"СОФТ ПИ АЙ"

SoftPI Flow Collector

Руководство пользователя

Версия документа: 2.00

Дата документа: май 2012

Назначение

Система SoftPI Flow Collector предназначена для сбора информации о сетевых потоках на основании данных протоколов NetFlow версий 5 или 9 (Cisco Systems), IPFIX или RFlow, а также агрегации собранной информации с последующим сохранением в хранилище одного из трёх типов:

- база данных Microsoft SQL,
- база данных MySQL
- текстовый файл.

Схема сбора данных о сетевых потоках с использованием SoftPI Flow Collector-а от различных сетевых устройств, которые применяют различные протоколы (NetFlow версии 5 и 9, а также IPFIX), представлена на рисунке 1.

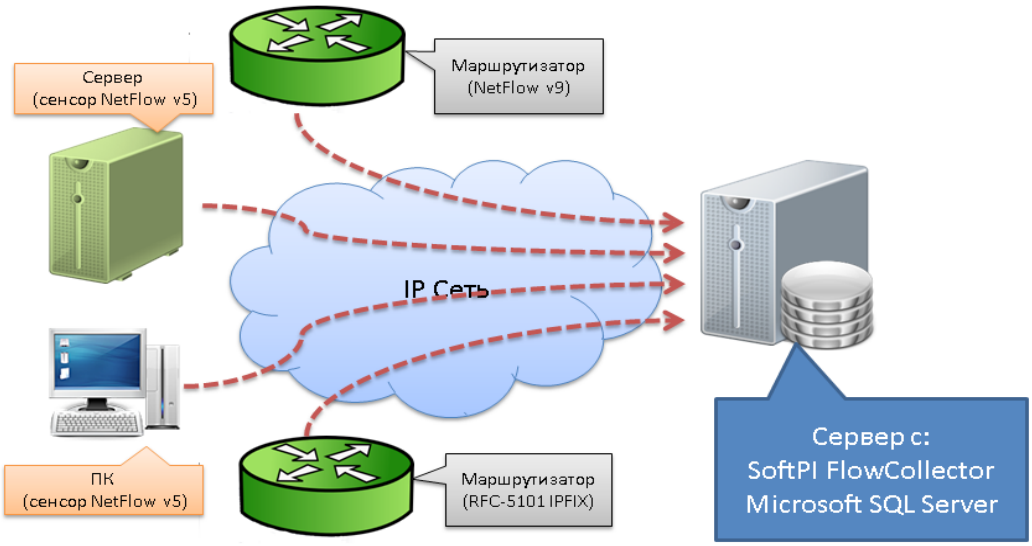

Рисунок 1

Как видно из этого рисунка, SoftPI Flow Collector установлен на сервере, и в качестве хранилища используется Microsoft SQL Server. Информация о сетевом трафике поступает с маршрутизаторов, один из которых использует протокол NetFlow версии 9, а другой IPFIX, а также с компьютеров, на которых установлен сенсор NetFlow потока версии 5. Этот вариант есть лишь примером использования SoftPI Flow Collector-а и, возможны другие конфигурации системы.

1. Основные функции

SoftPI Flow Collector (далее Flow коллектор или Коллектор) является реализацией NetFlow, RFlow и IPFIX коллекторов в виде одного коллектора, с возможностью агрегации данных и записи обработанных данных в различные типы хранилищ. Система работает под операционными система Windows 2000/XP/2003/Vista/2008/7.

Поддерживаемые форматы сетевых потоков

Коллектор позволяет собирать и обрабатывать информацию о сетевых потоках с использованием следующих протоколов:

- NetFlow версии 5,
- NetFlow версии 9,
- Rflow,
- IPFIX.

Поддерживается получение и хранение всего перечня полей указанных протоколов. При отсутствии необходимости в каких-то полях пользователь может задать только требуемые ему поля.

Для ознакомления с назначением и особенностями указанных протоколов рекомендуем познакомиться со следующими источниками: [1, 2].

Гибкая настройка обрабатываемых параметров, параметров агрегации и сохранения

При настойке параметров Коллектора обеспечивается:

- Настройка списка обрабатываемых полей.
- Настраиваемый список сохраняемых в хранилище полей.
- Настраиваемый список полей для агрегации.
- Отдельный бинарный лог для каждого из сенсоров или устройств NetFlow/IPFIX/RFlow.
- Возможность архивации лог файла сразу же после получения данных.
- Возможность одновременного получения данных через несколько IP портов.

Различные типы хранилищ

Поддерживается сохранение обработанной информации в одном из следующих хранилищ:

- текстовый файл,
- база данных Miscosoft SQL Server,
- база данных MySQL.

При выборе в качестве хранилища Microsoft SQL Server и выборе полей, соответствующих протоколу NetFlow версии 5, имеется возможность использования базы данных с дополнительными справочными таблицами данных: IP протоколов и IP портов. В этом случае также доступен перечень отчетов для анализа полученных данных.

Графический интерфейс настройки параметров

Все настройки параметров Flow коллектора осуществляются в удобном графическом интерфейсе.

Отсутствие ограничений на количество сетевых устройств

Flow коллектор не имеет ограничений на количество сетевых устройств, с которых он может одновременно получать информацию. В основном, ограничения могут быть обусловлены лишь параметрами сервера (компьютера), используемого для работы Flow коллектора.

Отчеты для анализа данных

Flow коллектор содержит набор форм отчетов и соответствующий генератор отчетов, обеспечивающих вывод обработанных данных в табличном и графическом видах. Отчеты доступны лишь при использовании Microsoft SQL Server-а и набора данных, соответствующего протоколу NetFlow версии 5.

Отчеты также могут формироваться с помощью службы отчетности SQL Server (SQL Server Reporting Services — SSRS).

Возможность редактирования отчетов и создания собственных

Пользователь, используя бесплатные продукты Microsoft: Report Builder v3.0 или Среду SQL Server Business Intelligence Development Studio из состава Microsoft SQL Server 2008 R2, может самостоятельно редактировать поставляемые с SoftPI Flow Collector-ом формы отчетов или создавать свои собственные.

2. Состав

В состав Flow коллектора входят:

- Служба Windows: SoftPI NetFlow/IPFIX Collector;
- Программа "Настройка коллектора сетевых потоков" (далее программа настройки).

Служба SoftPI NetFlow/IPFIX Collector (далее служба Flow Collector) выполняет приём, обработку и агрегацию сетевых потоков в форматах NetFlow версии 5 или 9, RFlow и IPFIX, а также запись обработанной информации в хранилище. Как указывалось выше эта служба может принимать одновременно данные от нескольких сетевых устройств, количество которых не ограничивается, через различные IP порты, обрабатывать полученные данные, записывая в хранилище только заданные пользователем поля, и использовать одно из 3-х типов хранилищ данных.

Программа "Настройка коллектора сетевых потоков" предназначена для:

- задания параметров службы Flow Collector-а,
- запуска и остановки работы службы Flow Collector-а,
- формирования табличных и графических отчетов по полученным данным.

3. Аппаратные и программные требования

Компьютер, на который будет устанавливаться SoftPI Flow Collector должен иметь параметры не хуже указанных ниже:

- Процессор с частотой 1 ГГц или более производительный.
- Оперативная память 512 Мб и выше.
- Жесткий диск (40 Гбайт).
- LAN порт (100 или 1000 Мбит/с).

Для работы системы необходимы следующие программные компоненты:

- Операционная система: Windows XP/Vista/7 или Windows Server 2003/2008;
- Среда .Net Framework 3.5. Если при инсталляции SoftPI Flow Collector компьютер имеет подключение к интернет и не содержит среду .Net Framework 3.5, то эта среда загрузится и установится автоматически. Если компьютер в момент инсталляции системы не будет иметь подключения к интернет, то для работы системы вы должны самостоятельно загрузить и установить среду .Net Framework 3.5.
- В зависимости от предполагаемого типа хранилища может потребоваться установка: MySQL 5.0 и выше (http://www.mysql.com/downloads/mysql/) или Microsoft SQL Server 2000/2005/2008 или 2000MSDE/2005 Express/2008 Express (http://www.microsoft.com/express/sql/default.aspx)

В случае установки Microsoft SQL Server 2008 R2 предлагаем воспользоваться рекомендациями статьи [3].

4. Инсталляция

После запуска инсталляционного файла (flowcollector.17.exe) пользователь в режиме мастера может задать требуемые параметры.

Первоначально появляется окно "Installer Language" (рисунок 2), предлагающее пользователю выбрать требуемый язык программы и процесса инсталляции.

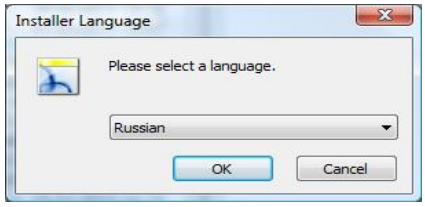

Рисунок 2

Вы можете выбрать либо русский язык (Russian), либо английский (English). После чего щелкните по кнопке "OK".
В появившемся следующем окне щелкните по кнопке "Далее".
Появится окно (рисунок 3), где можно задать папку, в которую будет установлена программа.

