IBM Security QRadar Incident Forensics
Versión 7.3.0

Guía del usuario de QRadar Packet Capture

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 29.

Información sobre el producto

Este documento corresponde a IBM QRadar Security Intelligence Platform V7.3.0 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.

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. Información preliminar sobre QRadar Packet Capture

IBM Security QRadar Packet Capture es una aplicación de captura y búsqueda del tráfico de red. El dispositivo de QRadar Packet Capture solo tiene un puerto de captura (DNA0) y puede instalar un transceptor de SFP 10G o 1G.

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.

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.

Los dispositivos de QRadar Packet Capture que tienen un transceptor de 10G dan soporte a clústers, lo que aumenta el almacenamiento de datos generales y la capacidad de cálculo en comparación con un servidor autónomo único. Los dispositivos de QRadar Packet Capture que tienen un transceptor de 1G no dan soporte a clústers.

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 estilo BPF (Berkeley Packet Filter) y/o series dominio HTTP o URL base para recuperar rápidamente paquetes interesantes en un intervalo de tiempo especificado.

Capacidad de clúster para aumentar la capacidad de datos de (sólo edición 10G).

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.

Para obtener más información sobre el reenvío de paquetes a QRadar Packet Capture, consulte la *Guía de administración de IBM Security QRadar*.

Conceptos relacionados:

Capítulo 3, “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 de red en un directorio preconfigurado. Cuando se llena el espacio del directorio, se sobrescriben los archivos existentes.

Capítulo 2. 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 Versión 44.0.2403.157 o posterior.
- Mozilla Firefox Versión 40.0.3 o 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. Para una configuración inicial deberá conectar un supervisor compatible con VGA.

Para la configuración inicial, siga estos pasos:

1. Active el dispositivo QRadar Packet Capture.
2. Utilice SSH y el puerto 4477 para iniciar la sesión como usuario root.

   El nombre de usuario predeterminado es `root`. La contraseña predeterminada es: `P@ck3t08..`

