IBM Security QRadar
Versión 7.2.6

Guía del usuario de Packet Capture

Nota

Antes de utilizar esta información y el producto al que sirve de complemento, lea la información contenida en la sección "Avisos" en la página 19.

Información sobre el producto

Este documento corresponde a IBM QRadar Security Intelligence Platform V7.2.6 y a todos los releases subsiguientes a menos sea reemplazado por una versión actualizada de este documento.

Contenido

Acerca de esta guía del usuario de Packet Capture

Esta documentación le proporciona la información que necesita para instalar y configurar IBM® Security QRadar Packet Capture. QRadar Packet Capture está soportado por IBM Security QRadar SIEM.

Público al que se dirige

Los administradores del sistema responsables de la instalación de QRadar Packet Capture deben estar familiarizados con los conceptos de seguridad de red y las configuraciones de dispositivos.

Documentación técnica

Para buscar documentación del producto IBM Security QRadar en la biblioteca de productos de QRadar, consulte Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Cómo ponerse en contacto con el servicio de soporte al cliente

Para obtener información acerca de cómo ponerse en contacto con el servicio de soporte al cliente, consulte la nota técnica sobre soporte y descarga (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Declaración de buenas prácticas de seguridad

La seguridad de los sistemas de TI implica la protección de sistemas e información mediante la prevención, la detección y la respuesta a accesos indebidos desde dentro o fuera de la empresa. Un acceso indebido puede alterar, destruir o dar un uso inapropiado de la información o puede ocasionar daños o un uso erróneo de sus sistemas, incluidos los ataques a terceros. Ningún producto ni sistema de TI debe considerarse completamente seguro, y ningún producto, servicio o medida de seguridad por sí solo debe considerarse totalmente eficaz para evitar el acceso o el uso indebidos. Los sistemas, productos y servicios de IBM están diseñados como parte de un procedimiento global de seguridad de acuerdo con la legalidad vigente, lo que implica necesariamente procedimientos operativos adicionales, y pueden requerir otros sistemas, productos o servicios para ser más eficaces. IBM NO GARANTIZA QUE LOS SISTEMAS, PRODUCTOS O SERVICIOS SEAN INMUNES, O HAGAN QUE SU EMPRESA SEA INMUNE, A LAS CONDUCTAS MALICIOSAS O ILEGALES DE TERCEROS.

Tenga en cuenta lo siguiente:

El uso de este programa puede estar sujeto a diversas leyes o regulaciones, incluidas las relacionadas con la privacidad, la protección de datos, el empleo y las comunicaciones y el almacenamiento electrónicos. IBM Security QRadar solamente se puede utilizar con fines legales y de forma legal. El cliente se compromete a utilizar este Programa de acuerdo con las leyes, disposiciones y políticas aplicables, y asume toda la responsabilidad de su cumplimiento. El licenciatario declara que obtendrá o ha obtenido los consentimientos, permisos o licencias necesarios para permitir el uso legal de IBM Security QRadar.

Capítulo 1. Novedades para los usuarios de QRadar Packet Capture V7.2.6

IBM Security QRadar Incident Forensics V7.2.6 presenta filtros de captura previa y recuperación de captura de paquetes más rápidos para ajustar la recopilación y el almacenamiento de datos.

Los resultados de búsqueda de QRadar Packet Capture se devuelven más rápidamente y en segmentos de datos discretos

Los datos de captura de paquetes se descargan en segmentos discretos de forma que los tiempos de transferencia son más cortos y puede ver datos más pronto. Puede acceder a los datos buscados más rápido porque los datos se dividen en segmentos más pequeños.  Más información...

Ajuste de la recopilación y el almacenamiento de datos mediante filtros de paquetes de captura previa

Puede conservar el espacio de disco definiendo lo que desea capturar. Si tiene un almacenamiento de captura de datos limitado, puede capturar solo el tráfico que considera que presenta un riesgo más elevado. Puede ajustar la prestación de recopilación de captura de paquetes para ajustarse a sus recursos de almacenamiento.