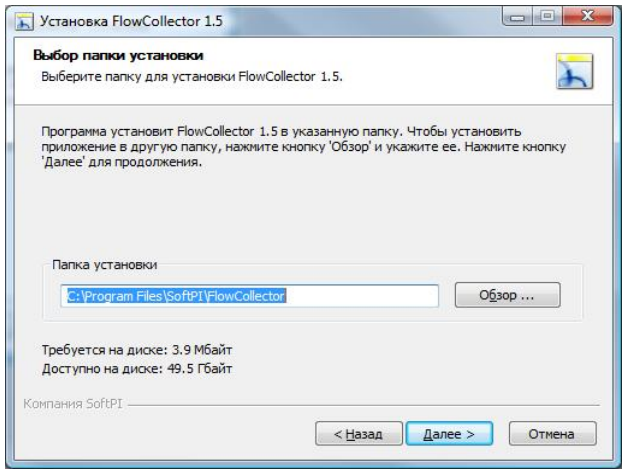

Рисунок 3

По умолчанию задается папка: \Program Files\SoftPI\FlowCollector
Щелкните по кнопке "Далее". Появится окно (рисунок 4), позволяющее отредактировать наименование программы, которое будет отображаться в меню кнопки "Пуск" (Windows). По умолчанию предлагается наименование SoftPI FlowCollector. Далее щелкните по кнопке "Установить" в результате чего программное обеспечение будет установлено на компьютере.

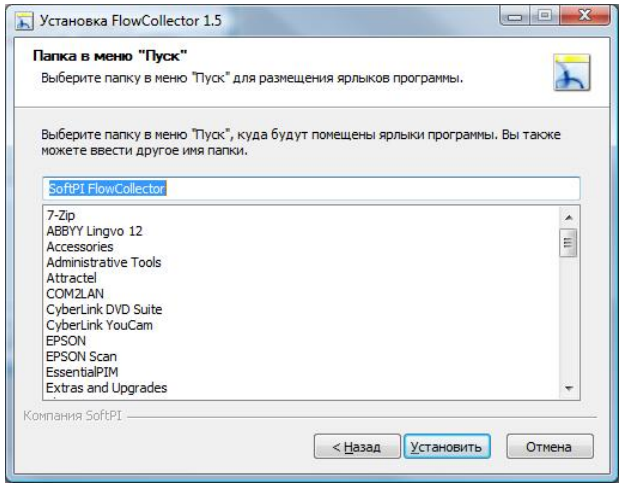

Рисунок 4

5. Деинсталляция

Для удаления из компьютера SoftPI Flow Collector-а необходимо:

- Открыть "Панель Управления" операционной системы Windows.
- В "Панели Управления", в зависимости от типа используемой операционной системы, выбрать пункт "Программы и компоненты" или “Установка и удаление программ”.
- Из появившегося списка выбрать пункт “Flow Collector 1.5” и щелкнуть по кнопке "Удалить/Изменить". Будет запущена программа деинсталляции.

Замечание

Удаление программы не приводит к удалению хранилища, на которое настроен Коллектор. Если для хранилища был выбран тип MS SQL (Microsoft SQL Server) или MySQL, то для удаления базы данных необходимо воспользоваться средствами администрирования соответствующей СУБД.

6. Настройка системы

Настройка и запуск системы производится в программе "Настройка коллектора сетевых потоков", и этот процесс состоит из следующих этапов:

- настройка параметров сбора данных (компонент "Сбор данных", описание в разделе 6.1);
- выбор типа хранилища, который будет использоваться. В случае если в качестве хранилища предполагается Microsoft SQL Server или MySQL, необходимо загрузить соответствующую инсталляцию и установить ее на компьютере*;
- настройка параметров хранилища данных (компонент "Хранилище", описание в разделе 6.2);
- настройка параметров агрегации при необходимости (компонент "Агрегация", описание в разделе 6.3);
- запуск службы (компонент "Служба", описание в разделе 6.4).

**В случае выбора в качестве хранилища Microsoft SQL Server 2008 R2 для его установки в системе можно воспользоваться рекомендациями, изложенными в* [3].

6.1. Настройка параметров сбора данных

Запустите программу "Настройка коллектора сетевых потоков" и выберите компонент "Сбор данных". Программа примет вид, как показано на рисунке 6.1. В позиции "Слушать порты" введите перечень IP портов, которые должны использоваться для приема данных службой Flow Collector (служба работает только с использованием UDP протокола). В случае использования более одного порта их номера должны вводится через запятую. По умолчанию задан IP порт 2055, который обычно используется для NetFlow протокола. Для IPFIX протокола в соответствии с RFC 5101 должен использоваться порт 4739 для незащищенного соединения, которое выполняется через UDP протокол. Однако, не все производители придерживаются этого требования. Поэтому в документации на телекоммуникационное оборудование следует точно определить номер IP порта, который используется для передачи данных NetFlow, IPFIX или RFlow протоколов.

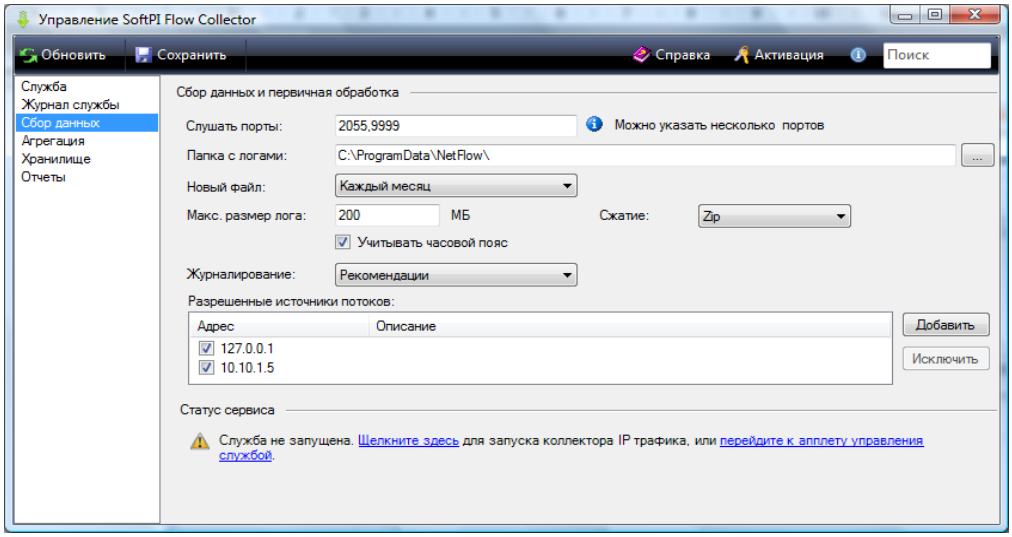

Рисунок 6.1

Flow коллектор кроме обработки поступающего потока данных и записи его в хранилище выполняет резервное копирование потока данных в бинарный файл в том виде, в каком эти данные поступили на сетевой интерфейс.

В позиции "Папка с логами" можно изменить путь к папке, куда будут записываться файлы с бинарной информацией, полученной от телекоммуникационного устройства. По умолчанию задается папка: \ProgramData\NetFlow\

Выберите в списке "Новый файл" период создания нового лог файла для бинарных данных, получаемых от телекоммуникационного устройства. Возможные варианты выбора:

- Не создавать;
- Каждый час;
- Каждый день;
- Каждый месяц.

Вне зависимости от выбранного периода в позиции "Новый файл" можно в позиции "Макс. размер лога" определить размер лог файла, по достижении которого будет создаваться новый файл. По умолчанию используется значение: 200 Мбайт.

Для уменьшения объема, занимаемого лог файлом, можно выполнять его сжатие. Сжатие выполняется сразу же при записи данных в файл. Возможно использование различных алгоритмов сжатия данных, что определяется выбором в списке "Сжатие". Возможные варианты:

- Без сжатия;
- Zip;
- Bzip;
- Zlib.

Служба Flow Collector может вести журнал результатов своей работы с различной степенью детализации. Степень детализации определяется значением параметра заданного в списке "Журналирование". Возможны следующие варианты:

- Статус,
- Критические ошибки,
- Ошибки,
- Предупреждения,
- Информация,
- Рекомендации,
- Отладка,

"Статус" — это наименее детальный уровень. "Отладка" — наиболее детальный уровень. По умолчанию задается уровень "Информация".

Задайте в разделе "Разрешенные источники потоков" IP адреса телекоммуникационных устройств, с которых служба Flow Collector должна получать информацию. Для добавления нового IP адреса щелкните по кнопке "Добавить". Появится окно "Источник данных", показанное на рисунке 6.2.

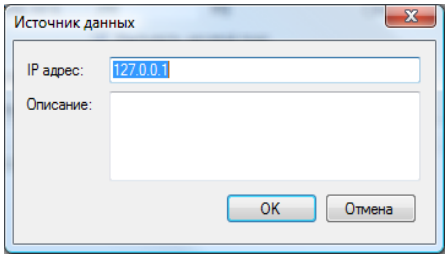

Рисунок 6.2

В позиции "IP адрес" введите IP адрес требуемого устройства.
Позиция "Описание" носит информационный характер и не обязательна для ввода.

Примечание. *Служба Flow Collector может сама добавлять в список "Разрешенные источники потоков" IP адреса телекоммуникационных устройств, от которых поступают данные. Но если для конкретного устройства не установлен флаг в этом списке, данные с этого устройства не будут обрабатываться. Соответственно, для обработки данных с требуемых источников данных установите флаг в столбце "Адрес".*

После ввода всех перечисленных выше параметров щелкните по кнопке "Сохранить", которая находится на панели инструментов программы.

