InfoWatch Device Control Adapter. Руководство по установке и конфигурированию

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

26.01.2017

СОДЕРЖАНИЕ

1 Введение 4

2 Обзор Device Control Adapter 5

2.1 Схема работы Device Control Adapter 5

2.2 Информация, передаваемая в InfoWatch Traffic Monitor 7

2.3 Состав Device Control Adapter 8

3 Подготовка к установке Device Control Adapter 9

3.1 Минимальные требования к аппаратному и программному обеспечению 9

3.2 Варианты установки Device Control Adapter 10

3.3 Подготовка учетных записей Device Control Adapter 12

3.3.1 Подготовка учетной записи для работы службы Device Control Adapter 13

3.4 Используемые порты 15

4 Установка Device Control Adapter 15

5 Настройка Device Control Adapter 18

5.1 Структура конфигурационного файла Device Control Adapter 19

5.2 Описание конфигурационных разделов Device Control Adapter 19

5.2.1 Раздел <applicationSettings> Device Control Adapter 19

5.2.2 Раздел <configSections> Device Control Adapter 20

5.2.3 Раздел <TMConnector> Device Control Adapter 21

5.2.4 Раздел <system.diagnostics> Device Control Adapter 24

5.3 Настройка уровня протоколирования Device Control Adapter 27

6 Мониторинг Device Control Adapter 28

6.1 Журнал приложений Windows для мониторинга Device Control Adapter 28

6.2 Счетчики производительности Windows для мониторинга Device Control Adapter 29

7 Диагностика и устранение неисправностей 29
7.1 Ошибки 29
7.2 Предупреждения 30
8 Удаление Device Control Adapter 30
9 Глоссарий DCA 31

Введение

Device Control Adapter – служба, осуществляющая передачу теневых копий текстов и файлов, получаемых с помощью систем SecureWave Sanctuary Device Control 4.2.2, Lumension Device Control 4.4, 4.6 и Dprint, в систему InfoWatch Traffic Monitor версий 3.x, 4.x, 5.x, 6.x.
В настоящем руководстве вы можете найти сведения по установке Device Control Adapter.
В настоящем руководстве не рассматриваются вопросы установки и настройки сервера SecureWave Sanctuary Device Control, Lumension Device Control и Dprint. За получением необходимых сведений обращайтесь к соответствующей документации.

Аудитория

Информация, содержащаяся в руководстве, предназначена для администраторов, выполняющих установку и настройку Device Control Adapter.
Руководство рассчитано на пользователей, знакомых с основами работы в среде операционной системы Microsoft Windows.

Обзор Device Control Adapter

Основные функции Device Control Adapter:

- Передача данных в InfoWatch Traffic Monitor с помощью XML-транспорта.
- Фильтрация теневых копий по размеру и типу (сигнатуре) файла.
- Получение теневых копий с Device Control Application Server (сервера Системы, с которой производится интеграция) хранящихся как в его локальной файловой системе, так и на удаленном сетевом ресурсе.
- Поддержка нескольких серверов Device Control 4.2.2, 4.4 и 4.6 одним приложением Device Control Adapter.

В этой главе содержится следующая информация:

- Схема работы Device Control Adapter;
- Информация, передаваемая в InfoWatch Traffic Monitor;
- Состав Device Control Adapter.

2.1 Схема работы Device Control Adapter

На рисунке 1 показан принцип работы Device Control Adapter на примере Lumension Device Control. Схема интеграции с SecureWave Sanctuary Device Control и Dprint будет выглядеть идентично ввиду аналогичной с Lumension Device Control структуры решений.
На схеме ниже и во всем документе:

- Lumension Device Control Application Server (LDC AS) – сервер Lumension или другой Системы, с которой происходит интеграция DCA.

- Lumension Device Control Database – база данных Lumension или другой Системы, с которой происходит интеграция DCA.
- Device Control Adapter (DCA) – сервер, на который устанавливается Device Control Adapter.

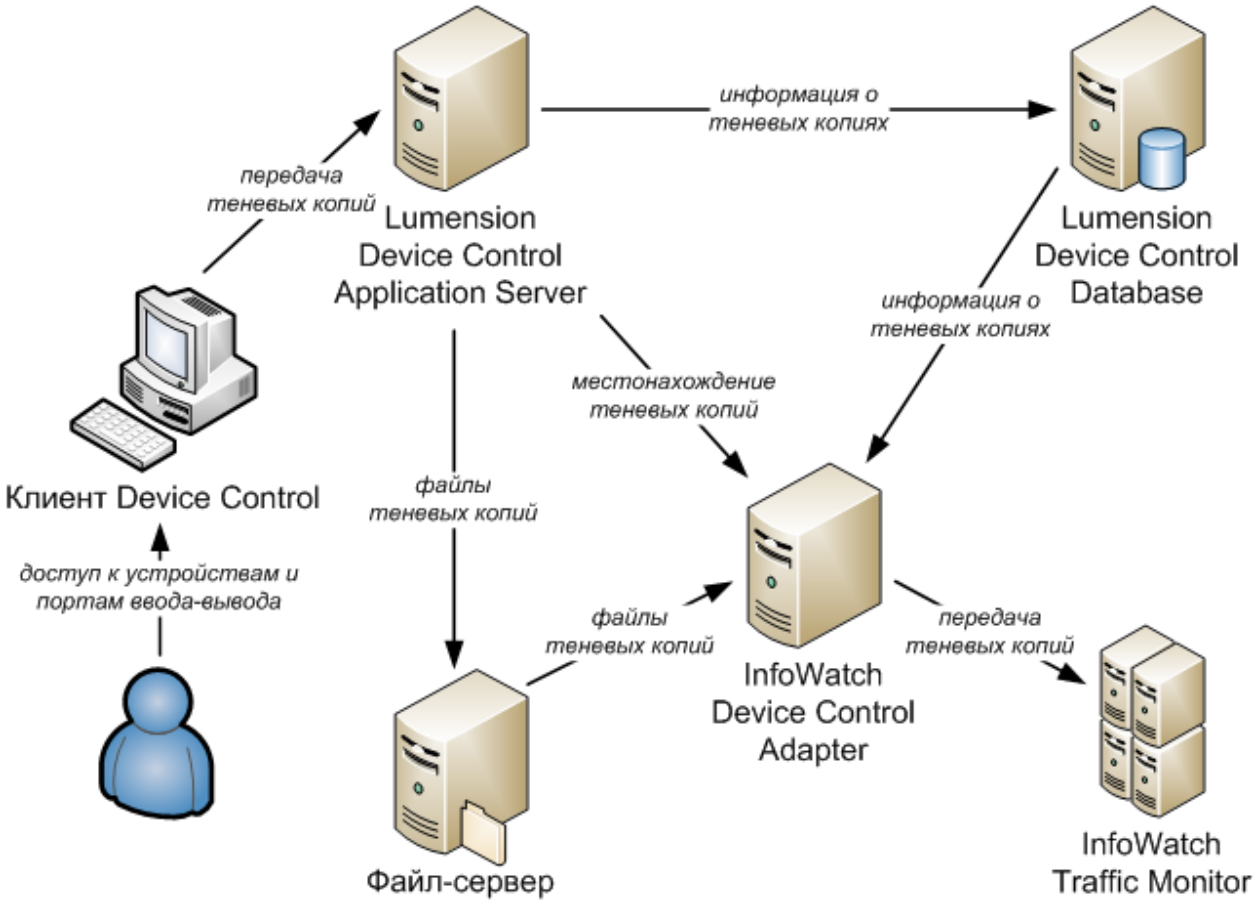


Рисунок 1. Принцип работы Device Control Adapter(вариант с хранением файлов теневых копий на сетевом ресурсе)

Device Control Adapter работает следующим образом:

1. Подключается к базе данных Lumension Device Control и проверяет её на наличие теневых копий удовлетворяющих заданным критериям таким как:
    - размер файла не меньше минимального и не больше максимального;
    - дата снятия теневой копии позднее, чем заданная в конфигурации адаптера.
2. Получает с хоста LDC AS местонахождение файлов теневых копий.
3. Копирует найденные теневые копии на хост с адаптером, и проверяет на соответствие сигнатурам, заданным в конфигурации адаптера.
4. Отправляет теневые копии, соответствующие какой-либо из заданных сигнатур, на Traffic Monitor.
5. Ведет учет идентификаторов отправленных копий во избежание повторной отправки.
6. В зависимости от настроек:

- оставляет теневую копию в LDC DB без изменений;
- удаляет файл теневой копии, оставляя информацию о ней в LDC DB;
- удаляет файл теневой копии, а также всю информацию о ней из LDC DB.