Capítulo 2. Información preliminar sobre QRadar Packet Capture

IBM Security QRadar Packet Capture es una aplicación de captura y búsqueda del tráfico de red.

Con QRadar Packet Capture, puede capturar paquetes de red a velocidades de hasta 10 Gbps desde un interfaz de red activa y grabarlos en archivos sin que haya pérdida de paquetes. QRadar Packet Capture utiliza el formato de archivo PCAP estándar para almacenar tráfico de red. El formato de archivo PCAP facilita la integración con herramientas de análisis de terceros existentes.

Puede utilizar QRadar Packet Capture para realizar búsquedas en tráfico de red capturado por hora y datos de sobre de paquetes. Con recursos de dispositivo suficientes y búsquedas adaptadas, puede utilizar simultáneamente los datos de búsqueda y de grabador sin que haya pérdida de datos. También proporciona registro de paquetes en disco de alto rendimiento.

Prestaciones de QRadar Packet Capture

A continuación se detallan algunas características incluidas con QRadar Packet Capture:

Formato de archivo PCAP estándar

Formato de archivo que se utiliza para almacenar tráfico de red. El formato de archivo se integra con las herramientas de análisis de terceros existentes.

Registro de paquetes en disco de alto rendimiento
Captura de paquetes de red de una red activa.

Soporte para varios núcleos de procesador
QRadar Packet Capture está diseñado para su uso con arquitecturas multinúcleo.

Acceso de disco de E/S directa
QRadar Packet Capture utiliza el acceso de E/S directa a los discos para obtener el máximo rendimiento de escritura en disco.

Indexación en tiempo real
QRadar Packet Capture puede generar un índice automáticamente durante la captura de paquetes. El índice se puede consultar con sintaxis de tipo BPF para recuperar rápidamente paquetes interesantes en un intervalo de tiempo especificado.

Capacidad de clúster para aumentar la capacidad de datos de captura.
Puede habilitar los nodos de datos para crear un clúster para la capacidad de almacenamiento añadida.

Formato de vuelco

Los archivos de captura se guardan en el formato de PCAP estándar con indicaciones de fecha y hora con una resolución de microsegundos. Los archivos de captura se almacenan en orden secuencial según el tamaño del archivo. Los archivos de captura se almacenan en directorios. Cuando se llena el espacio del

directorio, se sobrescriben los archivos de captura, de acuerdo con los parámetros de registro preconfigurados.

Velocidad de captura

Para aplicaciones de captura de paquetes, la velocidad de captura del tráfico de red depende de si tiene nodos de datos adjuntos al nodo maestro:

- Para aplicaciones de captura de paquetes que no tienen nodos de datos adjuntos, la velocidad de captura máxima es de 7 Gbps como máximo.
- Para aplicaciones de captura de paquetes que tienen nodos de datos adjuntos al nodo maestro, la velocidad de captura de datos aumenta hasta 10 Gbps.

Conceptos relacionados:

Capítulo 4, “Visión general del uso de las capturas”, en la página 9
Para capturar el tráfico en disco, inicie la aplicación de captura. El componente Recorder guarda los datos de tráfico en un directorio predefinido. Cuando se llena el espacio del directorio, se sobrescriben los archivos existentes.

Capítulo 3. Configuración de QRadar Packet Capture

Se necesitan algunas operaciones de configuración básicas antes de utilizar IBM Security QRadar Packet Capture.

Navegadores web soportados

Se da soporte a los siguientes navegadores web:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer V10 y posterior

Configuración de la red

Para poder acceder a QRadar Packet Capture de forma remota, se debe asignar una dirección IP a uno de los puertos Ethernet, habitualmente eth2, eth3 o eth4. De forma predeterminada, el sistema está configurado para utilizar DHCP. Sin embargo, para la configuración inicial deberá conectar un monitor VGA compatible, iniciar el sistema localmente, iniciar la sesión y configurar una dirección IP estática para su propia red. Después de iniciar el sistema, inicie la sesión como usuario `root` con estas credenciales:

```
username: root
password: P@ck3t08..)
```

Para la configuración inicial, siga estos pasos:

1. Conecte un monitor VGA.
2. Active el dispositivo QRadar Packet Capture.
3. Inicie la sesión del sistema operativo Linux como usuario `root`.