6.2. Настройка параметров хранилища данных

Как указывалось выше, перед настройкой параметров хранилища, пользователь должен определиться, какой тип хранилища будет использоваться. В случае если в качестве хранилища предполагается использовать Microsoft SQL Server или MySQL, необходимо загрузить соответствующую инсталляцию и установить на компьютере.

Выберите компонент "Хранилище". При этом программа примет вид, подобный показанному на рисунке 6.3.

Определите перечень полей, которые будут обрабатываться и сохраняться в хранилище информации. Для этого можно воспользоваться предустановленными наборами полей. Выбор предустановленных наборов полей выполняется в списке "Предустановка".

Можно выбрать один из следующих вариантов:

- **Основные NetFlow v5** – обеспечивается выбор наиболее часто используемых полей протокола NetFlow версии 5;
- **Основные NetFlow v9** - обеспечивается выбор наиболее часто используемых полей протокола NetFlow версии 9;
- **Основные IPFIX** - обеспечивается выбор наиболее часто используемых полей протокола IPFIX;
- **Все NetFlow v5** - обеспечивается выбор всех полей протокола NetFlow версии 5;
- **Все NetFlow v9** - обеспечивается выбор всех полей протокола NetFlow версии 9;
- **Все IPFIX** - обеспечивается выбор всех полей протокола IPFIX.

Если пользователя интересует какой-либо специфический набор, который не соответствует ни одному из перечисленных выше, пользователь может сам выбрать требуемые поля, установив флаги в столбце "#", в требуемых строках таблицы.

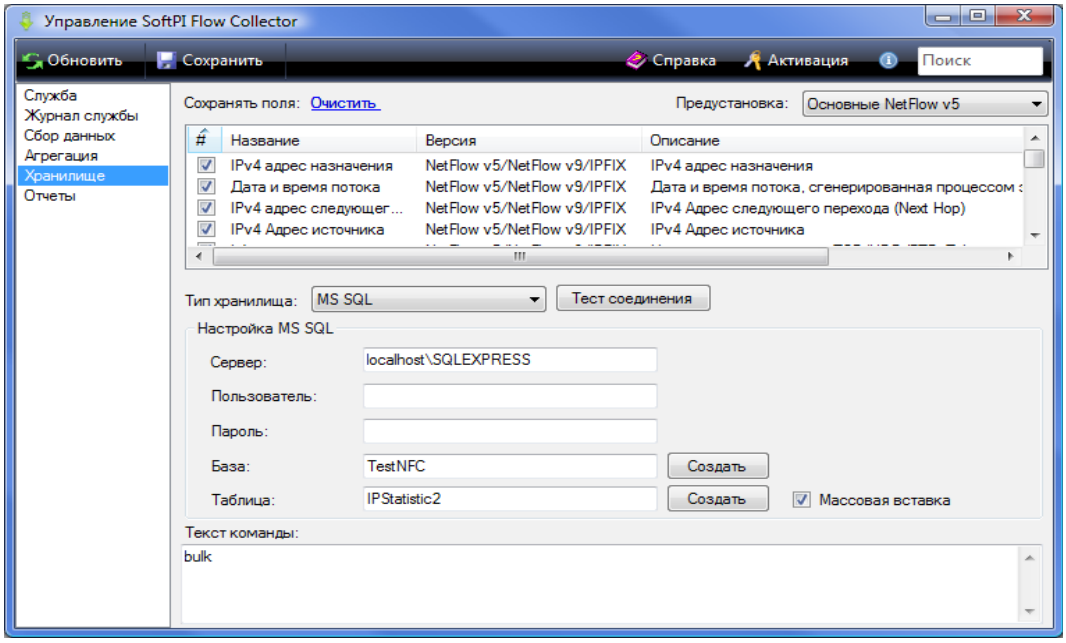

Рисунок 6.3

Если пользователь планирует получать данные от нескольких сетевых устройств, которые используют различные протоколы, то соответственно, необходимо выбрать поля для всех типов возможных протоколов.

Таблица полей содержит следующие столбцы:

- # - показывает выбрано или нет это поле.
- **Название** — отображает название поля и используется для выбора поля;
- **Версия** — отображает тип протокола и версию, к которому относится конкретное поле;
- **Описание** — приводится краткое описание поля;
- **Код поля** — имя поля, которое используется в базе данных. Это имя также используется в позиции "Текст команды" для автоматического создания запроса к базе данных для записи данных.

Таблица поддерживает возможности сортировки информации. Для этого необходимо щелкнуть по наименовании интересующего столбца.

Щелчок правой кнопкой мыши по строке таблице с наименованиями столбцов приводит к появлению меню, подобного тому, которое показанного на рисунке 6.4.

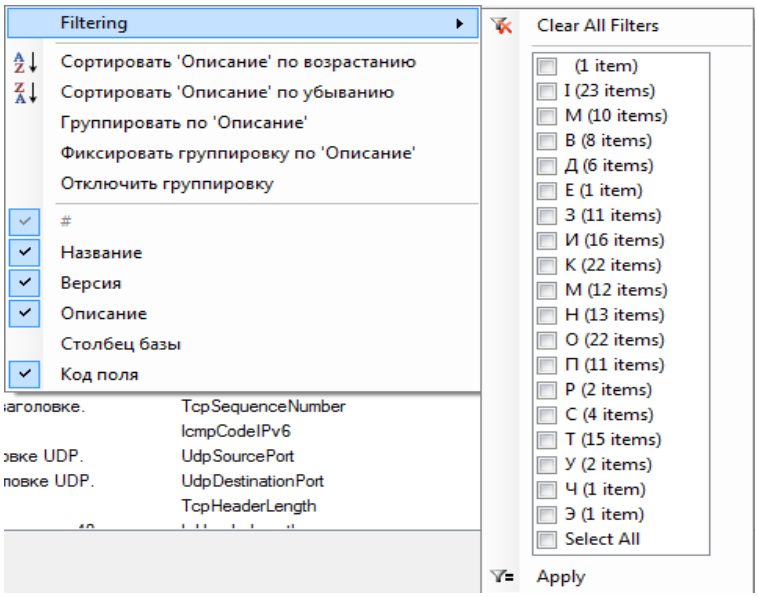

Рисунок 6.4

"**Filtering**" – щелчок по этому пункту меню приводит к появлению дополнительного меню, показанного справа на рисунке 6.4. Пункт меню "Filtering" позволяет отфильтровать только те поля, которые в любом из столбцов начинаются на выбранный в дополнительном меню символ. После выбора символа следует щелкнуть по пункту меню "Apply". Для удаление параметров фильтрации выберите в дополнительном меню пункт "Clear all Filters".

"**Сортировать 'XXXX' по возрастанию**". Позволяет отсортировать по возрастанию поле 'XXXX'. Выбранное поле 'XXXX' определяется тем, на наименовании какого из столбцов находился курсор в момент выполнения щелчка для вызова меню.

"**Сортировать 'XXXX' по убыванию**". Позволяет отсортировать по убыванию поле 'XXXX'.

"**Группировать по 'XXXX'**". Позволяет сгруппировать данные в таблице по первым буквам слов в выбранном столбце.

"**Фиксировать группировку по 'XXXX'**". Появляется в меню только после того, как установлена группировка по какому-либо столбцу. Этот режим меню отключает дальнейшую сортировку информации в таблице. Отключается этот пункт с помощью пункта меню "Отключить группировку".

"**Отключить группировку**". Отключает предварительно установленный режим группировки данных в таблице.

Для быстрого поиска требуемого параметра в таблице рекомендуется использовать режим поиска. Он осуществляется путем ввода искомой информации в позицию со словом "Поиск", расположенной в правой части панели инструментов программы.

Выберите из списка "Тип хранилища" требуемый тип. Возможные варианты:

- **MS SQL** – используется для хранилища на базе Microsoft SQL Server 2000/2005/2008. Если вы не имеете приобретенного Microsoft SQL Server и не планируете его приобретение, то рекомендуем использовать бесплатную редакцию Microsoft SQL Server 2008R2 Express. Рекомендации по установке этой редакции можно прочитать в [3].
- **MySQL** – используется для хранилища с соответствующим наименованием,
- **CSV file** – в качестве хранилища используется текстовый файл с разделителями (формат файла — CSV).

Если выбрали значение MS SQL, то в позиции "Сервер" введите наименование сервера или его IP адрес (при необходимости с именем сервера). Для примера, в случае использования Microsoft SQL Server 2008 R2 на локальном компьютере можно задать данные следующими вариантами:

1. localhost\sqlexpress
2. 127.0.0.1\sqlexpress
3. .\sqlexpress
4. 10.10.1.111\sqlexpress , где 10.10.1.111 — IP адрес компьютера.

В позициях "Пользователь", "Пароль" введите соответственно имя пользователя и его пароль, используя которые служба Flow Collector будет подключаться к SQL серверу. При использовании Microsoft SQL Server на том же компьютере, где производится настройка и будет работать служба Flow Collector, по умолчанию будет использоваться Windows аутентификация. В этом случае ввод имени пользователя и пароля не нужен.

В позиции "База" введите наименование базы данных, в которую будут помещаться данные. При первоначальной настройке такую базу нужно создать. Для этого щелкните по кнопке "Создать", которая находится в той же строке, что и позиция "База". В случае успешного завершения операции создания базы данных на экране появится сообщение: "База данных 'xxxxxxxx' создана успешно", где xxxxxxxx – наименование базы данных.