2.2 Информация, передаваемая в InfoWatch Traffic Monitor

В таблице 1 приведен список данных передаваемых из LDC DB в TM, и названия TM, куда попадают переданные данные.

Таблица 1. Передаваемая в TM информация

Поле LDC	Поле TM	Комментарий
–	Сервер перехвата	Имя сервера LDC AS, хранящего теневую копию. В Lumension Endpoint Security Management Console не отображается.
Computer	Рабочая станция	Машина, на которой совершена операция.
Device Class	Тип устройства	Тип устройства, с которым произошла операция (например: Floppy, Cdrom, Removable). Названия типов, используемые в Lumension Endpoint Security Management Console, отличаются от хранимых в LDC DB, хотя и обозначают один и тот же тип устройства. В TM передаются названия типов из LDC DB.
Device Model	Имя устройства	Имя устройства, с которым произошла операция. Обычно здесь указывается производитель и/или модель устройства.
File Name (Full)	Конечный файл	Полный путь и имя файла, с которого снята теневая копия.
Process Name	Приложение	Приложение, совершившее операцию. LDC всегда оставляет это поле пустым.
Size	Размер объекта	Размер файла, с которого снята теневая копия.
Transferred On (UTC)	Дата перехвата	Локальное время на сервере LDC AS в момент регистрации теневой копии в LDC DB. **Примечание:** если адаптер не может запросить часовой пояс сервера LDC AS, то он использует часовой пояс машины, на которой установлен.

Поле LDC	Поле TM	Комментарий
Type	Операция	Действие пользователя, приведшее к созданию теневой копии. В TM передаются события только для следующих типов: WRITE-GRANTED (в TM - Запись разрешена) WRITE-DENIED (в TM - Запись запрещена) READ-GRANTED (в TM - Чтение разрешено) READ-DENIED (в TM - Чтение запрещено)
User	[ЗК] domain	Домен пользователя, совершившего операцию. В Lumension Endpoint Security Management Console отображается вместе с именем пользователя.
User	[ЗК] login	Имя пользователя, совершившего операцию. В Lumension Endpoint Security Management Console отображается вместе с доменом пользователя.
User	Отправитель	Комбинированное значение домена и имени пользователя. TM генерирует значение этого поля из полей [ЗК] domain и [ЗК] login.

2.3 Состав Device Control Adapter

Компоненты, входящие в состав Device Control Adapter, перечислены в таблице 2.

Таблица 2. Компоненты Device Control Adapter

Компонент	Назначение	Имя файла
Database provider	Библиотека, обеспечивающая работу с БД.	`InfoWatch.DeviceMonitor.Database.Core.dll`
Service Core	Общие компоненты службы Device Control Adapter (осуществление бизнес-логики работы с Lumension Device Control и вспомогательные компоненты).	`InfoWatch.DeviceControlAdapter.Service.Core.dll`
InfoWatch Traffic Monitor Connector	Обеспечение взаимодействия с InfoWatch Traffic Monitor.	`InfoWatch.DeviceControlAdapter.Service.Connector.dll`
File type detector	Обеспечение детектирования типов файлов.	`InfoWatch.DeviceLockAdapter.Core.FileType.dll`
Encoding detector	Обеспечение детектирования кодировок текстовых файлов.	`EncodingTools.dll`
Service	Исполняемый файл службы Windows.	

Компонент	Назначение	Имя файла
		`InfoWatch. DeviceControlAdapter.exe`
Service Configuration File	Конфигурационный файл службы Device Control Adapter.	`InfoWatch. DeviceControlAdapter.exe. config`

Подготовка к установке Device Control Adapter

В этой главе содержится следующая информация:

- Минимальные требования к аппаратному и программному обеспечению;
- Варианты установки Device Control Adapter;
- Подготовка учетных записей Device Control Adapter;
- Используемые порты.

3.1 Минимальные требования к аппаратному и программному обеспечению

Минимальные требования к аппаратному обеспечению, необходимому для работы Device Control Adapter, перечислены в таблице 3.

Таблица 3. Аппаратное обеспечение Device Control Adapter

Оборудование	Минимальные требования
Процессор	Pentium 4 с частотой 3 ГГц
Оперативная память	1 Гб
Сетевая карта	100/1000 Мбит/с

Требования к программному обеспечению:

- Lumension Device Control 4.4, 4.6, SecureWave Sanctuary Device Control 4.2.2 или Dprint;
- операционная система Microsoft Windows 2003 Server Service Pack 1 и выше;
- Microsoft .NET Framework 3.0.

3.2 Варианты установки Device Control Adapter

Варианты установки приведены на примере Lumension Device Control. Установка с SecureWave Sanctuary Device Control и Dprint будет выглядеть идентично ввиду аналогичной с Lumension Device Control структуры решений.

При установке Device Control Adapter вам потребуется указать

- Учетную запись, под которой будет работать служба DCA (локальная учетная запись (LOCAL_SYSTEM) или специально созданная учетная запись – см. п. 2.3.1);
- Способ авторизации на сервере MS SQL, где работает база данных Device Control (авторизация в Windows или встроенная учетная запись SQL Server).

Локальная учетная запись (LOCAL_SYSTEM) может быть использована, только если DCA и LDC AS установлены на одной машине. Во всех остальных случаях необходимо создавать специальную учетную запись.

Способ авторизации на сервере LDC DB, определяется параметрами учетной записи службы DCA. Авторизация Windows может быть использована в двух случаях: если служба DCA будет работать под специально созданной учетной записью; а также, если служба DCA устанавливается на тот же компьютер, где расположена LDC DB. Во всех остальных случаях необходимо указывать параметры учетной записи SQL Server имеющей роли **db_datareader** и **db_datawriter** на базу LDC (по-умолчанию sx).

Возможности выбора параметров учетной записи службы DCA зависят от того, где LDC AS хранит теневые копии, и куда будет устанавливаться сама служба DCA. Ниже рассмотрены различные варианты расположения этих объектов и описаны соответствующие им параметры установки.

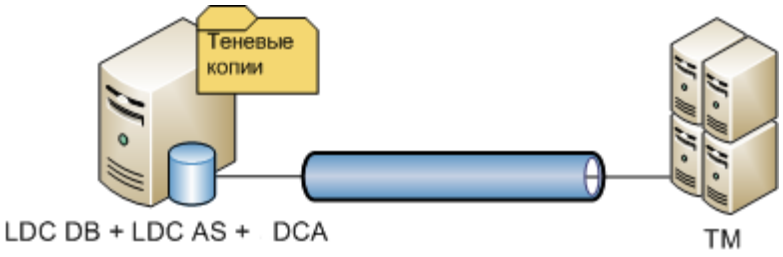
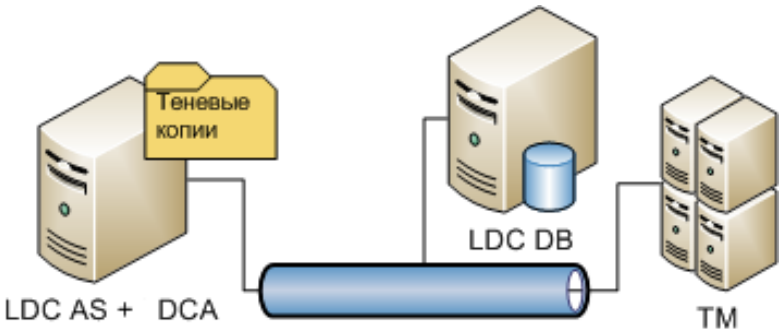
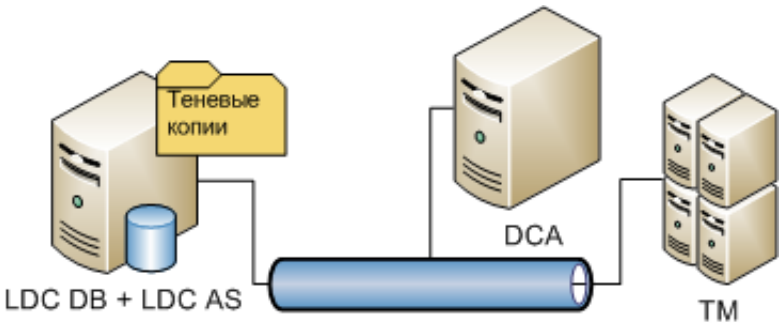
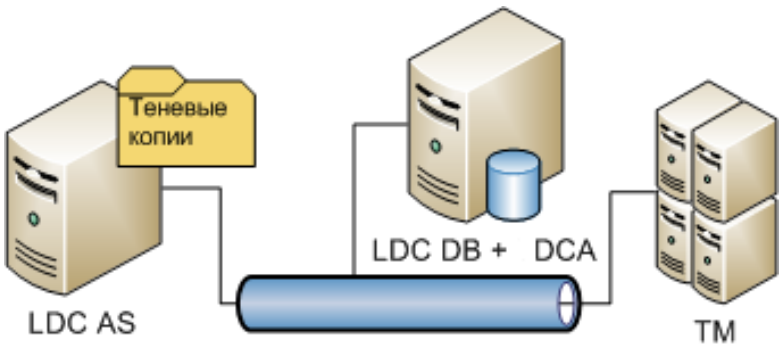
Приведенные варианты описаны с учетом того, что теневые копии хранятся в файловой системе компьютера, на котором работает Device Control Application Server. Это стандартная настройка, установленная для Device Control по-умолчанию. Если в вашей системе теневые файлы хранятся в другом месте, то учетная запись DCA должна иметь доступ на чтение/запись этих файлов.