   `Nombre de usuario: root`

   `Contraseña: P@ck3t08..`

   Para cambiar la contraseña predeterminada, consulte “Cambio de la contraseña de la cuenta de sistema operativo” en la página 6.
4. Para asegurarse de que el sistema está actualizado, aplique los arreglos de software disponible en IBM Fix Central (www.ibm.com/support/fixcentral/).
5. Defina una dirección IP estática para su propia red:
   a. Para obtener la dirección MAC o la interfaz eth2, teclee el mandato siguiente:

      `ifconfig | grep eth2`

      Las interfaces eth0 y eth1 no están disponibles. Utilice eth2 para el hardware de M4 xSeries.
   b. Anote la dirección MAC.
   c. Edite los valores en el archivo `/etc/sysconfig/network-scripts/ifcfg-eth2`:
      - Añada el texto siguiente como la primera línea: `DEVICE=eth2`
      - Elimine el comentario de la dirección MAC del puerto eth2: `HWADDR=xx:xx:xx:xx:xx`
      - Asegúrese de que el valor siguiente está configurado: `BOOTPROTO=static`
      - Asegúrese de utilizar información relevante para la red y de que la salida se parece al ejemplo estático siguiente:

```
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. Guarde el archivo.
7. Para aplicar los valores, ejecute el mandato siguiente:
   `service network restart`
8. Verifique el valor de la interfaz ejecutando el mandato siguiente:
   `ifconfig | more`

Ejemplo para DHCP: En CentOS6.2, edite los valores siguientes en el archivo `/etc/sysconfig/network-scripts/ifcfg-eth0` o en el archivo `/etc/sysconfig/network-scripts/ifcfg-eth1`.

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

Inicio de sesión remoto

Después de configurar una dirección IP localmente, puede administrar el dispositivo iniciando sesión de forma remota mediante SSH en el puerto 4477.

Cambio de la contraseña de la cuenta de sistema operativo

Después de configurar el dispositivo, cambie la contraseña predeterminada del sistema operativo para IBM Security QRadar Packet Capture.

Debe ser el usuario root para cambiar la cuenta de sistema operativo.

Las contraseñas de QRadar Packet Capture son independientes de las contraseñas de sistema operativo. Las cuentas de usuario `adminusername` y `continuum` deben cambiar sus contraseñas cuando inician la sesión por primera vez.

Procedimiento

1. Utilice SSH para iniciar la sesión como usuario `root`.
   La contraseña predeterminada para el usuario root es `P@ck3t08..`
2. Para cambiar las contraseñas para las cuentas de usuario `continuum` y `root`, utilice el mandato **`passwd`** *nombre de usuario*.

Sincronizar la hora del servidor de QRadar Packet Capture con la hora del sistema de la QRadar Console

Para asegurar que los despliegues de IBM Security QRadar tengan valores de hora coherentes a fin de que las búsquedas y funciones relacionadas con datos trabajen debidamente, todos los dispositivos se deben sincronizar con el dispositivo de la QRadar Console. Un administrador debe actualizar iptables en el dispositivo de la QRadar Console y luego configurarlo para aceptar comunicación rdate en el puerto 37.

Antes de empezar

Es necesario que conozca la dirección IP o nombre de host de la QRadar Console. La resolución del nombre de host se debe realizar correctamente mediante nslookup.

De forma predeterminada, la zona horaria del dispositivo de QRadar Packet Capture está establecida en UTC (Hora Universal Coordinada).

Procedimiento

1. >Utilice SSH para iniciar una sesión en el dispositivo de QRadar Packet Capture como usuario `root`.
2. Para desactivar el servicio Network Time Protocol (NTP), escriba el mandato siguiente: `service ntpd stop`.
3. Para desactivar la comprobación de la configuración para NTP, escriba el mandato siguiente: `chkconfig ntpd off`.
4. Planifique la sincronización como trabajo cron editando el archivo `crontab` (crontable).
   a. Escriba el mandato siguiente: `crontab -e`.
   b. Para configurar el dispositivo a fin de sincronizarlo con la QRadar Console cada 10 minutos, escriba el mandato siguiente: `*/10 * * * * rdate -s` *`dirección_IP_consola`*`.`

