device Monitor Frontend 7.17.1 выполните команду:

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

3. Распакуйте архив с дистрибутивом Device Monitor Frontend новой версии. В примере архив будет распакован в каталог `/tmp/iwdm`:

```
mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.17.4.343.tar.xz -C /
tmp/iwdm
```

4. Для установки Device Monitor Frontend перейдите в каталог `/tmp/iwdm` и выполните команду:

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

5. Следуйте инструкциям инсталлятора.

Если вы обновляете распределенную установку:

1. Обновите центральную ноду и продукты на ней, если они не были обновлены ранее до поддерживаемых версий.
2. Обновите на офисной ноде основной (**Primary**) Сервер Device Monitor и Device Monitor Frontend.
3. Обновите второстепенные (**Secondary**) Серверы Device Monitor.

Чтобы обновить Сервер Device Monitor:

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

```
mkdir -p /tmp/dmsl_distr && tar xvf dmsl_setup_7.17.4.343.tar.gz -C /tmp/dmsl_distr
```

3. Перейдите в созданный каталог.
4. Добавьте файлу **setup.sh** атрибут "*исполняемый*":

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

5. Запустите установщик Сервера Device Monitor, выполнив команду:

```
./setup.sh
```

6. Для обновления выберите **Update**.
7. Установщик определит установленную версию Device Monitor и запросит подтверждение, чтобы запустить обновление.
8. Выберите **Yes**.
9. После обновления основного (**Primary**) Сервера Device Monitor запустите вручную обновление компонентов Device Monitor Frontend. Для этого:
   a. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.17. В примере архив будет распакован в каталог `/tmp/iwdm`:

```
mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.17.4.343.tar.xz -C /
tmp/iwdm
```

   b. Перейдите в каталог `/tmp/iwdm` и выполните команду:

```
./setup.py update
```

   Дождитесь окончания процесса.

10. Обновите все установленные второстепенные (**Secondary**) Серверы Device Monitor, выполнив шаги 1-9 инструкции.
11. Чтобы освободить место на диске, вы можете удалить каталог `/tmp/iwdm`.
12. Чтобы вывести на экран информацию о продуктах в кластере, выполните команду:

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

13. После завершения процесса обновления проверьте статус службы сервера Device Monitor, выполнив команду:

```
systemctl status iwdms
```

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 **Mac OS** 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.

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
   ```

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.

8 Удаление Device Monitor

В этом разделе:

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

8.1 Удаление Платформы и Сервера Device Monitor

Чтобы удалить Платформу:

1. Перейдите в директорию на сервере, в которую был распакован архив с дистрибутивом при установке.
2. Распакуйте архив с дистрибутивом Device Monitor Frontend версии 7.17:

```
tar xvf data/ui/iw_devicemonitor_setup_7.17.0.310.tar.xz
```

3. Выполните команду:

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

4. Дождитесь завершения удаления. Программа удалит компоненты Платформы и веб-интерфейса Центра расследований.

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

Чтобы удалить Сервер Device Monitor:

1. По умолчанию файл скрипта не помечен как исполняемый. Чтобы сделать его исполняемым, перейдите в указанный каталог и добавьте ему атрибут "*исполняемый*", используя команды:

```
cd /opt/iw/dmserver/bin/
sudo chmod +x ./remove.sh
```

2. Скрипт должен выполняться от имени суперпользователя **root**. Запустите скрипт удаления:

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

3. Подтвердите запрос на удаление, нажав **Y**. При этом можно выбрать:
4. Дождитесь остановки службы сервера и определения его типа.

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

5. Если сервер основной, то подтвердите последующее удаление БД. Нажмите **Y** и введите пароль пользователя БД для подтверждения удаления.
6. Если требуется удалить каталог с файлами журнала (логами), нажмите **Y**.

7. Если требуется удалить каталог файловой очереди, нажмите **Y**. Если ввести **N**, то каталог с теневыми копиями событий будет сохранен, так как в нем могут быть еще не отправленные в Traffic Monitor или Activity Monitor события.
8. Дождитесь окончания процесса удаления, который включает в себя:
   - удаление СУБД. Если 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.
9. В процессе удаления возможно появление ошибок. Например, в случаях, когда сервер был не полностью сконфигурирован, БД оказалась недоступной на момент удаления или возникли ошибки при определении типа сервера. В этом случае в консоли вы увидите текст ошибки и вопрос, нужно ли продолжить удаление только файлов сервера Device Monitor.

8.2 Удаление Агентов Device Monitor

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

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

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 находится 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 Рабочая станция:

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

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
   ```