IBM Security QRadar Incident Forensics
Versión 7.2.6

Guía de instalación

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 33.

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

Introducción a la instalación de IBM Security QRadar Incident Forensics

Información sobre la instalación de IBM® Security QRadar Incident Forensics y la integración del producto con IBM Security QRadar. Los dispositivos de QRadar Incident Forensics contienen software preinstalado y el sistema operativo Red Hat Enterprise Linux. También puede instalar el software QRadar Incident Forensics en su propio hardware.

Destinatarios

Los administradores de red que son responsables de la instalación y configuración de los sistemas QRadar Incident Forensics.

Los administradores requieren un conocimiento de trabajo de las redes y de los sistemas operativos Linux.

Documentación técnica

Para encontrar la documentación del producto IBM Security QRadar en la web, incluyendo toda la documentación traducida, acceda a la IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Para obtener información sobre cómo acceder a la documentación más técnica de la biblioteca de productos de QRadar, consulte la Nota técnica Acceso a la documentación de IBM Security (www.ibm.com/support/docview.wss?rs=0 &uid=swg21614644).

Cómo ponerse en contacto con el servicio de soporte al cliente

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

Declaración de buenas prácticas de seguridad

La seguridad del sistema de TI implica proteger los sistemas y la información a través de la prevención, detección y respuesta al acceso inadecuado desde dentro y fuera de su empresa. El acceso incorrecto puede provocar la alteración, destrucción, apropiación indebida o mala utilización de la información o puede provocar daños o uso inadecuado de los sistemas, incluido el ataque contra otros. Ningún sistema o producto de TI debe ser considerado completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectivo para impedir el acceso o uso inadecuado. Los sistemas, productos y servicios de IBM están diseñados para ser parte de un enfoque integral de seguridad legal, que implicará necesariamente procedimientos operativos adicionales y puede requerir otros sistemas, productos o servicios para ser más eficaz. IBM NO GARANTIZA QUE CUALQUIER SISTEMA, PRODUCTO O SERVICIO SEA INMUNE A, NI QUE VAYA A CONVERTIR A SU EMPRESA EN INMUNE A, LA CONDUCTA MALINTENCIONADA O ILEGAL POR PARTE 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 conformidad con las leyes, regulaciones 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.

Nota

IBM Security QRadar Incident Forensics está diseñado para ayudar a las empresas a mejorar el entorno y los datos de seguridad. Más concretamente, IBM Security QRadar Incident Forensics está diseñado para ayudar a las empresas a investigar y comprender mejor lo que ha ocurrido en incidencias de seguridad de la red. La herramienta permite a las empresas indexar y buscar datos de paquete de red capturados (PCAP) e incluye una característica que puede reconstruir dichos datos en su formato original. Esta característica de reconstrucción puede reconstruir datos y archivos, incluidos los mensajes de correo electrónico, archivos adjuntos de imagen y archivo, llamadas telefónicas VoIP y sitios web. Los manuales y el resto de documentación que acompaña al programa contienen información adicional acerca de las características y funciones del programa y cómo configurarlas. El uso de este programa puede estar sujeto a diversas leyes o regulaciones, incluyendo las relacionadas con la privacidad, la protección de datos, el empleo y las comunicaciones electrónicas y almacenamiento. IBM Security QRadar Incident Forensics sólo puede utilizarse con fines legales y de forma legal. El cliente se compromete a utilizar este programa de conformidad con las leyes, regulaciones y políticas aplicables, y asume toda la responsabilidad de su cumplimiento. Ser licenciatario implica que obtendrá o ha obtenido las autorizaciones, permisos o licencias necesarias para permitir el uso legal de IBM Security QRadar Incident Forensics.

Capítulo 1. Actualización de QRadar Incident Forensics

Debe actualizar todos los productos de IBM Security QRadar de su despliegue a la misma versión. Puede actualizar IBM Security QRadar Incident Forensics V7.2.5 a V7.2.6 mediante un instalador de actualizaciones. Durante la actualización, la versión de RedHat Enterprise Linux se actualiza a la versión 6.7.

Si desea actualizar de QRadar Incident Forensics V7.2.4 o versiones anteriores y desea conservar los datos, póngase en contacto con el representantes de ventas de IBM. De lo contrario, si desea actualizar de QRadar Incident Forensics V7.2.4 o versiones anteriores pero no desea conservar los datos, puede actualizar directamente a V7.2.6 realizando una instalación nueva.

Restricción: El redimensionamiento de volúmenes lógicos mediante un gestor de volúmenes lógicos (LVM) no está soportado.

Procedimiento

1. Descargue el archivo <*QRadar_patchupdate*>.*sfs* de IBM Fix Central (www.ibm.com/support/fixcentral).
2. Utilice SSH para iniciar la sesión en el sistema como usuario root.
3. Copie el archivo de parche en el directorio `/tmp` o en otra ubicación que tenga suficiente espacio en disco.
4. Para crear el directorio `/media/updates`, escriba el mandato siguiente:

   ```
   mkdir -p /media/updates
   ```
5. Cambie al directorio donde ha copiado el archivo de parche.
6. Para montar el archivo de parche en el directorio `/media/updates`, escriba el mandato siguiente :

   ```
   mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates/
   ```
7. Para ejecutar el instalador de actualizaciones, escriba el mandato siguiente:

   ```
   /media/updates/installer
   ```

   La primera vez que ejecuta el script del instalador de parches, puede haber un retardo antes de que se visualice el primer menú del instalador de parches.
8. Proporcione respuestas a las preguntas de preinstalación en función del despliegue.
9. Utilice el instalador de actualizaciones para actualizar todos los hosts de su despliegue.

   Si no selecciona **Patch All**, debe actualizar los sistemas por el orden siguiente:

   - QRadar Console
   - QRadar Incident Forensics

   Si su sesión SSH se desconecta mientras la actualización está en curso, la actualización continúa. Cuando vuelve a abrir la sesión SSH y vuelve a ejecutar el instalador, la instalación se reanuda.
10. Una vez completada la actualización, desmonte la actualización de software utilizando el mandato siguiente: **`umount /media/updates`**

Qué hacer a continuación

Actualice los dispositivos de captura de paquetes. Para obtener más información, consulte el manual *IBM Security QRadar Packet Capture Quick Reference Guide*.

Capítulo 2. Componentes de instalación de QRadar Incident Forensics

QRadar Incident Forensics se integra en la arquitectura escalable de IBM QRadar Security Intelligence Platform. En función de sus necesidades, puede instalar los componentes de IBM Security QRadar Incident Forensics en un solo dispositivo (*all-in-one*) o en varios dispositivos.

Opciones de instalación

Según los componentes que instale, no estarán disponibles todas las prestaciones de seguridad. Por ejemplo, si instala QRadar Incident Forensics en un único dispositivo, solamente están disponibles los análisis forenses de la red. Sin embargo, si instala un host gestionado de QRadar Incident Forensics, habrá más prestaciones de seguridad disponibles. Para la mayoría de las instalaciones, instale QRadar Console, al menos un QRadar Incident Forensics Processor y uno o varios dispositivos de QRadar Packet Capture.

En el diagrama siguiente se resumen las diversas prestaciones de seguridad y la infraestructura arquitectónica de IBM QRadar Security Intelligence Platform.

