IBM Security QRadar Incident Forensics
версия 7.3.0

Захват пакетов QRadar: Руководство пользователей

Примечание

Прежде чем воспользоваться этой информацией и описанным в ней продуктом, прочтите информацию в разделе “Замечания” на стр. 29.

Информация о продукте

Данный документ относится к IBM QRadar Security Intelligence Platform V7.3.0 и последующим его версиям, если не будет заменен обновленной версией этого документа.

Содержание

Об этом руководстве пользователя по захвату пакетов v

Глава 1. Введение в Захват пакетов QRadar 1

Глава 2. Настройка Захват пакетов QRadar 3
Конфигурирование лицензии 4
Администрирование пользователей 5
Изменение пароля учетной записи операционной системы 5
Синхронизация времени сервера Захват пакетов QRadar с системным временем QRadar Console 6

Глава 3. Использование захвата - Обзор 9

Глава 4. Имя 13
Как включить узлы данных 13

Глава 5. Графики Захват пакетов QRadar 15

Глава 6. Поиск пакетов в диапазоне времени для диагностического тестирования 17

Глава 7. Конфигурирование фильтров перед захватом 19

Глава 8. Конфигурирование активных триггеров 21

Глава 9. Диагностика ошибок программы Захват пакетов QRadar 23

Замечания 29
Товарные знаки 30
Положения и условия для документации по продукту 31
Заявление IBM об онлайновой конфиденциальности 32

Об этом руководстве пользователя по захвату пакетов

Эта документация содержит информацию, которая нужна при установке и конфигурировании Захват пакетов IBM® Security QRadar.

Для кого предназначена эта книга

Системные администраторы, отвечающие за установку Захват пакетов QRadar, должны быть знакомы с понятиями защиты сети и конфигурацией устройств.

Техническая документация

Чтобы узнать, как найти документацию по продукту IBM Security QRadar в библиотеке продуктов QRadar, смотрите Техническое замечание по получению доступа к документации IBM Security (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

Как обратиться в службу поддержки заказчиков

Информацию о том, как обратиться в службу поддержки заказчиков, смотрите в документе Техническое замечание по поддержке и загрузке (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Заявление о рекомендуемых методах защиты

Защита ИТ-систем включает в себя защиту систем и информации за счет предотвращения, обнаружения и реакции на неправильный доступ из вашего предприятия и извне вашего предприятия. Неправильный доступ может привести к изменению, уничтожению, незаконному присвоению или неправильному использованию информации либо может вызвать повреждение или неправильное использованием ваших систем, включая использование для атак на других людей. Никакие ИТ-системы или продукты не должны считаться полностью защищенными, и никакой один продукт, служба или мера защиты не могут быть полностью эффективны для предотвращения неправильного использования или доступа. Системы, продукты и службы IBM разработаны как часть правомерного комплексного подхода к защите, который обязательно включает в себя дополнительные рабочие процедуры и может потребовать максимальной эффективности других систем, продуктов или служб. IBM НЕ ГАРАНТИРУЕТ, ЧТО КАКИЕ-ЛИБО СИСТЕМЫ, ПРОДУКТЫ ИЛИ СЛУЖБЫ ОКАЖУТСЯ НЕ ПОДВЕРЖЕНЫ ВРЕДНОМУ ИЛИ НЕЗАКОННОМУ ПОВЕДЕНИЮ ЛЮБОЙ СТОРОНЫ И НЕ ОБЕСПЕЧИВАЕТ ВАШЕМУ ПРЕДПРИЯТИЮ ЗАЩИТУ ОТ ТАКОВЫХ.

Пожалуйста, обратите внимание:

Использование этой Программы может затрагивать различные законы или нормативы, включая те из них, которые связаны с конфиденциальностью, защитой данных, наймом на работу и электронными взаимодействиями и хранением. IBM Security QRadar можно использовать только для законных целей и правомерным образом. Заказчик соглашается использовать эту Программу в соответствии с применимыми законами, нормативами и правилами политики и принимает на себя всю ответственность за их соблюдение. Лицензиат соглашается с тем, что он получил

или получит все согласия, разрешения или лицензии, необходимые для правомерного использования им продукта IBM Security QRadar.

Глава 1. Введение в Захват пакетов QRadar

Захват пакетов IBM Security QRadar - это приложение по захвату сетевого трафика и поиску. У устройства Захват пакетов QRadar есть только один порт захвата (DNA0), и вы можете установить приемопередатчик 10G или 1G SFP.

Используя Захват пакетов QRadar, можно записывать в файлы сетевые пакеты со скоростью до 10 Гбит/сек из активного сетевого интерфейса без потери пакетов.

Можно использовать Захват пакетов QRadar для поиска в захваченном сетевом трафике по времени и данным конвертов пакетов. При достаточных ресурсах устройств и настроенных поисках можно использовать поиск и записывать данные одновременно без потери данных.

Устройства Захват пакетов QRadar, у которых есть приемопередатчик 10G, поддерживают кластеры, которые способны расширить общую емкость хранения и вычислительные возможности склада данных по сравнению с одним автономным сервером. Устройства Захват пакетов QRadar, на которых есть приемопередатчик 1G, не поддерживают кластеры.

Возможности Захват пакетов QRadar

Некоторые функции, включенные в Захват пакетов QRadar:

Стандартный формат файлов PCAP

Формат файлов, используемый для хранения сетевого трафика. Формат файлов интегрируется с существующими инструментами анализа сторонних производителей.

Высокопроизводительная запись пакетов на диск

Захват сетевых пакетов из активной сети.

Поддержка нескольких ядер

Продукт Захват пакетов QRadar предназначен для использования в сочетании с архитектурами, содержащими несколько ядер.

Доступ к диску с прямым вводом-выводом

Захват пакетов QRadar использует доступ к дискам с прямым вводом-выводом для получения максимальной пропускной способности записи на диск.

Индексация в реальном времени

Захват пакетов QRadar может автоматически создавать индекс при захвате пакетов. Можно запрашивать индекс с использованием синтаксиса, подобного Berkeley Packet Filter (BPF) и/или строк домена HTTP или базового URL, чтобы быстро получать интересующие вас пакеты за заданный интервал времени.

