IBM Security QRadar
версия 7.2.6

Руководство пользователя по захвату пакетов

Примечание

Прежде чем начинать пользоваться этой информацией и поддерживаемым ею продуктом, прочтите информацию в разделе “Замечания” на стр. 19.

Информация о продукте

Этот документ относится к IBM QRadar Security Intelligence Platform V7.2.6 и к последующим выпускам, если не будет заменен обновленной версией данного документа.

Содержание

Об этом руководстве пользователя по захвату пакетов

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

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. Что нового для пользователей в Захват пакетов QRadar V7.2.6

В Экспертиза инцидентов IBM Security QRadar V7.2.6 появилось более быстрое получение захваченных пакетов и фильтры перед захватом для тонкой настройки сбора и хранения данных.

Результаты поиска Захват пакетов QRadar возвращаются быстрее и в виде дискретных сегментов данных

Данные захваченных пакетов загружаются в виде дискретных сегментов, так что время передачи становится меньше, и вы можете быстрее увидеть данные. Вы можете быстрее получить доступ к искомым данным, так как данные разбиваются на меньшие сегменты. Узнать подробнее...

Производите тонкую настройку сбора и хранения данных с использованием фильтров пакетов перед захватом

Вы можете сэкономить пространство на диске, указав, что именно вы хотите захватить. Если у вас ограниченное пространство хранения захваченных пакетов, вы сможете захватывать только трафик, который, как вы считаете, находится под максимальной угрозой. Вы можете произвести тонкую настройку возможности сбора захваченных пакетов в соответствии с вашими ресурсами хранения.

Глава 2. Введение в Захват пакетов QRadar

Захват пакетов IBM Security QRadar - это приложение по захвату сетевого трафика и поиску.

Используя Захват пакетов QRadar, можно записывать в файлы сетевые пакеты со скоростью до 10 Гбит/сек из активного сетевого интерфейса без потери пакетов. Захват пакетов QRadar использует стандартный формат файлов PCAP для хранения сетевого трафика. Форма файлов PCAP обеспечивает простую интеграцию с существующими инструментами анализа сторонних производителей.

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. Это также обеспечивает высокопроизводительную запись пакетов на диск.

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 передавать запросы индекса с использованием синтаксиса, подобного BPF, чтобы быстро получать интересующие вас пакеты за заданный интервал времени.

Поддержка кластеров, чтобы повысить емкость захвата данных.

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.

Понятия, связанные с данным:

Глава 4, “Использование захвата - Обзор”, на стр. 9
Чтобы захватить трафик на диск, запустите приложение захвата. Компонент функции записи (Recorder) сохраняет данные трафика в предварительно сконфигурированном каталоге. Когда пространство в каталоге заполнится, существующие файлы будут перезаписаны.

Глава 3. Настройка Захват пакетов QRadar

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

Поддерживаемые веб-браузеры

Поддерживаются следующие веб-браузеры:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer V10 и новее

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. Однако при первоначальном конфигурировании вам, возможно, придется подключить VGA-совместимый монитор, запустить систему с локального компьютера, войти в систему и сконфигурировать статический IP-адрес для вашей собственной сети. После запуска системы войдите в нее от имени пользователя `root`, используя следующие учетные данные:

```
имя пользователя: root
пароль: P@ck3t08..)
```

Чтобы выполнить первоначальное конфигурирование, сделайте следующее:

1. Соединитесь с VGA-совместимым монитором.
2. Включите устройство Захват пакетов QRadar.
3. Войдите в операционную систему Linux от имени пользователя `root`.