   Para cambiar la contraseña predeterminada, consulte “Cambio de la contraseña de la cuenta de sistema operativo” en la página 5.
3. Para asegurarse de que el sistema está actualizado, aplique los arreglos de software disponible en IBM Fix Central (www.ibm.com/support/fixcentral/).
4. 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"
```

5. Guarde el archivo.
6. Para aplicar los valores, ejecute el mandato siguiente:
   `service network restart`
7. 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.

Configuración de la licencia

Antes de utilizar QRadar Packet Capture, debe configurar una licencia para el dispositivo de QRadar Packet Capture y el software de QRadar Packet Capture.

Procedimiento

1. Para configurar la licencia de un dispositivo QRadar Packet Capture que tienen un transceptor SFP de 1G instalado, siga estos pasos:
   a. Póngase en contacto con el representante de IBM para obtener la clave de licencia del nodo maestro.
   b. En QRadar Packet Capture, pulse **Ayuda** > **Actualizar licencia maestra**.
   c. Para aplicar una licencia a un dispositivo QRadar Packet Capture, pegue el valor en el campo **Clave de licencia**.
   d. Pegue los valores de **ID del sistema** y **Clave de licencia** en los campos respectivos.
   e. Pulse **Actualizar licencia maestra** para aplicar los cambios.
2. Para configurar la licencia de un dispositivo QRadar Packet Capture que tienen un transceptor SFP+ de 10G instalado, siga estos pasos:
   a. Póngase en contacto con el representante de IBM para obtener una clave de licencia de los nodos de datos.
   b. En QRadar Packet Capture, para aplicar la licencia maestra, pulse **Ayuda** > **Actualizar licencia maestra**.
   c. Pegue los valores de **Clave de licencia** e **ID del sistema** en los campos respectivos.
   d. Pulse **Actualizar licencia maestra** para aplicar los cambios.
   e. En función del número de nodos de datos que tenga en un clúster, deberá actualizar pulsando **Ayuda** > **Nodo1**.
   f. Para actualizar las licencias de nodo de datos, pegue los valores de **Clave de licencia** e **ID del sistema** en los campos respectivos.

g. Para actualizar el nodo de datos, pulse **Actualizar licencia de nodo1** para aplicar los cambios.

Administración de usuarios

Para permitir que los usuarios accedan a IBM Security QRadar Packet Capture y lo utilice, debe añadir un usuario, asignarle un rol adecuado y configurar las credenciales de inicio de sesión correspondientes.

Antes de empezar

Asegúrese de haber iniciado la sesión en QRadar Packet Capture como usuario `root`. También puede comprobar que pueda utilizar un mandato `sudo` para crear un usuario.

Procedimiento

1. Para crear un usuario, ejecute el mandato siguiente:

   ```
   ./usr/local/nc/bin/nc_user_manager add <nombre_usuario> <contraseña>
   <Admin|Guest>
   ```

   Si ya hay un nombre de usuario existente <*nombre_usuario*>, este mandato falla.

   Si el rol especificado no es admin ni guest este mandato falla.

   Cuando se añade un usuario, puede utilizar los mismos nombre de usuario y contraseña para el inicio de sesión del producto y el inicio de sesión de la API REST.
2. Para suprimir un usuario, ejecute el mandato siguiente:

   ```
   ./usr/local/nc/bin/nc_user_manager delete <nombre_usuario> <contraseña>
   ```

   Si ya hay un nombre de usuario existente <*nombre_usuario*>, este mandato falla.

   Este mandato falla si el <*nombre_usuario*> y la <*contraseña*> no coinciden con lo que se registra en QRadar Packet Capture.

   Cuando se suprime un usuario, puede utilizar los mismos nombre de usuario y contraseña para el inicio de sesión del producto y el inicio de sesión de la API REST.

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 aplicación de QRadar Packet Capture son independientes de las contraseñas de sistema operativo.

Procedimiento

1. Utilice SSH para iniciar la sesión como usuario `root`.

   La contraseña predeterminada para el usuario root es `P@ck3t08..`
2. Para cambiar la contraseña de las cuentas de usuario `root`, utilice el mandato **`passwd`** *nombre_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 3, “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 de red en un directorio preconfigurado. Cuando se llena el espacio del directorio, se sobrescriben los archivos existentes.

Capítulo 3. 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 de red en un directorio preconfigurado. 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 escriba el URL siguiente:
   `https://`*`Dirección_IP_PCAP`*`:41390`
2. Inicie la sesión con la información de cuenta de usuario siguiente:
   Usuario: `continuum`
   Contraseña: `P@ck3t08..`

Resolución de problemas: Si un usuario introduce una contraseña incorrecta cinco veces seguidas dentro de un periodo de 10 minutos, el usuario queda bloqueado durante 30 minutos. Un administrador del sistema puede desbloquear manualmente la cuenta de usuario.

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

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.`

Resolución de problemas

Para ver la información del sistema sobre las interfaces de captura configuradas, pulse **Resolución de problemas**.

Información del servidor

Para ver la información del servidor, pulse **Información del servidor**.

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 1, “Información preliminar sobre QRadar Packet Capture”, en la página 1
IBM Security QRadar Packet Capture es una aplicación de captura y búsqueda del tráfico de red. El dispositivo de QRadar Packet Capture solo tiene un puerto de captura (DNA0) y puede instalar un transceptor de SFP 10G o 1G.

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 4. Clúster

Utilice el dispositivo QRadar Packet Capture como servidor autónomo único o como un clúster de servidores.

Las ediciones 10G dan soporte a clústers lo que amplía la capacidad de almacenamiento de datos y la capacidad de cálculo cuando se compara con un único servidor autónomo. Los clústers contienen un maestro. Puede conectar hasta dos dispositivos de nodos de datos de QRadar Packet Capture a cada sistema maestro de QRadar Packet Capture.

La pestaña **Clúster** visualiza dos nodos de datos, conjuntamente con su estado actual.