Поддержка кластеров, чтобы повысить емкость захвата данных (только для издания 10G). Можно включить узлы данных, чтобы создать кластер для дополнительной емкости хранения.

Формат дампа

Захваченные файлы сохраняются в стандартном формате PCAP с временными отметками с точностью до микросекунд. Захваченные файлы сохраняются последовательно на основе размера файла. Захваченные файлы хранятся в каталогах. Когда пространство в каталоге заполнится, файлы захвата будут перезаписаны на основе заранее сконфигурированных параметров записи.

Скорость захвата

В случае устройств захвата пакетов скорость сетевого трафика захвата зависит от того, есть ли у вас узлы данных, подключенные к главному узлу:

- Для устройств захвата пакетов, к которым не подключены никакие узлы данных, максимальная скорость захвата составляет до 7 Гбит/сек.
- Для устройств захвата пакетов, у которых к главному узлу подключены узлы данных, скорость захвата повышается до 10 Гбит/сек.

Более подробную информацию о переадресации пакетов в Захват пакетов QRadar смотрите в публикации *IBM Security QRadar: Руководство администратора*.

Понятия, связанные с данным:

Глава 3, “Использование захвата - Обзор”, на стр. 9
Чтобы захватить трафик на диск, запустите приложение захвата. Компонент функции записи (Recorder) сохраняет данные сетевого трафика в предварительно сконфигурированном каталоге. Когда пространство в каталоге заполнится, существующие файлы будут перезаписаны.

Глава 2. Настройка Захват пакетов QRadar

Прежде чем вы сможете использовать Захват пакетов IBM Security QRadar, требуется выполнить некоторые базовые шаги по конфигурированию.

Поддерживаемые веб-браузеры

Поддерживаются следующие веб-браузеры:

- Google Chrome версии 44.0.2403.157 или позднее.
- Mozilla Firefox версии 40.0.3 или позднее.

Настройка вашей сети

Чтобы сделать продукт Захват пакетов QRadar доступным с удаленного компьютера, в качестве IP-адреса нужно назначить один из портов Ethernet, как правило, eth2, eth3 или eth4. По умолчанию, система конфигурируется для использования DHCP. При первоначальной конфигурации вам может потребоваться соединиться с VGA-совместимым монитором.

Чтобы выполнить первоначальное конфигурирование, выполните следующие шаги:

1. Включите устройство Захват пакетов QRadar.
2. Используйте SSH и порт 4477, чтобы войти в систему от имени пользователя root.

   Имя пользователя по умолчанию - `root`. Пароль по умолчанию - `P@ck3t08..`

   Чтобы узнать, как изменить пароль по умолчанию, смотрите раздел “Изменение пароля учетной записи операционной системы” на стр. 5.
3. Чтобы убедиться, что система соответствует современным требованиям, примените доступные исправления программы, которые есть в IBM Fix Central (www.ibm.com/support/fixcentral/).
4. Сконфигурируйте статический IP-адрес для вашей собственной сети:
   a. Чтобы получить MAC-адрес или интерфейс eth2, введите следующую команду:

      ```
      ifconfig | grep eth2
      ```

      Интерфейсы eth0 и eth1 недоступны. Используйте eth2 для оборудования M4 xSeries.
   b. Запишите MAC-адрес.
   c. Измените параметры в файле `/etc/sysconfig/network-scripts/ifcfg-eth2`:
      - Добавьте следующий текст в качестве первой строки: `DEVICE=eth2`
      - Раскомментируйте MAC-адрес порта eth2: `HWADDR=xx:xx:xx:xx:xx`
      - Убедитесь, что сконфигурирован следующий параметр: `BOOTPROTO=static`
      - Убедитесь, что вы используете информацию, относящуюся к вашей сети, и что выходные данные похожи на следующий статический пример:

        ```
        DEVICE=eth2
        #HWADDR=xx:xx:xx:xx:xx
        BOOTPROTO="static"
        BROADCAST="192.168.1.255"
        DNS1="0.0.0.0"
        DNS2="0.0.0.0"
        GATEWAY="192.168.1.2"
        ```

```
IPADDR="192.168.1.1"
NETMASK="255.255.255.0"
NM_CONTROLLED="no"
ONBOOT="yes"
```

5. Сохраните файл.
6. Чтобы применить параметры, введите следующую команду:

   ```
   service network restart
   ```

7. Проверьте параметр интерфейса, введя следующую команду:

   ```
   ifconfig | more
   ```

Пример DHCP: В CentOS6.2 измените следующие параметры в файле `/etc/sysconfig/network-scripts/ifcfg-eth0` или в файле `/etc/sysconfig/network-scripts/ifcfg-eth1`.

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

Дистанционный вход в систему

После того как вы настроите IP-адрес на локальном компьютере, вы можете администрировать устройство, дистанционно войдя в систему с использованием SSH на порту 4477.

Конфигурирование лицензии

Прежде чем использовать Захват пакетов QRadar, вы должны сконфигурировать лицензию для устройства Захват пакетов QRadar и программы Захват пакетов QRadar.

Процедура

1. Чтобы сконфигурировать лицензирование для устройства Захват пакетов QRadar, на котором установлен приемопередатчик SFP 1G, выполните следующие шаги:
   a. Чтобы получить лицензионный ключ для главного узла, обратитесь к своему представителю IBM.
   b. В Захват пакетов QRadar выберите **Справка > Обновить главную лицензию**.
   c. Чтобы применить лицензию к устройству Захват пакетов QRadar, вставьте значение в поле **Лицензионный ключ**.
   d. Вставьте значения для полей **ID системы** и **Лицензионный ключ** в соответствующие поля.
   e. Щелкните по **Обновить главную лицензию**, чтобы применить изменения.
2. Чтобы сконфигурировать лицензирование для устройства Захват пакетов QRadar, на котором установлен приемопередатчик SFP+ 10G, выполните следующие шаги:
   a. Чтобы получить лицензионный ключ для узлов данных, обратитесь к своему представителю IBM.
   b. В Захват пакетов QRadar, чтобы применитмь главную лицензию, выберите **Справка > Обновить главную лицензию**.
   c. Вставьте значения для полей **Лицензионный ключ** и **ID системы** в соответствующие поля.
   d. Щелкните по **Обновить главную лицензию**, чтобы применить изменения.
   e. В зависимости от числа узлов данных, которые есть в кластере, вы должны произвести обновление, выбрав **Справка > Узел 1**.

f. Чтобы обновить лицензии для узлов данных, вставьте значения для полей **Лицензионный ключ** и **ID системы** в соответствующие поля.

g. Чтобы обновить узел данных, щелкните по **Обновить лицензию узла 1**, чтобы применить изменения.