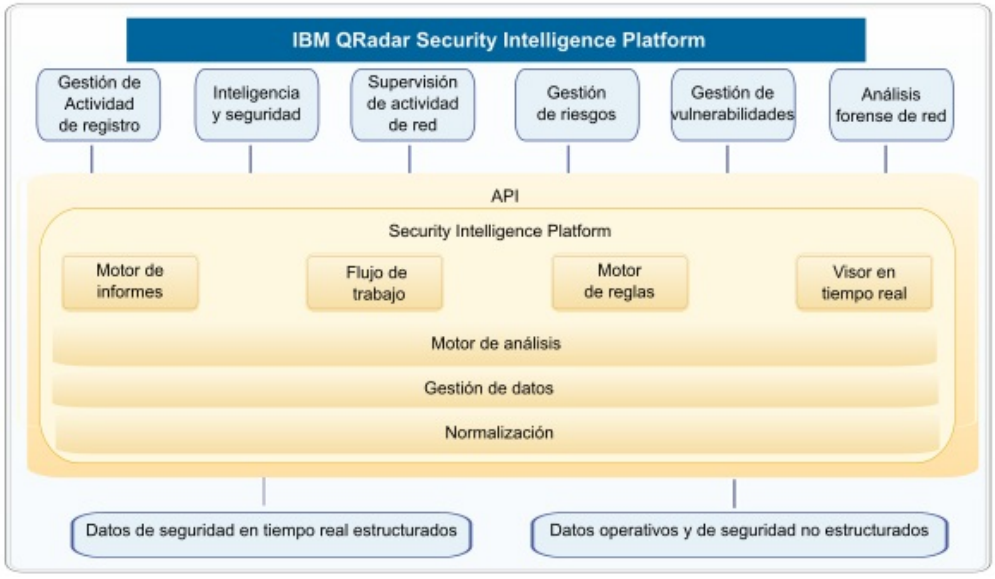


Figura 1. Visión general de la arquitectura de inteligencia y seguridad de QRadar

Despliegues integrales (all-in-one)

En los despliegues autónomos o integrales, instale el software de IBM Security QRadar Incident Forensics Standalone. Estos despliegues de un solo dispositivo son similares a la instalación de QRadar Console y un host gestionado de QRadar Incident Forensics en un solo dispositivo, pero sin gestión de registros, supervisión de la actividad de la red ni otras características de inteligencia y seguridad. En el caso de una solución de análisis forense de red autónoma, instale QRadar Incident Forensics Standalone en despliegues de tamaño pequeño o mediano.

Tal como se muestra en el diagrama siguiente, puede conectar dispositivos de QRadar Packet Capture a IBM Security QRadar Incident Forensics Standalone.

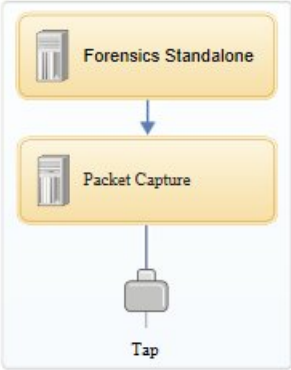


Figura 2. Ejemplo de despliegue de IBM Security QRadar Incident Forensics Standalone

Restricción: No se pueden añadir hosts gestionados a QRadar Incident Forensics Standalone ni conectar QRadar Incident Forensics Standalone a QRadar Console.

Despliegues distribuidos

En los despliegues donde se necesita tanto el análisis forense de la red como otras prestaciones de inteligencia y seguridad, o cuando es necesario distribuir la carga de trabajo para las recuperaciones forenses, instale QRadar Console y uno o varios hosts gestionados de QRadar Incident Forensics. QRadar Console proporciona información y gestión de sucesos (SIEM), gestión de registros, detección de anomalías, gestión de riesgos y gestión de vulnerabilidades.

En un despliegue distribuido hay tres dispositivos:

- QRadar Console
- Host gestionado de QRadar Incident Forensics (QRadar Incident Forensics Processor)
- QRadar Packet Capture (opcional)

Las versiones de software para todos los dispositivos de IBM Security QRadar de un despliegue deben coincidir y tener el mismo nivel de arreglo. Los despliegues con versiones diferentes de software no están soportados.

En el diagrama siguiente se muestra que puede conectar varios hosts gestionados de QRadar Incident Forensics a QRadar Console. Puede conectar dispositivos de QRadar Packet Capture a los hosts gestionados de QRadar Incident Forensics (QRadar Incident Forensics Processor).

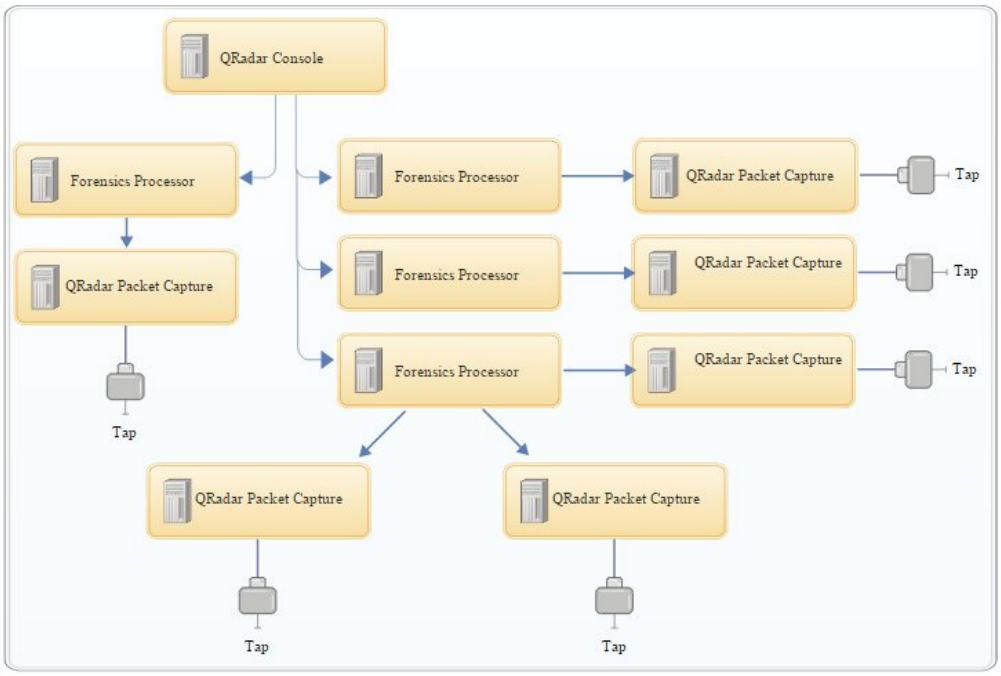


Figura 3. Ejemplo de despliegue distribuido

Componentes de QRadar Incident Forensics

Los despliegues de QRadar pueden incluir los siguientes componentes:

QRadar Console

Proporciona la interfaz de usuario del producto QRadar. La interfaz proporciona vistas de sucesos y flujos en tiempo real, informes, delitos, información de activos y funciones administrativas.

En los despliegues distribuidos, utilice QRadar Console para gestionar varios hosts de QRadar Incident Forensics Processor.

