

INFOWATCH

InfoWatch Device Monitor for Linux. Руководство по установке

13/01/2025

© 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 16

5.1 Состав дистрибутива 16

5.2 Схема развертывания Device Monitor 16

5.3 Подготовка окружения 19

5.3.1 Установка .NET на примере операционной системы Альт 21

5.3.2 Установка .NET на примере операционной системы Astra Linux 22

5.3.3 Установка .NET на примере операционной системы РЕД ОС 23

5.3.4 Установка conntrack и socat на примере операционной системы РЕД ОС 23

5.4 Новая установка 24

5.4.1 Возможные режимы установки Device Monitor: 25

5.4.2 Шаги установки в режиме "Все-в-одном" с миграцией данных: 25

5.4.3 Шаги распределенной установки Device Monitor: 29

5.4.4 Миграция сервера DM с ОС Windows на ОС семейства Linux 30

5.5 Настройка проверки сертификатов удаленных серверов 31

5.5.1 Чтобы настроить проверку сертификатов удаленных серверов при установлении SSL-сессии: 32

5.5.2 Чтобы установить сертификат службы XAPI Traffic Monitor: 33

5.5.3 Чтобы установить сертификат веб-сервера Traffic Monitor Traffic Monitor: 33

5.5.4 Чтобы установить сертификат службы EPEVENTS Платформы: 34

5.5.5 Просмотр логов 34

5.6 Установка Агентов Device Monitor 35

5.6.1 Локальная установка Агентов 39

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью msi-пакета с последующим вводом параметров вручную: 39

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС Microsoft Windows с помощью msi-пакета в тихом режиме: 40

Установка Агента InfoWatch Device Monitor на компьютер под управлением ОС семейства Linux: 43

5.6.2 Установка Агентов с помощью задачи распространения 45

6 Настройка сетевых правил доступа 48

7 Обновление Device Monitor 50

7.1 Обновление Сервера Device Monitor 50
7.1.1 Шаги обновления с версий 7.13 и 7.14: 50
7.1.2 Шаги обновления с версии 7.15 на 7.15.X: 52
7.2 Обновление Агентов Device Monitor 52
8 Удаление Device Monitor 55
8.1 Удаление Платформы и Сервера Device Monitor 55
8.2 Удаление Агентов Device Monitor 56

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

1 Аудитория

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

2 Комплект документов

В документацию входят:

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

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

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

3 Техническая поддержка пользователей

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

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

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

4 Аппаратно-программные требования

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

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

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
Сервер Device Monitor на Платформе				
Не менее 100 GB свободного пространства для установки. Также понадобится свободное пространство для анализа данных, объем зависит от нагрузки на сервер	От 4 ядер (частота - 3.1 ГГц, разрядность - 64 bit, с поддержкой инструкций SSE 4.2)	От 16 GB	ОС : • РЕД ОС 7.3; • Astra Linux 1.7 "Смоленск"; • Альт Сервер Виртуализации 10. СУБД: PostgreSQL версии 11 и более поздних	• На сервере ТМ должен быть включен автозапуск процесса **iw_xapi_xapi** • Наличие локального DNS для перевода доменных имен в адреса • Режим FIPS должен быть отключен • Должен поддерживаться протокол TLS 1.2
Агент Device Monitor для рабочих станций				
Не менее 1 GB свободного пространства для установки. Также понадобится свободное пространство для временного хранения файлов, предназначенных для передачи на анализ	От 2 ядер	От 2.5 GB	ОС: • [1]Microsoft Windows 7 Service Pack 1; • Microsoft	**Поддерживаемые версии ядра Astra Linux Special Edition "Смоленск" версии 1.6 (все пакеты безопасности)** • 4.15.3-1-generic • 4.15.3-1-hardened • 4.15.3-2-generic

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			Windows 8 и 8.1; • Microsoft Windows 10; • Microsoft Windows 11; • [1]Microsoft Windows Server 2008 R2; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Microsoft Windows Server 2022; • Astra Linux Special Edition	• 4.15.3-2-hardened • 4.15.3-154-generic • 4.15.3-154-hardened • 4.15.3-177-generic • 4.15.3-177-hardened • 5.4.0-110-generic • 5.4.0-110-hardened • 5.4.0-162-generic • 5.10.142-1-generic • 5.10.190-1-generic • 5.15.0-33-generic • 5.15.0-83-generic **Поддерживаемые версии ядра Astra Linux Common Edition "Орел" версии 2.12** • 4.9.135-1-generic • 4.15.3-1-generic • 4.15.3-1-hardened • 4.15.3-2-generic • 4.15.3-2-hardened • 4.15.3-3-generic • 4.15.3-3-hardened • 4.15.3-141-generic • 4.15.3-141-hardened • 4.19.0-1-generic • 5.2.13-050213-generic • 5.4.0-54-generic • 5.4.0-54-hardened • 5.4.0-71-generic • 5.4.0-71-hardened • 5.4.0-110-generic • 5.4.0-110-hardened • 5.10.0-1038.40-generic • 5.10.0-1038.40-hardened • 5.10.0-1057-generic • 5.10.142-1-generic • 5.10.142-1-hardened • 5.15.0-33-generic • 5.15.0-33-hardened • 5.15.0-70-generic