В позиции "Таблица" введите наименование таблицы в созданной базе данных, в которую будут помещаться данные. При первоначальной настройке такую таблицу нужно

создать. Для этого щелкните по кнопке "Создать", которая находится в той же строке, что и позиция "Таблица". Появится окно, подобное тому, которое показано на рисунке 6.5.

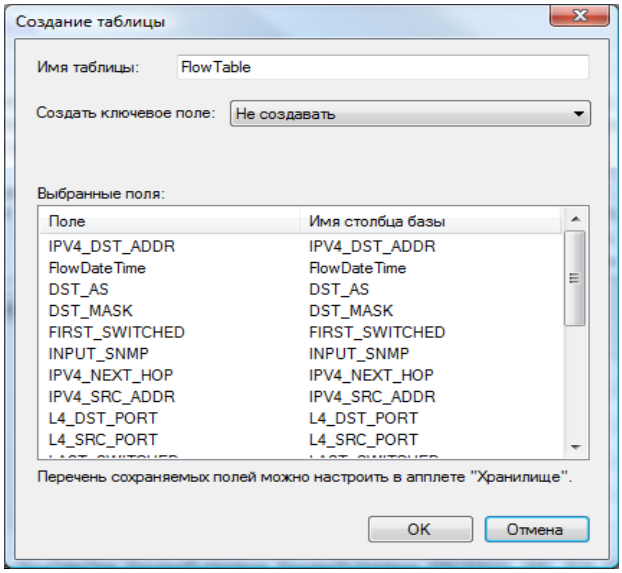

Рисунок 6.5

Позиция "Имя таблицы" отображает имя создаваемой таблицы.
Таблица "Выбранные поля" содержит поля, которые пользователь выбрал в окне, показанном на рисунке 6.3.
Поле "Создать ключевое поле" используется для задания ключевого поля в таблице, которое в дальнейшем при выборках данных из таблицы позволяет выбрать конкретную запись по ее уникальному идентификатору (ключевому слову). Возможны следующие варианты:

- **Не создавать**. Используется по умолчанию, когда не предполагается выполнять указанные выше выборки. Отсутствие ключевого поля позволяет несколько снизить объем базы данных.
- **bigint**. Число формата bigint. рекомендуется устанавливать при необходимости в ключевом поле и относительно невысоком трафике и соответствующем объеме информации, поступающей в базу данных.
- **GUID**. Глобальный уникальный 128-и битовый идентификатор. Рекомендуется его использовать при необходимости в ключевом поле и высоком трафике, которому соответствует большой объем информации, поступающей в базу данных.

После выбора требуемых параметров, щелкните по кнопке "ОК". В случае успешного завершения операции создания таблицы на экране появится сообщение: "Таблица 'xxxxxxxx' успешно создана", где xxxxxxx – наименование таблицы.

Для проверки правильности заданных параметров Microsoft SQL Server-а щелкните по кнопке "Тест соединения". В случае удачного соединения с SQL сервером появится сообщение: "Соединение проверено". При неудачной попытке подключения следует проверить правильность введенных параметром.

Если не требуется какой-либо специальной обработки полей, записываемых в базу данных, и имеется большой поток данных от NetFlow устройств, установите флаг в позиции "Массовая вставка". При этом в поле "Текст команды" отразиться "**bulk**". Использование массовой вставки предполагает ввод данных в базу данных с помощью команды "BULK INSERT", которая позволяет в несколько раз повысить скорость записи данных в базу данных.

В случае выбора в списке "Тип хранилища" значения "MySQL" рядом с позицией "Сервер" появляется позиция "Порт", где задается номер IP порта, по которому осуществляется подключение к MySQL серверу. По умолчанию в этом поле установлено значение: 3306.

В случае выбора в списке "Тип хранилища" значения "CSV file" окно программы частично меняет вид (рисунок 6.6), по сравнению с тем какой показан на рисунке 6.3.

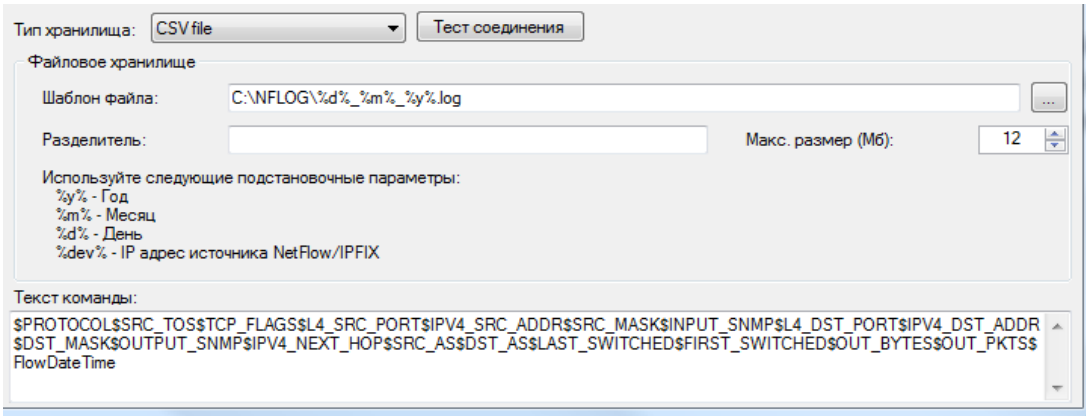

Рисунок 6.6

В позиции "Шаблон" задаются путь и шаблон для наименования файла. При этом для задания имени файла используются следующие обозначения:
%y% - год;
%m% - месяц;
%d% - день;
%dev% - IP адрес оборудования, с которого собираются данные.
Файл по умолчанию имеет расширение log.
В позиции "Разделитель" пользователь может ввести символ разделителя полей в файле.
В позиции "Макс. размер" задается максимально допустимый размер файла. При достижении установленного значения автоматически будет создан новый файл.

После задания всех требуемых параметров в компоненте "Хранилище" щелкните по кнопке "Сохранить" на панели инструментов программы.

6.3. Настройка параметров агрегации

Настройку параметров агрегации следует выполнять, когда планируется агрегировать данные по какому-то из полей. Применение агрегации может существенно снизить объем базы данных, но за счет потери полной детализации о трафике.

Для установки параметров агрегации выберите компонент "Агрегация". Окно программы примет вид, подобный рисунку 6.7.

Пользователь может установить агрегацию по любому из полей, указанных в таблице "Агрегировать данные по полям". Таблица содержит 4-е столбца:

- **Имя поля**. Отображает имя поля и используется для выбора конкретного поля.
- **Версия**. Отображается тип протокола и номер версии, к которым принадлежит поле.
- **Описание**. Приводится краткое описание поля.
- **Тип данных**. Указывается тип данных, которые хранятся в конкретном поле.

Внимание. По умолчанию установлено агрегирование по ряду полей. Если вы не нуждаетесь в таком агрегировании, то удалите флажки с выбранных полей.

Значение по умолчанию для параметра "Интервал записи в базу" составляет 3000 миллисекунд. Пользователь может по своему усмотрению изменить период записи в базу данных. При этом следует иметь в виду, что уменьшение значения интервала записи в базу

приводит к увеличению нагрузки на процессор компьютера. Увеличение этого интервала снижает нагрузку на процессор, но пользователь в течение этого интервала не может иметь доступа к данным полученным в этот период и, соответственно, их анализировать.

В случае задания нескольких полей для агрегирования, агрегирование будет выполняться для совокупности заданных полей.

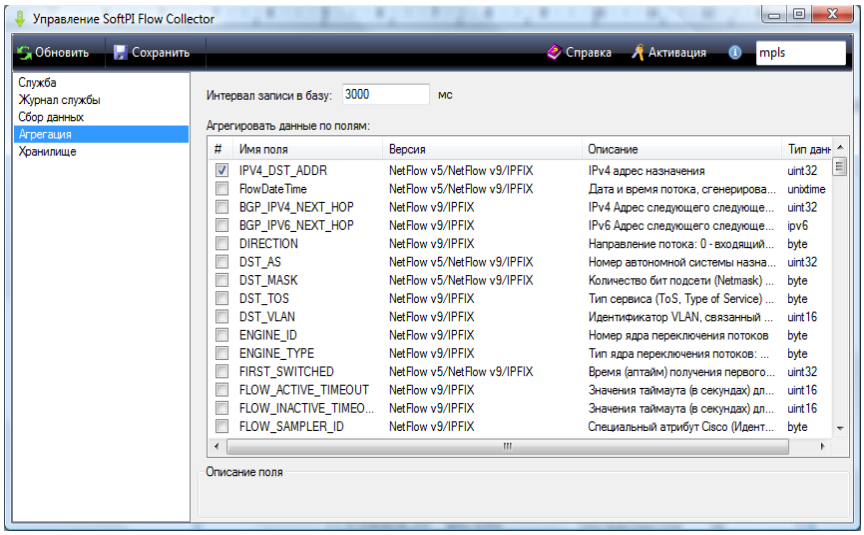

Рисунок 6.7

Для работы с данными таблицы (сортировка, группирование, поиск) применимы те же методы, которые описаны для таблицы компонента "Хранилище".

6.4. Установка и запуск службы Flow Collector

Для установки и запуска службы Flow Collector выберите компонент "Служба" в программе "Настройка коллектора сетевых потоков". Окно программы примет вид, показанный на рисунке 6.8.