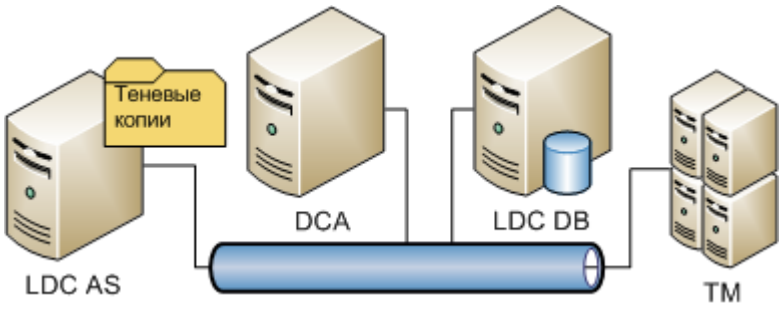
В случае если DCA и LDC AS установлены на различных машинах, и файлы теневых копий хранятся локально на сервере LDC AS, учетная запись DCA должна иметь доступ на чтение /запись административного ресурса, соответствующего диску, хранящему теневые копии. Например, если теневые копии хранятся в **C:\DataFileDirectory**, учетная запись DCA должна иметь доступ по сети к **C$**.

В случае если DCA и LDC AS установлены на различных машинах, на стороне LDC AS должна работать стандартная служба Windows “**Удаленный реестр**” (Remote Registry service), и учетная запись DCA должна иметь доступ на чтение следующих ключей:

- **HKLM\SYSTEM\CurrentControlSet\Services\sxs\parameters**

- **HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation**

Сервер, куда устанавливается DCA	Схема расположения серверов DCA, TM, LDC DB и LDC AS	Параметры установки
Тот же, где установлены LDC AS и LDC DB.		Служба DCA **может** работать под учетной записью локальной системы.
Тот же, где установлен LDC AS. При этом LDC DB находится на другом сервере.		Служба DCA **может** работать под учетной записью локальной системы. Авторизация в LDC DB через учетную запись SQL Server.
Отличный от того, где установлены LDC AS и LDC DB.		Служба DCA **не может** работать под учетной записью локальной системы. Авторизация в LDC DB через учетную запись SQL Server.
Тот же, где установлена LDC DB. LDC AS установлен на отдельном сервере.		Служба DCA **не может** работать под учетной записью локальной системы.

Сервер, куда устанавливается DCA	Схема расположения серверов DCA, TM, LDC DB и LDC AS	Параметры установки
Отличный от того, где установлены LDC AS и LDC DB. LDC AS и LDC DB установлены на различные сервера.		Служба DCA **не может** работать под учетной записью локальной системы. Авторизация в LDC DB через учетную запись SQL Server.

3.3 Подготовка учетных записей Device Control Adapter

Подготовка учетных записей приведена на примере Lumension Device Control. Учетные записи для установки с SecureWave Sanctuary Device Control и Dprint будут иметь идентичные параметры ввиду аналогичной с Lumension Device Control структуры решений.

При установке Device Control Adapter необходимо определить учетные записи, с помощью которых будет работать служба DCA и производиться соединение с базой данных Lumension Device Control. В зависимости от варианта установки (см. статью "Варианты установки Device Control Adapter") существуют следующие варианты:

- **Служба DCA будет работать под учетной записью локальной системы (LOCAL_SYSTEM), при доступе к LDC DB будет использоваться авторизация в Windows** – это возможно, только если служба DCA запускается на том же компьютере, где установлен LDC AS и расположена LDC DB. При этом никаких дополнительных учетных записей подготавливать не требуется.
- **Служба DCA будет работать под учетной записью локальной системы (LOCAL_SYSTEM), при авторизации в LDC DB будет использоваться запись SQL Server** – необходимо подготовить встроенную запись SQL сервера, назначив ей роли **db_datareader** и **db_datawriter** на базу LDC.
- **Служба DCA не может работать под учетной записью локальной системы (LOCAL_SYSTEM), при доступе к LDC DB будет использоваться авторизация в Windows** – вы можете выбрать один из вариантов:

- подготовить специальную учетную запись Windows (см. статью "Подготовка учетной записи для работы службы Device Control Adapter");

- в качестве учетной записи службы указать уже существующую учетную запись с правами на LDC DB (например, использовавшуюся при установке Lumension Device Control), подготовив ее так, как описано в статье "Подготовка учетной записи для работы службы Device Control Adapter ".

- **Служба DCA не может работать под учетной записью локальной системы (LOCAL_SYSTEM), при авторизации в LDC DB будет использоваться учетная запись SQL Server** – необходимо подготовить две записи: учетную запись Windows (см. статью " Подготовка учетной записи для работы службы Device Control Adapter") и встроенную запись SQL сервера, назначив ей роли **db_datareader** и **db_datawriter** на базу LDC.

3.3.1 Подготовка учетной записи для работы службы Device Control Adapter

Если работа Device Control Adapter под учетной записью локальной системы невозможна, то необходимо заранее подготовить специальную учетную запись Windows, под которой будет запущена служба Device Control Adapter.

Если машины с LDC AS, LDC DB и DCA находятся в домене, то чтобы подготовить учетную запись домена Windows для службы Device Control Adapter, выполните следующие действия:

1. Создайте учетную запись домена Windows.
2. Предоставьте этой записи права локального администратора на машине, где установлен DCA (неободимо для создания счетчика производительности Windows).
3. Если LDC AS хранит файлы теневых копий на локальном диске, дайте учетной записи DCA права локального администратора на машине с LDC AS (необходимо для доступа к локальному диску, через административные ресурсы C$, D$ и т.д.).
4. Если LDC AS установлен на машине с ОС **Windows Server 2008**, и хранит файлы на локальном диске, необходимо добавить в реестр этой машины **DWORD** параметр **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilter** со значением 1. Это позволит DCA подключаться к административным ресурсам C$, D$ и т.д. на этой машине.
5. Если LDC AS хранит файлы теневых копий на файловом сервере, дайте учетной записи DCA права на чтение/запись этих файлов (права на запись нужны только при использовании DCA в режимах удаления теневых копий после передачи их в TM).
6. Разрешите подготовленной учетной записи запускать процесс как службу, для этого на контроллере домена:
   a) В **Панели управления** откройте компонент **Администрирование ► Доменная политика безопасности**.
   b) В открывшемся диалоговом окне выберите узел **Локальные политики ► Назначение прав пользователя**.
   c) Справа в области сведений дважды щелкните право **Вход в качестве службы**.
   d) На вкладке **Параметр локальной безопасности** добавьте подготовленную учетную запись.