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			"Смоленск" (x64) версии 1.6 с установленным обновлением безопасности Update 5, 6 или 12; • Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" и "Смоленск"; • Astra Linux Common Edition "Орёл" (x64) версии 2.12; • РЕД ОС 7.3; • Альт Рабочая	• 5.15.0-70-hardened **Поддерживаемые версии ядра Astra Linux Special Edition 1.7 в редакциях "Орел", "Воронеж" и "Смоленск"** • 5.4.0-54-generic • 5.4.0-54-hardened • 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) • 5.15.0-33-generic • 5.15.0-33-hardened • 5.15.0-70-generic • 5.15.0-70-hardened • 5.15.0-83-generic • 5.15.0-111-generic (начиная с версии 7.15.1) • 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)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
			станция 10; • Альт Сервер 10.1 с профилем "Офисный сервер" • Альт Сервер 10.1 СП (сертифицированный).	**Поддерживаемые версии ядра РЕД ОС 7.3** • 5.15.10-1 • 5.15.10-2 • 5.15.10-3 • 5.15.10-4 • 5.15.35-1 • 5.15.35-4 • 5.15.35-5 • 5.15.72-1 (начиная с версии 7.7.1) • 5.15.78-2 (начиная с версии 7.8) • 5.15.87-1 (начиная с версии 7.8.1) • 5.15.106-1 • 5.15.117-1 • 5.15.125-1 • 5.15.131-1 • 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) **Поддерживаемые версии ядра Альт Рабочая станция 10** • 5.10.133-std-def-alt1 • 5.10.135-std-def-alt1 • 5.10.136-std-def-alt1 • 5.10.163-std-def-alt1 • 5.10.164-std-def-alt1 • 5.10.165-std-def-alt1 • 5.10.168-std-def-alt1 • 5.10.170-std-def-alt1 • 5.10.172-std-def-alt1

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 5.10.174-std-def-alt1 • 5.10.176-std-def-alt1 • 5.10.177-std-def-alt1 • 5.10.179-std-def-alt1 • 5.10.182-std-def-alt1 • 5.10.185-std-def-alt1 • 5.10.186-std-def-alt1 • 5.10.191-std-def-alt1 • 5.10.194-std-def-alt1 • 5.10.195-std-def-alt1 • 5.10.197-std-def-alt1 • 5.10.198-std-def-alt1 • 5.10.199-std-def-alt2 • 5.10.200-std-def-alt1 • 5.10.203-std-def-alt1 • 5.10.204-std-def-alt1 • 5.10.205-std-def-alt1 • 5.10.206-std-def-alt1 • 5.10.207-std-def-alt1 (начиная с версии 7.12.1) • 5.10.208-std-def-alt1 (начиная с версии 7.12.1) • 5.10.209-std-def-alt2 (начиная с версии 7.12.2) • 5.10.211-std-def-alt1 • 5.10.212-std-def-alt1 • 5.10.213-std-def-alt1 (начиная с версии 7.13.1) • 5.10.216-std-def-alt1 (начиная с версии 7.13.6) • 5.10.217-std-def-alt1 (начиная с версии 7.13.9) • 5.10.218-std-def-alt1 (начиная с версии 7.13.10)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 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) • 5.15.94-un-def-alt1 • 5.15.109-un-def-alt1 • 6.1.29-un-def-alt1 • 6.1.32-un-def-alt1 • 6.1.42-un-def-alt1 • 6.1.49-un-def-alt1 (начиная с версии 7.13.2) • 6.1.67-un-def-alt0.c10f.1 (начиная с версии 7.12.4) • 6.1.75-un-def-alt1 (начиная с версии 7.12.2) • 6.1.77-un-def-alt1 (начиная с версии 7.12.2) • 6.1.78-un-def-alt1 (начиная с версии 7.12.4) • 6.1.79-un-def-alt1 (начиная с версии 7.12.5) • 6.1.80-un-def-alt1 • 6.1.81-un-def-alt1 • 6.1.82-un-def-alt1 (начиная с версии 7.13.1)

Дисковая подсистема	Процессор	Оперативная память	Программные требования	Дополнительные требования
				• 6.1.83-un-def-alt1 (начиная с версии 7.13.2) • 6.1.84-un-def-alt1 (начиная с версии 7.13.4) • 6.1.85-un-def-alt1 (начиная с версии 7.13.4) • 6.1.90-un-def-alt1 (начиная с версии 7.13.8) • 6.1.94-un-def-alt1 (начиная с версии 7.14.1) • 6.1.96-un-def-alt1 (начиная с версии 7.14.1) • 6.1.99-un-def-alt1 (начиная с версии 7.14.2) • 6.1.112-un-def-alt1 (начиная с версии 7.15.0) • 6.1.113-un-def-alt1 (начиная с версии 7.15.1) • 6.1.115-un-def-alt1 (начиная с версии 7.15.2)
Веб-консоль Device Monitor				
	Дополнительно 1 ядро	1 GB на каждую вкладку браузера	Браузеры: • Google Chrome • Яндекс. Браузер	В браузере должна быть реализована аппаратная поддержка WebGL/ WebGL2 Платформа версии 1.7 и выше

Примечание:

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

Примечание:

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

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

5 Установка Device Monitor

Рекомендуется соблюдать следующий порядок установки:

1. Подготовка окружения.
2. Установка Платформы 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 директории с файлами:

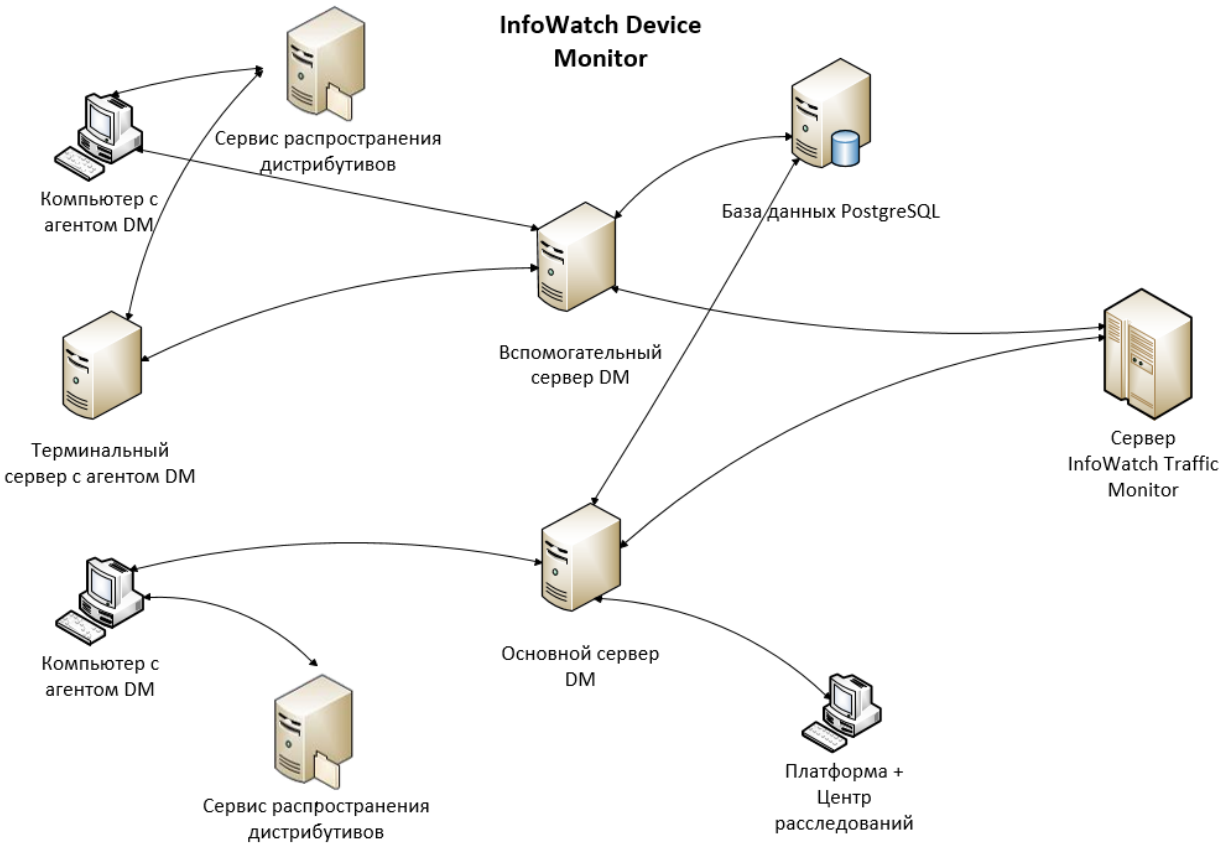
- `data/iwdms` – содержит архив с исполняемыми файлами Сервера Device Monitor и скрипт для его установки с поддержкой установки через параметры командной строки.
- `scripts/include` – содержит вспомогательные скрипты, необходимые для корректной работы setup.sh и install_iwdms.sh;
- `data/ui` – дистрибутив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

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, можно использовать 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.

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 DM**.
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. Установить пакеты `conntrack` (или `conntrack-tools`) и `socat`.
5. Настроить антивирус для совместной работы с Системой (см. статью Базы знаний "Настройка антивируса для Device Monitor Server на ОС Linux").
6. Настроить правила POD сети или отключить межсетевой экран (см. статьи Базы знаний "Конфликты при взаимодействии firewalld и Kubernetes", "Полное отключение межсетевого экрана").
7. Установить интерпретатор языка Python версии 2.7. Пакет с интерпретатором не входит в состав дистрибутива продукта.
8. Если установка проводится на ОС Альт:
   a.
      - 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
```

9. Установить СУБД PostgreSQL на другом компьютере. Вы можете установить СУБД PostgreSQL совместно с сервером Device Monitor, если необходимо получать события от небольшого количества Агентов.

   > **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.

10. Подготовить СУБД:
    a. Откройте конфигурационный файл `postgresql.conf` и присвойте параметру `"max_connections"` значение `250`.
    b. Настройте файл доступа `pg_hba.conf`. Для более точного подбора параметров используйте калькулятор PGTune.

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

5.3.1 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`

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

global.json file:
  Not found

Host:
  Version:      6.0.20
  Architecture: x64
  Commit:       6.0.20-alt

.NET SDKs installed:
  No SDKs were found.

.NET runtimes installed:
  Microsoft.AspNetCore.App 6.0.20 [/usr/lib64/dotnet/shared/Microsoft.AspNetCore.App]
  Microsoft.NETCore.App 6.0.20 [/usr/lib64/dotnet/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@dmalt ~]#
```