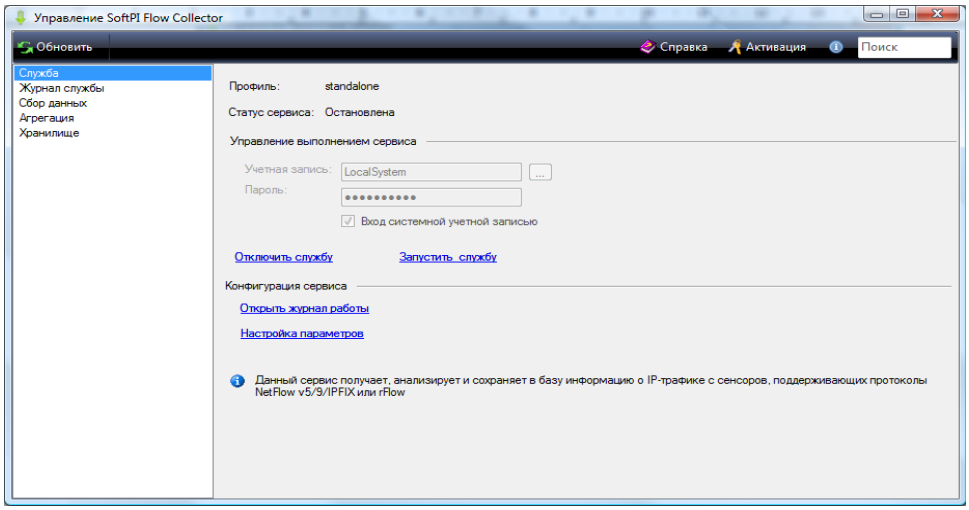

Рисунок 6.8

В позиции "Статус сервиса" отображается текущее состояния службы.

Для запуска службы щелкните по ссылке "Запустить службу". При удачном запуске эта ссылка будет заменена на "Остановить службу", а ссылка отключить службу станет неактивной.

Для остановки службы щелкните по ссылке "Остановить службу". После остановки службы ссылка изменить свое значение на "Запустить службу" и станет активной ссылка "Отключить службу".

Для отслеживания подробностей работы службы Flow Collector щелкните по ссылке "Открыть журнал работы" или же выберите этот компонент в перечне компонентов программы.

Ссылка "Настройка параметров" приводит к переходу программы для работы с компонентом "Сбор данных".

7. Отслеживание работы службы

Для отслеживания работы службы Flow Collector следует использовать компонент "Журнал службы". При его выборе программа приобретает вид, подобный тому, который показан на рисунке 7.

Подробности журнала определяются параметром, который был задан в списке "Журналирование" компонента "Сбор данных".

Для любого типа в журнале всегда отображается время запуска службы, основные параметры, с которыми стартовала служба и сообщения об ошибках при запуске модулей.

При выборе режима отладка в журнале в реальном времени отображается информация об источниках данных и обработке этой информации (рисунок 7.1). Поэтому этот режим рекомендуется использовать на этапе наладки системы, чтобы убедится в том, что данные с требуемого источника поступают на Flow Collector.

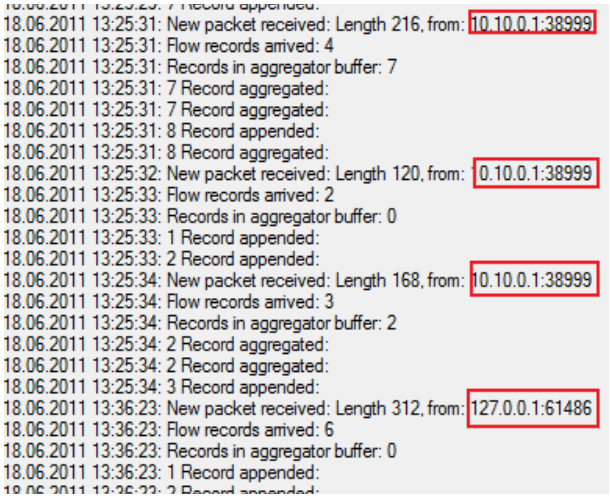

Рисунок 7.1

После отладки системы рекомендуем установить уровень журналирования "Информация", которого достаточно для обычной работы, но журналы работы будут занимать существенно меньше места, чем в режиме "Отладка".

При необходимости работы непосредственно с файлом, в котором хранится журнал работы службы Flow Collector следует щелкнуть по иконке на панели инструментов программы, обведенной красным кружком на рисунке 7.2.

При постоянном нахождении в компоненте "Журнал службы" данные журнала автоматически не обновляются. Для их обновления следует щелкнуть по иконке "Обновить" на панели инструментов программы.

При необходимости очистки журнала щелкните по иконке "Очистка журнала".

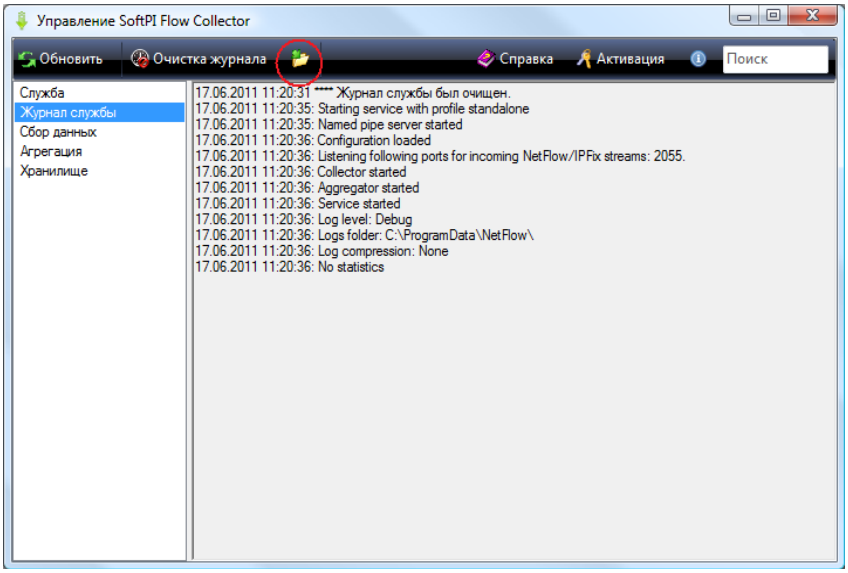

Рисунок 7.2

8. Обработка и анализ собранных данных

Режим "Отчеты" программы "Настройка коллектора сетевых потоков" доступен лишь в том случае, когда:

- в качестве хранилища используется Microsoft SQL Server 2008 R2,
- поля базы данных соответствуют полям протокола NetFlow версии 5.

Пользователь может отредактировать любой из отчетов, поставляемых с системой или создать свои собственные отчеты. Для этого можно использовать **Среду SQL Server Business Intelligence Development Studio** из состава Microsoft SQL Server 2008 R2 или редактор **Microsoft SQL Server Reporting Services Report Builder 3.0** (http://www.microsoft.com/sqlserver/en/us/solutions-technologies/business-intelligence/reporting-services.aspx).

Отчеты, входящие в состав системы или созданные самостоятельно пользователем при использовании им Microsoft SQL Server 2008 R2 могут быть доступны через Web-сайт при использовании службы отчетности SQL Server (SQL Server Reporting Services - SSRS), которая входит в состав SQL сервера.

Если используется SQL сервер 2008 R2, но необходим другой набор полей, чем для протокола NetFlow версии 5, например, используется протокол IPFIX или NetFlow версии 9 для получения информации об IPv6, то в этом случае, воспользовавшись указанными выше средствами, пользователь может самостоятельно создать отчеты, которые также будут доступны из программы "Настройка коллектора сетевых потоков".

В тех случаях, когда используется хранилище другого типа, чем Microsoft SQL Server 2008 R2, для анализа данных необходимо применить другие программы, которые обеспечивают работу с конкретным типом хранилища данных.

Для формирования необходимого отчета в программе "Настройка коллектора сетевых потоков" необходимо выбрать соответствующий апплет и в списке "Отчет" выбрать необходимое наименование файла отчета. Доступны следующие отчеты:

Наименование файла отчета	**Краткое описание**
Applications pie.rdl	Обеспечивает получение круговой диаграммы и таблицы использования IP портов назначения.
Equipment IPv6 traffic .rdl	Обеспечивает получение круговой диаграммы и таблицы

	использования IP портов назначения.
Equipment traffic .rdl	Отображается распределение трафика по сетевому оборудованию, с которого получаются данные, если это оборудование имеет IP адреса версии 6 (IPv6).
IP traffic-compact .rdl	Отображается информация по сетевым потокам с агрегированием по IP адресам и портам.
IP traffic-details.rdl	Отображается детальная информация по сетевым потокам.
Protocols pie .rdl	Отображается распределение трафика по IP протоколам.
Speed per hour.rdl	Отображает график средней скорости передачи в час (объем данных за час делится на 60 минут)
Traffic-day.rdl	Отображается трафик данных в сети за день
Traffic-hour.rdl	Отображает трафик данных по часам. Рекомендуется отображать данные не более, чем за одни сутки.

Окно апплета "Отчеты" показано на рисунке 8.1.