7. Если для доступа к LDC DB планируется использовать авторизацию Windows:
   a) включите созданную запись в состав учетных записей СУБД MS SQL Server на сервере, где находится LDC DB;
   b) назначьте подготовленной записи роли **db_ datareader** и **db_ datawriter** на базу LDC (по-умолчанию sx).

Если машины с LDC AS, LDC DB и DCA находятся НЕ в домене, то чтобы подготовить учетную запись Windows для службы Device Control Adapter, выполните следующие действия:

1. Создайте идентичные учетные записи Windows на машинах с DCA и LDC AS.
2. Предоставьте права локального администратора для записи на машине, где установлен DCA (неохбодимо для создания счетчика производительности Windows).
3. На машине с DCA, разрешите подготовленной учетной записи запускать процесс как службу, для этого:
   a) В **Панели управления** откройте компонент **Администрирование ► Локальная политика безопасности**.
   b) В открывшемся диалоговом окне выберите узел **Локальные политики ► Назначение прав пользователя**.
   c) Справа в области сведений дважды щелкните право **Вход в качестве службы**.
   d) На вкладке **Параметр локальной безопасности** добавьте подготовленную учетную запись.
4. Если LDC AS хранит файлы теневых копий на локальном диске, дайте учетной записи DCA права локального администратора на машине с LDC AS (необходимо для доступа к локальному диску, через административные ресурсы C$, D$ и т.д.).
5. Если LDC AS установлен на машине с ОС **Windows Server 2008**, и хранит файлы на локальном диске, необходимо добавить в реестр этой машины **DWORD** параметр **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilter** со значением 1. Это позволит DCA подключаться к административным ресурсам C$, D$ и т.д. на этой машине.
6. Если LDC AS хранит файлы теневых копий на файловом сервере, создайте на файловом сервере учетную запись идентичную созданным на шаге 1, и дайте ей права на чтение /запись теневых копий (права на запись нужны только при использовании DCA в режимах удаления теневых копий после передачи их в ТМ).
7. Если для доступа к LDC DB планируется использовать авторизацию Windows:
   a) создайте на машине с LDC DB учетную запись идентичную созданным на шаге 1;
   b) включите созданную запись в состав учетных записей СУБД MS SQL Server на сервере, где находится LDC DB;
   c) назначьте записи роли **db_ datareader** и **db_ datawriter** на базу LDC (по-умолчанию sx).

3.4 Используемые порты

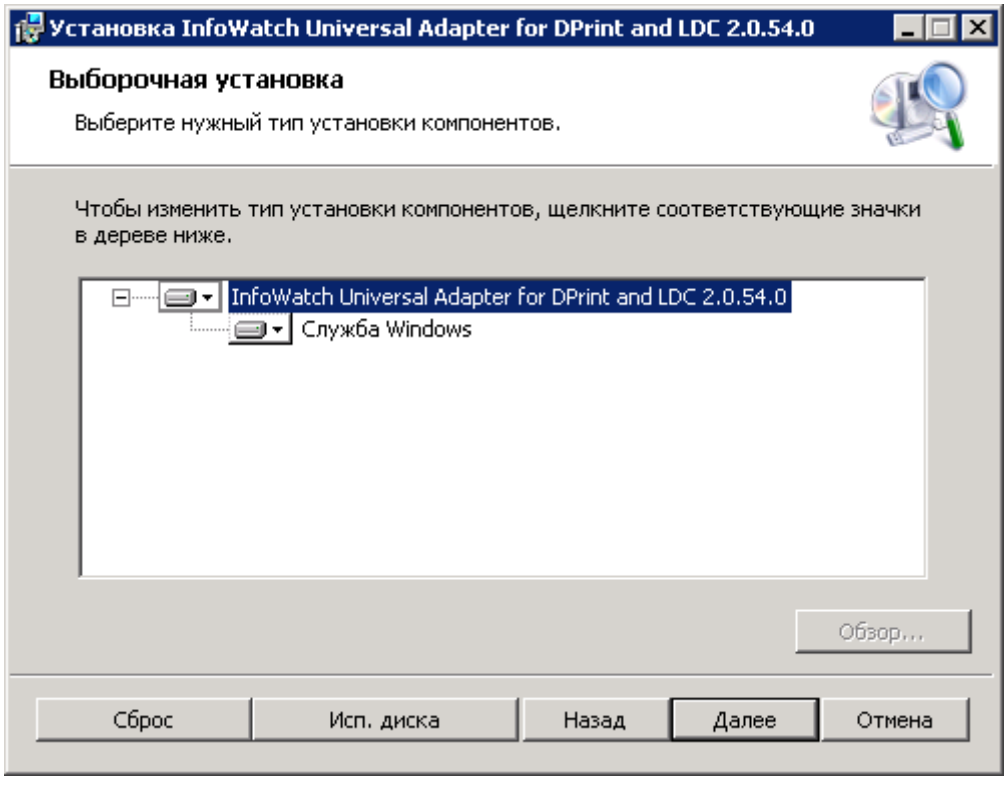
Если между DCA и серверами LDC находится брандмауэр, необходимо разрешить машине с DCA подключения по следующим портам:

- TCP 1433 – для подключения к LDC DB;
- TCP 139 и 445 – для подключения к файловому серверу или серверу LDC AS, если файлы хранятся локально;
- TCP 139 – для подключения к службе удаленного реестра на сервере LDC AS;
- TCP 4101 – для подключения к серверу TM.

Установка Device Control Adapter

Чтобы установить Device Control Adapter:

1. Запустите установочный пакет `setup.DCA.x.x.xx.x.ru.msi`, где `x.x.xxx` – номер версии.
2. В окне приветствия мастера установки InfoWatch Universal Adapter for DPrint and LDC нажмите **Далее**.
3. На шаге **Выборочная установка** укажите каталог, в который будут установлены компоненты DCA.

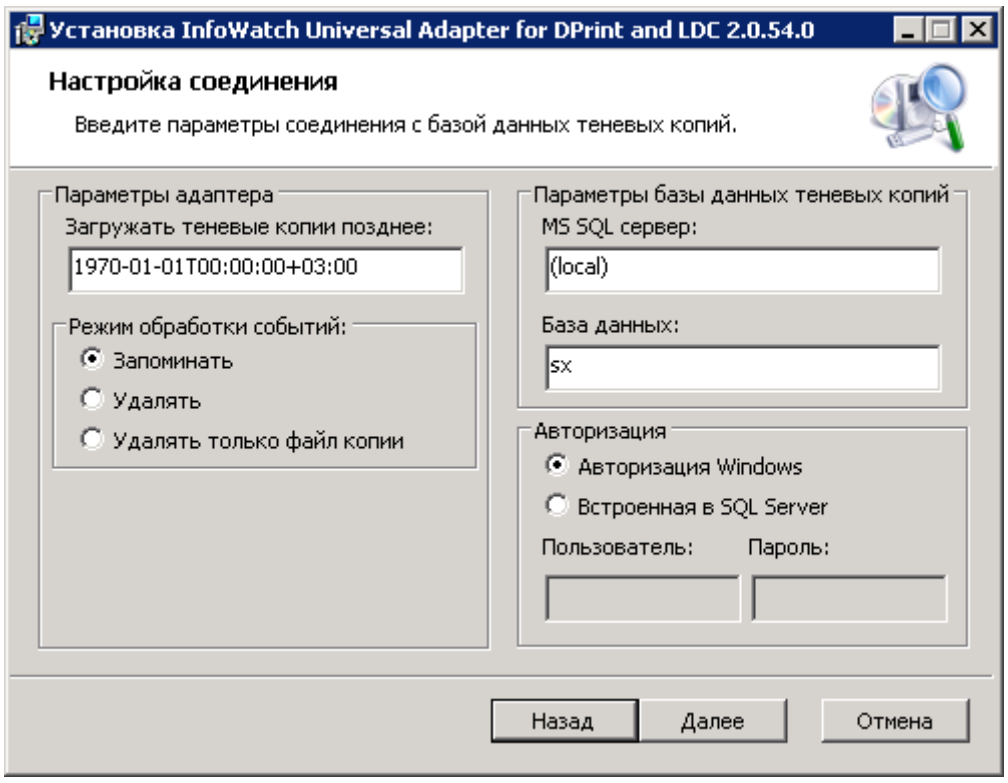


Чтобы изменить папку, в которую будет произведена установка, в дереве компонентов выберите **Служба Windows** и нажмите **Обзор**. В открывшемся окне укажите папку установки.
Нажмите кнопку **Далее**.