      Utilice una dirección IP o nombre de host para la variable *dirección_IP_consola*.
   c. Guarde los cambios de configuración.
   d. Active crond tecleando los mandatos siguientes:

      ```
      service crond start
      chkconfig crond on
      ```
5. Actualice las iptables en la QRadar Console para aceptar tráfico rdate procedente de dispositivos de QRadar Packet Capture.
   a. >Utilice SSH para iniciar una sesión en el dispositivo de QRadar Console como usuario `root`.
   b. Edite el archivo `/opt/qradar/conf/iptables.pre`.
   c. Escriba el mandato siguiente:

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

      Si tiene varios dispositivos de QRadar Packet Capture, añada cada dirección IP en una sola línea.

      Ejemplo:

      ```
      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. Guarde el archivo `iptables.pre`.
   e. Actualice las iptables en la QRadar Console escribiendo el mandato siguiente:

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

Conceptos relacionados:

Capítulo 4, “Visión general del uso de las capturas”, en la página 9
Para capturar el tráfico en disco, inicie la aplicación de captura. El componente Recorder guarda los datos de tráfico en un directorio predefinido. Cuando se llena

el espacio del directorio, se sobrescriben los archivos existentes.

Capítulo 4. Visión general del uso de las capturas

Para capturar el tráfico en disco, inicie la aplicación de captura. El componente Recorder guarda los datos de tráfico en un directorio predefinido. Cuando se llena el espacio del directorio, se sobrescriben los archivos existentes.

Resolución de problemas: Si observa que no se recopila ningún dato, compruebe que existe tráfico en las conexiones. Para capturar tráfico, debe utilizar un puerto Tap o SPAN (duplicado). Cuando utiliza un puerto SPAN en un conmutador, si el conmutador asigna una prioridad menor al puerto SPAN, se podrían eliminar algunos paquetes.

Cómo empezar

Después de configurar el sistema, inicie la sesión en IBM Security QRadar Packet Capture siguiendo estos pasos:

1. Abra un navegador web y especifique la dirección IP del dispositivo.
2. Inicie la sesión con la información de usuario siguiente:

   Usuario: `continuum`

   Contraseña: `P@ck3t08..`

De forma predeterminada, se abre la página Estado de captura. Para controlar los registros, pulse **Iniciar captura** o **Detener captura**.

Consejo: Puede ver el número de versión del producto en la esquina superior derecha de la ventana.

Estado de captura

La página Estado de captura proporciona la información siguiente:

- **Interfaz en la que se captura**
- **Estado de la captura**
- **Hora de inicio/detención**
- **Intervalo de tiempo durante el cual el sistema ha realizado capturas**
- **Tasa de rendimiento**
- **Paquetes capturados**
- **Bytes capturados**
- **Paquetes descartados**
- **Espacio de almacenamiento disponible**

En una configuración de clúster, se visualiza el uso de almacenamiento para cada nodo de datos habilitado. Si no se puede acceder al Nodo de datos de QRadar Packet Capture debido a un problema de configuración o a una conexión inadecuada, en lugar de las estadísticas de almacenamiento se visualiza el mensaje siguiente: `El nodo esclavo está habilitado pero no se puede alcanzar actualmente.`

Caracterización de la red

Puede ver el rendimiento de la red en formato gráfico.

El rendimiento máximo predeterminado de captura en disco es de 10 Gbps.

Historial de capturas

Ver el historial de las capturas de paquetes que han tenido lugar o que están en curso.

Compresión en línea

Para permitir las investigaciones forenses, puede conservar el contenido de los paquetes en bruto por un periodo mayor aumentando el almacenamiento virtual disponible sin añadir discos físicos. Ahora puede utilizar la nueva opción de compresión en línea para almacenar cantidades mayores de datos en el dispositivo de QRadar Packet Capture.