5.3.2 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:~#
```

5.3.3 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:

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

5.3.4 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`).

5.4.1 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. Режим подходит для новой чистой установки Device Monitor, а также при переходе на Device Monitor for Linux с ОС Windows.
- **Распределенная** установка Сервера Device Monitor на офисную ноду Платформы на отдельном 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 "Миграция сервера DM с ОС Windows на ОС семейства Linux".
- На шаге 23 инструкции выберите **Update an existing database**.

5.4.2 Шаги установки в режиме "Все-в-одном" с миграцией данных:

1. Создайте директорию на жестком диске.
2. Скопируйте в нее папку **data** и скрипт **setup.sh** в созданную директорию.

   Важно!

   Для корректной установки путь к дистрибутиву не должен содержать пробелы.

3. Добавьте файлу **setup.sh** атрибут "*исполняемый*":

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

4. 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

5. Выберите тип установки **Install**. Будет доступен список компонентов:
   - **IWDM 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 IWDM Service** – установка только Сервера Device Monitor
6. Выберите **IWDM 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 34-36.

   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.
7. Выберите режим **Central.** Начнется процесс установки Платформы
8. Ознакомьтесь с условиями лицензионного соглашения. Оно содержит несколько страниц. Для перехода на следующую страницу используйте клавишу **Enter**.
9. Введите **y**, чтобы принять лицензионное соглашение, и нажмите **Enter**.
10. Введите IP-адрес сервера в формате IPv4: `"xxx.xxx.xxx.xxx"` и нажмите **Enter**.
11. Выделите объем оперативной памяти для размещения данных Clickhouse (по умолчанию 80%) и нажмите **Enter**.
12. Укажите путь для размещения данных Clickhouse (по умолчанию: `/mnt/chdata`) и нажмите **Enter**.
13. Укажите путь для размещения данных PostgreSQL (по умолчанию: `/mnt/pgdata`) и нажмите **Enter**.
14. Укажите путь для размещения данных NATS (по умолчанию: `/mnt/natsdata`) и нажмите **Enter**.
15. Укажите путь для хранения данных (по умолчанию `/mnt/dsdata`) и нажмите **Enter**.
16. Укажите порт подключения к веб-интерфейсу (по умолчанию `443`) и нажмите **Enter**.
17. 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 DM
       - /opt/iw/dmserver/bin - каталог с файлами сервера DM
       - /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**

18. Выберите язык устанавливаемого сервера и нажмите **Enter**. Это определит названия предустановленных групп, политик и правил.
19. Ознакомьтесь с лицензионным соглашением и выберите необходимое действие. Для продолжения установки необходимо принять лицензионное соглашение. Выберите **Accept and continue** и нажмите **Enter**
20. Далее можно выбрать, какой тип сервера необходимо установить: основной или второстепенный.
21. Если вы устанавливаете Систему впервые или в режиме "Все-в-одном", выберите **Primary** (основной сервер). Для установки второстепенного сервера (**Secondary**) выполните шаги 24-28 и далее начиная с шага 31.
22. Настройте взаимодействие с Базой данных:
    - **Create new database** – чтобы создать новую Базу данных;
    - **Update an existing database** – чтобы настроить существующую Базу данных.
23. Выберите **Update an existing database**.
24. Укажите имя или IP-адрес сервера, на котором располагается СУБД PostgreSQL. Используйте СУБД Postgresql, ранее используемую для установки Сервера Device Monitor на ОС Windows.
25. Укажите порт для настройки взаимодействия. Если порт не указан, будет использован порт по умолчанию – `5432`.
26. Введите имя базы данных. По умолчанию – `iwdm.`
27. Введите имя пользователя СУБД. По умолчанию – `postgres.`
28. Введите пароль.
29. 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 учёта 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 DM - 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 DM. В этой таблице поле `TmAddress` может присутствовать несколько раз (по количеству серверов в пуле).

30. 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.
31. Укажите **Yes**, чтобы установить сервис распространения дистрибутивов. В этом случае точка распространения сможет распространять дистрибутивы агентов на рабочие станции, кроме рабочих станций под управлением ОС Windows;
32. 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.
33. Если вы 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**
34. Если вы устанавливаете продукт распределенно или потом ставите другой продукт IW, 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
```

35. Выберите в меню пункт **Utilities**. Раздел содержит утилиты:
    a. **Fix n.yaml file** – если на текущем компьютере установлен Device Monitor в роли первичного 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 первичного 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".
36. Выберите **Fix n.yaml file**. Дождитесь окончания процесса.
37. Запустите скрипт установки:

```
./setup.sh
```

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

```
systemctl restart iwdms
```

Распределенная установка используется, когда нужно для уменьшения нагрузки установить Сервер Device Monitor на компьютере, отличном от центральной ноды Платформы с другими установленными продуктами InfoWatch.