4. На шаге **Настройка рабочих параметров службы** укажите следующие настройки:
Настройки фильтрации:
Минимальный размер файла (байт) - определяет минимальный размер файла, отправляемого в InfoWatch Traffic Monitor, в байтах. Файлы меньше этого размера отправляться не будут. Допустимые значения от 0 до 9223372036854775806. Значение по умолчанию 10.
Максимальный размер файла (байт) - определяет максимальный размер файла, отправляемого в InfoWatch Traffic Monitor. Файлы больше этого размера отправляться не будут. Допустимые значения от 1 до 9223372036854775807. Значение по умолчанию 9223372036854775807.
Фильтровать по сигнатуре - определяет, производить ли фильтрацию файлов, отправляемых в InfoWatch Traffic Monitor, по их типу (сигнатуре). Если файл не попадает ни под одну из представленных сигнатур — его отправка не производится (файл отфильтровывается).

> **Примечание:**
>
> Переопределить настройки фильтрации, а также изменить список сигнатур файлов можно при настройке Device Control Adapter, в элементе конфигурационного файла <EventFilter>: см. статью "Элемент <EventFilter> Device Control Adapter".

5. Учетная запись службы:
для работы службы под учетной записью локальной системы выберите **Local System**;
для работы под другой учетной записью выберите Пользователя и укажите **Имя пользователя** и **Пароль учетной записи**.
Нажмите **Далее**.
6. Настройте параметры соединения с сервером Device Control:



Параметры адаптера:

Загружать теневые копии позднее — определяет начальную дату и время создания теневых копий. Т.е. все теневые копии, полученные позднее этой даты, должны отправляться в InfoWatch Traffic Monitor. Более ранние копии отправляться не будут. Формат даты: ГГГГ-ММ-ДДТЧЧ:ММ:СС+ЧЧ:ММ, например: 1970-01-01T00:00:00+03:00 — 1-е января 1970 года, полночь; время по Гринвичу плюс три часа (московское время).

Режим обработки событий:

Запоминать – оставлять файл теневой копии и информацию о нем в системе Lumension Device Control.

Удалять – удалять файл теневой копии и информацию о нем из системы Lumension Device Control.

Удалять только файл копии – удалять только файл теневой копии, оставляя информацию о нем в системе Lumension Device Control.

Параметры базы данных теневых копий MS SQL сервер:

MS SQL сервер — NetBIOS имя сервера СУБД Microsoft SQL Server, где расположена база данных Device Control; или NetBIOS\<имя экземпляра>, если этот сервер имеет именованные экземпляры;

База данных — имя базы данных Device Control.

Авторизация:

Авторизация в Windows — авторизация в LDC DB выполняется с использованием учетной записи Windows.

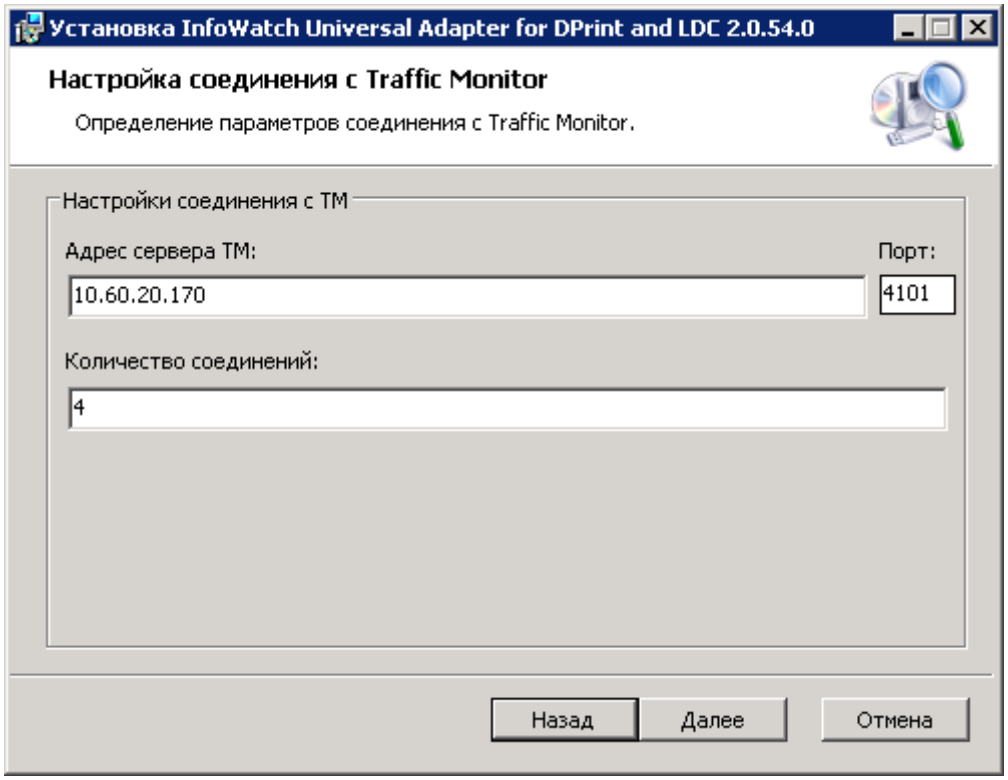
Встроенная в SQL Server — при авторизации в LDC DB используются учетные записи СУБД Microsoft SQL Server. Для этого типа авторизации укажите имя пользователя и пароль встроенной запись SQL сервера, которой назначены роли **db_datareader** и **db_datawriter** на базу LDC (по-умолчанию sx).

Примечание:

Если требуется, чтобы Device Control Adapter поддерживал работу одновременно с несколькими серверами Device Control, то дополнительные сервера и их параметры можно указать при настройке Device Control Adapter, в элементе конфигурационного файла <LdcServers>: см. статью "Элемент <LdcServers> Device Control Adapter".

Нажмите **Далее**.

7. Настройте параметры соединения с сервером InfoWatch Traffic Monitor:



8. **Адрес сервера ТМ**. Адрес сервера InfoWatch Traffic Monitor. Введите IP-адрес или DNS-имя сервера.
9. **Количество соединений**. Количество соединений с сервером InfoWatch Traffic Monitor. Вы можете задать от 1 до 32 соединений.
   Нажмите **Далее**.
10. Нажмите кнопку **Установить**, чтобы начать установку.
11. После успешного завершения установки Device Control Adapter мастер установки отобразит окно с уведомлением. Нажмите **Готово**.

Настройка Device Control Adapter

Настройка Device Control Adapter осуществляется с помощью конфигурационного XML-файла `InfoWatch.DeviceControlAdapter.exe.config`. Конфигурационный файл размещается в том же каталоге, что и исполняемый файл Сервера `InfoWatch.Device ControlAdapter.exe`.

> **Примечание:**
>
> По умолчанию после установки Сервер расположен в каталоге `C:\Program Files\InfoWatch\Device Control Adapter\Service` для 32-битных систем и `C:\Program Files (x86)\InfoWatch\Device Control Adapter\Service` для 64-битных систем.

Конфигурационный файл можно просматривать и редактировать при помощи любого текстового или XML-редактора. Кодировка файла – UTF-8.

5.1 Структура конфигурационного файла Device Control Adapter

Корневым элементом конфигурационного файла является элемент <configuration>. Корневой элемент включает в себя дочерние элементы (конфигурационные разделы). Перечень конфигурационных разделов приведен в таблице.

Таблица 4. Разделы конфигурационного файла

Конфигурационный раздел	Описание
`<configSections>`	Служебный раздел. Содержит описание всех остальных разделов. Редактирование этого раздела не разрешается
`<applicationSettings>`	Содержит настройки отдельных компонентов Device Control Adapter.
`<TMConnector>`	Содержит настройки, специфичные для коннектора Traffic Monitor Server.
`<system.diagnostics>`	Содержит настройки протоколирования. Протоколирование может быть полезно при диагностике работы компонентов Device Control Adapter

5.2 Описание конфигурационных разделов Device Control Adapter

5.2.1 Раздел <applicationSettings> Device Control Adapter

Данный раздел состоит из двух подразделов, определяющих настройки компонентов Device Control Adapter:

- `<InfoWatch.DeviceControlAdapter.Service.Connector.Properties.Settings>` — базовые настройки коннектора Traffic Monitor Server.
- `<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings>` — настройки низкоуровневого драйвера базы данных.