El grado de compresión está relacionado con el volumen de contenido de vídeo comprimido existente en la carga útil. Por ejemplo, si tiene vídeo comprimido al 5% en la carga útil, obtiene una compresión 13:1. La proporción compresión/almacenamiento es la proporción entre el tamaño no comprimido y el tamaño comprimido.

Tabla 1. Proporciones de compresión en línea

Porcentaje (%) de carga útil de vídeo comprimida	Proporción compresión/ampliación de almacenamiento
0	17:1
5	13:1
10	6:1
20	4:1
40	2,4:1

Conceptos relacionados:

Capítulo 2, “Información preliminar sobre QRadar Packet Capture”, en la página 3
IBM Security QRadar Packet Capture es una aplicación de captura y búsqueda del tráfico de red.

Tareas relacionadas:

“Sincronizar la hora del servidor de QRadar Packet Capture con la hora del sistema de la QRadar Console” en la página 6
Para asegurar que los despliegues de IBM Security QRadar tengan valores de hora coherentes a fin de que las búsquedas y funciones relacionadas con datos trabajen debidamente, todos los dispositivos se deben sincronizar con el dispositivo de la QRadar Console. Un administrador debe actualizar iptables en el dispositivo de la QRadar Console y luego configurarlo para aceptar comunicación rdate en el puerto 37.

Capítulo 5. Habilitación de nodos de datos

Después de conectar físicamente el dispositivo de IBM Security QRadar Packet Capture maestro con los Nodos de datos de QRadar Packet Capture, debe habilitar los Nodos de datos de QRadar Packet Capture. Al habilitar los Nodos de datos de QRadar Packet Capture se crea un clúster para la capacidad de almacenamiento adicional.

Para obtener información sobre cómo conectar los dispositivos, consulte la *Guía de consulta rápida de QRadar Packet Capture.*

Restricción: Cuando inhabilita un Nodo de datos de QRadar Packet Capture, la recuperación forense no puede acceder a los datos capturados en ese nodo.

Procedimiento

1. En la pestaña Panel de control, inicie y detenga la captura del tráfico
2. En la pestaña Clúster, para cada nodo de datos, seleccione **Habilitar**. El estado muestra **Conectado**.
3. Vuelva a iniciar la captura

   Los Nodos de datos de QRadar Packet Capture están ahora habilitados. Si los Nodos de datos de QRadar Packet Capture están conectados y en ejecución, el estado de los Nodos de datos de QRadar Packet Capture del clúster cambia a "conectado".

   Si el Nodo de datos1 o el Nodo de datos2 tienen licencia, la columna de licencia muestra **Permanente** o **Evaluación**, lo que depende de la licencia utilizada.

   Una vez que el nodo maestro conecta con un nodo de datos, el tamaño del almacenamiento comprimido (virtual) que se visualiza en el panel de control, incluye el tamaño del almacenamiento de los nodos de datos conectados.

Capítulo 6. Búsqueda de paquetes dentro de un intervalo temporal para la prueba de diagnóstico

Los datos de índice creados en el momento de la captura se utilizan para generar un archivo de captura de paquetes (pcap) que contiene los paquetes que coinciden con la información de intervalo temporal y metadatos de paquete especificada.

Restricción: Estas búsquedas se realizan solo a efectos de diagnóstico. Es necesario realizar una limpieza manual para evitar el llenado de la partición de extracción.

Procedimiento

1. Pulse la página **Buscar**.

   Los valores predeterminados ya se han especificado.
2. Seleccione la interfaz para el tráfico capturado en el que desea buscar.

   Si tiene una sola configuración de interfaz, esta se selecciona automáticamente.
3. Especifique un valor o cambie los valores predeterminados para el principio y el fin del intervalo temporal dentro del que desea buscar.
4. Especifique un filtro BPF (Berkeley Packet Filter).

   Utilice la sintaxis BPF para especificar filtros BPF. Una expresión consta de uno o varios primitivos. Las expresiones de filtro complejas se construyen con operadores AND, OR y NOT.

   Estos ejemplos son filtros primitivos

   ```
   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
   ```

   Estos ejemplos son filtros complejos

   ```
   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. Especifique el número de paquetes a extraer.