Администрирование пользователей

Чтобы дать пользователям возможность получать доступ к продукту Захват пакетов IBM Security QRadar и использовать его, нужно добавить пользователя, назначить для него соответствующую роль и сконфигурировать для него учетные данные для входа в систему.

Прежде чем начать

Убедитесь, что вы вошли в систему Захват пакетов QRadar в качестве пользователя `root`. Либо убедитесь, что вы можете создать пользователя, используя команду `sudo`.

Процедура

1. Чтобы создать пользователя, введите следующую команду:

   ```
   ./usr/local/nc/bin/nc_user_manager add <имя_пользователя> <пароль>
   <Admin|Guest>
   ```

   Если уже существует пользователь с именем <*имя_пользователя*>, эта команда завершится неудачно.

   Если заданная роль не является ролью admin или guest, эта команда завершится неудачно.

   При добавлении пользователя можно использовать одно и то же имя пользователя и пароль как для входа в продукт, так и для входа в API REST.

2. Чтобы удалить пользователя, введите следующую команду:

   ```
   ./usr/local/nc/bin/nc_user_manager delete <имя_пользователя> <пароль>
   ```

   Если уже существует пользователь с именем <*имя_пользователя*>, эта команда завершится неудачно.

   Если значения <*имя_пользователя*> и <*пароль*> не совпадают с тем, что записано в Захват пакетов QRadar, эта команда завершится неудачно.

   При удалении пользователя можно использовать одно и то же имя пользователя и пароль как для входа в продукт, так и для входа в API REST.

Изменение пароля учетной записи операционной системы

После настройки устройства измените пароль операционной системы по умолчанию для Захват пакетов IBM Security QRadar.

Чтобы изменить учетную запись операционной системы, нужно быть пользователем root.

Пароли приложения Захват пакетов QRadar не зависят от паролей операционной системы.

Процедура

1. Используйте SSH, чтобы войти в систему от имени пользователя `root`.

   Пароль по умолчанию для пользователя root - `P@ck3t08..`

2. Чтобы изменить пароли для учетных записей пользователей `root`, используйте команду **`passwd`** *имя_пользователя*.

Синхронизация времени сервера Захват пакетов QRadar с системным временем QRadar Console

Чтобы убедиться, что параметры внедрения IBM Security QRadar являются непротиворечивыми, так что поиски и функции, связанные с данными, работают правильно, все устройства должны синхронизироваться с устройством QRadar Console. Администратор должен обновить таблицы IP (iptables) на устройстве QRadar Console, а затем сконфигурировать его для приема взаимодействий rdate на порту 37.

Прежде чем начать

Вы должны знать IP-адрес или имя хоста QRadar Console. Имя хоста должно правильно разрешаться при использовании nslookup.

По умолчанию, в качестве часового пояса для устройства Захват пакетов QRadar назначено универсальное координированное время (Coordinated Universal Time, UTC).

Процедура

1. Используйте SSH, чтобы войти на устройство Захват пакетов QRadar от имени пользователя `root`.
2. Чтобы выключить службу Network Time Protocol (NTP), введите следующую команду: `service ntpd stop`.
3. Чтобы выключить проверку конфигурации для NTP, введите следующую команду: `chkconfig ntpd off`.
4. Запланируйте синхронизацию как задание хрона, изменив файл `crontab` (crontable).
   a. Введите следующую команду: `crontab -e`.
   b. Чтобы сконфигурировать устройство для синхронизации с QRadar Console каждые 10 минут, введите следующую команду: `*/10 * * * * rdate -s` *`IP_адрес_консоли`*`.`

      Используйте IP-адрес или имя хоста для переменной *IP_адрес_консоли*.
   c. Сохраните изменения конфигурации.
   d. Выключите crond, введя следующие команды:

      ```
      service crond start
      chkconfig crond on
      ```
5. Обновите iptables в QRadar Console, чтобы принимать трафик rdate с устройств Захват пакетов QRadar.
   a. Используйте SSH, чтобы войти на устройство QRadar Console от имени пользователя `root`.
   b. Отредактируйте файл `/opt/qradar/conf/iptables.pre`.
   c. Введите следующую команду:

      ```
      -A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src <адрес PCAP_IP>
      ```

      Если у вас несколько устройств Захват пакетов QRadar, добавьте каждый IP-адрес в виде одной строки.

      Пример:

      ```
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.12
      ```
   d. Сохраните файл `iptables.pre`.
   e. Обновите iptables в QRadar Console, введя следующую команду:

```
./opt/qradar/bin/iptables_update.pl
```

Понятия, связанные с данным:

Глава 3, “Использование захвата - Обзор”, на стр. 9
Чтобы захватить трафик на диск, запустите приложение захвата. Компонент функции записи (Recorder) сохраняет данные сетевого трафика в предварительно сконфигурированном каталоге. Когда пространство в каталоге заполнится, существующие файлы будут перезаписаны.

Глава 3. Использование захвата - Обзор

Чтобы захватить трафик на диск, запустите приложение захвата. Компонент функции записи (Recorder) сохраняет данные сетевого трафика в предварительно сконфигурированном каталоге. Когда пространство в каталоге заполнится, существующие файлы будут перезаписаны.

Устранение ошибок: Если вы видите, что никакого сбора данных не производится, убедитесь, что по соединению идет трафик. Чтобы захватывать трафик, нужно использовать порт Tap или SPAN (зеркало). При использовании порта SPAN на коммутаторе, если коммутатор назначает более низкий приоритет для порта SPAN, часть пакетов может быть отброшена.