Эти подразделы имеют одинаковую структуру – состоят из набора элементов `<setting>`, предназначенных для настройки параметров компонента. Каждый элемент `<setting>` имеет следующие атрибуты:

- `name` — имя параметра;
- `serializeAs` — способ сериализации данных. Данные всегда сериализуются в виде строки (используется тип данных string).

Значения параметров компонента определяются дочерним элементом `<value>`. Например:

```
<setting name="RemotingPort" serializeAs="String">
<value>15003</value>
</setting>
```

Описание параметров для каждого компонента приводится в таблице.

Таблица 5. Параметры раздела `<applicationSettings>`

Имя параметра	Описание, возможные значения
`<InfoWatch.DeviceControlAdapter.Service.Connector.Properties.Settings>`	
`DBPollTime`	Период (в миллисекундах) опроса базы данных, в процессе которого проверяется наличие событий в базе данных
`CultureName`	Язык диагностических и других сообщений компонента. Возможные значения: • `ru` – русский • `en` - английский
`NumberOfConnections`	Количество соединений с InfoWatch Traffic Monitor. Значение по умолчанию `4` Максимальное значение `32`
`QueueSendLimit`	Максимальное количество событий, которые могут быть переданы из базы данных в InfoWatch Traffic Monitor за одну транзакцию. Значение по умолчанию `200`
`<InfoWatch.DeviceMonitor.Database.Core.Properties.Settings>`	
`CultureName`	Язык диагностических и других сообщений компонента. Возможные значения: • ru - русский • en - английский

5.2.2 Раздел <configSections> Device Control Adapter

Содержит описание всех остальных разделов. Редактирование этого раздела не разрешается.

5.2.3 Раздел <TMConnector> Device Control Adapter

Раздел предназначен для расширенных настроек коннектора InfoWatch Traffic Monitor. В разделе определяется структура и различные параметры сообщений, отправляемых в InfoWatch Traffic Monitor.

- `<TMAddress>`. Адрес сервера InfoWatch Traffic Monitor.

Взаимодействие осуществляется по *xml* схеме. Формат параметра - `xml://host:port`, где *host* — доменное имя или IP-адрес сервера InfoWatch Traffic Monitor, а *port* — порт сервера InfoWatch Traffic Monitor, через который будет осуществляться доставка событий. Порт по умолчанию: `4101`.

- `<EventHandlingMode>`. Режим работы адаптера. Поддерживаются следующие режимы:

- `Remember` после отправки в TM, оставить без изменений файл теневой копии и информацию о нем в системе Lumension Device Control.

- `Delete` после отправки в TM, удалить файл теневой копии, а также всю информацию о нем из системы Lumension Device Control.

- `DeleteShadow` после отправки в TM, удалить только файл теневой копии, оставив информацию о нем в системе Lumension Device Control.

- `<MailHeaderPrefix>`. Префикс, который будет добавляться к именам всех заголовков почтового сообщения.
    - `<UserLogin>`. Имя заголовка, в котором будет отправляться информация об учетной записи пользователя (без указания домена).
    - `<UserDomain>`. Имя заголовка, в котором будет отправляться информация о домене, в котором зарегистрирован пользователь.
- `<From>`. Адрес отправителя сообщения.
    - `<To>`. Адрес получателя сообщения.
    - `<SubjectTemplate>`. Шаблон темы почтового сообщения. В качестве параметров шаблона можно использовать имена атрибутов из параметров `<CommonAttributes>` и `<ShadowAttributes>`.

Параметр задается следующим образом:

`$(<имя атрибута>)`

Например:

`$(Destination)`

Вместо параметра `$(Destination)` будет подставлено имя файла на съемном носителе, в который производилась запись. Имена атрибутов в шаблоне необходимо указывать в точном соответствии с XML-схемой (`<Attribute>name`).

Например,

```
<SubjectTemplate>LDCA. Shadow copy of:
[$(Destination)] from:
[$(WorkstationAddress)] account:
[$(UserAccount)]</SubjectTemplate>
```

В этом шаблоне будет произведена подстановка имени файла, созданного (путем копирования или записи) на съемном носителе. Также здесь содержатся сведения о контролируемой рабочей станции, на которой была перехвачена операция создания файла, и об имени пользователя, выполнившем данную операцию.

В разделе `<TMConnector>` также определены атрибуты сообщений, отправляемых в InfoWatch Traffic Monitor.

> **Важно!**
>
> Значения атрибутов менять не разрешается.

Атрибуты определены в следующих подразделах:

- `<CommonAttributes>`. Определение общих атрибутов сообщений, отправляемых в InfoWatch Traffic Monitor. Внутреннее имя атрибута в Device Control Adapter определяется элементом name. Значение этого элемента менять не разрешается.
- `<ShadowAttributes>`. Для событий теневого копирования. Внутреннее имя атрибута в Device Control Adapter определяется элементом name. Значение этого элемента менять не разрешается.

Описание параметров приведено в таблице.

Таблица 6. Параметры подразделов `<CommonAttributes>` и `<ShadowAttributes>`

Имя параметра	Описание
`<CommonAttributes>`	
`Id`	Идентификатор события
`Interceptor`	Перехватчик (в настоящее время только Shadow)
`Action`	Заблокировано ли событие перехватчиком. Формируется в зависимости от типа операции Lumension.
`EventType`	Тип события (в настоящее время ShadowFull — событие с теневой копией)
`Operation`	Перехваченная операция (запись, печать и т.д.)
`ServerName`	Имя сервера DL ES

Имя параметра	Описание
WorkstationAddress	Имя рабочей станции, с которой была снята теневая копия
WorkstationDns	DNS-имя рабочей станции, с которой была снята теневая копия
WorkstationIp	IP-адрес рабочей станции, с которой была снята теневая копия
WorkstationType	Тип устройства, с которого была снята теневая копия
UserAccount	Учетная запись пользователя, выполнившего перехваченную операцию
Application	Приложение, выполнившее перехваченную операцию
OccurredAt	Дата и время операции
<ShadowAttributes>	
DeviceName	Имя устройства
Device Type	Тип устройства
Destination	Имя конечного файла или документа (если речь идет о печати)
Size	Размер теневой копии в байтах
ShadowId	Идентификатор теневой копии в БД DL ES
ShadowCopy	Наличие теневой копии
Direction	Направление операции

Также в разделе <TMConnector> настраивается фильтрация теневых копий, отправляемых в InfoWatch Traffic Monitor (см. статью "Элемент <EventFilter> Device Control Adapter") и сервера Device Control к которым подключается адаптер (см. статью "Элемент <LdcServers>").

Элемент <EventFilter> Device Control Adapter

Данный элемент содержит определение настроек фильтрации теневых копий, отправляемых в InfoWatch Traffic Monitor.

Элемент содержит атрибут isFilterBySignatures определяющий использовать или нет фильтрацию теневых копий по сигнатурам. Значение true включает фильтрацию, false выключает.

Элемент содержит следующие дочерние элементы, определяющие настройки фильтрации:

- `<MinFileSizeInBytes>`. Определяет минимальный размер файла, отправляемого в InfoWatch Traffic Monitor, в байтах. Файлы меньше этого размера отправляться не будут. Допустимые значения от 0 до 9223372036854775806. Значение по умолчанию 10.
- `<MaxFileSizeInBytes>`. Определяет максимальный размер файла, отправляемого в InfoWatch Traffic Monitor, в байтах. Файлы больше этого размера отправляться не будут. Допустимые значения от 1 до 9223372036854775807. Значение по умолчанию 9223372036854775807.
- `<AcceptableSignatures>`. Определяет список сигнатур файлов, отправляемых в InfoWatch Traffic Monitor. Если файл не попадает ни под одну из представленных сигнатур, — он не отправляется (отфильтровывается). Элемент содержит дочерние элементы `<Signature>`, каждая из которых определяет имя сигнатуры.

Элемент <LdcServers> Device Control Adapter

Данный элемент определяет настройки подключения к каждому из серверов баз данных Device Control, с которыми должен работать Device Control Adapter.

Элемент содержит один или несколько дочерних элементов <Server>, по одному на каждый из серверов LDC DB.