QRadar Incident Forensics Processor

Proporciona la interfaz del producto QRadar Incident Forensics. La interfaz proporciona herramientas para hacer un seguimiento paso a paso de las acciones de los delincuentes cibernéticos, reconstruir los datos de red en bruto que están relacionados con un incidente de seguridad, realizar búsquedas en los datos no estructurados disponibles y reconstruir visualmente las sesiones y los sucesos.

Debe añadir QRadar Incident Forensics Processor como host gestionado para poder utilizar la prestación de análisis forense de inteligencia y seguridad.

QRadar Incident Forensics Standalone

Proporciona la interfaz de usuario del producto QRadar Incident Forensics. La instalación de QRadar Incident Forensics Standalone proporciona las herramientas que necesita para realizar investigaciones forenses. Solamente están disponibles las funciones de investigación forense y las funciones administrativas relacionadas.

QRadar Packet Capture

Puede instalar un dispositivo de QRadar Packet Capture opcional. Si no se despliega ningún otro dispositivo de captura de paquetes (PCAP) de red,

puede utilizar este dispositivo para almacenar los datos utilizados por QRadar Incident Forensics. Puede instalar tantos dispositivos de este tipo como desee como TAP de red o subred para recopilar los datos de paquetes en bruto.

Si no hay ningún dispositivo de captura de paquetes conectado, puede cargar manualmente los archivos de captura de paquetes en la interfaz de usuario o mediante FTP.

Capítulo 3. Visión general de la instalación de QRadar Incident Forensics

Instale el software de QRadar Incident Forensics en un dispositivo propio o en un dispositivo virtual. En los dispositivos de QRadar Incident Forensics se instala el software de QRadar Incident Forensics.

QRadar Incident Forensics debe instalarse en un sistema operativo Red Hat Enterprise Linux.

Selección de ID de dispositivo

Para QRadar Incident Forensics, en la mayoría de los casos se instalan al menos dos imágenes ISO:

- QRadar Console

  Los productos de QRadar utilizan la misma imagen de software de instalación. La *clave de activación* determina el tipo de dispositivo y los componentes que se instalarán. Cuando especifique la clave de activación, se le solicitará que identifique el tipo de dispositivo. Debe instalar QRadar Console.
- 6000 QRadar Incident Forensics Processor (host gestionado)

  Debido a los controles de exportación, los componentes de QRadar Incident Forensics se instalan desde una imagen ISO diferente. Debe instalar el host gestionado de QRadar Incident Forensics y configurarlo para que se conecte a QRadar Console.

Para las instalaciones integrales (all-in-one), instale solamente la imagen ISO de 6100 QRadar Incident Forensics y seleccione el componente QRadar Incident Forensics Standalone.

Cuando instala QRadar Incident Forensics, una clave de licencia predeterminada le proporciona acceso durante cinco semanas. Antes de que caduque la licencia predeterminada, debe asignar una clave de licencia al sistema.

Pasos de la instalación

En las instalaciones distribuidas, siga estos pasos, que le guiarán a través del proceso de instalación.

1. Revise los requisitos de hardware y software.
2. Instale el software de QRadar Console.
3. Instale el host gestionado de QRadar Incident Forensics.
4. Despliegue el host gestionado de QRadar Incident Forensics.
5. Añada dispositivos de captura de paquetes.

Claves de activación y claves de licencia

Al instalar dispositivos de IBM Security QRadar, debe especificar una clave de activación. Después de la instalación, debe aplicar las claves de licencia. Para evitar especificar una clave incorrecta en el proceso de instalación, es importante comprender la diferencia entre las claves.

Clave de activación

La clave de activación es una serie de caracteres alfanuméricos de 4 partes y 24 dígitos que recibe de IBM. Todas las instalaciones de productos QRadar utilizan el mismo software. Sin embargo, la clave de activación especifica qué módulos de software deben aplicarse a cada tipo de dispositivo. Por ejemplo, utilice la clave de activación de IBM Security QRadar QFlow Collector para instalar sólo los módulos de QRadar QFlow Collector.

Puede obtener la clave de activación desde las ubicaciones siguientes:

- Si ha adquirido un dispositivo que está preinstalado con el software de QRadar, la clave de activación está incluida en un documento del CD incluido.
- Si ha adquirido software de QRadar o una descarga de dispositivo virtual, se incluye una lista de claves de activación en el documento *Cómo empezar*. El documento *Cómo empezar* está adjunto al correo electrónico de confirmación.

Clave de licencia

El sistema incluye una clave de licencia temporal que le proporciona acceso al software de QRadar durante cinco semanas. Después de instalar el software y antes de que caduque la clave de licencia predeterminada, debe añadir las licencias adquiridas.

Al adquirir un producto de QRadar, se envía desde IBM un correo electrónico que contiene la clave de licencia permanente. Estas claves de licencia amplían las prestaciones de su tipo de dispositivo y definen los parámetros de funcionamiento del sistema. Debe aplicar las claves de licencia antes de que caduque la licencia predeterminada.

Accesorios de hardware y software de escritorio necesarios para las instalaciones de QRadar

Antes de instalar productos de IBM Security QRadar , asegúrese de que tiene acceso a los accesorios de hardware y al software de escritorio necesarios.

Accesorios de hardware

Asegúrese de que tiene acceso a los siguientes componentes de hardware:

- Monitor y teclado
- Fuente de alimentación ininterrumpible (UPS) para todos los sistemas que almacenan datos, tales como QRadar Console, componentes de Procesador de sucesos o componentes de QRadar QFlow Collector

Importante: los productos QRadar admiten implementaciones de RAID (matriz redundante de discos independientes), pero no admiten instalaciones RAID basadas en software.

Requisitos de software de escritorio

Asegúrese de que las aplicaciones siguientes están instaladas en todos los sistemas de escritorio que se utilizan para acceder a la interfaz de usuario del producto QRadar:

- Java™ Runtime Environment (JRE) versión 1.7 o IBM 64 bits Runtime Environment for Java V7.0

- Adobe Flash versión 10.x

Navegadores web soportados

La tabla siguiente muestra los navegadores web soportados:

Tabla 1. Navegadores web soportados para los productos de QRadar

Navegador web	Versiones soportadas
Mozilla Firefox	38.0 Extended Support Release
Microsoft Internet Explorer de 32 bits o 64 bits con la modalidad de documento o la modalidad de navegador habilitada.	10.0
Microsoft Internet Explorer de 64 bits con modalidad Microsoft Edge habilitada.	11.0
Google Chrome	Versión 46

Si utiliza Microsoft Internet Explorer, debe habilitar la modalidad de documento y la modalidad de navegador:

1. En el navegador web Internet Explorer, pulse F12 para abrir la ventana Herramientas de desarrollo.
2. Pulse **Modo de explorador** y seleccione la versión del navegador web.
3. Pulse **Modo de documento**.
   - Para Internet Explorer V9.0, seleccione **Estándares de Internet Explorer 9**.
   - Para Internet Explorer V10.0, seleccione **Estándares de Internet Explorer 10**.

La comunicación entre hosts de QRadar Incident Forensics requiere puertos abiertos

El la tabla siguiente se indican los puertos que deben estar abiertos entre hosts de QRadar Incident Forensics:

Tabla 2. Puertos abiertos entre hosts

Puerto	Descripción
443	Necesario para análisis de artefactos.
28080	Necesario para búsquedas distribuidas

Capítulo 4. Instalaciones de software de QRadar Incident Forensics en un dispositivo propio

Para garantizar una instalación correcta de IBM Security QRadar Incident Forensics en su propio dispositivo, debe instalar el sistema operativo Red Hat Enterprise Linux, QRadar Console y el host gestionado de QRadar Incident Forensics.