Начинаем работу

После того как вы настроите систему, войдите в Захват пакетов IBM Security QRadar, выполнив следующие шаги:

1. Откройте веб-браузер и введите следующий URL:

   `https://`*`IP_адрес_PCAP`*`:41390`
2. Войдите в систему, используя следующую информацию об учетной записи пользователя:

   Пользователь: `continuum`

   Пароль: `P@ck3t08..`

Устранение ошибок: Если пользователь не сможет ввести пароль пять раз в строке в течение 10-минутного периода, пользователь будет заблокирован на 30 минут. Учетную запись пользователя может вручную разблокировать системный администратор.

По умолчанию откроется страница Состояние захвата. Вы можете контролировать запись, щелкая по **Запустить захват** или по **Остановить захват**.

Состояние захвата

Указанная ниже информация представлена на странице Состояние захвата:

- **Запись интерфейса включена**
- **Состояние захвата**
- **Время запуска/остановки**
- **Время, в течение которого система производит захват**
- **Скорость пропускания**
- **Захваченные пакеты**
- **Захваченные байты**
- **Отброшенные пакеты**
- **Доступное пространство хранения**

В конфигурации кластера показано использование пространства хранения для каждого включенного узла данных. Если узел данных Захват пакетов QRadar недоступен из-за проблемы конфигурации сети или из-за неправильного соединения, вместо статистики пространства хранения появится следующее сообщение: `Ведомый`

узел включен, но он в настоящий момент недоступен.

Устранение ошибок

Чтобы просмотреть системную информацию о сконфигурированных интерфейсах захвата, щелкните по **Устранение ошибок**.

Информация сервера

Чтобы просмотреть информацию о пространстве хранения на сервере, щелкните по **Информация о сервере**.

Характеристика сети

Просмотрите пропускную способность сети в графическом формате.

Максимальная пропускная способность захвата на диск по умолчанию - 1- ГБ/сек.

Хронология захватов

Просмотрите хронологию выполненного или выполняемого захвата пакетов.

Поточное сжатие

Чтобы обеспечить поддержку исследований на основе экспертизы, можно сохранить неструктурированное содержимое пакетов в течение более длительного времени, увеличив доступную емкость виртуального хранилища без добавления физических дисков. Теперь вы сможете использовать новую опцию поточного сжатия, чтобы сохранить большие объемы данных на устройстве Захват пакетов QRadar.

Объем сжатия связан с объемом сжатого видеосодержимого в служебной нагрузке. Например, если у вас есть 5% сжатого видео в служебной нагрузке, вы получите сжатие 13:1. Коэффициент сжатие/хранение - это соотношение между несжатым размером и сжатым размером.

Таблица 1. Коэффициенты поточного сжатия

Процент (%) сжатой служебной видеонагрузки	Сжатие:коэффициент расширения хранилища
0	17:1
5	13:1
10	6:1
20	4:1
40	2,4:1

Понятия, связанные с данным:

Глава 1, “Введение в Захват пакетов QRadar”, на стр. 1
Захват пакетов IBM Security QRadar - это приложение по захвату сетевого трафика и поиску. У устройства Захват пакетов QRadar есть только один порт захвата (DNA0), и вы можете установить приемопередатчик 10G или 1G SFP.

Задачи, связанные с данной:

“Синхронизация времени сервера Захват пакетов QRadar с системным временем QRadar Console” на стр. 6
Чтобы убедиться, что параметры внедрения IBM Security QRadar являются непротиворечивыми, так что поиски и функции, связанные с данными, работают правильно, все устройства должны синхронизироваться с устройством QRadar Console. Администратор должен обновить таблицы IP (iptables) на устройстве QRadar Console, а затем сконфигурировать его для приема взаимодействий rdate на порту 37.

Глава 4. Имя

Используйте устройство Захват пакетов QRadar как один автономный сервер или как кластер серверов.

Выпуски 10G поддерживают кластеры, которые расширяют общую емкость хранения и вычислительные возможности склада данных по сравнению с одним автономным сервером. Кластеры содержат главный компонент. Каждую главную систему Захват пакетов QRadar можно соединить с устройствами узлов данных Захват пакетов QRadar в количестве, достигающем двух.

На вкладке **Кластер** показаны два узла данных вместе с их текущим состоянием.

Узлы данных не являются частью кластера по умолчанию и находятся в выключенном состоянии.

Как включить узлы данных

После того как вы физически соедините узлы данных Захват пакетов IBM Security QRadar с главным узлом Захват пакетов QRadar, вы должны включить узлы данных Захват пакетов QRadar. Включенные и соединенные узлы данных Захват пакетов QRadar создают кластер для добавленной емкости хранения и усовершенствованной производительности захвата.

Информацию о соединении устройств смотрите в публикации *Захват пакетов QRadar: Руководство Быстрая справка*.

Прежде чем начать

Убедитесь, что сервер захвата работает.

Процедура

1. Чтобы включить узлы данных, выполните следующие шаги:
   a. На вкладке **Кластер** выберите **Включить** для каждого узла данных. Будет показано состояние **Соединен**.
   b. Перезапустите сервер захвата. Теперь у вас включены узлы данных Захват пакетов QRadar.

   Если узлы данных Захват пакетов QRadar соединены и работают, их состояние в кластере изменится на “соединены”.

   После того как главный узел соединится с узлом данных, в сжатый размер (виртуального) пространства хранения, показанный в инструментальной панели, будет включен размер хранения для соединенных узлов данных.
2. Чтобы выключить узлы данных, выполните следующие шаги:
   a. На вкладке Кластер выберите **Выключить** для каждого узла данных. В качестве состояния будет показано **Разъединен**.
   b. Перезапустите сервер захвата. Теперь узлы данных Захват пакетов QRadar выключены и больше не связаны с главным узлом.

   На отсоединенном узле данных никаких данных больше не хранится.

   После отключения главного узла размер сжатого (виртуального) пространства хранения в инструментальной панели уменьшится.

Если узел данных 1 или узел данных 2 лицензированы, в столбце лицензии появится либо **Постоянно**, либо **Оценка** - в зависимости от используемой вами лицензии.