Элемент <Server> содержит следующие дочерние элементы, определяющие настройки соединения с LDC DB:

- `<DBConnectionString>`. Определяет строку соединения с БД в формате ADO.NET для данного экземпляра сервера Device Control.

Пример:

```
Data Source=(local);Initial Catalog=Device ControlDB;Integrated Security=True
```

> **Примечание:**
>
> Если несколько серверов Device Control работают с одной и той же БД, то Device Control Adapter отправляет в InfoWatch Traffic Monitor все копии, записи о которых хранятся в этой БД, независимо от того, с какого сервера Device Control они получены и где хранятся.

- `<TransferShadowsLaterThen>`. Определяет начальную дату и время теневых копий. Т.е. все теневые копии, полученные позднее этой даты, должны отправляться в InfoWatch Traffic Monitor. Более ранние копии отправляться не будут. Формат даты: ГГГГ-ММ-ДДТЧЧ:ММ:СС+ЧЧ:ММ, например: 1970-01-01T00:00:00+03:00, — 1-е января 1970 года полночь, время по Гринвичу плюс три часа (московское время)

5.2.4 Раздел <system.diagnostics> Device Control Adapter

Раздел предназначен для настройки параметров диагностики работы адаптера. Включает в себя следующие элементы:

- `<trace>` — общие настройки диагностики.
- `<sources>` — настройки, необходимые для диагностики отдельных компонентов адаптера.
- `<switches>` — управление уровнем протоколирования диагностической системы в целом. Если для разных компонентов требуются разные настройки протоколирования, то их можно настроить с помощью фильтра в элементе <sources>.

Элемент <trace> Device Control Adapter

Используется для описания глобальных настроек диагностики.

Элемент `<trace>` имеет следующие атрибуты:

- `autoflush` — параметр сохранения данных из потока диагностических сообщений на жесткий диск: `true` – данные сохраняются, `false` – сохранение не производится;
- `indentsize` — величина отступов в сообщениях.

Элемент <sources> Device Control Adapter

Используется для настройки отдельных компонентов приложения. Включает в себя дочерние элементы <source> – по одному на каждый компонент приложения.

Элемент `<source>` имеет следующие атрибуты:

- `name` — имя компонента;
- `switchName` — имя компонента, определяющего уровень протоколирования диагностических сообщений (детализатора);
- `switchType` — тип компонента, определяющего уровень протоколирования диагностических сообщений. Всегда имеет значение System.Diagnostics.SourceSwitch.

В каждом элементе `<source>` также содержится определение приемников диагностических сообщений (`<listeners>`). Приемниками диагностических сообщений могут быть:

- журнал приложений Windows (Application log) – является приемником по умолчанию;
- системный отладочный вывод (можно просматривать с помощью специальных инструментов, например DebugView: http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx);
    - текстовый файл.

Элемент `<listeners>` может включать в себя следующие дочерние элементы:

- `<remove>` — удаление приемника диагностических сообщений по умолчанию (журнал приложений Windows).

Чтобы исключить журнал приложений Windows из перечня приемников сообщений:

установите имя элемента равным `Default`:

```
<remove name="Default" />
```

- `<add>` — добавление нового приемника диагностических сообщений. Элемент содержит следующие атрибуты:

- `name` — имя приемника диагностических сообщений.

- `type` — полное имя типа приемника диагностических сообщений: из библиотеки классов .NET Framework или собственного типа.

> **Примечание:**
>
> В библиотеке классов .NET Framework определены следующие типы приемников диагностических сообщений:
>
> – System.Diagnostics.EventLogTraceListener. Журнал приложений Windows (Application log);
>
> – System.Diagnostics.ConsoleTraceListener. Вывод сообщений в консольном приложении;
>
> – System.Diagnostics.TextWriterTraceListener. Вывод в текстовый файл;
>
> – System.Diagnostics.DefaultTraceListener. Отладочный вывод Windows (по умолчанию включен).

- `initializeData`. Идентификатор компонента адаптера. Как правило, это значение совпадает с именем соответствующего компонента. Если в качестве приемника используется журнал приложений Windows, этот идентификатор будет отображаться для событий Device Control Adapter в столбце **Source**.

Элемент `<add>` также содержит фильтр диагностических сообщений. Данный фильтр выводит только те сообщения с уровнем важности, не превышающим заданный в настройках фильтра.

Чтобы определить фильтр диагностических сообщений:

укажите необходимый уровень протоколирования, например:

```
<filter type="System.Diagnostics.EventTypeFilter" initializeData="Information"/>
```

В приведенном примере будут протоколироваться события с уровнем **Warning**, **Error**, **Critical** и **Information**

> **Примечание:**
>
> Подробнее о настройке уровня протоколирования см. статью "Настройка уровня протоколирования Device Control Adapter".

Элемент <switches> Device Control Adapter

Определяет глобальный (для всего сервера) уровень протоколирования сообщений диагностической системы. Если отдельным компонентам адаптера требуется более низкий уровень протоколирования, то в этом случае можно воспользоваться фильтром в элементе `<sources>`.

По-умолчанию элемент `<switches>` содержит только один дочерний элемент:

`<add name="eventLog" value="Warning"/>`.

Уровень протоколирования задается как значение атрибута `value`.

> **Примечание:**
>
> Подробнее о настройке уровня протоколирования см. статью "Настройка уровня протоколирования Device Control Adapter".

5.3 Настройка уровня протоколирования Device Control Adapter

Определяя уровень протоколирования, можно настроить вывод только тех диагностических сообщений, чей уровень превышает заданный в настройках. Определены следующие уровни протоколирования (приведены в порядке возрастания):

- **Critical**. Критический уровень. Регистрируются только серьёзные нарушения в работе, которые могут привести к неработоспособности адаптера.
- **Error**. Уровень ошибок. Регистрируются ошибки, мешающие корректной работе Системы (т.е. ошибки, требующие исправления).
- **Warning**. Уровень предупреждения. Помимо событий, входящих в уровни **Critical** и **Error**, регистрируются некритичные ошибки в работе адаптера, такие как неожиданное прекращение соединения с сервером Device Control или Traffic Monitor, истекший таймаут соединения и пр.
- **Information**. Информационный уровень. Помимо событий, входящих в уровни **Critical**, **Error** и **Warning**, регистрируются события, не связанные с ошибками, такие как, например, информация об изменении параметров сервера.
- **Verbose**. Отладочный уровень, в журнале регистрируются все события. Данный уровень нужно применять только для отладки адаптера. Не разрешается устанавливать данный уровень для адаптера, работающего в нормальном режиме, так как это приводит к значительному снижению производительности.

Уровень протоколирования диагностических сообщений настраивается в двух местах конфигурационного файла:

- В элементе `<switches>` — глобальный уровень для всего адаптера;

- В элементе `<add>` для каждого из `<listeners>` элемента `<source>` —для каждого из компонентов.

При определении глобального уровня протоколирования необходимо следить, чтобы он был не меньше, чем, максимальный установленный уровень протоколирования компонентов. В противном случае события с более высоким уровнем, чем определено глобально, не будут регистрироваться.

Пример 1

Установлен глобальный уровень протоколирования **Verbose**, а для фильтра одного из компонентов – **Warning**. В таком случае для этого компонента будут протоколироваться события с уровнем **Warning**, **Error** и **Critical**, но отфильтровываться - события с уровнем **Information** и **Verbose**.

Пример 2

Установлен глобальный уровень протоколирования **Error**, а для фильтра одного из компонентов – **Warning**. В таком случае для этого компонента будут протоколироваться события с уровнем **Error** и **Critical**, но отфильтровываться - события с уровнем **Warning**, **Information** и **Verbose**. Это происходит потому, что общий уровень протоколирования — **Error**, т. е. вне зависимости от того, как настроены фильтры, регистрируются только сообщения с уровнем **Error** и меньше.

Мониторинг Device Control Adapter

Глава содержит информацию о мониторинге состояния Системы:

- Журнал приложений Windows для мониторинга Device Control Adapter;
- Счетчики производительности Windows для мониторинга Device Control Adapter.