En las instalaciones de software nuevo que integran QRadar Incident Forensics con IBM Security QRadar, instale dos archivos ISO:

- QRadar

  Se utiliza un solo ISO para instalar cada producto de QRadar excepto para QRadar Incident Forensics. La clave de activación que especifique determina el tipo de dispositivo de QRadar que se instala.
- QRadar Incident Forensics

  Esta imagen ISO contiene QRadar Incident Forensics Processor y QRadar Incident Forensics Standalone. Debe instalar QRadar Incident Forensics Processor.

Requisitos previos para la instalación de QRadar Incident Forensics en un dispositivo propio

Antes de instalar el sistema operativo Red Hat Enterprise Linux (RHEL) en un dispositivo propio, asegúrese de que el sistema cumple los requisitos del sistema.

En la tabla siguiente se describen los requisitos del sistema:

Tabla 3. Requisitos del sistema para instalaciones de RHEL en un dispositivo propio

Requisito	**Detalles**
Versión de software soportada	Versión 6.7
Versión de bits	64 bits
Discos Kickstart	No soportados
Memoria (RAM) para el procesador de Forensics	Mínimo 128 GB **Importante:** Debe actualizar la memoria del sistema antes de instalar QRadar.
Espacio de disco libre para el procesador de Forensics	Mínimo de un 5% del espacio de disco total **Importante:** Para obtener un rendimiento óptimo, debe estar disponible un espacio de disco adicional que sea 2 o 3 veces mayor que el espacio mínimo de disco.
Configuración de cortafuegos	WWW (http, https) habilitado SSH habilitado **Importante:** Antes de configurar el cortafuegos, inhabilite la opción SELinux. La instalación de QRadar incluye una plantilla de cortafuegos predeterminada que puede actualizar en la ventana Configuración del sistema.

Restricción: El redimensionamiento de volúmenes lógicos mediante un gestor de volúmenes lógicos (LVM) no está soportado.

Propiedades de partición del sistema operativo Linux para las instalaciones de QRadar en su propio dispositivo

Si utiliza su propio dispositivo, puede suprimir y volver a crear las particiones en el sistema operativo Red Hat Enterprise Linux, en lugar de modificar las particiones predeterminadas.

Utilice los valores de la tabla siguiente como guía cuando vuelva a crear las particiones en el sistema operativo Red Hat Enterprise Linux.

Restricción: El redimensionamiento de volúmenes lógicos mediante un gestor de volúmenes lógicos (LVM) no está soportado.

Tabla 4. Guía de particiones para RHEL

Partición	Descripción	Punto de montaje	Tipo de sistema de archivos	Tamaño	Se obliga a que sea primaria	SDA o SDB
/boot	Archivos de arranque del sistema	/boot	EXT4	200 MB	Sí	SDA
intercambio	Se utiliza como memoria cuando la RAM está llena.	vacío	intercambio	Sistemas con entre 4 y 8 GB de RAM; el tamaño de la partición de intercambio debe coincidir con la cantidad de RAM Sistemas con entre 8 y 24 GB de RAM; configure el tamaño de la partición de intercambio para que sea el 75% de la RAM, con un valor mínimo de 8 GB y un valor máximo de 24 GB.	No	SDA
/	Área de instalación de QRadar, el sistema operativo y los archivos asociados.	/	EXT4	20000 MB	No	SDA
/store/tmp	Área de almacenamiento para los archivos temporales de QRadar	/store/tmp	EXT4	20000 MB	No	SDA
/var/log	Área de almacenamiento para QRadar y archivos de registro del sistema	/var/log	EXT4	20000 MB	No	SDA

Tabla 4. Guía de particiones para RHEL (continuación)

Partición	Descripción	Punto de montaje	Tipo de sistema de archivos	Tamaño	Se obliga a que sea primaria	SDA o SDB
/store	Área de almacenamiento para los datos de QRadar y los archivos de configuración	/store	XFS	[1]En los dispositivos de Console: aprox. el 80% del almacenam. disponible. En los hosts gestionados que no sean recopiladores de QFlow ni recopiladores de sucesos de almacenam. y reenvío: aprox. el 90% del almacenam. disponible.	No	SDA Si hay dos discos, SDB
/store/transient	Área de almacenamiento para cursor de base de datos de ariel	/store/transient	XFS en las consolas EXT4 en los hosts gestionados	[1]En los dispositivos de Console: el 20% del almacenam. disponible. En los hosts gestionados que no sean recopiladores de QFlow ni recopiladores de sucesos de almacenam. y reenvío: el 10% del almacenam. disponible.	No	SDA Si hay dos discos, SDB

[1] /store y /store/transient ocupan el 100% del espacio de disco que queda después de crear las cinco primeras particiones.

Restricciones

Las actualizaciones de software futuras podrían fallar si reformatea alguna de las siguientes particiones o sus subparticiones:

- /store
- /store/tmp
- /store/ariel
- /store/transient

Instalación de RHEL en un dispositivo propio

Puede instalar el sistema operativo Red Hat Enterprise Linux en su propio dispositivo para utilizarlo con QRadar Incident Forensics.

Procedimiento

1. Copie el ISO del DVD del sistema operativo Red Hat Enterprise Linux en uno de los siguientes dispositivos de almacenamiento portátil:
   - DVD (Digital Versatile Disk)

- Unidad flash USB de arranque

  Para obtener más información sobre la creación de una unidad de memoria flash USB de arranque, consulte el manual *IBM Security QRadar Installation Guide*.

2. Inserte el dispositivo de almacenamiento portátil en el dispositivo y reinicie el dispositivo.
3. En el menú de inicio, seleccione una de las opciones siguientes.
   - Seleccione la unidad `USB` o `DVD` como opción de arranque.
   - Para instalar en un sistema que da soporte a EFI (Extensible Firmware Interface), debe iniciar el sistema en modalidad de `legado`.
4. Cuando se le solicite, inicie la sesión en el sistema como usuario root.
5. Para evitar un problema con la denominación de la dirección de la interfaz Ethernet, en la página de Bienvenida, pulse el tabulador y, al final de la línea `Vmlinuz initrd=initrd.image`, añada `biosdevname=0`.
6. Siga las instrucciones del asistente de instalación para completar la instalación:
   a. Seleccione la opción **Dispositivos de almacenamiento básico**.
   b. Cuando configure el nombre de host, la propiedad **Hostname** puede incluir letras, números y guiones.
   c. Al configurar la red, en la ventana Conexiones de red, seleccione **System eth0** y luego pulse **Editar** y seleccione **Conectar automáticamente**.
   d. En la pestaña **Valores de IPv4**, en la lista **Método**, seleccione **Manual**.
   e. En el campo **Servidores DNS**, escriba una lista separada por comas.
   f. Seleccione la opción **Crear diseño personalizado**.
   g. Configure `EXT4` para el tipo de sistema de archivos para la partición `/boot`.
   h. Reformatee la partición de intercambio con un tipo de sistema de archivos de intercambio.
   i. Seleccione **Servidor básico**.
7. Cuando la instalación haya finalizado, pulse **Rearrancar**.
8. Asegúrese de que las interfaces de red se denominan `eth0`, `eth1`, `eth2` y `eth3`.