5.4.3 Шаги распределенной установки Device Monitor:

1. На другом компьютере создайте директорию на жестком диске.
2. Скопируйте в нее папку **data** и скрипт **setup.sh** в созданную директорию.

> **Важно!**
>
> Для корректной установки путь к дистрибутиву не должен содержать пробелы.

3. Добавьте файлу **setup.sh** атрибут "*исполняемый*":

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

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

```
./setup.sh
```

5. Выберите тип установки **Install**. Будет доступен список компонентов:
6. Выберите **IWDM 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 34-36.

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.

7. Выберите **Office.**
8. Введите IP-адрес центральной ноды Платформы, установленной ранее.
9. Получите токен центральной ноды. Для этого на сервере с центральной нодой выполните команду:

```
kubeadm token list
```

10. Скопируйте полученный токен. Начнется установка Платформы.
11. Введите полученный токен на ноде офисной Платформы.
12. Укажите лейбл для офисной ноды Платформы
13. Выполните шаги 11-17 инструкции выше. Дождитесь установки офисной ноды Платформы.
14. Выполните шаги 18-21, чтобы установить Сервер Device Monitor.
15. Если на шаге 21 вы выбрали **основной** сервер, то укажите путь до PFX-файла ключа шифрования канала между Сервером DM и агентами. Если путь не указывать, то будет использован путь, предложенный по умолчанию, – `/opt/iw/dmserver/ssl.pfx`
16. 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 DM, выполните команду:

```
systemctl status iwdms
```

Далее перейдите в Центр расследований, введя в браузере IP-адрес центральной ноды Платформы.

5.4.4 Миграция сервера DM 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. Убедитесь, что база данных поддерживает миграцию, т.е. не содержит правил, которые не поддерживаются в новой версии. Для этого:
   a. В дистрибутиве по пути `7.15.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 DM.
   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.

2. Удалите все серверы Device Monitor, оставив базу данных и сохранив секретный ключ сервера. Для этого воспользуйтесь инструкцией для вашей версии продукта.
3. Установите серверы Device Monitor на новую ОС на существующую базу данных. Для этого воспользуйтесь инструкцией из статьи "Новая установка". На шаге 23 выберите пункт **Update an existing database**.

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 почтового трафика Outlook
- Контроль мессенджеров: WhatsApp (десктопная и веб-версия), Skype (десктопная и веб-версия), Yandex Messenger (веб-версия), 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

Неподдерживаемые настройки:

- сегментов сетей, 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.

Device Monitor осуществляет проверку следующих сертификатов:

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

Чтобы успешно подключиться к удаленному серверу для отправки событий:

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

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

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

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

5.5.1 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.

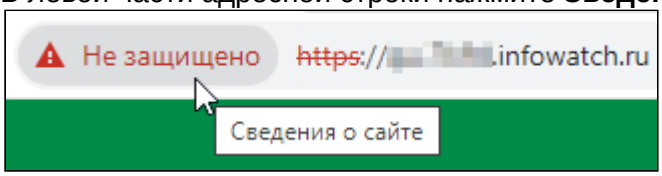
5.5.2 Чтобы установить сертификат службы XAPI Traffic Monitor:

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.

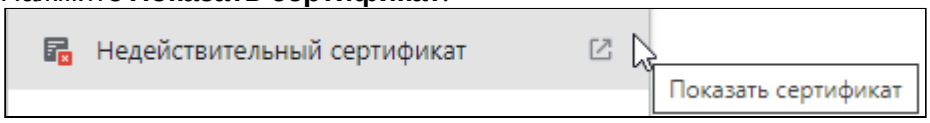
5.5.3 Чтобы установить сертификат веб-сервера Traffic Monitor Traffic Monitor:

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

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

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

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

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

d. Для применения изменений в настройках ОС Astra Linux, перезагрузить сервер с помощью команды:
`reboot`

> **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`

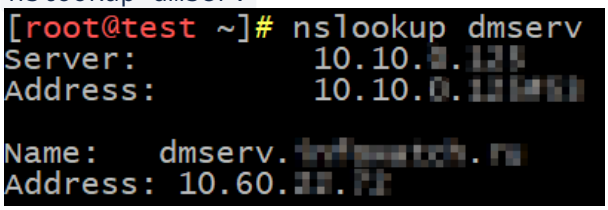
        > **Примечание:**
        >
        > Значение IP-адреса в строке может быть равно 127.0.1.1 или 127.0.0.1.

> **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!**

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

Важно!

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

Важно!

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

Примечание:

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

Примечание:

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

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

При необходимости установите ее:

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

Примечание:

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

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

Примечание:

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

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

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

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

Важно!

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

5.6.1 Локальная установка Агентов

Важно!

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

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

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

1. **Запуск мастера установки**
   Вставьте внешний носитель с дистрибутивом Агента в компьютер. Затем откройте каталог `Client`. В данном каталоге найдите и запустите пакет установки для требуемой платформы для развертывания в соответствии с заданными при формировании пакетов параметрами, например, `InfoWatch.DeviceMonitor.Client.7.15.0.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	Значение по умолчанию	Описание
`/quiet`	-	Запуск установки без отображения пользовательского интерфейса
`/i <имя_пакета_установки>`	-	Запуск установки продукта с помощью указанного файла
`PREDEFINED_CLIENTDIR`	"`%ProgramFiles%\Infowatch\DeviceMonitor\Client`"	Директория для установки продукта **Важно!** Путь к каталогу может содержать следующие символы: 0-9,a-z,A-Z, ":", ".", "_", "-", "\", " ". При наличии в пути других символов, установка Агента будет некорректной.