Los nodos de datos no forman marte del clúster de forma predeterminada y su estado es inhabilitado.

Habilitación de nodos de datos

Después de conectar físicamente los Nodos de datos de IBM Security QRadar Packet Capture con la modalidad maestra de QRadar Packet Capture, debe habilitar los Nodos de datos de QRadar Packet Capture. Los Nodos de datos de QRadar Packet Capture crean un clúster para aumentar la capacidad de almacenamiento y mejorar el rendimiento de captura.

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

Antes de empezar

Asegúrese de que el servidor de capturas se está ejecutando.

Procedimiento

1. Para habilitar los nodos de datos, siga estos pasos:
   a. En la pestaña **Clúster**, para cada nodo de datos, seleccione **Habilitar**. El estado muestra **Conectado**.
   b. Reinicie el servidor de capturas. Los Nodos de datos de QRadar Packet Capture están ahora habilitados.

   Cuando los Nodos de datos de QRadar Packet Capture están conectados y en ejecución, el estado correspondiente en el clúster cambia a “conectado”.

   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.
2. Para inhabilitar nodos de datos, siga estos pasos:
   a. En la pestaña Clúster, para cada nodo de datos, seleccione **Inhabilitar**. El estado muestra **Desconectado**.
   b. Reinicie el servidor de capturas. Los Nodos de datos de QRadar Packet Capture están ahora inhabilitados y ya no están asociados al maestro.

   Un nodo de datos desconectado ya no almacena datos.

Una vez que el nodo maestro está inhabilitado, el tamaño de almacenamiento comprimido (virtual) en el panel de control disminuye.

Si el Nodo de datos1 o el Nodo de datos2 tienen licencia, la columna de licencia muestra **Permanente** o **Evaluación**, en función la licencia utilizada.

Capítulo 5. Gráficos de QRadar Packet Capture

En IBM Security QRadar Packet Capture, utilice un gráfico en directo o histórico para visualizar estadísticas de captura de paquetes.

Gráfico en directo

El gráfico en directo hace un seguimiento de las estadísticas de captura de paquetes siguientes acerca de la captura de paquetes actual:

- Rendimiento en Gbps (gigabits por segundo)
- Paquetes totales por segundo
- Paquetes TCP por segundo
- Paquetes UDP por segundo
- Paquetes por segundo para tráfico no UDP
- Número de sucesos del sistema
- Proporción de compresión de paquetes

Pase el puntero del ratón sobre el gráfico y obtenga las estadísticas correspondientes a ese punto del gráfico.

Puede pulsar el gráfico sobre un momento específico y generar automáticamente una solicitud de búsqueda. También puede pulsar sobre los iconos de estilo de visualización para cambiar la vista del gráfico.

Gráfico histórico

El gráfico histórico proporciona una visión general a largo plazo del historial de captura de paquetes. Las opciones de línea temporal de historial incluyen 1 hora, 1 día y 1 semana.

Pase el puntero del ratón sobre el gráfico y obtenga las estadísticas correspondientes a ese punto del gráfico.

Pulse el gráfico sobre un momento específico para generar automáticamente una solicitud de búsqueda.

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. En la columna **Acción** de la página de búsqueda utilice la opción **Fragmentación** (chunking) para dividir los resultados de la búsqueda 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 primero el número de archivo PCAP y pulsando después **Descargar archivo de PCAP**.

Los segmentos de datos tienen 128MB y el último segmento de datos puede tener cualquier tamaño por debajo de 128MB.

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. Configuración de filtros de captura previa

Los filtros de captura previa filtran el tráfico de red antes de grabar los datos capturados en el disco.

Procedimiento

1. Cree un filtro de captura previa.
   a. Pulse el menú **Filtro de captura previa**.
   b. Especifique los valores de las opciones Nombre de filtro y Filtro de búsqueda.

      Un filtro de captura tiene la forma de expresiones primitivas conectadas por conjunciones (and/or) y que pueden ir precedidas por not.

      En el ejemplo siguiente, se descarta todo el tráfico destinado al puerto 80:

      ```
      not dst port 80
      ```

      En el ejemplo siguiente, sólo se captura el tráfico de estos dos hosts y se descarta el resto del tráfico:

      ```
      host 1.2.3.4 or host 1.1.1.1
      ```

   c. Complete el filtro de captura previa pulsando **Añadir**. El último filtro de captura previa añadido a la lista es el filtro activo. También se visualiza el historial de filtros anteriores.
2. Reinicie el servidor de capturas para activar el filtro recién añadido.
3. Suprima permanentemente el filtro seleccionado **Suprimir**. Debe reiniciar el servidor de capturas.

Capítulo 8. Configuración de desencadenantes activos

Los desencadenantes activos alertan cuando se produce un suceso especificado en la red. Por ejemplo, puede especificar una dirección IP como filtro de búsqueda para que se produzca una alerta cuando se capture el tráfico que contiene la dirección IP.

Procedimiento

1. Cree un desencadenante activo.
   a. Pulse el menú **Desencadenante activo**.
   b. Especifique los valores de las opciones Nombre de desencadenante e Intervalo de tiempo.
   c. Complete el desencadenante activo pulsando **Añadir**.

   Restricción: Puede especificar hasta cinco desencadenantes activos.
2. Revise los sucesos de desencadenante en el **Registro de sucesos** conforme se producen. Al pulsar un suceso desencadenante activo se genera automáticamente una solicitud de búsqueda dentro de los parámetros de tiempo especificados alrededor del suceso desencadenado. El tiempo de búsqueda incluye segundos antes y segundos después del suceso.
3. Suprima el desencadenante configurado seleccionando **Suprimir**.

Capítulo 9. 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.

¿Está HyperThreading habilitado en la BIOS?

HyperThreading está habilitado en la BIOS de forma predeterminada. Ejecute el mandato `lscpu` y revise la salida para asegurarse de que "Hebra(s) por núcleo es igual a 2". A continuación se proporciona la salida de ejemplo del mandato para 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
```