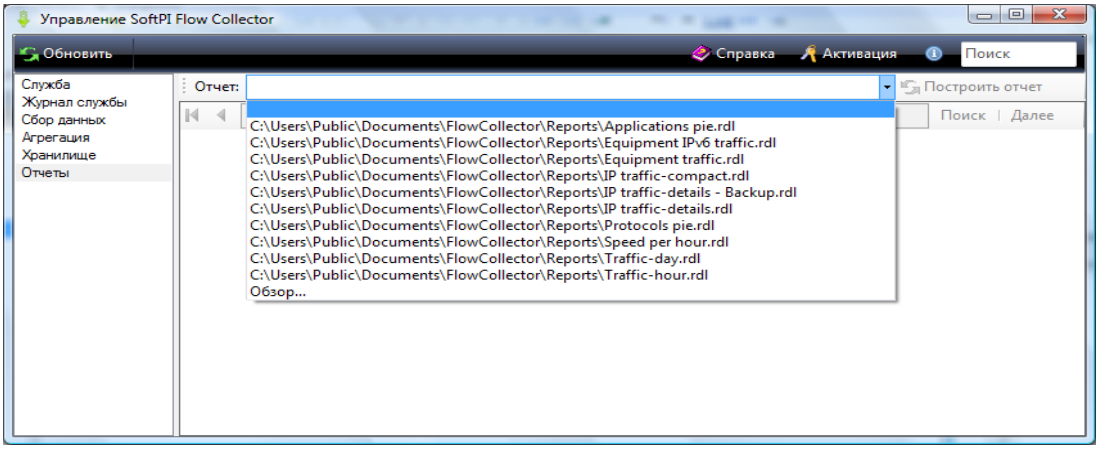

Рисунок 8.1

Для создания необходимого отчета следует открыть список в позиции "Отчеты", выбрать необходимую строку и щелкнуть по кнопке "Построить отчет". После чего появится окно "Параметры отчета". Для различных типов отчетов это окно содержит различное число параметров. Параметры позволяют ограничить диапазон обрабатываемых данных, например, временным промежутком. При необходимости, пользователь путем редактирования отчета может изменить существующие параметры или добавить новые. После задания параметров начинается процесс формирования отчета. В зависимости от объема обрабатываемых данных, параметров компьютера, на котором производится обработка, его загруженностью другими задачами, процесс формирования отчета может занять различное время.

Апплет "Отчеты" содержит панель инструментов. В левой стороне панели инструментов отображается текущая страница отчета, а справа и слева от этой позиции находятся кнопки перехода по страницам отчета. При наведении мыши на любую из кнопок панели инструментов отображается ее наименование. Кроме указанных выше кнопок на панели инструментов содержатся также:

- кнопка "Назад к предыдущему отчету" - она бывает активной лишь в случае связных отчетов, то есть когда в одном из отчетов содержатся ссылки, позволяющие сформировать новые отчеты;
- кнопка "Остановить генерацию отчета";
- кнопка "Обновить" - позволяет обновлять содержимое отчета. Актуальна в том случае, если обрабатываются текущие данные;

- кнопка "Печать отчета";
- кнопка "Разметка страницы" - позволяет отобразить отчет так, как он будет виден в распечатанном виде;
- кнопка "Параметры страницы" - позволяет изменить параметры страницы отчета, которые будут использоваться при печати;
- кнопка "Экспорт отчета" - щелчок по ней приводит к открытию меню, содержащего следующие пункты: Excel, PDF, Word;
- список "Управление масштабом";
- позиция и кнопка "Поиск" - позволяют находить требуемые данные в текстовом отчете;
- кнопка "Далее" - обеспечивает поиск данных далее в отчете после того, как уже был выполнен поиск.

Практически все отчеты кроме графических данных также содержат и данные представленные в виде таблицы. В большинстве отчетов, они содержатся на следующих страницах отчетов.

Для формирования, редактирования, а также создания новых отчетов пользователь может воспользоваться Службами Отчетности SQL сервера (SQL Server Reporting Services - SSRS), которые устанавливаются в Windows одновременно при инсталляции Microsoft SQL Server 2008R2. Учебник на русском языке по этому программному продукту доступен по следующей ссылке: http://msdn.microsoft.com/ru-ru/library/bb522859.aspx

В отличие от использования апплета "Отчеты", Службы Отчетности SQL сервера позволяют сохранить отчет в файлы с расширенным набором форматов:

- XML;
- CSV;
- TIFF;
- PDF;
- MHTML;
- Excel;
- Word.

Перечень всех полей, которые могут быть в хранилище данных, их краткое описание и тип, которые могут использоваться Flow Collector-ом приведено в Приложении 1. Следует учитывать, что в зависимости от выбранного набора полей, таблица данных может содержать лишь часть, тех, что указаны в Приложении 1.

Приложение 1. Перечень полей

Имя поля	Название	Краткое описание	Тип поля	Протокол/ версия
IPV4_DST_ADDR	IPv4 адрес назначения	IPv4 адрес назначения	uint32	
FlowDateTime	Дата и время потока	Дата и время потока, сгенерированная процессом экспорта	unixtime	
BGP_IPV4_NEXT_HOP	BGP IPV4 адрес следующего узла (хопа)	IPv4 Адрес следующего следующего перехода (Next Hop) в домене BGP	uint32	
BGP_IPV6_NEXT_HOP	BGP IPV6 адрес следующего узла (хопа)	IPv6 Адрес следующего следующего перехода (Next Hop) в домене BGP	ipv6	
DIRECTION	Направление потока	Направление потока: 0 - входящий, 1 - исходящий	byte	
DST_AS	AS назначения	Номер автономной системы назначения (BGP)	uint32	
DST_MASK	Маска назначения	Количество бит подсети (Netmask) в адресе назначения (маска в формате /xx)	byte	
DST_TOS	TOS назначения	Тип сервиса (ToS, Type of Service) для исходящего пакета	byte	
DST_VLAN	VLAN назначения	Идентификатор VLAN, связанный с исходящим интерфейсом	uint16	
ENGINE_ID	ID ядра	Номер ядра переключения потоков	byte	
ENGINE_TYPE	Тип ядра	Тип ядра переключения потоков: RP = 0, VIP/Linecard = 1	byte	
FIRST_SWITCHED	Время первого пакета	Время (аптайм) получения первого пакета потока	uint32	
FLOW_ACTIVE_TIMEOUT	Активный таймаут	Значения таймаута (в секундах) для активных элементов в кеше NetFlow	uint16	
FLOW_INACTIVE_TIMEOUT	Неактивный таймаут	Значения таймаута (в секундах) для неактивных элементов в кеше NetFlow	uint16	
FLOW_SAMPLER_ID	ID модуля выборки	Специальный атрибут Cisco (Идентификатор из "show flow-sampler")	byte	
FLOW_SAMPLER_MODE	Режим выборки потока	Тип алгоритма, используемого для выборки данных: 0x02 - случайная выборка. Используется совместно с FLOW_SAMPLER_MODE	byte	
FLOW_SAMPLER_RANDOM_INTERVAL	Интервал случайной выборки	Интервал выборки пакетов. Используется совместно с FLOW_SAMPLER_MODE	uint32	
FLOWS	Потоков	Количество потоков, которые были объединены	uint32	
FORWARDING_STATUS	Статус маршрутизации	Статус маршрутизации потока	byte	
FRAGMENT_OFFSET	Смещение фрагмента	Смещение фрагмента в фрагментированных пакетах	uint32	
ICMP_TYPE	Тип ICMP	Тип пакета Internet Control Message Protocol (ICMP) (ICMP Type - старший байт, код ICMP - младший байт)	uint16	
IF_DESC	Описание интерфейса	Полное название интерфейса	string	
IF_NAME	Имя интерфейса	Укороченное название интерфейса	string	
IN_BYTES	Входящих байт	Количество байтов, принятых в потоке	uint64	
IN_DST_MAC	Входящий MAC назначения	Входящий MAC-адрес назначения	mac	

IN_PERMANENT_BYTES	Входящих постоянных байт	Количество байтов, переданных в постоянном потоке	uint64	
IN_PERMANENT_PKTS	Входящих постоянных пакетов	Количество байтов, переданных в постоянном потоке	uint64	
IN_PKTS	Входящих пакетов	Количество входящих пакетов, переданных в потоке	uint64	
IN_SRC_MAC	Входящий MAC-адрес источника	Входящий MAC-адрес источника	mac	
INPUT_SNMP	Входящий интерфейс	Номер входящего интерфейса	uint32	
IP_PROTOCOL_VERSION	Версия IP протокола	Версия IP протокола: 4 - IPv4, 6 - IPv6. По умолчанию - 4	byte	
IPV4_DST_PREFIX	IPv4 Префикс адреса назначения	IPv4 Префикс адреса назначения	uint32	
IPV4_IDENT	IPv4 идентификатор	IPv4 Уникальный идентификатор пакета	uint16	
IPV4_NEXT_HOP	IPv4 адрес следующего перехода	IPv4 Адрес следующего перехода (Next Hop)	uint32	
IPV4_SRC_ADDR	IPv4 Адрес источника	IPv4 Адрес источника	uint32	
IPV4_SRC_PREFIX	IPv4 Префикс адреса источника	IPv4 Префикс адреса источника	uint32	
IPV6_DST_ADDR	IPv6 Адрес назначения	IPv6 Адрес назначения	binary	
IPV6_DST_MASK	IPv6 Длина маски назначения	IPv6 Длина маски назначения (количество бит маски)	byte	
IPV6_FLOW_LABEL	IPv6 Метка потока	IPv6 Метка потока (RFC 2460)	uint32	
IPV6_NEXT_HOP	IPv6 Адрес следующего перехода	IPv6 Адрес следующего перехода (Next Hop)	ipv6	
IPV6_OPTION_HEADERS	IPv6 опции из заголовка	IPv6 Поле битовых флагов заголовка пакетов из потока	uint32	
IPV6_SRC_ADDR	IPv6 Адрес источника	IPv6 Адрес источника	ipv6	
IPV6_SRC_MASK	IPv6 Маска источника	IPv6 Длина маски источника (количество бит маски)	byte	
L4_DST_PORT	L4 порт назначения	Номер порта назначения TCP/UDP (FTP, Telnet, и т.д.)	uint16	
L4_SRC_PORT	L4 порт источника	Номер порта источника TCP/UDP (FTP, Telnet, и т.д.)	uint16	
LAST_SWITCHED	Время последнего пакета	Время (аптайм) последнего обработанного пакета из потока	uint32	
MAX_PKT_LNGTH	Максимальная длина пакета	Максимальная длина пакета	uint16	
MAX_TTL	Максимальное TTL	Максимальное время жизни (TTL) для принятых пакетов потока	byte	
MIN_PKT_LNGTH	Минимальная длина пакета	Минимальная длина пакета	uint16	
MIN_TTL	Минимальное TTL	Минимальное время жизни (TTL) для принятых пакетов потока	byte	
MPLS_LABEL_1	MPLS Label 1	MPLS метка в позиции 1 в стеке	uint32	
MPLS_LABEL_10	MPLS Label 10	MPLS метка в позиции 10 в стеке	uint32	
MPLS_LABEL_2	MPLS Label 2	MPLS метка в позиции 2 в стеке	uint32	
MPLS_LABEL_3	MPLS Label 3	MPLS метка в позиции 3 в стеке	uint32	
MPLS_LABEL_4	MPLS Label 4	MPLS метка в позиции 4 в стеке	uint32	
MPLS_LABEL_5	MPLS Label 5	MPLS метка в позиции 5 в стеке	uint32	
MPLS_LABEL_6	MPLS Label 6	MPLS метка в позиции 6 в стеке	uint32	
MPLS_LABEL_7	MPLS Label 7	MPLS метка в позиции 7 в стеке	uint32	