Ключ	Значение по умолчанию	Описание
`UNINSTALL_PASSWORD_SHA1_HASH`	Отсутствует	Хеш-значение пароля деинсталляции в шестнадцатеричном формате, вычисленное по алгоритму SHA-1. Если задать данный параметр, то удалить Агента Device Monitor можно будет только введя правильный пароль. **Важно!** Хеш-значение пароля необходимо вычислять для кодировки Юникод UTF-16LE. Указывайте хеш-значение, используя только заглавные буквы и цифры.
`IWPROXYDN`	"`CN=InfoWatch Transparent Proxy Root,C=RU,O=ZAO InfoWatch,OU=TechDep,ST=Moscow`"	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
`SHOW_USER_NOTIFICATION`	"`#x01000000`"	Показывать пользователю уведомление о необходимости перезагрузить компьютер. Возможные значения: • "`#x01000000`" - показывать • "`#x00000000`" - не показывать
`WAITING_REBOOT_PERIOD`	"0"	Время ожидания перезагрузки рабочей станции до момента, когда Агент начнет показывать пользователю уведомление о необходимости перезагрузить компьютер. Указывается в часах
`REBOOT_NOTIFICATION_PERIOD`	"-1"	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. Чтобы показывать уведомление бесконечно и не перезагружать компьютер принудительно, укажите значение "`-1`".
`REBOOT_NOTIFICATION_RATE`	-	Частота, с которой Агент показывает пользователю уведомление о необходимости перезагрузить компьютер. Указывается в минутах. **Примечание:** Если параметр не задан, уведомление показывается каждые 10 секунд

Ключ	Значение по умолчанию	Описание
`REBOOT_NOTIFY_MESSAGE`	"`Необходимо как можно скорее перезагрузить компьютер`"	Текст уведомления о необходимости перезагрузить компьютер. Сообщение может содержать не более 255 символов
`FORCE_REBOOT`	"0"	Отправить финальное уведомление перед принудительной перезагрузкой. Возможные значения: • "`0`" - 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`	"`#x00000000`"	Скрывать присутствие Агента Device Monitor от пользователя рабочей станции. Возможные значения: • "`#x01000000`" - скрывать Агента • "`#x00000000`" - 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`	"0"	Не устанавливать компонент перехвата сетевого трафика. Возможные значения: • "`0`" – установить компонент • "`1`" – не устанавливать компонент
`NOIWNBG`	"0"	Не устанавливать компонент контроля периметра сети. Возможные значения: • "`0`" – установить компонент • "`1`" – не устанавливать компонент