¿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.

¿Esta habilitado el Nodo de datos de QRadar Packet Capture?

Cuando el Nodo de datos de QRadar Packet Capture está físicamente conectado al nodo maestro, también debe asegurarse de que esté habilitado en la interfaz de usuario para trabajar con el servidor maestro. El sistema soporta actualmente hasta dos Nodos de datos de QRadar Packet Capture.

Si la pestaña **Clúster** muestra que los Nodos de datos de QRadar Packet Capture están conectados y habilitados y el valor **ID del sistema** no se encuentra en la pantalla **Actualizar licencia de nodo(n)** bajo la pestaña **Admin**, debe asegurarse de que el Nodo de datos de QRadar Packet Capture específico tenga la misma versión de software de Nodo de datos de QRadar Packet Capture instalada que el nodo maestro. Asegúrese de que este requisito se cumple después de actualizar a la versión de software más reciente.

Como usuario de `root`, ejecute el mandato siguiente para comprobar la versión de software que está instalada en el Nodo de datos de QRadar Packet Capture y el nodo maestro:

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

La versión de software del Nodo de datos de QRadar Packet Capture debe ser la misma versión que la que está instalada en el nodo maestro.

¿Cómo se aplica una licencia para el Nodo de datos de QRadar Packet Capture desde la línea de mandatos?

Para asegurarse de que está en el Nodo de datos de QRadar Packet Capture, como usuario `root`, ejecute el mandato siguiente:

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

Para verificar que está conectado al Nodo de datos de QRadar Packet Capture, busque una D añadida al final del número de versión, por ejemplo, 7.2.7.256D.

Para aplicar la licencia al Nodo de datos de QRadar Packet Capture, como usuario `root`, ejecute el script: `nc_set_license.sh` como `root`.

Notas:

- Para hacer efectiva la licencia nueva, debe reiniciar el Nodo de datos de QRadar Packet Capture.
- Si el Nodo de datos de QRadar Packet Capture ya tiene licencia en el momento de fabricación, no es necesario ejecutar el script. La licencia es efectiva en cuanto se inicia el sistema.