MPLS_LABEL_8	MPLS Label 8	MPLS метка в позиции 8 в стеке	uint32	
MPLS_LABEL_9	MPLS Label 9	MPLS метка в позиции 9 в стеке	uint32	
MPLS_TOP_LABEL_IP_ADDR	MPLS top label IP address	Класс эквивалента маршрутизации (Forwarding Equivalent Class), соответствующий MPLS Top Label	uint32	
MPLS_TOP_LABEL_TYPE	Тип MPLS Top Label	Тип MPLS Top Label: 0x00 UNKNOWN 0x01 TE-MIDPT 0x02 ATOM 0x03 VPN 0x04 BGP 0x05 LDP	byte	
MUL_DST_BYTES	Multicast байт	Количество исходящих байт multicast пакетов, переданных в потоке	uint64	
MUL_DST_PKTS	Multicast пакетов	Количество исходящих multicast пакетов, переданных в потоке	uint64	
MUL_IGMP_TYPE	Тип Multicast IGMP	Тип пакета Internet Group Management Protocol (IGMP)	byte	
OUT_BYTES	Исходящих байт	Количество исходящих байт, переданных в потоке	uint64	
OUT_DST_MAC	Исходящий MAC назначения	Исходящий MAC-адрес назначения	mac	
OUT_PKTS	Исходящих пакетов	Количество исходящих пакетов, переданных в потоке	uint64	
OUT_SRC_MAC	Исходящий MAC источника	Исходящий MAC-адрес источника	mac	
OUTPUT_SNMP	Исходящий интерфейс	Номер исходящего интерфейса	uint32	
PROTOCOL	Протокол	IP-протокол	byte	
SAMPLER_NAME	Имя выборки	Имя выборки потоков Netflow	string	
SAMPLING_ALGORITHM	Алгоритм выборки	Тип алгоритма для выборок NetFlow: 0x01 Deterministic Sampling ,0x02 Random Sampling	byte	
SAMPLING_INTERVAL	Частота выборок	Частота выборок NetFlow (100 означает что выбирается 1 из 100 пакетов)	uint32	
SRC_AS	AS Источника	Номер автономной системы источника (BGP)	uint32	
SRC_MASK	Маска источника	Количество бит подсети (Netmask) в адресе источника (маска в формате /xx)	byte	
SRC_TOS	TOS источника	Тип сервиса (ToS, Type of Service) для входящего пакета	byte	
SRC_VLAN	Входящий VLAN	Идентификатор VLAN, связанный с входящим интерфейсом	uint16	
TCP_FLAGS	TCP флаги	Все TCP флаги потока	byte	
TOTAL_BYTES_EXP	Всего байт экспортировано	Количество байтов, переданных доменом обзора	uint64	
TOTAL_FLOWS_EXP	Всего потоков экспортировано	Количество потоков, переданных доменом обзора	uint64	
TOTAL_PKTS_EXP	Всего пакетов экспортировано	Количество пакетов, переданных доменом обзора	uint64	
BgpNextAdjacentAsNumber	bgpNextAdjacentAsNumber	Номер первой автономной системы (AS) в пути к IP адресу назначения.	uint32	
BgpPrevAdjacentAsNumber	bgpPrevAdjacentAsNumber	Номер последней автономной системы (AS) в пути к IP адресу назначения.	uint32	
ExporterIPv4Address	IPv4 адрес сенсора	IPv4 адрес процесса экспорта.	uint32	
ExporterIPv6Address	IPv6 адрес сенсора	IPv6 адрес процесса экспорта.	ipv6	
DroppedOctetDeltaCount	droppedOctetDeltaCount	Количество отброшенных октетов (с момента последнего отчета).	uint64	
DroppedPacketDeltaCount	droppedPacketDeltaCount	Количество отброшенных пакетов (с момента последнего отчета).	uint64	
DroppedOctetTotalCou	droppedOctetTotalCoun	Общее количество отброшенных октетов с	uint64	

nt	t	момента инициализации процесса мониторинга для данной точки наблюдения. Количество октетов включает размер IP заголовка и данных.		
DroppedPacketTotalCount	droppedPacketTotalCount	Общее количество отброшенных пакетов с момента инициализации процесса мониторинга для данной точки наблюдения.	uint64	
FlowEndReason	flowEndReason	Причина завершения потока.	byte	
CommonPropertiesId	commonPropertiesId	Идентификатор набора общих свойств, уникальных для точки наблюдения и данной транспортной сессии.	uint64	
ObservationPointId	observationPointId	Идентификатор точки наблюдения, уникальный в пределах домена наблюдения.	uint32	
IcmpTypeCodeIPv6	icmpTypeCodeIPv6	Тип и код IPv6 ICMP сообщения. Данные представлены в виде (тип ICMP * 256) + ICMP код.	uint16	
MplsTopLabelIPv6Address	mplsTopLabelIPv6Address	IPv6 адрес системы, на которую будет перенаправлен этот поток согласно данной MPLS метке.	ipv6	
LineCardId	lineCardId	Идентификатор line card, уникальный для устройства IPFIX, содержащего точку наблюдения.	uint32	
PortId	portId	Идентификатор порта, уникальный для устройства IPFIX, содержащего точку наблюдения.	uint32	
MeteringProcessId	meteringProcessId	Идентификатор процесса наблюдения, уникальный для устройства IPFIX.	uint32	
ExportingProcessId	exportingProcessId	Идентификатор процесса экспорта, уникальный для устройства IPFIX.	uint32	
TemplateId	templateId	Идентификатор шаблона, который является уникальным в пределах транспортной сессии и домена наблюдения. Шаблон наборов данных нумеруется от 256 до 65535.	uint16	
WlanChannelId	wlanChannelId	Идентификатор используемого канала 802.11 (Wi-Fi).	byte	
WlanSSID	wlanSSID	Значение Service Set IDentifier (SSID) используемой сети 802.11 (Wi-Fi). В соответствии с IEEE.802-11.1999, SSID закодирован в строке максимум 32 байта.	string	
FlowId	flowId	Идентификатор потока, уникальный в пределах домена наблюдения.	uint64	
ObservationDomainId	observationDomainId	Идентификатор домена наблюдения, уникальный для процесса экспорта.	uint32	
FlowStartSeconds	flowStartSeconds	Метка времени первого пакета из потока (секунды).	uint32	
FlowEndSeconds	flowEndSeconds	Метка времени последнего пакета из потока (секунды).	uint32	
FlowStartMilliseconds	flowStartMilliseconds	Метка времени первого пакета из потока (миллисекунды).	uint64	
FlowEndMilliseconds	flowEndMilliseconds	Метка времени последнего пакета из потока (миллисекунды).	uint64	
FlowStartMicroseconds	flowStartMicroseconds	Метка времени первого пакета из потока (микросекунды).	uint64	
FlowEndMicroseconds	flowEndMicroseconds	Метка времени последнего пакета из потока (микросекунды)	uint64	
FlowStartNanoseconds	flowStartNanoseconds	Метка времени первого пакета из потока (наносекунды).	uint64	