Qué hacer a continuación

Capítulo 7, “Instalación de QRadar Console”, en la página 21

Capítulo 5. Instalación del software QRadar Incident Forensics en un dispositivo de QRadar Incident Forensics

Los dispositivos de IBM Security QRadar Incident Forensics se preinstalan con un sistema operativo Red Hat Enterprise Linux y el software de QRadar.

En las instalaciones de software nuevo que integran QRadar Incident Forensics con IBM Security QRadar, configure los dos archivos ISO precargados:

- QRadar

  Se utiliza un solo ISO para instalar cada producto de QRadar excepto para QRadar Incident Forensics. La clave de activación que especifique determina el tipo de dispositivo de QRadar que se instala.
- QRadar Incident Forensics

  Esta imagen ISO contiene QRadar Incident Forensics Processor y QRadar Incident Forensics Standalone. Debe instalar QRadar Incident Forensics Processor.

En las instalaciones de software nuevo en las que solamente necesita las prestaciones de análisis forense, instale QRadar Incident Forensics Standalone a partir del ISO de QRadar Incident Forensics.

Capítulo 6. Instalaciones de dispositivo virtual para QRadar Incident Forensics

Puede instalar IBM Security QRadar Incident Forensics en un dispositivo virtual. Debe utilizar un dispositivo virtual soportado que cumpla los requisitos mínimos del sistema.

Un dispositivo virtual es un sistema de QRadar Incident Forensics que consta de software de QRadar Incident Forensics que está instalado en una máquina virtual de VMWare ESX .

Un dispositivo virtual proporciona la misma visibilidad y función en la infraestructura de red virtual que los dispositivos de QRadar proporcionan en el entorno físico del usuario.

Proceso de instalación

Para instalar un dispositivo virtual, siga los pasos siguientes por orden:

__ • Cree una máquina virtual.

__ • Instale el software de IBM Security QRadar Incident Forensics en la máquina virtual.

__ • Si ha instalado QRadar Incident Forensics Processor, añada el dispositivo virtual al despliegue.

Requisitos del sistema para dispositivos virtuales

Antes de instalar el dispositivo virtual, compruebe que se cumplen los requisitos mínimos siguientes:

Tabla 5. Requisitos para dispositivos virtuales.

Requisito	Descripción
Cliente de VMware	VMware ESXi Versión 5.0 VMware ESXi Versión 5.1 VMware ESXi Versión 5.5 Para obtener más información sobre clientes de VMWare, consulte el sitio web de VMware (www.vmware.com)
Tamaño de disco virtual	Mínimo: 256 GB **Importante:** Para obtener un rendimiento óptimo, debe estar disponible un espacio de disco que sea 2 o 3 veces mayor que el espacio de disco mínimo.

Crear la máquina virtual

Para instalar un dispositivo virtual, primero debe utilizar VMWare ESX para crear una máquina virtual.

Procedimiento

1. Desde el VMware vSphere Client, pulse **Archivo** > **Nuevo** > **Máquina virtual**.
2. Añada el valor de **Nombre y ubicación** y seleccione un valor en **Almacén de datos** para la nueva máquina virtual.
3. Siga los pasos siguientes como guía para las opciones disponibles:
   a. En el panel **Configuración** de la ventana Crear máquina virtual nueva, seleccione **Personalizada**.
   b. En el panel **Versión de máquina virtual**, seleccione **Versión de máquina virtual: 7**.
   c. Para **Sistema operativo**, seleccione **Linux** y **Red Hat Enterprise Linux 6 (64 bits)**.
   d. En la página **CPUs**, defina el número de procesadores virtuales que desee para la máquina virtual. Seleccione 40 o más.
   e. En el campo **Tamaño de memoria**, escriba o seleccione la memoria RAM necesaria para el despliegue. Seleccione 128 GB o más.
   f. Utilice la tabla siguiente para configurar las conexiones de red.

Tabla 6. Descripciones de los parámetros de configuración de red

Parámetro	Descripción
Cuántos controladores de interfaz de red desea conectar	Debe añadir como mínimo un controlador de interfaz de red
Adaptador	VMXNET3

   g. En la página **Controlador SCSI**, seleccione **VMware Paravirtual**.
   h. En el panel **Disco**, seleccione **Crear disco virtual nuevo** y utilice la tabla siguiente para definir los parámetros de disco virtual.

Tabla 7. Valores para los parámetros de tamaño de disco virtual y política de suministro

Propiedad	Opción
Capacidad	2 o superior (TB)
Suministro de disco	Suministro ligero
Opciones avanzadas	No configurar

4. En la página **Listo para completar**, revise los valores y pulse **Finalizar**.

Qué hacer a continuación

Instale el software de QRadar en la máquina virtual.

Instalar el software de QRadar Incident Forensics en una máquina virtual

Después de crear la máquina virtual, debe instalar en ella el software de IBM Security QRadar.

Restricción: El redimensionamiento de volúmenes lógicos mediante un gestor de volúmenes lógicos (LVM) no está soportado.

Procedimiento

1. En el panel de navegación izquierdo del VMware vSphere Client, seleccione la máquina virtual.

2. En el panel derecho, pulse la pestaña **Resumen**.
3. En el panel **Mandatos**, pulse **Editar valores**.
4. En el panel izquierdo de la ventana **Propiedades de máquina virtual**, pulse **Unidad de CD/DVD 1**.
5. En el panel **Estado de dispositivo**, seleccione la casilla **Conectar al encender**.
6. En el panel **Tipo de dispositivo**, seleccione **Archivo ISO de almacén de datos** y pulse **Examinar**.
7. En la ventana Examinar almacenes de datos, localice y seleccione el archivo ISO del producto, pulse **Abrir** y luego pulse **Aceptar**.
8. Después de instalar la imagen ISO del producto, pulse con el botón derecho en la máquina virtual y seleccione **Alimentación** > **Encender**.
9. Inicie una sesión en la máquina virtual escribiendo `root` para el nombre de usuario.

   El nombre de usuario distingue entre mayúsculas y minúsculas.
10. Compruebe que aparece el Acuerdo de licencia de usuario final (EULA).

    Consejo: Pulse la barra espaciadora para avanzar por el documento.
11. En la página **Select the Appliance ID** , elija el componente de QRadar Incident Forensics que se instalará.
    - Para una instalación distribuida, seleccione **6000 QRadar Incident Forensics Processor**,
    - Para los despliegues autónomos, seleccione **6100 QRadar Incident Forensics Standalone**.
12. Para el tipo de instalación, seleccione **normal**.
13. Siga las instrucciones del asistente de instalación para completar la instalación.

    La tabla siguiente contiene descripciones y notas para ayudarle a configurar la instalación.

Tabla 8. Descripción de valores de red

Valor de red	Descripción
Nombre de host	Nombre de dominio completo
Dirección del servidor DNS secundario	Opcional
Dirección IP pública para redes que utilizan Network Address Translation (NAT)	No soportados
El nombre de servidor de correo electrónico	Si no tiene un servidor de correo electrónico, utilice `localhost`.
Contraseña raíz	La contraseña debe cumplir los siguientes criterios: • Contener al menos 5 caracteres • No contener espacios • Puede incluir los siguientes caracteres especiales : @, #, ^, *.