Si la licencia aplicada no es válida, se visualiza un mensaje de error:

```
Aviso: LicenseKey *NO* es válida.
```

¿Qué es el formato de registro LEEF 2.0?

Los mensajes LEEF (Log Event Extended Format) se añaden al archivo `/var/log/messages` en el formato siguiente:

```
<FechaHora> <IPServidor> LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|<ID>|cat=<categoría> msg=<mensaje>
```

Por ejemplo, cuando el servidor de captura de paquetes se inicia en un sistema cuya dirección IP es 10.91.170.20, se añade el mensaje LEEF siguiente al archivo /var/log/messages:

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

¿Por qué la solicitud Crear búsqueda devuelve un error NoSpace?

Si el directorio /extraction está lleno cuando crea una búsqueda, el servidor devuelve el error NoSpace.

¿Qué ocurre cuando se detiene una búsqueda?

Una búsqueda se detiene cuando el espacio utilizado en el directorio /extraction supera los 6,7 GB. Se envía un mensaje LEEF a Syslog indicando que se detiene la búsqueda. El registro de sucesos visualiza un aviso parecido a:

```
!AVISO: Almacenamiento de extracción lleno! ¡La búsqueda no puede
continuar!
```

Para asegurarse de que una búsqueda detenida se reanuda, debe crear espacio suprimiendo búsquedas antiguas ya completadas. Para suprimir una búsqueda antigua, siga estos pasos:

1. Pulse la opción de menú principal **Buscar**.
2. En el marco **Buscar registro de solicitud** suprima búsquedas antiguas pulsando **Suprimir búsqueda**.

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

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. Los materiales de estos sitios web no forman parte de los materiales de IBM para este producto, y el uso que se haga de estos sitios web será responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le proporcione de cualquier modo que considere adecuado 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
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 y los ejemplos de clientes citados se presentan solamente a efectos ilustrativos. Los resultados de rendimiento reales pueden variar en función de las configuraciones y las condiciones operativas específicas.

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.

Las declaraciones relativas a la dirección o intenciones futuras de IBM pueden cambiar o ser retiradas sin previo aviso, y sólo representan propósitos 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 estos nombres son ficticios y cualquier similitud con nombres reales de personas o empresas es pura coincidencia.

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.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

Términos y condiciones de la documentación de producto

Se otorga permiso para el uso de estas publicaciones si se cumplen estos términos y condiciones.

Aplicabilidad

Estos términos y condiciones se añaden a los términos de uso del sitio web de IBM.

Uso personal

Puede reproducir estas publicaciones para su uso personal, no comercial, siempre que se conserven todos los avisos sobre derechos de propiedad. No puede realizar trabajos derivados de estas publicaciones, ni de partes de las mismas, ni reproducirlas, distribuirlas o visualizarlas, sin el consentimiento expreso de IBM.

Uso comercial

Puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de la empresa a condición de que se conserven todos los avisos de propiedad. No puede realizar trabajos derivados de estas publicaciones, ni de partes de las mismas, ni reproducirlas, distribuirlas o visualizarlas fuera de la empresa, sin el consentimiento expreso de IBM.

Derechos

Salvo lo aquí permitido de forma expresa, no se conceden otros permisos, licencias o derechos, ni implícitos ni explícitos, para las publicaciones o cualquier información, datos software u otra propiedad intelectual que en ellas se incluya.

IBM se reserva el derecho de retirar los permisos que se hayan proporcionado siempre que, bajo su discreción, el uso de las publicaciones sea perjudicial para sus intereses o, según determine IBM, no se estén siguiendo adecuadamente las instrucciones detalladas anteriormente.

No se puede descargar, exportar o reexportar si no es en total cumplimiento con todas las leyes y reglamentos aplicables, incluidas las leyes y reglamentos de los EE.UU. en materia de exportación.

IBM NO GARANTIZA EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, YA SEAN EXPLÍCITAS O IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN,

NO INFRACCIÓN Y ADECUACIÓN A UN FIN DETERMINADO.

Declaración de privacidad en línea de IBM

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.

Impreso en España