FlowEndNanoseconds	flowEndNanoseconds	Метка времени последнего пакета из потока (наносекунды)	uint64	
FlowStartDeltaMicroseconds	flowStartDeltaMicroseconds	Отрицательное смещение времени первого наблюдаемого пакета данного потока относительно времени указанного в заголовке IPFIX пакета.	uint64	
FlowEndDeltaMicroseconds	flowEndDeltaMicroseconds	Отрицательное смещение времени последнего наблюдаемого пакета данного потока относительно времени указанного в заголовке IPFIX пакета.	uint64	
SystemInitTimeMilliseconds	systemInitTimeMilliseconds	Время инициализации системы (миллисекунды)	uint64	
FlowDurationMilliseconds	flowDurationMilliseconds	Продолжительность потока (миллисекунды)	uint64	
FlowDurationMicroseconds	flowDurationMicroseconds	Продолжительность потока (микросекунды)	uint64	
ObservedFlowTotalCount	observedFlowTotalCount	Общее количество потоков в точке наблюдения	uint64	
IgnoredPacketTotalCount	ignoredPacketTotalCount	Общее количество проигнорированных пакетов	uint64	
IgnoredOctetTotalCount	ignoredOctetTotalCount	Общее количество октетов в проигнорированных пакетах	uint64	
NotSentFlowTotalCount	notSentFlowTotalCount	Общее количество потоков, отброшенных процессом измерения	uint64	
NotSentPacketTotalCount	notSentPacketTotalCount	Общее количество пакетов, отброшенных процессом измерения	uint64	
NotSentOctetTotalCount	notSentOctetTotalCount	Общее количество октетов в пакетах, созданных процессом измерения и отброшенных процессом экспорта (не отправленных коллектору).	uint64	
DestinationIPv6Prefix	destinationIPv6Prefix	IPv6 Префикс адреса назначения.	ipv6	
SourceIPv6Prefix	sourceIPv6Prefix	IPv6 Префикс адреса источника.	ipv6	
PostOctetTotalCount	postOctetTotalCount	То же самое, что 'octetTotalCount', но представляет из себя потенциально модифицированное точкой наблюдения значение.	uint64	
PostPacketTotalCount	postPacketTotalCount	То же самое, что 'packetTotalCount', но после того, как пакет прошел через точку наблюдения.	uint64	
FlowKeyIndicator	flowKeyIndicator	Данный набор битовых полей используется для маркировки информационных элементов, используемых как ключ потока.	uint64	
PostMCastPacketTotalCount	postMCastPacketTotalCount	Общее количество исходящих пакетов групповой передачи в данном потоке.	uint64	
PostMCastOctetTotalCount	postMCastOctetTotalCount	Общее количество исходящих байт групповой передачи в данном потоке.	uint64	
IcmpTypeIPv4	icmpTypeIPv4	Тип IPv4 ICMP сообщения.	uint16	
IcmpCodeIPv4	icmpCodeIPv4	Код IPv4 ICMP сообщения.	uint16	
IcmpTypeIPv6	icmpTypeIPv6	Тип IPv6 ICMP сообщения.	uint16	
IcmpCodeIPv6	icmpCodeIPv6	Код IPv6 ICMP сообщения.	uint16	
UdpSourcePort	udpSourcePort	Порт источника, указанных в заголовке UDP.	uint16	
UdpDestinationPort	udpDestinationPort	Порт назначения, указанных в заголовке UDP.	uint16	
TcpSourcePort	tcpSourcePort	Порт источника, указанных в заголовке TCP	uint16	
TcpDestinationPort	tcpDestinationPort	Порт назначения, указанных в заголовке TCP	uint16	

TcpSequenceNumber	tcpSequenceNumber	Номер последовательности в TCP заголовке.	uint32	
TcpAcknowledgementNumber	tcpAcknowledgementNumber	Номер acknowledgement в заголовке TCP.	uint32	
TcpWindowSize	tcpWindowSize	Поле окна в заголовке TCP.	uint16	
TcpUrgentPointer	tcpUrgentPointer	Указатель срочности в заголовке TCP.	uint16	
TcpHeaderLength	tcpHeaderLength	Длина заголовка TCP.	byte	
IpHeaderLength	ipHeaderLength	Длина IP заголовка. Для IPv6 данное поле=40.	byte	
TotalLengthIPv4	totalLengthIPv4	Общая длина пакета IPv4.	uint16	
PayloadLengthIPv6	payloadLengthIPv6	Значение поля Payload Length в IPv6 заголовке.	uint16	
IpTTL	ipTTL	Для IPv4 содержит значение поля времени жизни (Time to Live, TTL) в заголовке IPv4. Для IPv6, содержит значения поля Hop Limit в заголовке IPv6.	byte	
NextHeaderIPv6	nextHeaderIPv6	Значение поля следующего заголовка (Next Header)в заголовке IPv6.	byte	
MplsPayloadLength	mplsPayloadLength	Размер пакета MPLS без стека меток.	uint32	
IpDiffServCodePoint	ipDiffServCodePoint	Значение Differentiated Services Code Point (DSCP) кодированного в поле Differentiated Services.	byte	
IpPrecedence	ipPrecedence	Значение IP Precedence. Поле закодировано в первых трех битах поля TOS IPv4 или поля Traffic Class field IPv6.	byte	
FragmentFlags	fragmentFlags	Свойства фрагментации, указанные в полях фрагментации (Fragment) IPv4 и IPv6.	byte	
OctetDeltaSumOfSquares	octetDeltaSumOfSquares	Квадрат числа октетов на входящий пакет с момента предыдущего отчета для данного потока в пределах точки наблюдения.	uint64	
OctetTotalSumOfSquares	octetTotalSumOfSquares	Квадрат числа октетов на входящий пакет для данного потока в пределах точки наблюдения с момента инициализации процесса измерения. Содержит длину заголовка и данных.	uint64	
MplsTopLabelTTL	mplsTopLabelTTL	Значение поля TTL из стека MPLS меток.	byte	
MplsLabelStackLength	mplsLabelStackLength	Длина стека MPLS в октетах.	uint32	
MplsLabelStackDepth	mplsLabelStackDepth	Количество меток в стеке MPLS.	uint32	
MplsTopLabelExp	mplsTopLabelExp	Поле Exp из стека MPLS меток для последней метки.	byte	
IpPayloadLength	ipPayloadLength	Эффективная длина данных IP пакета	uint32	
UdpMessageLength	udpMessageLength	Значение поля длины заголовка в UDP заголовке	uint16	
IsMulticast	isMulticast	Если IP адрес назначения не является зарезервированным адресом групповой передачи, значение всех битов октета равно нулю.	byte	
Ipv4IHL	ipv4IHL	Значение поля длины заголовка (IHL) в IPv4 заголовке.	byte	
Ipv4Options	ipv4Options	Опции IPv4 в пакетах этого потока.	uint32	
TcpOptions	tcpOptions	Опции TCP в пакетах этого потока.	uint64	
PaddingOctets	paddingOctets	Значение этого элемента всегда последовательность нулей.	uint32	
CollectorIPv4Address	collectorIPv4Address	IPv4 адрес, на который отправляются данные о потоках (адрес коллектора).	uint32	
CollectorIPv6Address	collectorIPv6Address	IPv6 адрес, на который отправляются данные	ipv6	

		о потоках (адрес коллектора).		
ExportInterface	exportInterface	Номер интерфейса, с которого отправляются IPFIX сообщения.	uint32	
ExportProtocolVersion	exportProtocolVersion	Версия протокола, используемая процессом экспорта для отправки информации о потоках.	byte	
ExportTransportProtocol	exportTransportProtocol	Тип сетевого протокола, используемый процессом экспорта для отправки информации о потоках.	byte	
CollectorTransportPort	collectorTransportPort	Порт назначения, на который процесс экспорта отправляет информацию о потоках.	uint16	
ExporterTransportPort	exporterTransportPort	Исходящий порт, с которого процесс экспорта отправляет информацию о потоках.	uint16	
TcpSynTotalCount	tcpSynTotalCount	Общее количество пакетов с установленным флагом TCP "Synchronize sequence numbers" (SYN).	uint64	
TcpFinTotalCount	tcpFinTotalCount	Общее количество пакетов с установленным флагом TCP "No more data from sender" (FIN)	uint64	
TcpRstTotalCount	tcpRstTotalCount	Общее количество пакетов с установленным флагом TCP "Reset the connection" (RST).	uint64	
TcpPshTotalCount	tcpPshTotalCount	Общее количество пакетов с установленным флагом TCP "Push Function" (PSH)	uint64	
TcpAckTotalCount	tcpAckTotalCount	Общее количество пакетов с установленным флагом TCP "Acknowledgment field significant" (ACK).	uint64	
TcpUrgTotalCount	tcpUrgTotalCount	Общее количество пакетов с установленным флагом TCP "Urgent Pointer field significant" (URG).	uint64	
IpTotalLength	Общая длина IP пакета	Общая длина IP пакета	uint64	
PostMplsTopLabelExp	postMplsTopLabelExp	То же, что и 'mplsTopLabelExp', но представляет из себя потенциально модифицированное точкой наблюдения значение.	byte	
TcpWindowScale	Размер окна TCP	Размер окна TCP в заголовке.	uint16	

Литература

1. Что такое NetFlow. http://softpi.com.ua/files/what_is_NetFlow.pdf
2. Что такое IPFIX. http://softpi.com.ua/files/IPFIX.pdf
3. Установка SQL Server 2005/2008. http://www.tariscope.com/ru/support/knowledge-base/9-tariscope-3x/66-sql-server-2005-2008-install.html

Контактная информация

По вопросам приобретения продукции и сотрудничества:

Телефон: +38-057-393-06-11
E-mail: office@softpiua.com
или по адресу: 61115, г. Харьков, ул. Соколова, 3, офис 5.

По вопросам технической поддержки и активации:

E-mail: support@softpiua.com
Сайт компании: http://www.softpiua.com/