   El número máximo de paquetes a extraer predeterminado es 10.000. Si cambia el número a 0, se extraen todos los paquetes que coinciden con la línea temporal y el filtro.
6. Pulse **Iniciar búsqueda**.
7. Como puede ver en la columna **Acción** de la página de búsqueda, los resultados de la búsqueda se dividen en segmentos de datos más pequeños para que pueda acceder a los datos mientras que se sigue ejecutando toda la solicitud de búsqueda. Puede solicitar una búsqueda especificando el número de archivo PCAP y pulsando el botón **Descargar archivo de PCAP**.

Los segmentos de datos tienen 128Mb y el último segmento de datos puede tener cualquier tamaño.

8. Para ver el estado de la cola de búsqueda, vea **Buscar en cola de solicitudes**.
9. Para ver un historial de todas las búsquedas completadas, vea **Registro de solicitudes**.
10. Haga una limpieza de búsquedas manuales para asegurarse de que hay espacio suficiente para procesos de recuperación forense:
    a. Inicie la sesión como root.

       username: root

       password: P@ck3t08..

    b. Ejecute el mandato siguiente:

       `rm -r /extraction/<nombre_de_búsqueda>`

       La variable <*nombre_de_búsqueda*> es la columna de nombre en la página Búsquedas completadas.

Capítulo 7. Resolución de problemas de QRadar Packet Capture

La resolución de problemas es un método sistemático para solucionar un problema. El objetivo de la resolución de problemas consiste en determinar por qué algo no funciona tal como se esperaba y explicar cómo resolver el problema.

¿Está instalada la versión más reciente del software de QRadar Packet Capture?

Actualice siempre a la versión más reciente del software. Inmediatamente después de aplicar una actualización de software o después de una instalación nueva reciente, asegúrese de reiniciar el sistema para que se apliquen los cambios. En las configuraciones de clúster, asegúrese siempre de que tanto el sistema maestro como los sistemas de nodos de datos se actualizan a la misma versión.

¿Tiene el firmware sugerido para el controlador RAID y los discos duros?

Si se producen problemas de fiabilidad o rendimiento relacionados con la revisión de firmware instalada en los discos duros y el controlador RAID 3650 M4, asegúrese de tener las revisiones de firmware mínimas:

- Para el 3650 M4, la revisión del firmware del controlador RAID M5200: versión 24.7.0-0052 el 27 de mayo de 2015 o posterior.

  Ejecute los archivos `.bin` en la línea de mandatos de Red Hat Linux.
- Para IBM Lenovo, revisión del 15 de mayo de 2015 o posteriores.

  Ejecute los archivos `.bin` en la línea de mandatos de Red Hat Linux.

¿El puerto de captura está conectado correctamente?

El dispositivo IBM Security QRadar Packet Capture solo puede capturar en la Interfaz 0.

¿La conexión a la red Ethernet está correctamente configurada?

Para asegurarse de que una interfaz Ethernet está asignada a una dirección IP, ejecute el mandato `ifconfig` para la interfaz que está conectada.

Si no hay ninguna dirección configurada, edite el archivo `ifcfg-eth*` correspondiente para configurar una dirección.