Глава 5. Графики Захват пакетов QRadar

В Захват пакетов IBM Security QRadar используйте либо живой, либо хронологический график, чтобы визуализировать статистику захвата пакетов.

Живой график

Живой график отслеживает следующие статистические показатели захвата пакетов для текущего захвата пакетов:

- Пропускная способность в ГБ/сек (гигабитах в секунду)
- Всего пакет в секунду
- Пакетов TCP в секунду
- Пакетов UDP в секунду
- Пакетов в секунду для трафика не UDP
- Число системных событий
- Коэффициент сжатия пакетов

Установите указатель мыши на график и получите статистику для этой точки на графике.

Можно щелкнуть по графику в момент времени и автоматически сгенерировать требование поиска. Также можно щелкнуть по значкам стиля вывода на экран, чтобы изменить представление графика.

Хронологический график

На хронологическом графике представлен долгосрочный обзор хронологии захвата пакетов. Опции временной шкалы хронологии включают в себя 1 час, 1 день и 1 неделю.

Установите указатель мыши на график и получите статистику для этой точки на графике.

Щелкните по графику в момент времени, чтобы автоматически сгенерировать требование поиска.

Глава 6. Поиск пакетов в диапазоне времени для диагностического тестирования

Данные индекса, создаваемые во время захвата, используются, чтобы создать файл захвата пакетов (packet capture, pcap), соответствующий заданному диапазону времени и информации о метаданных пакета.

Ограничение: Эти операции поиска подходят только для диагностических целей. Чтобы на заполнять раздел извлечения, потребуется очистка вручную.

Процедура

1. Щелкните по странице **Поиск**.

   Значения по умолчанию уже введены.
2. Выберите интерфейс для захваченного трафика, в котором вы хотите производить поиск.

   Если у вас одна конфигурация интерфейса, она будет выбрана автоматически.
3. Задайте значение или измените значения по умолчанию для начала и окончания диапазона времени, в рамках которого вы хотите производить поиск.
4. Задайте фильтр Berkeley Packet Filter (BPF).

   Чтобы задавать фильтры BFP, используйте синтаксис BPF. Выражение состоит из одного или нескольких простых элементов. Сложные выражения фильтров строятся с использованием операторов AND, OR и NOT.

   Эти примеры представляют собой примитивные фильтры

   ```
   ether host 00:11:22:33:44:55
   ether src host 00:11:22:33:44:55

   ip host 192.168.0.1
   ip dst host 192.168.0.1

   ip6 host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
   ip6 src host 2001:0db8:85a3:0042:0000:8a2e:0371:7334

   ip net 192.168.1.0/24
   ip src net 192.168.1

   port 80
   udp port 9000
   tcp src port 80
   ```

   Эти примеры представляют собой сложные фильтры

   ```
   ip host 192.168.1.1 and 192.168.1.2
   ip src 192.168.1.1 and dst 192.168.1.2
   ip host 192.168.1.1 and tcp port (80 or 443)
   (ip host 192.168.1.1 or 192.168.1.2) and (port 80 or 443)
   ```
5. Задайте число пакетов, которые нужно извлечь.

   Максимальное число пакетов по умолчанию, которые нужно извлечь, равно 10000. Если вы измените число на 0, будут извлечены все пакеты, соответствующие временной шкале и фильтру.
6. Щелкните по **Запустить поиск**.
7. В столбце **Действие** на странице поиска используйте опцию **Разбить на чанки**, чтобы разбить требования поиска на более мелкие сегменты данных, тогда вы

сможете получить доступ к данным, пока все требование поиска еще выполняется. Поиск можно затребовать поиск, указав номер файла PCAP и щелкнув затем по **Загрузить файл PCAP**.

Сегменты данных составляют 128 МБ, и последний сегмент данных может быть любого размера, менее 128 МБ.

8. Чтобы увидеть состояние очереди поиска, смотрите **Очередь требований поиска**.
9. Чтобы увидеть хронологию всех выполненных поисков, смотрите **Журнал требований**.
10. Произведите очистку поисков вручную, чтобы обеспечить достаточно пространства для процессов восстановления экспертизы.
    a. Войдите в систему от имени пользователя root.

       username: root

       password: P@ck3t08..

    b. Введите следующую команду:

       `rm -r /extraction/<имя_поиска>`

       Переменная <*имя_поиска*> - это столбец имени на странице Завершенные поиски.

Глава 7. Конфигурирование фильтров перед захватом

Фильтры перед захватом позволяют применить фильтр к сетевому трафику перед записью захваченных данных на диск.

Процедура

1. Создайте фильтр перед захватом.
   a. Щелкните по меню **Фильтр перед захватом**.
   b. Введите параметры для опций Имя фильтра и Фильтр поиска.

      Фильтр захвата принимает вид примитивных выражений, соединенных привязками (and/or) и перед которыми (необязательно) стоит оператор not.

      В следующем примере весь трафик, предназначенный для порта 80, отбрасывается.

      ```
      not dst port 80
      ```

      В следующем примере захватывается только трафик для указанных ниже двух хостов, а весь остальной трафик отбрасывается.

      ```
      host 1.2.3.4 or host 1.1.1.1
      ```

   c. Заполните фильтр перед захватом, щелкнув по **Добавить**. Последний фильтр перед захватом, добавленный в список, является активным фильтром. Также показана хронология предыдущих фильтров.
2. Перезапустите сервер захвата, чтобы активировать только что добавленный фильтр.
3. Удалите фильтр навсегда, выбрав **Удалить**. Вы должны будете перезапустить сервер захвата.

Глава 8. Конфигурирование активных триггеров

Активные триггеры оповещают вас, когда в сети происходит указанное вами событие. Например, вы задаете IP-адрес в качестве фильтра поиска. чтобы получать оповещение при захвате трафика, содержащего этот IP-адрес.

Процедура

1. Создайте активный триггер.
   a. Щелкните по меню **Активный триггер**.
   b. Введите параметры для опций имени триггера и периода данных.
   c. Завершите создание активного триггера, нажав на **Добавить**.