Después de configurar los parámetros de instalación, se visualiza una serie de mensajes. El proceso de instalación puede tardar varios minutos.

Qué hacer a continuación

Si no instala IBM Security QRadar Incident Forensics Standalone, consulte Capítulo 9, “Adición de un host gestionado de QRadar Incident Forensics aQRadar Console”, en la página 25.

Capítulo 7. Instalación de QRadar Console

En las instalaciones distribuidas, instale QRadar Console en un dispositivo y el host gestionado de IBM Security QRadar Incident Forensics en otro dispositivo.

Restricción: Las versiones de software para todos los dispositivos de un despliegue deben coincidir y tener el mismo nivel de arreglo. Los despliegues con versiones diferentes de software no están soportados.

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos:

- El hardware necesario está instalado.
- Hay un teclado y un monitor conectados mediante conexión VGA.
- La clave de activación está disponible.
- Si desea configurar interfaces de red vinculadas, consulte www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/).

Procedimiento

1. Para las instalaciones en su propio hardware o en máquinas virtuales, añada la imagen ISO de QRadar Console en el directorio raíz.
   a. Cree el directorio `/media/dvd` escribiendo el mandato siguiente:
      ```
      mkdir /media/dvd
      ```
   b. Monte la imagen ISO de QRadar Console escribiendo el mandato siguiente:
      ```
      mount -o loop <ISO_QRadar> /media/dvd
      ```
2. Utilice el script de configuración para iniciar la instalación.
   a. Cambie el directorio de trabajo escribiendo el mandato: `cd /media/dvd`
   b. Inicie el script de configuración escribiendo el mandato: `setup.sh`
3. Siga las instrucciones del asistente de instalación.
   - En **Enter your activation key below**, cuando se le solicite la clave de activación, especifique la serie alfanumérica de 4 partes y 24 dígitos que ha recibido de IBM.

     La letra I y el número 1 (uno) se tratan de la misma manera. La letra O y el número 0 (cero) también se tratados de la misma manera.
   - En la página **Enter the network information to use**, si no tiene un servidor de correo electrónico, escriba `localhost` en el campo **Email server name**.
   - En el campo **Root password**, cree una contraseña que cumpla los siguientes criterios:
     – Contiene al menos 5 caracteres
     – No contiene espacios
     – Puede incluir los siguientes caracteres especiales : @, #, ^, *.

   El proceso de instalación puede tardar varios minutos.
4. Aplique la clave de licencia.
   a. Inicie sesión en QRadar:
      `https://Dirección_IP_QRadar`

El nombre de usuario predeterminado es `admin`. La contraseña es la contraseña de la cuenta de usuario root.

b. Pulse **Iniciar sesión en QRadar**.
c. Pulse la pestaña **Admin**.
d. En el panel de navegación, pulse **Configuración del sistema**.
e. Pulse el icono **Gestión del sistema y licencias**.
f. En el recuadro de lista **Visualizar**, seleccione **Licencias** y cargue su clave de licencia.
g. Seleccione la licencia asignada y pulse **Asignar sistema a licencia**.
h. En la lista de sistemas, seleccione un sistema y pulse **Asignar sistema a licencia**.

Qué hacer a continuación

Ahora puede instalar QRadar Incident Forensics.

Capítulo 8. Instalación de QRadar Incident Forensics

En las instalaciones distribuidas, instale QRadar Console en un dispositivo y el host gestionado de IBM Security QRadar Incident Forensics (QRadar Incident Forensics Processor) en otro dispositivo. En los despliegues autónomos, instale únicamente el componente QRadar Incident Forensics Standalone.

Restricción: Las versiones de software para todos los dispositivos de un despliegue deben coincidir y tener el mismo nivel de arreglo. Los despliegues con versiones diferentes de software no están soportados.

Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos:

__ • El hardware necesario está instalado.

__ • Hay un teclado y un monitor conectados mediante conexión VGA.

__ • La clave de activación está disponible.

Restricción: El redimensionamiento de volúmenes lógicos mediante un gestor de volúmenes lógicos (LVM) no está soportado.

Procedimiento

1. Para las instalaciones en su propio hardware o en máquinas virtuales, añada la imagen ISO de QRadar Incident Forensics en el directorio raíz.
   a. Cree el directorio `/media/dvd` escribiendo el mandato siguiente:
      `mkdir /media/dvd`
   b. Monte la imagen ISO de QRadar Console escribiendo el mandato siguiente:
      `mount -o loop <ISO_QRadar_Incident_Forensics>/media/dvd`
2. Utilice el script de configuración para iniciar la instalación.
   a. Cambie el directorio de trabajo escribiendo el mandato: `cd /media/dvd`
   b. Inicie el script de configuración escribiendo el mandato: `setup.sh`
3. Siga las instrucciones del asistente de instalación.

   En la página **Select the Appliance ID** , elija el componente de QRadar Incident Forensics que se instalará.
   - Para una instalación distribuida, seleccione **6000 QRadar Incident Forensics Processor**,
   - Para los despliegues autónomos, seleccione **6100 QRadar Incident Forensics Standalone**.

   Restricción: Las opciones de configuración siguientes no están soportadas para QRadar Incident Forensics:
   - En la página Choose the type of setup, la opción **HA Recovery Setup**
   - En la página Select if you want to use bonded interface configuration mode, la opción **Use bonded interface configuration mode**

   Si instala QRadar Incident Forensics Processor, el proceso de instalación puede tardar varios minutos.
4. Aplique la clave de licencia.
   a. Inicie sesión en QRadar:

`https://Dirección_IP_QRadar`

El nombre de usuario predeterminado es `admin`. La contraseña es la contraseña de la cuenta de usuario root.

b. Pulse el inicio de sesión.
c. Pulse la pestaña **Admin**.
d. En el panel de navegación, pulse **Configuración del sistema**.
e. Pulse el icono **Gestión del sistema y licencias**.
f. En el recuadro de lista **Visualizar**, seleccione **Licencias** y cargue la clave de licencia.
g. Seleccione la licencia asignada y pulse **Asignar sistema a licencia**.
h. En la lista de licencias, seleccione una licencia y pulse **Asignar licencia a sistema**.

Debe asignar dos claves de licencia al dispositivo de IBM Security QRadar Incident Forensics Standalone. Una licencia es para QRadar Incident Forensics Standalone y la otra es para el acceso a la pestaña **Análisis forense**.

Qué hacer a continuación

Despliegue el host gestionado de QRadar Incident Forensics Processor. Para obtener más información, consulte el apartado Capítulo 9, “Adición de un host gestionado de QRadar Incident Forensics aQRadar Console”, en la página 25.

Capítulo 9. Adición de un host gestionado de QRadar Incident Forensics aQRadar Console

En las instalaciones distribuidas, debe añadir IBM Security QRadar Incident Forensics Processor como host gestionado a QRadar Console.

Un *host gestionado* es cada uno de los dispositivos de QRadar no de consola que hay en el despliegue. Para la distribución de los procesos, puede añadir más de un QRadar Incident Forensics Processor como host gestionado.

Restricción: El uso del Editor de despliegue para añadir o eliminar hosts gestionados de QRadar Incident Forensics no está soportado. Debe utilizar la herramienta Gestión del sistema y licencias.