- En este ejemplo de DHCP, edite los valores siguientes en `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* y sustituya l *eth2* por el valor adecuado.

  ```
  BOOTPROTO="dhcp"
  NM_CONTROLLED="no"
  ONBOOT="yes"
  ```
- En este ejemplo de dirección IP estática, edite los valores siguientes en `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* y sustituya l *eth2* por el valor adecuado.

  ```
  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
```

Después de cambiar los valores, ejecute el mandato `ifconfig` para configurar la interfaz de red.

¿La hora del sistema está correctamente configurada?

De forma predeterminada, la hora del sistema está establecida en UTC (Hora universal coordinada) y está configurada para utilizar el protocolo NTP (Protocolo de hora en red) y servidores públicos para mantener la hora del sistema correcta.

¿Hay problemas con el hardware del sistema?

1. Asegúrese de que el tráfico se esté generando adecuadamente y de que lo esté recibiendo la NIC (Tarjeta de interfaz de red).

   Mire las luces situadas justo a la derecha de la conexión de la Interfaz 0. La inferior debe estar encendida, lo que significa que hay un enlace. La superior debe estar parpadeando, lo que significa que hay actividad de red.
2. Ejecute el mandato `/usr/local/nc/bin/dpdk_nic_bind.py –status`.

   El resultado del mandato debe parecerse a la salida siguiente:

```
Network devices using DPDK-compatible driver
============================================
0000:0f:00.0 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
0000:0f:00.1 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
Network devices using kernel driver
===================================
0000:07:00.0 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=igb_uio
*Active*
0000:07:00.1 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=igb_uio
0000:07:00.2 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=igb_uio
Other network devices
=====================
<none>
```

¿El sistema está capturando tráfico?

Para confirmar si el sistema está capturando tráfico una vez iniciada una sesión de captura, utilice uno de los métodos siguientes:

- Mire las luces situadas justo a la derecha de la conexión de la Interfaz 0. La superior debe estar parpadeando, lo que significa que hay actividad de red.
- En la página Caracterización de la red, verá una salida gráfica.
- En la línea de mandatos, ejecute el mandato `du –h /storage0/int0`.

  El resultado se parece a la salida siguiente:

```
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/
```

Si ejecuta este mandato repetidamente, el número de subdirectorios y las cantidades de asignación devueltas aumentan.

¿Está funcionando la interfaz REST?

Ejecute el mandato siguiente y sustituya la contraseña por la contraseña correcta (no predeterminada) para el usuario continuum:

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

El resultado se parece a la salida siguiente:

```
About to connect() to localhost port 443 (#0)
* Trying ::1... connected
* Connected to localhost (::1) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* warning: ignoring value of ssl.verifyhost
* skipping SSL peer certificate verification
* SSL connection using TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* Server certificate:
* subject: E=root@localhost.localdomain,CN=localhost.localdomain,
OU=SomeOrganizationalUnit,
O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
* start date: Mar 27 17:10:01 2014 GMT
* expire date: Mar 27 17:10:01 2015 GMT
* common name: localhost.localdomain
* issuer: 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
> User-Agent: 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
> Host: localhost
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Mon, 13 Oct 2014 20:08:20 GMT
< Server: Apache/2.2.15 (Red Hat)
< X-Powered-By: PHP/5.3.3
< Set-Cookie: PHPSESSID=54cf36otmg899b6bau03lu6jh6; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Content-Length: 85
< Connection: close
< Content-Type: application/json
<
* Closing connection #0
{"status":"success","message":"QRadar Packet Capture (c), Version 7.2.4.209\n"}
```

Cómo restablecer la contraseña de usuario continuum

No puede cambiar la contraseña de usuario continuum en la interfaz de usuario de QRadar Packet Capture. Para restablecer la contraseña al valor predeterminado de fábrica, debe utilizar el script `reset_default.sh`. Se solicitará al usuario que cambie la contraseña la próxima vez que inicie la sesión.

Para ejecutar el script `reset_default.sh`, inicie la sesión en la línea de mandatos como usuario root y teclee el mandato siguiente:

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

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos.