   Ограничение: Можно задать до пяти активных триггеров.
2. Проверяйте события триггеров в **журнале событий** по мере того, как они происходят. При щелчке по активному событию триггера автоматически генерируется требование поиска с заданными параметрами времени около инициируемого триггером события. Время поиска включает в себя число секунд до и число секунд после события.
3. Удалите сконфигурированный триггер, выбрав **Удалить**.

Глава 9. Диагностика ошибок программы Захват пакетов QRadar

Диагностика ошибок - это систематический подход к устранению проблемы. Цель диагностики ошибок заключается в том, чтобы определить, почему что-то не работает так, как ожидается, и объяснить, как устранить проблему.

Установлена ли последняя версия программы Захват пакетов QRadar?

Всегда производите обновление до выпуска программы последней версии. Сразу же после применения обновления программы или после любой новой установки убедитесь, что вы перезапустили систему, чтобы изменения были применены. В конфигурациях кластера всегда удостоверьтесь, что как система главного узла, так и все системы узлов данных обновлены до одной и той же версии.

Есть ли у вас рекомендуемое промежуточное ПО для контроллера RAID и жестких дисков?

Если вы обнаружите проблемы, отрицательно влияющие на надежность или производительность и связанные с исправлением промежуточного ПО, установленным на контроллере 3650 M4 RAID и жестких дисках, убедитесь, что у вас есть минимальные исправления промежуточного ПО:

- В случае 3650 M4, исправление промежуточного ПО контроллера M5200 RAID: версия 24.7.0-0052 от 27 мая 2015 г. или новее.

  Запустите файлы `.bin` в командной строке Red Hat Linux.
- В случае IBM Lenovo, исправление от 15 мая 2015 г. или новее.

  Запустите файлы `.bin` в командной строке Red Hat Linux.

Включена ли функция HyperThreading в BIOS?

По умолчанию, функция HyperThreading включена в BIOS. Введите команду `lscpu` и проверьте выходную информацию, чтобы убедиться, что “Потоки на ядро равны 2”. Ниже приводится пример выходной информации команды для IBM 3650-M4:

```
[root@3650M4-001 bin]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                40
On-line CPU(s) list:   0-39
Thread(s) per core:    2
Core(s) per socket:    10
Socket(s):             2
NUMA node(s):          2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 62
Stepping:              4
CPU MHz:               2800.000
BogoMIPS:              5592.04
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              25600K
NUMA node0 CPU(s):     0-9,20-29
NUMA node1 CPU(s):     10-19,30-39
```

Правильно ли подсоединен порт захвата?

Устройство Захват пакетов IBM Security QRadar может захватывать данные только на интерфейсе 0.

Правильно ли сконфигурировано сетевое соединение Ethernet?

Чтобы убедиться, что интерфейс Ethernet назначен для IP-адреса, введите команду `ifconfig` для соединенного интерфейса.

Если никакого адреса не сконфигурирговано, измените соответствующий файл `ifcfg-eth*`, чтобы сконфигурировать адрес.

- В этом примере DHCP измените следующие параметры в `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* и замените *eth2* на соответствующий параметр.

  ```
  BOOTPROTO="dhcp"
  NM_CONTROLLED="no"
  ONBOOT="yes"
  ```

- В этом примере со статическим IP-адресом измените следующие параметры в `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* и замените *eth2* на соответствующий параметр.

  ```
  BOOTPROTO="static"
  BROADCAST="192.168.1.255"
  DNS1="0.0.0.0"
  DNS2="0.0.0.0"
  GATEWAY="192.168.1.2"
  IPADDR="192.168.1.1"
  NETMASK="255.255.255.0"
  NM_CONTROLLED="no"
  ONBOOT="yes
  ```

После изменения параметров введите команду `ifconfig`, чтобы сконфигурировать сетевой интерфейс.

Правильно ли сконфигурировано системное время?

По умолчанию, в качестве системного времени задано координированное универсальное время (Coordinated Universal Time, UTC), и оно сконфигурировано для использования протокола сетевого времени (Network Time Protocol, NTP) и общедоступных серверов для управления правильным системным временем.

Есть ли проблемы с системным оборудованием?

1. Убедитесь, что трафик генерируется правильно и восстанавливается картой сетевого интерфейса (Network Interface Card, NIC).

   Посмотрите на световые индикаторы, которые находятся непосредственно справа от соединения интерфейса 0. Нижний должен постоянно гореть, что указывает на связь. Верхний должен мигать, что указывает на активность трафика.

2. Введите команду `/usr/local/nc/bin/dpdk_nic_bind.py -status`.

   Результат команды должен быть похож на следующую выходную информацию:

```
Сетевые устройства, использующие DPDK-совместимый драйвер
==========================================
0000:0f:00.0 'Сетевое соединение 82599ES 10-Гигабит SFI/SFP+' drv=igb_uio
unused=ixgbe
0000:0f:00.1 'Сетевое соединение 82599ES 10-Гигабит SFI/SFP+' drv=igb_uio
unused=ixgbe
Сетевые устройства, использующие драйвер ядра
==================================
0000:07:00.0 'Сетевое соединение I350 Гигабит' if=eth2 drv=igb unused=igb_uio
*Активно*
0000:07:00.1 'Сетевое соединение I350 Гигабит' if=eth3 drv=igb unused=igb_uio
0000:07:00.2 'Сетевое соединение I350 Гигабит' if=eth4 drv=igb unused=igb_uio
Другие сетевые устройства
====================
<нет>
```

Захватывает ли система трафик?

Чтобы убедиться, что система захватывает трафик после запуска сеанса захвата, используйте один из следующих методов:

- Посмотрите на световые индикаторы, которые находятся непосредственно справа от соединения интерфейса 0. Верхний должен мигать, что указывает на активность трафика.
- На странице Характеристика системы вы увидите графическую выходную информацию.
- Введите в командной строке команду `du -h /storage0/int0`.

  Результат будет напоминать следующую выходную информацию:

```
4.4G /storage0/int0/1_0
4.9G /storage0/int0/2_0
6.4G /storage0/int0/3_0
4.9G /storage0/int0/4_0
4.9G /storage0/int0/5_0
4.9G /storage0/int0/6_0
.
.
.
1.4T /storage0/int0/
```

  Если вы запустите эту команду повторно, возвращенное число подкаталогов и выделяемые объемы увеличатся.