Antes de empezar

Debe instalar el software de QRadar Console en primer lugar. Para obtener más información, consulte el Capítulo 7, “Instalación de QRadar Console”, en la página 21.

Procedimiento

1. Inicie sesión en QRadar Console como administrador:

   `https://`*`Dirección_IP_QRadar`*

   El nombre de usuario predeterminado es `admin`. La contraseña es la contraseña de la cuenta de usuario root especificada durante la instalación.
2. Pulse la pestaña **Administración**.
3. En el panel **Configuración del sistema**, pulse **Gestión del sistema y licencias**.
4. En la tabla de hosts, pulse el host de QRadar Console y pulse > **Acciones de despliegue** > **Añadir host**.
5. Especifique la información para el dispositivo de QRadar Incident Forensics Processor y luego pulse **Añadir**.

   Restricción: Las propiedades **Cifrar host** y **Conversión de direcciones de red** no están soportadas.
6. En la barra de menús de la pestaña **Admin**, pulse **Desplegar cambios**.
7. Renueve el navegador web.

   La pestaña **Análisis forense** está ahora visible.

Qué hacer a continuación

Puede añadir un dispositivo de IBM Security QRadar Packet Capture a QRadar Incident Forensics Processor. Para obtener más información, consulte el apartado “Añadir dispositivos de captura de paquetes a hosts de QRadar Incident Forensics” en la página 30.

Eliminación de un host gestionado de QRadar Incident Forensics

Para cambiar los valores de configuración de red o si existe algún un problema para ver la pestaña **Análisis forense**, puede eliminar el host gestionado de QRadar Incident Forensics (IBM Security QRadar Incident Forensics Processor) del despliegue de QRadar. Si el host gestionado de QRadar Incident Forensics era responsable de la recuperación forense, los datos se pierden cuando se vuelve a añadir QRadar Incident Forensics Processor.

Si no elimina el host gestionado de QRadar Incident Forensics, sino que deja de responder temporalmente debido a una corte en la corriente o cualquier otro problema, los trabajos del host gestionado siguen planificados y se procesan cuando el host gestionado vuelve a estar en línea.

Restricción: El uso del Editor de despliegue para añadir o eliminar hosts gestionados de QRadar Incident Forensics no está soportado. Debe utilizar la herramienta Gestión del sistema y licencias.

Procedimiento

1. Inicie sesión en QRadar Console como administrador:

   `https://`*`Dirección_IP_QRadar`*

   El nombre de usuario predeterminado es `admin`. La contraseña es la contraseña de la cuenta de usuario root especificada durante la instalación.
2. Pulse la pestaña **Admin**.
3. En el panel **Configuración del sistema**, pulse **Gestión del sistema y licencias**.
4. En la tabla de hosts, pulse el host de QRadar Incident Forensics Processor que desea eliminar y pulse > **Acciones de despliegue** > **Eliminar host**.
5. En la barra de menús de la pestaña **Admin**, pulse **Desplegar cambios**.
6. Renueve el navegador web.

Capítulo 10. Conexiones entre dispositivos de captura de paquetes y QRadar Incident Forensics

Para recuperar datos de captura de paquetes, debe conectar uno o varios dispositivos de captura de paquetes a un host gestionado de IBM Security QRadar Incident Forensics o a un componente de QRadar Incident Forensics Standalone. Si no hay ningún dispositivo de captura de paquetes conectado, puede cargar manualmente los archivos de captura de paquetes en la interfaz de usuario o mediante FTP.

Sistema maestro de captura de paquetes

Dependiendo de los requisitos de la red y de captura de paquetes, puede conectar hasta cinco dispositivos de captura de paquetes a un dispositivo de QRadar Incident Forensics. Cuando se envía una recuperación, se envían trabajos independientes para cada dispositivo de captura de paquetes en cada dispositivo de QRadar Incident Forensics. Por ejemplo, si instala dos hosts gestionados de QRadar Incident Forensics y cada uno tiene dos paquetes de captura, se envían cuatro trabajos.

Los diagramas siguientes muestran que se pueden conectar varios dispositivos de captura de paquetes a un host gestionado de QRadar Incident Forensics (QRadar Incident Forensics Processor) o a dispositivos de QRadar Incident Forensics Standalone.

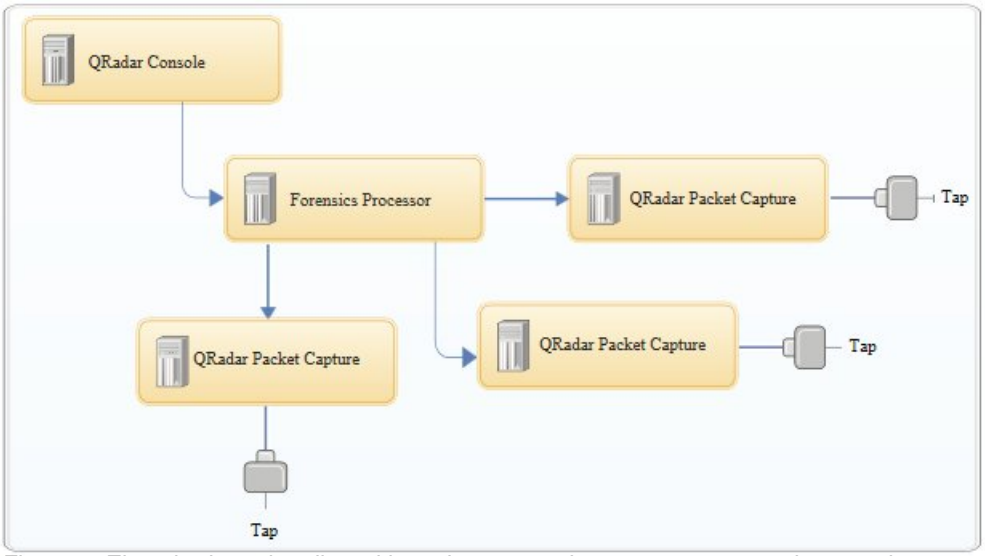


Figura 4. Ejemplo de varios dispositivos de captura de paquetes conectados a un host gestionado de QRadar Incident Forensics