Ключ	Значение по умолчанию	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>` 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.7.12.5.192.msi
   PREDEFINED_CLIENTDIR="%ProgramFiles%\Infowatch\DeviceMonitor\Client"
   UNINSTALL_PASSWORD_SHA1_HASH="DB588811D533F6FC41F14C7325E9E71E8F0863A5"
   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.7.12.5.192.log
   ```
2. Дождитесь завершения установки.
3. Перезагрузите компьютер.

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

Важно!

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

Важно!

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

Примечание:

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

1. **Подготовка к установке:**
   a. Если на компьютере под управлением ОС Astra Linux 1.6 ранее было установлено обновление безопасности (например, Update 5):
      i. Узнайте текущую версию ядра Astra Linux (например, `4.15.3-2-generic`):
      `uname -r`
      ii. Проверьте, что директория `/boot` не содержит старых пакетов ядра с более ранней версией, чем в предыдущем шаге (например, `initrd.img-4.15.3-1-generic` или `initrd.img-4.15.3-1-hardened`).
      iii. Удалите такие пакеты при наличии:
      `apt-get purge linux-image-4.15.3-1`
      iv. Удалите неиспользуемые Системой пакеты:
      `apt-get autoremove`
      `apt-get autoclean`
   b. Скопируйте на компьютер архив, в котором содержатся пакет и скрипты для установки и удаления Агента Device Monitor. Архив поставляется в составе дистрибутива. Название архива может отличаться в зависимости от используемой ОС:
      - `Setup.AstraLinuxSE-1.6-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.6;
      - `Setup.AstraLinuxCE-2.12-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Common Edition 2.12;
      - `Setup.AstraLinux-1.7-iwdm.x64.x.x.x.xx.tar.gz` - для Astra Linux Special Edition 1.7;
      - `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz` - для РЕД ОС 7.3.1;
      - `Setup.AltLinux-10.0-iwdm.x64.x.x.x.xx.tar.gz` - для Альт Рабочая станция 10.
      `x.x.x.xx` - номер сборки.
      Далее мы рассмотрим пример установки и удаления Агента на РЕД ОС 7.3. Установка и удаление на других поддерживаемых ОС аналогичны.
      В нашем примере:
      `Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`
   c. Перейдите в директорию, в которую скопирован архив, и введите команду для распаковки:
      `sudo tar -xvzf Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`
      Пример команды для Агента на Alt Linux:
      `tar -xvzf Setup.AltLinux-10.0-iwdm.x64.7.11.0.126.tar.gz`
      В результате будут созданы файлы `install.sh`, `remove.sh`, `upgrage.sh`, `iwdm_<версия_агента>.deb`.

d. Если вы не хотите устанавливать компонент перехвата сетевого трафика, то создайте переменную окружения `IWDM_NO_PROXY` со значением "`1`":
`export IWDM_NO_PROXY=1`

> **Примечание:**
>
> Чтобы убедиться, что переменная окружения создалась, выполните команду:
> `env | grep IWDM_NO_PROXY`

2. **Установка Агента InfoWatch Device Monitor:**
   a. Перейдите в директорию, в которую распаковано содержимое архива **`Setup.RedOS-7.3-iwdm.x64.x.x.x.xx.tar.gz`**.
   b. Для установки Агента запустите скрипт, выполнив команду:
   `sudo ./install.sh <сервер>:<порт>`
   где `<сервер>` - ip-адрес или доменное имя Сервера InfoWatch Device Monitor, `<порт>` - порт подключения к Серверу InfoWatch Device Monitor.
   В нашем примере команда будет следующей:
   `sudo ./install.sh dm-server:15101`
   Пример команды для Агента на Alt Linux:
   `su -c "./install.sh dm-server:15101"`
   Продукт будет установлен в директорию `/opt/iw/dmagent`.
   c. Проверить статус сервисов можно командой:
   `sudo systemctl status iwdm*`
   Пример команды для Агента на Alt Linux:
   `su - -c "systemctl status iwdm*"`

> **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.

> **Важно!**
>
> Для корректной работы функциональности на ОС семейства Linux необходимо перезагрузить компьютер после установки Агента.

5.6.2 Установка Агентов с помощью задачи распространения

Для установки Агентов Device Monitor на рабочие станции с помощью задачи распространения в веб-консоли Device Monitor необходимо наличие установленного сервиса распространения (подробнее см. "Новая установка", Шаг 30).

Важно!

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

Для установки Агентов на рабочие станции под управлением ОС Linux выполните шаги:

1. В разделе **Задачи** веб-консоли создайте задачу первичного распространения (см. "Задача первичного распространения и обновления").
2. Сформируйте список рабочих станций для установки Агентов .
3. Запустите задачу, нажав .
4. Введите учетные данные пользователя, от имени которого запускается задача, и нажмите **Запустить**.
5. Дождитесь окончания выполнения задачи. В области **Выполнение задачи** будет отображен список рабочих станций с информацией об Агентах.

Примечание:

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

Примечание:

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

Важно!

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

Важно!

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

Важно!

На рабочих станциях под управлением ОС Astra Linux Special Edition версий 1.6 и 1.7 необходимо настроить максимальный уровень мандатного доступа для пользователя, от имени которого будет произведена установка Агента. Например, чтобы повысить уровень доступа для пользователя root, используйте команду:

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

Важно!

Для корректной работы функциональности на ОС семейства Linux необходимо перезагрузить компьютер после установки Агента.

6 Настройка сетевых правил доступа

Для корректной работы Системы должны быть разрешены соединения:

<table>
<tr><th rowspan="2">Компонент Системы, для работы которого необходимо соединение</th><th colspan="2">Взаимодействие между компонентами</th><th rowspan="2">Порт</th><th colspan="2" rowspan="2">Назначение порта</th></tr>
<tr><th>Источник</th><th>Получатель</th></tr>
<tr><td rowspan="9">Сервер Device Monitor (DM)</td><td>Платформа</td><td>Сервер DM</td><td>TCP 15007</td><td colspan="2">Взаимодействие Платформы с Сервером DM</td></tr>
<tr><td>Сервер DM</td><td>Сервер БД</td><td>TCP 5432</td><td colspan="2">Взаимодействие Сервера DM с базой данных</td></tr>
<tr><td>Агент DM</td><td>Сервер DM</td><td>TCP 15004</td><td rowspan="4">Защищенное соединение Сервера DM с Агентами</td><td>Передача теневых копий (шифрованный канал)</td></tr>
<tr><td>Агент DM</td><td>Сервер DM</td><td rowspan="2">UDP 15100</td><td rowspan="2">Уведомление Агентов</td></tr>
<tr><td>Сервер DM</td><td>Агент DM</td></tr>
<tr><td>Агент DM</td><td>Сервер DM</td><td>TCP 15101</td><td>Передача теневых копий</td></tr>
<tr><td>Агент DM</td><td>Сервер DM</td><td>TCP 15200</td><td colspan="2">Инициация загрузки дистрибутива Агента с Сервера DM на рабочую станцию</td></tr>
<tr><td>Сервер DM</td><td>Агент DM</td><td>TCP 15505</td><td colspan="2">Установка и удаление Агента</td></tr>
<tr><td>Рабочая станция Офицера безопасности</td><td>Платформа</td><td>TCP 443</td><td colspan="2">Взаимодействие Офицера безопасности с Веб-консолью Сервера DM</td></tr>
<tr><td>Агент DM на ОС семейства Linux</td><td>Сервер DM</td><td>Рабочая станция сотрудника</td><td>TCP 22</td><td colspan="2">Установка Агента</td></tr>
</table>

Примечание:

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

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

или

- измените их на порты из таблицы:

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

7 Обновление Device Monitor

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

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

7.1 Обновление Сервера Device Monitor

Важно!

При обновлении сервера Device Monitor с версий 7.13 или 7.14 до версии, начиная с 7.15, в случае, если вам необходимо продолжать работать с правилами контроля устройств и с функциональностью белых списков, потребуется установить систему Device Control и перенести правила и белые списки. Важно учитывать, что перенос поддерживается только для БД Postgres. В случае, если у вас установлена более ранняя версия сервера, то необходимо сначала обновить сервер до версии 7.13 или 7.14, а затем обновить его до версии 7.15.

Важно!

Для обновления кластера из нескольких серверов сначала обновите по инструкции основной (**Primary**) сервер Device Monitor, а затем второстепенные (**Secondary**) серверы.

Важно!

Для корректного обновления путь к дистрибутиву не должен содержать пробелы.

7.1.1 **Шаги обновления с версий 7.13 и 7.14:**

1. Распакуйте архив с дистрибутивом Платформы. В примере - в папку `/tmp/iwdm`:

```
mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.15.0.200.tar.xz -C /tmp/iwdm
```

2. Выполните сброс установки Платформы:

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

3. Удалите старые образы контейнеров:

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

4. Остановите службы iwdms на всех установленных серверах:

```
systemctl stop iwdms
```

5. Добавьте файлу **setup.sh** атрибут "*исполняемый*" :

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

6. 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** и далее следуйте шагам 8-16, описанным в инструкции по установке "Установка "Все-в-одном"", указывая старые каталоги хранения данных
7. 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.
   d. Если необходимо работать с правилами контроля устройств и белыми списками, выберите **Using Device Control is required, migrate rules and white lists**. Все имеющиеся правила контроля устройств и белые списки будут перенесены. Дождитесь окончания процесса миграции. В противном случае выберите **Using Device Control is not required, delete rules and white lists**. Все имеющиеся правила контроля устройств и белые списки будут удалены.
8. Пропишите в файл **n.yaml** настройки и получите открытый ключ службы **nguard** Платформы и сохраните его в каталоге Сервера. Для этого:
   a. Снова запустите скрипт установки:

```
./setup.sh
```

   b. Выберите в меню пункт **Utilities**.
   c. Выберите **Fix n.yaml file**.
   d. Укажите IP-адрес компьютера, на котором был установлен iwdms. Если он был установлен на текущем компьютере, нажмите **Enter**. Дождитесь окончания процесса.
   e. Запустите скрипт установки:

```
./setup.sh
```

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

9. Перезапустите службу iwdms :

```
systemctl restart iwdms
```

10. Обновите таким же образом все установленные второстепенные (**Secondary**) Сервера Device Monitor.

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

7.1.2 Шаги обновления с версии 7.15 на 7.15.X:

1. Распакуйте архив с дистрибутивом Платформы. В примере - в папку `/tmp/iwdm` :

```
mkdir -p /tmp/iwdm && tar xvf data/ui/iw_devicemonitor_setup_7.15.X.200.tar.xz -C /tmp/iwdm
```

2. Перейдите в папку с архивом и выполните обновление Платформы:

```
/tmp/iwdm/setup.py update
```

Дождитесь окончания процесса

3. Обновите Сервер Device Monitor. Для этого перейдите в каталог, где находится скрипт **setup.sh** и добавьте ему атрибут "*исполняемый*" :

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

4. Запустите скрипт **setup.sh**:

```
./setup.sh
```

5. Выберите **Update**. Будет определена версия установленного Сервера Device Monitor
6. Для начала обновления выберите **Yes** и дождитесь окончания процесса.
7. Если необходимо работать с правилами контроля устройств и белыми списками, выберите **Using Device Control is required, migrate rules and white lists**. Все имеющиеся правила контроля устройств и белые списки будут перенесены. Дождитесь окончания процесса миграции. В противном случае выберите **Using Device Control is not required, delete rules and white lists**. Все имеющиеся правила контроля устройств и белые списки будут удалены.

7.2 Обновление Агентов Device Monitor

Обновление Агентов Device Monitor на рабочих станциях может быть выполнено:

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

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

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

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

1. Выполните *Шаг 1* инструкции по локальной установке (см. "Локальная установка Агентов").
2. Перейдите в директорию, в которую было распаковано содержимое архива.
3. Запустите скрипт обновления, выполнив команду:
   `sudo ./upgrade.sh`
4. Дождитесь окончания обновления. Проверить статус выполнения можно, выполнив команду:
   `sudo systemctl status iwdm*`

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

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

Примечание:

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

Важно!

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

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

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. Выполните команду:

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

3. 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

Удаление Агентов Device Monitor производится локально на рабочих станциях.

Чтобы удалить Агент InfoWatch Device Monitor на ОС Windows:

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

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

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

Важно!

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

В случае возникновения трудностей при удалении Агента рекомендуем обратиться в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.
Вы также можете посетить раздел технической поддержки на нашем сайте: http://www.infowatch.ru/services/support.