Включен ли узел данных Захват пакетов QRadar?

Если узел данных Захват пакетов QRadar физически соединен с главным узлом, вы, чтобы работать с главным сервером, также должны убедиться, что он включен в пользовательском интерфейсе. Система в настоящий момент поддерживает до двух узлов данных Захват пакетов QRadar.

Если на вкладке **Кластер** показано, что узлы данных Захват пакетов QRadar соединены и включены, а параметр **ID системы** отсутствует в окне **Обновить лицензию на узлы (n)** на вкладке **Администрирование**, вы должны убедиться, что на отдельном узле данных Захват пакетов QRadar установлена та же версия программы узла данных Захват пакетов QRadar, что и на главном узле. После обновления до последней версии программы убедитесь, что это требование выполнено.

От имени пользователя `root` введите указанную ниже команду, чтобы проверить версию программы, установленную на узле данных Захват пакетов QRadar и на главном узле:

```
cat /root/version.txt
```

Версия программы узла данных Захват пакетов QRadar должна совпадать с версией, установленной на главном узле.

Как лицензия на узел данных Захват пакетов QRadar применяется из командной строки?

Чтобы убедиться, что вы находитесь на узле данных Захват пакетов QRadar как пользователь `root`, введите следующую команду:

```
cat /root/version.txt
```

Чтобы проверить, соединены ли вы с узлом данных Захват пакетов QRadar, ищите символ D, присоединенный в конец номера версии, например, 7.2.7.256D.

Чтобы применить лицензию к узлу данных Захват пакетов QRadar, от имени пользователя `root` запустите сценарий: `nc_set_license.sh` as `root`.

Примечания:

- Чтобы новая лицензия вступила в силу, нужно перезапустить узел данных Захват пакетов QRadar.
- Если узел данных Захват пакетов QRadar уже лицензирован во время производства, запускать сценарий не нужно. Лицензия сразу же вступит в силу при запуске системы.

Если примененная вами лицензия недействительна, появится сообщение об ошибке:

```
Предупреждение: Лицензионный ключ *НЕДЕЙСТВИТЕЛЕН*.
```

Формат записи в журнал LEEF 2.0: что это такое?

В файл `/var/log/messages` добавляются сообщения LEEF (Log Event Extended Format) в следующем формате:

```
<дата_время> <IP_сервера> LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|<ID>|cat=<категория> msg=<сообщение>
```

Например, если сервер захвата пакетов запускается в системе с IP-адресом 10.91.170.20, в файл `/var/log/messages` добавляется следующее сообщение LEEF:

```
May 24 22:27:49 IP_10_91_170_20 LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|Started|cat=PacketCapture
```

Почему требование Создать поиск возвращает ошибку `Нет места`?

Если при создании поиска каталог `/extraction` окажется переполнен, сервер возвратит ошибку `Нет места`.

Что происходит, когда поиск приостанавливается?

Поиск приостанавливается, если используемое пространство в каталоге `/extraction` превышает 6,7 ГБ. В `Syslog` отправляется сообщение LEEF, указывающее, что поиск приостановлен. В журнале событий появится предупреждение аналогичное следующему:

```
!ПРЕДУПРЕЖДЕНИЕ: Пространство хранения для извлечения переполнено!
Продолжить поиск нельзя!!
```

Чтобы убедиться, что приостановленный поиск возобновился, нужно создать пространство, удалив старые, ранее выполненные поиски. Чтобы удалить старый поиск, выполните следующие шаги:

1. Щелкните по опции главного меню **Поиск**.
2. В фрейме **Журнал требований поиска** удалите старые поиски, щелкнув по **Удалить поиск**.

Замечания

Данная публикация разработана для продуктов и услуг, предлагаемых в США.

IBM может не предоставлять в других странах продукты, услуги и аппаратные средства, описанные в данном документе. За сведениями о продуктах и услугах, предоставляемых в вашей стране, обращайтесь в местное представительство IBM . Ссылки на продукты, программы или услуги IBM не означают и не предполагают, что можно использовать только указанные продукты, программы или услуги IBM . Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако при этом пользователь сам несет ответственность за оценку и проверку работы продуктов, программ и услуг, которые получены не от IBM.

IBM может располагать патентами или рассматриваемыми заявками на патенты, относящимися к предмету данной публикации. Получение данного документа не означает предоставления каких-либо лицензий на эти патенты. С запросами по поводу лицензий обращайтесь в письменной форме по адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

По поводу лицензий, связанных с использованием наборов двухбайтных символов (DBCS), обращайтесь в отдел интеллектуальной собственности IBM или направьте запрос в письменной форме по адресу:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

КОРПОРАЦИЯ INTERNATIONAL BUSINESS MACHINES ПРЕДОСТАВЛЯЕТ ДАННУЮ ПУБЛИКАЦИЮ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ОТСУТСТВИЯ НАРУШЕНИЙ, КОММЕРЧЕСКОЙ ПРИГОДНОСТИ ИЛИ СООТВЕТСТВИЯ КАКОЙ-ЛИБО КОНКРЕТНОЙ ЦЕЛИ. В ряде стран для некоторых сделок не допускается отказ от явных или предполагаемых гарантий; в таком случае данное положение может к вам не относиться.

В приведенной здесь информации могут встретиться технические неточности или типографские опечатки. В публикацию время от времени вносятся изменения, которые будут отражены в следующих изданиях. IBM может в любой момент без какого-либо предварительного уведомления внести изменения в продукты и/или программы, описанные в настоящей публикации.

Любые ссылки в этой публикации на веб-сайты, не принадлежащие IBM, приведены только для удобства и никоим образом не служат для их поддержки. Материалы на этих веб-сайтах не входят в число материалов по данному продукту IBM и весь риск пользования этими веб-сайтами несет сам пользователь.

IBM оставляет за собой право на использование и распространение любых предоставленных вами сведений любыми приемлемыми способами, не принимая на себя никаких обязательств перед вами.

Если обладателю лицензии на данную программу понадобятся сведения о возможности: (i) обмена данными между независимо разработанными программами и другими программами (включая данную) и (ii) совместного использования таких данных, он может обратиться по адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Такую информацию можно получить при соблюдении определенных условий, включая в некоторых случаях уплату определенной суммы.