Es posible que IBM no ofrezca en otros países los productos, servicios o características que se describen en este documento. Póngase en contacto con el representante local de IBM, que le informará sobre los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende indicar ni implicar que solo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente en tramitación que abarquen la materia descrita en este documento. La posesión de este documento no le confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785, EE. UU.

Para consultas sobre licencias en las que se solicite información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de Propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

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

El párrafo siguiente no es aplicable en el Reino Unido ni en ningún otro país en el que tales disposiciones sean incompatibles con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícita ni explícita, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no sea aplicable en su caso.

Esta información podría incluir imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias hechas en esta publicación a sitios web que no son de IBM se proporcionan sólo para la comodidad del usuario y no constituyen un aval de estos sitios web. El contenido de esos sitios web no forma parte del contenido de este producto de IBM, por lo que la utilización de dichos sitios es responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le proporcione del modo que estime apropiado sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir:(i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se haya intercambiado, deberán ponerse en contacto con:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, EE. UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones correspondientes, incluyendo, en algunos casos, el pago de una tarifa.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del contrato de cliente IBM, el contrato internacional de licencia de programa de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento incluidos en este documento se han obtenido en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Algunas mediciones pueden haberse realizado en sistemas en nivel de desarrollo y no existe garantía alguna de que estas mediciones sean iguales en los sistemas de disponibilidad general. Además, es posible que algunas mediciones se hayan calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, compatibilidad o cualquier otra declaración relacionada con los productos que no son de IBM. Las preguntas relativas a las prestaciones de los productos que no son de IBM deberán dirigirse a los proveedores de dichos productos.

Todas las declaraciones relativas a la orientación o intención futura de IBM están sujetas a cambio o anulación sin previo aviso y representan solamente metas y objetivos.

Todos los precios de IBM mostrados son precios de venta al público sugeridos por IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de los distribuidores pueden variar.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales cotidianas. Para ilustrarlos de la manera más completa posible, los ejemplos incluyen los nombres de personas, empresas, marcas y productos. Todos

esos nombres son ficticios y cualquier similitud con los nombres y direcciones utilizados por empresas reales es mera coincidencia.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas o marcas comerciales registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Hay disponible una lista actual de marcas registradas de IBM en la web, en sección "Copyright and trademark information" de www.ibm.com/legal/copytrade.shtml.

Otros nombres de empresas, productos o servicios pueden ser marcas registradas o marcas de servicio de terceros.

Consideraciones sobre la política de privacidad

Los productos de software de IBM, incluido el software que se ofrece como soluciones de servicio (Ofertas de software), pueden utilizar cookies u otras tecnologías para recopilar información de uso del producto, ayudar a mejorar la experiencia del usuario final, ajustar las interacciones con el usuario final o para otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras Ofertas de software pueden ayudarle a recopilar información de identificación personal. Si esta Oferta de software utiliza cookies para recopilar información de identificación personal, a continuación se define información sobre el uso de cookies de esta oferta.

En función de las configuraciones desplegadas, esta Oferta de software puede utilizar cookies de sesión que recopilan el ID de sesión de cada usuario para la gestión y autenticación de sesiones. Estas cookies se pueden inhabilitar, pero si se inhabilitan también se elimina la función que estas cookies habilitan.

Si las configuraciones desplegadas para esta oferta de software le ofrecen como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnologías, debe buscar asesoramiento jurídico sobre la legislación aplicable a esa recopilación de datos, que incluye cualquier requisito de aviso y consentimiento.

Para obtener más información sobre el uso de diversas tecnologías, incluidos los cookies, para estos fines, consulte la política de privacidad de IBM en http://www.ibm.com/privacy y la declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details, la sección titulada “Cookies, Web Beacons and Other Technologies” y la declaración “IBM Software Products and Software-as-a-Service Privacy Statement” en http://www.ibm.com/software/info/product-privacy.