   `Имя пользователя: root`

   `Пароль: P@ck3t08..`

   Чтобы узнать, как изменить пароль по умолчанию, смотрите раздел “Изменение пароля учетной записи операционной системы” на стр. 6.
4. Чтобы убедиться, что система соответствует современным требованиям, примените доступные исправления программы, которые есть в IBM Fix Central (www.ibm.com/support/fixcentral/).
5. 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"
```

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

   `service network restart`
8. 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.

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 Захват пакетов QRadar не зависят от паролей операционной системы. Учетные записи `adminusername` и `continuum` должны изменить свои пароли, когда они впервые войдут в систему.

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 `continuum` и `root`, используйте команду **`passwd`** *имя_пользователя*.

Синхронизация времени сервера Захват пакетов QRadar с системным временем Консоль QRadar

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 Консоль QRadar. Администратор должен обновить таблицы IP (iptables) на устройстве Консоль QRadar, а затем сконфигурировать его для приема взаимодействий rdate на порту 37.

Прежде чем начать

Вы должны знать IP-адрес или имя хоста Консоль QRadar. 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 Консоль QRadar 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 Консоль QRadar, чтобы принимать трафик rdate с устройств Захват пакетов QRadar.
   a. Используйте SSH, чтобы войти на устройство Консоль QRadar 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 Консоль QRadar, введя следующую команду:

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

Понятия, связанные с данным:

Глава 4, “Использование захвата - Обзор”, на стр. 9
Чтобы захватить трафик на диск, запустите приложение захвата. Компонент функции записи (Recorder) сохраняет данные трафика в предварительно сконфигурированном каталоге. Когда пространство в каталоге заполнится, существующие файлы будут перезаписаны.

Глава 4. Использование захвата - Обзор

Чтобы захватить трафик на диск, запустите приложение захвата. Компонент функции записи (Recorder) сохраняет данные 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 IP-адрес устройства.
2. Войдите в систему, используя следующую информацию о пользователе:

   Пользователь: `continuum`

   Пароль: `P@ck3t08..`

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

Совет: Номер версии продукта можно увидеть в правом верхнем углу окна.

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.`

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 2, “Введение в Захват пакетов QRadar”, на стр. 3
Захват пакетов IBM Security QRadar - это приложение по захвату сетевого трафика и поиску.

Задачи, связанные с данной:

“Синхронизация времени сервера Захват пакетов QRadar с системным временем Консоль QRadar” на стр. 7
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 Консоль QRadar. Администратор должен обновить таблицы IP (iptables) на устройстве Консоль QRadar, а затем сконфигурировать его для приема взаимодействий rdate на порту 37.

Глава 5. Как включить узлы данных

После того как вы физически соедините главное устройство Захват пакетов IBM Security QRadar с узлами данных Захват пакетов QRadar, вы должны включить узлы данных Захват пакетов QRadar. При включении узлов данных Захват пакетов QRadar создается кластер для добавленной емкости хранения.

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

Ограничение: При выключении узла данных Захват пакетов QRadar захваченные данные на этом узле становятся недоступны для восстановления экспертизы.

Процедура

1. На вкладке Инструментальная панель запустите и остановите захват трафика.
2. На вкладке Кластер выберите **Включить** для каждого узла данных. Будет показано состояние **Соединен**.
3. Снова запустите захват.

   Теперь у вас включены узлы данных Захват пакетов QRadar. Если узды данных Захват пакетов QRadar соединены и работают, состояние кластера узлов данных Захват пакетов QRadar изменится на Соединен.

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

   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.

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. Как видно в столбце **Действие** на странице поиска, требования поиска разбиваются на более мелкие сегменты данных, так что вы можете получить

доступ к данным, пока все требование поиска еще выполняется. Вы можете затребовать поиск, указав номер файла PCAP и нажав затем кнопку **Загрузить файл PCAP**.

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

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. Диагностика ошибок 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 QRadar Packet Capture?

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.

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.

Работает ли интерфейс REST?

Введите указанную ниже команду и замените пароль на правильный пароль (не являющийся паролем по умолчанию) для пользователя continuum:

```
curl -k -v -X POST -G -d "username=continuum&password=пароль&action
=ping" https://localhost/rest/forensics_fetch.php
```

Результат будет напоминать следующую выходную информацию:

```
Программа собирается выполнить метод connect() с localhost, порт 443 (#0)
* Попытка ::1... установлено соединение
* Установлено соединение с localhost (::1) порт 443 (#0)
* Инициализация NSS с путем сертификата: sql:/etc/pki/nssdb
* предупреждение: значение ssl.verifyhost игнорируется
* проверка сертификата партнера SSL пропускается
* Соединение SSL, использующее TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* Сертификат сервера:
* subject: E=root@localhost.localdomain,CN=localhost.localdomain,
OU=SomeOrganizationalUnit,
O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
* начальная дата: Map 27 17:10:01 2014 GMT
* дата окончания действия: Map 27 17:10:01 2015 GMT
* общее имя: localhost.localdomain
* эмитент: E=root@localhost.localdomain,CN=localhost.localdomain,
OU=SomeOrganizationalUnit,
O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
> POST /rest/forensics_fetch.php?username=continuum&password=
test&action=ping HTTP/1.1
> Пользователь-Агент: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
> Хост: localhost
> Принять: */*
>
< HTTP/1.1 200 OK
< Дата: Пон, 13 окт 2014 20:08:20 GMT
< Сервер: Apache/2.2.15 (Red Hat)
< Управление X от: PHP/5.3.3
< Задать Cookie: PHPSESSID=54cf36otmg899b6bau03lu6jh6; path=/
< Окончание действия: Втр, 19 ноя 1981 08:52:00 GMT
< Управление кэшем: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Указание: no-cache
< Длина содержимого: 85
< Соединение: close
< Тип содержимого: application/json
<
* Закрывается соединение #0
{"status":"success","message":"QRadar Packet Capture (c), версия 7.2.4.209\n"}
```

Как переустановить пароль пользователя continuum

Изменить пароль пользователя continuum в пользовательском интерфейсе Захват пакетов QRadar нельзя. Чтобы произвести сброс пароля к фабричному значению по умолчанию, нужно использовать сценарий `reset_default.sh`. Пользователю предложат изменить пароль при следующем входе в систему.

Чтобы запустить сценарий `reset_default.sh`, войдите в командную строку от имени пользователя root и введите следующую команду:

```
sh /var/www/html/mysql/reset_default.sh continuum
```

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

Приведенный ниже абзац не относится к Великобритании и к тем странам, в которых подобные положения не соответствуют местному законодательству:

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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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.

Все приводимые здесь данные о производительности были получены в контролируемой среде. Поэтому результаты, полученные в других операционных средах, могут заметно отличаться от приведенных. Некоторые измерения производились в системах разработчиков, и нет никаких гарантий, что в обычно используемых системах результаты будут такими же. Кроме того, результаты некоторых измерений были получены экстраполяцией. Реальные результаты могут быть другими. Пользователи должны проверить данные в своей собственной среде.

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.

Все заявления о будущих планах и намерениях IBM могут быть изменены или отменены без уведомлений, и описывают исключительно цели фирмы.

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 и названия являются вымышленными, и всякое сходство с именами, названиями и адресами, используемыми в реальной предпринимательской деятельности, являются не более чем совпадением.

При просмотре этого документа на компьютере фотографии и цветные иллюстрации могут быть не видны.

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.

Прочие названия фирм, продуктов или услуг могут являться товарными знаками или марками сервиса других фирм.

Замечания, касающиеся политики 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.