IBM предоставляет лицензионную программу, описанную в данном документе, и все прилагаемые к ней лицензионные материалы на основании положений Соглашения между IBM и Заказчиком, Международного Соглашения о Лицензиях на Программы IBM (IBM International Program License Agreement) или любого эквивалентного соглашения между IBM и заказчиком.

Данные производительности и примеры клиентов представлены только для иллюстрации. Фактическая производительность зависит от конкретной конфигурации и условий работы.

Информация, касающаяся продуктов других компаний (не IBM) была получена от поставщиков этих продуктов, из опубликованных ими заявлений или из прочих общедоступных источников. IBM не производила тестирование этих продуктов и никак не может подтвердить информацию о точности их работы и совместимости, а также прочие заявления относительно продуктов других компаний (не IBM). Вопросы относительно возможностей продуктов других компаний (не IBM) следует адресовать поставщикам этих продуктов.

Сведения, касающиеся намерений и планов IBM, могут быть изменены без предварительного предупреждения; они приведены здесь только для обозначения целей и задач IBM.

Все приведенные здесь цены IBM - это розничные цены, установленные IBM; они действительны на текущий момент и могут быть изменены без предварительного уведомления. Цены дилеров могут отличаться от них.

Эта информация может содержать примеры данных и отчетов, иллюстрирующие типичные деловые операции. Чтобы эти примеры были правдоподобны, в них включены имена лиц, названия компаний и товаров. Все эти имена являются вымышленными и любое их сходство с реальными именами и адресами предприятий является случайным.

Товарные знаки

IBM, логотип IBM и ibm.com - товарные знаки или зарегистрированные товарные знаки International Business Machines Corp., зарегистрированные во многих странах мира. Прочие имена продуктов и услуг могут быть товарными знаками IBM или других компаний. Текущий список товарных знаков IBM есть в Интернете на

странице "Copyright and trademark information" (Информация об авторских правах и товарных знаках) по адресу: www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT и логотип Windows - товарные знаки Microsoft Corporation в США и/или других странах.

Положения и условия для документации по продукту

Разрешения на использование данных публикаций предоставляются в соответствии со следующими положениями и условиями.

Применимость

Данные правила и условия являются дополнением к правилам использования для сайта IBM.

Личное использование

Вам предоставляется право воспроизводить эти публикации в личных некоммерческих целях при условии, что будут воспроизведены все замечания об авторских правах. Вам запрещается распространять эти публикации, полностью или по частям, демонстрировать их или создавать из них производные продукты без явного на то согласия от IBM.

Коммерческое использование

Вам предоставляется право воспроизводить эти публикации исключительно в пределах своего предприятия при условии, что будут воспроизведены все замечания об авторских правах. За пределами вашего предприятия вам запрещается распространять эти публикации, полностью или по частям, демонстрировать их или создавать из них производные продукты без явного на то согласия от IBM.

Права

За исключением прав, явным образом предоставляемых настоящим разрешением, никаких иных разрешений, лицензий и прав, ни явных, ни подразумеваемых, в отношении публикаций и любой содержащейся в них информации, данных, программ или иной интеллектуальной собственности, не предоставляется.

IBM оставляет за собой право отозвать разрешения, предоставленные этим документом, если, по мнению IBM, использование публикаций наносит ущерб IBM или, как это установлено IBM, вышеприведенные инструкции не соблюдаются должным образом.

Вы имеете право загружать, экспортировать или реэкспортировать эту информацию только при условии соблюдения всех применимых законов и нормативных актов, включая все законы и нормативные акты США, касающиеся экспорта.

IBM НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ ОТНОСИТЕЛЬНО СОДЕРЖАНИЯ ЭТИХ ПУБЛИКАЦИЙ. ПУБЛИКАЦИИ ПРЕДСТАВЛЯЮТСЯ "КАК ЕСТЬ", БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ (НО НЕ ОГРАНИЧИВАЯСЬ ТАКОВЫМИ) ПРЕДПОЛАГАЕМЫЕ ГАРАНТИИ ОТСУТСТВИЯ НАРУШЕНИЙ, КОММЕРЧЕСКОЙ ПРИГОДНОСТИ ИЛИ СООТВЕТСТВИЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ.

Заявление IBM об онлайновой конфиденциальности

В программных продуктах IBM, включая программы как решения служб (“Программные Предложения”), могут использоваться cookies или другие технологии для сбора информации по использованию продукта, чтобы помочь конечному пользователю в работе, настроить взаимодействия с конечным пользователем или для иных целей. Во многих случаях никакой личной идентификационной информации Программные Предложения не собирают. Некоторые из наших Программных Предложений могут помочь вам производить сбор личной идентификационной информации. Если в таком Программном Предложении используются cookies для сбора личной идентификационной информации, ниже представлена конкретная информация об использовании cookies в данном предложении.

В зависимости от внедренных конфигурации это Программное Предложение может использовать cookies сеанса, которые собирают ID сеанса каждого пользователя для управления сеансом и аутентификации. Эти cookies можно отключить, но при их отключении также будут устранены функции, которые они поддерживают.

Если конфигурации, внедренные для этого Предложения относительно программ, обеспечивают вам, как заказчику, возможность собирать информацию для идентификации личности от конечных пользователей через cookies и другие технологии, вы должны обратиться за местной юридической рекомендацией о том, существуют ли какие-либо законы, применимые к такому сбору данных, включая все требования относительно замечаний и согласований.

Более подробную информацию об использовании различных технологий, включая cookies, для этих целей смотрите на странице политики конфиденциальности IBM по адресу: http://www.ibm.com/privacy, и в Заявлении об электронной конфиденциальности IBM по адресу: http://www.ibm.com/privacy/details, в разделе “Cookies, Web Beacons and Other Technologies” (Cookies, веб-маяки и другие технологии) и в документе “IBM Software Products and Software-as-a-Service Privacy Statement” (Заявление о конфиденциальности программных продуктов IBM и программ в качестве услуг) http://www.ibm.com/software/info/product-privacy.

Напечатано в Дании