6.1 Журнал приложений Windows для мониторинга Device Control Adapter

Стандартный журнал приложений Windows (**Event Viewer –> Applications**) регистрирует сообщения от службы Device Control Adapter как поступившие от источников, начинающихся с `InfoWatch.DeviceControlAdapter` или `InfoWatch.DeviceMonitor`. Каждый источник определяет модуль службы, сгенерировавший данное журнальное сообщение:

- `InfoWatch.DeviceControlAdapter.Service.Connector` — модуль взаимодействия с TM;
- `InfoWatch.DeviceControlAdapter.Service.Core` — ядро службы;
- `InfoWatch.DeviceControlAdapter.Core.FileType` — детектор сигнатур;
- `InfoWatch.DeviceMonitor.Database.Core` — модуль взаимодействия с БД.

6.2 Счетчики производительности Windows для мониторинга Device Control Adapter

Мониторинг длины очереди событий, ожидающих отправки в TM, (отдельной для каждого из подключенных к Device Control Adapter серверов Device Control) осуществляется с помощью счетчиков производительности Windows. Для каждого сервера Device Control определен свой экземпляр счетчика. Имя экземпляра счетчика состоит из имени сервера и идентификатора этого сервера в LDC DB.

Чтобы наблюдать длину очереди теневых копий, ожидающих отправки в TM:

1. Откройте стандартную оснастку мониторинга производительности (**Control Panel –> Administrative Tools –> Performance**).
2. Добавьте новый счетчик:

- В качестве категории счетчиков выберите `InfoWatch DeviceControl Adapter`.

В списке счетчиков длины очереди будет выбран единственный счетчик `Device Control Event Queue Length`.

- Выберите имя необходимого экземпляра сервера Device Control или выберите счетчик `_Total` (суммарная длина очереди событий от всех серверов Device Control).

Диагностика и устранение неисправностей

В ходе своей работы адаптер может фиксировать в EventLog сообщения об ошибках. Наличие таких сообщений может сигнализировать о неисправностях в работе ПО. В следующих главах приведены примеры ошибок и предупреждений, которые могут быть выведены в EventLog и общие рекомендации по их исправлению:

- Ошибки;
- Предупреждения.

7.1 Ошибки

- `Ошибка конфигурации: <описание ошибки>`

Пример: `Ошибка конфигурации: неверный режим обработки событий: 'Romember'.`
Решение: Проверьте конфигурационный файл на наличие некорректно заданных параметров и исправьте неверное значение. Перезапустите сервис адаптера.

- `Нет соединения с Traffic Monitor`

Причина: Соединение с ТМ отсутствует.
Решение: Проверьте настройки соединения с ТМ, наличие связи между сервером адаптера и сервером ТМ, работоспособность сервера ТМ.

- `Нет прав на использование реестра на <имя сервера>`

Причина: Недостаточно прав для чтения реестра на сервере LDC.
Решение: Проверьте настройки прав доступа для пользователя, от имени которого выполняется сервис адаптера.

- `Ошибка при проверке связи с БД LDC: <текст ошибки>`

Причина: Не удалось выполнить тестовый запрос к базе данных LDC.
Решение: Проверьте конфигурацию адаптера, наличие связи между сервером адаптера и сервером БД LDC. Проверьте настройки БД LDC (разрешены ли подключения к БД по сети).

7.2 Предупреждения

- `Есть <N> потерянных событий которые не были отправлены из-за ошибок. Отправляем.`

Причина: Во время отправки событий ранее возникла какая-то ошибка. Будет осуществляться повторная передача событий.
Решение: Проверьте системный лог адаптера на наличие ошибок.

- `Установлено <N> из <M> соединений с ТМ.`

`При этом N < M.`
Причина: Не все соединения с ТМ удалось установить.
Решение: Проверьте соответствие настроек адаптера настройкам ТМ в части количества соединений.

- `Не найден файл <путь к файлу> теневой копии`

Причина: Файл теневой копии был удалён или нет прав доступа к файлу.
Решение: Проверьте наличие прав доступа для пользователя, от имени которого выполняется адаптер, к указанному пути.

Удаление Device Control Adapter

Для того чтобы удалить Device Control Adapter, запустите файл установки `Setup.Service.ru.msi` (для русскоязычного интерфейса мастера установки) или `Setup.Service.en.msi` (для англоязычного интерфейса мастера установки).

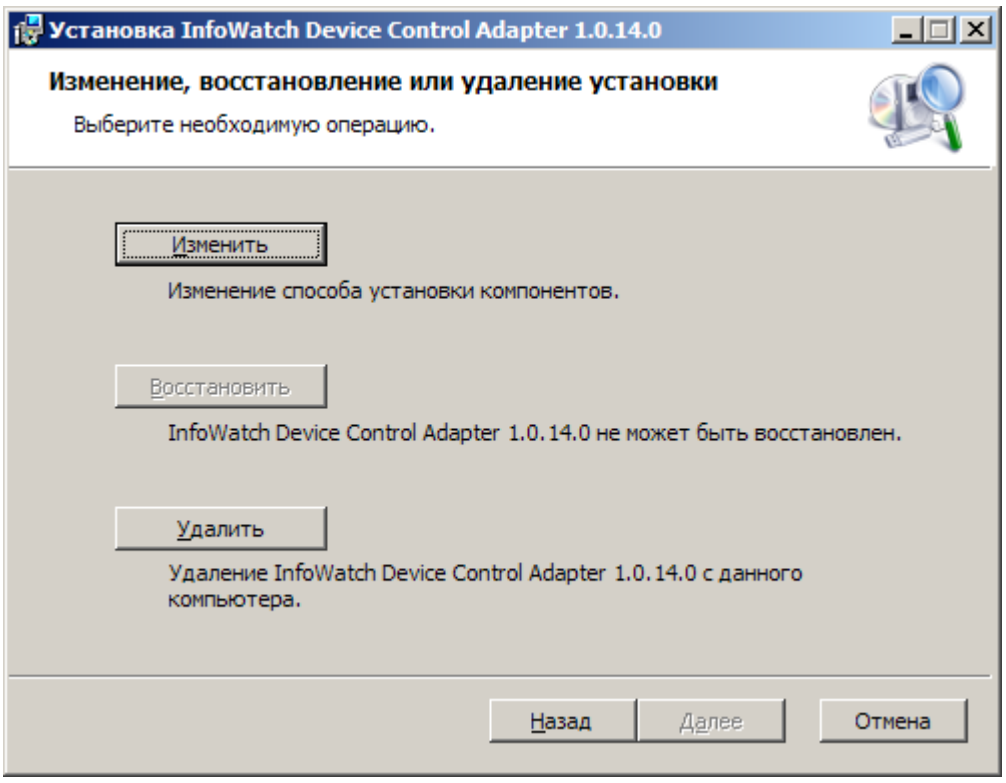


Рисунок 2. Удаление Device Control Adapter

Нажмите кнопку **Удалить**.

Все файлы Device Control Adapter будут удалены с компьютера вместе с созданными в процессе установки папками.

Глоссарий DCA

Device Control

Система контроля доступа к периферийным устройствам компьютерной системы. Также производит мониторинг информации, переносимой с рабочих станций на съемные устройства или отправляемой на печать.

LDC

Смотри Device Control.

LDC DB

Lumension Device Control Database – база данных Lumension или другой Системы, с которой происходит интеграция DCA.

LDC AS

Lumension Device Control Application Server – сервер Lumension или другой Системы, с которой происходит интеграция DCA, который отвечает за прием теневых копий от агентов LDC и загрузку их в LDC DB.

DCA

Служба Device Control Adapter.

InfoWatch Traffic Monitor

Система, предназначенная для перехвата, фильтрации и анализа информационных потоков компьютерной системы.

TM

Система InfoWatch Traffic Monitor.

БД

База данных.

Контроль доступа к периферийным устройствам

Разграничение прав на работу с периферийными устройствами компьютерной системы. Определение уровня доступа к различным типам периферийных устройств выполняется в соответствии с требованиями корпоративной политики безопасности. Для разных групп пользователей и групп рабочих станций может быть настроен разный уровень доступа к тому или иному периферийному устройству.

СУБД

Система управления базами данных.

Теневая копия текста

Копия текста, выделенного из документа, отправленного на печать.

Теневая копия файла

Копия файла, создаваемого на съемном устройстве. Создается только при успешном завершении операции сохранения файла на съемное устройство. Анализ теневых копий файлов выполняется в системе InfoWatch Traffic Monitor.