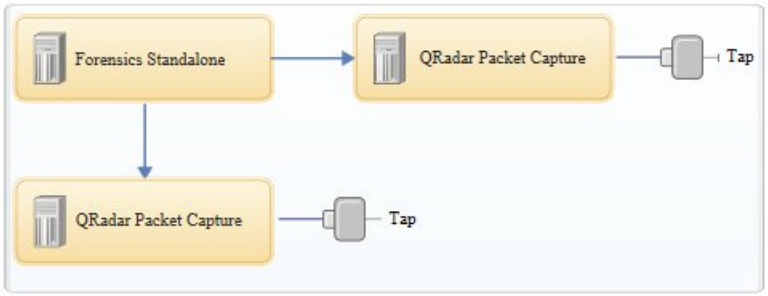
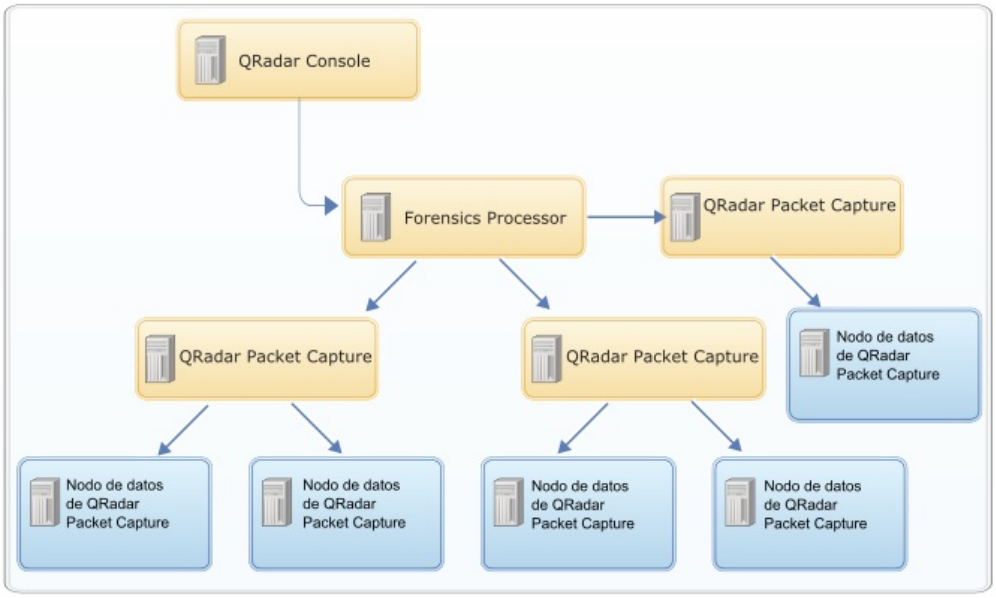


Figura 5. Ejemplo de varios dispositivos de captura de paquetes conectados a un host de QRadar Incident Forensics Standalone

Dispositivos de nodo de datos de QRadar Packet Capture

Para obtener capacidad de almacenamiento adicional, puede conectar hasta dos dispositivos de nodo de datos de QRadar Packet Capture a cada sistema maestro de QRadar Packet Capture. Cada dispositivo de nodo de datos PCAP proporciona 37 TB de almacenamiento adicional.



Después de conectar los dispositivos de nodo de datos de QRadar Packet Capture al sistema maestro, puede configurar el clúster en la interfaz de usuario de QRadar Packet Capture.

Para obtener más información acerca de las conexiones físicas del dispositivo maestro al dispositivo de nodo de datos de QRadar Packet Capture, consulte la publicación *QRadar Packet Capture Guía de consulta rápida*. Para obtener más información sobre la configuración del clúster de captura de paquetes, consulte la publicación *QRadar Packet Capture Guía del usuario*.

Instalación del software de QRadar Packet Capture en su dispositivo

Para garantizar una instalación correcta de IBM Security QRadar Packet Capture en un dispositivo propio, debe instalar el sistema operativo Red Hat Enterprise Linux y el software de QRadar Packet Capture. También debe asegurarse de que el dispositivo cumple los requisitos del sistema.

Importante: El sistema en el que se instala el software de QRadar Packet Capture debe estar dedicado a QRadar Packet Capture. No instale paquetes RPM que no estén aprobados por IBM. Las instalaciones de RPM no aprobadas pueden provocar errores de dependencias al actualizar, así como problemas de rendimiento en el despliegue. No utilice YUM para actualizar el sistema operativo ni instalar software no aprobado en QRadar Packet Capture.

Restricción: Las instalaciones del software en una máquina virtual no están soportadas.

Antes de empezar

Asegúrese de que el dispositivo cumple los requisitos del sistema siguientes:

Tabla 9. Requisitos del sistema para una instalación de software de QRadar Packet Capture

Especificación	Descripción
Procesadores	Procesadores Intel E5 Series V2 o V3 con 6 núcleos o más. Deben dar soporte a los estándares de Intel AES y AVX introducidos por Intel en 2011.
Memoria	16 GB
Controlador RAID de hardware y almacenamiento de captura y extracción	Controlador RAID 0 (banda) en un mínimo de 4 unidades de disco duro, donde cada unidad de disco duro tiene un rendimiento de al menos 7200 RPM y un mínimo de 1 TB por unidad, y donde la unidad es una unidad RAIDable de clase empresarial SATA o SAS
Unidad del sistema operativo	Unidad de disco duro de clase empresarial SATA o SAS de 500 GB y 7200 RPM como mínimo
Sistema operativo	Red Hat Enterprise Linux V6.5
Adaptador de servidor de puerto cuádruple	Adaptador Intel E1G44ET2BLK de puerto cuádruple Ethernet PCI Express http://ark.intel.com/products/49187/Intel-Gigabit-ET2-Quad-Port-Server-Adapter que dé soporte a un puerto de captura Intel 82576 Gigabit Ethernet Controller http://ark.intel.com/products/series/32261/Intel-82576-Gigabit-Ethernet-Controller

Procedimiento

1. Inserte el disco del sistema operativo Red Hat Enterprise Linux en el dispositivo y reinicie el dispositivo.
2. Siga las instrucciones del asistente de instalación para completar la instalación:
   a. Seleccione la opción **Dispositivos de almacenamiento básico**.
   b. Cuando configure el nombre de host, la propiedad **Hostname** puede incluir letras, números y guiones.
   c. En la pestaña **Valores de IPv4**, en la lista **Método**, seleccione **Manual**.

d. En la página Which type of installation would you like, seleccione **Use All Space** y después seleccione la partición más pequeña (partición de arranque) para instalar en ella el sistema operativo.
e. Seleccione solamente la opción **Base System** para la instalación.

3. Cuando la instalación haya finalizado, pulse **Rearrancar**.
4. Copie el archivo SFS de QRadar Packet Capture en el dispositivo.
5. Monte el archivo SFS de QRadar Packet Capture.
   a. Cree el directorio `/tmp/qpc_install` escribiendo el mandato siguiente:
      ```
      mkdir -p /tmp/qpc_install
      ```
   b. Monte el archivo SFS de QRadar Packet Capture escribiendo el mandato siguiente:
      ```
      mount -o loop -t squashfs <archivo_QRadar_Packet_Capture.sfs>
      /tmp/qpc_install
      ```
   c. Vaya al directorio `/tmp/qpc_install`.
      ```
      cd /tmp/qpc_install
      ```
6. Para ejecutar el script de instalación, escriba el mandato siguiente:
   ```
   sh installer.sh
   ```

Añadir dispositivos de captura de paquetes a hosts de QRadar Incident Forensics

Para proporcionar a los investigadores acceso a la información de captura de paquetes, puede conectar hasta cinco dispositivos de captura de paquetes a un host gestionado de IBM Security QRadar Incident Forensics o a un host de IBM Security QRadar Incident Forensics Standalone. Los dispositivos de captura de paquetes conectados procesan los archivos capturados para las recuperaciones forenses.

Si no hay ningún dispositivo de captura de paquetes conectado, puede cargar manualmente los archivos de captura de paquetes en la interfaz de usuario o mediante FTP.

Restricción: El uso del Editor de despliegue para añadir dispositivos de captura de paquetes no está soportado. Debe utilizar la herramienta Gestión del sistema y licencias.

Antes de empezar

Debe instalar y desplegar un host gestionado de QRadar Incident Forensics o instalar un host de QRadar Incident Forensics Standalone. Para obtener más información, consulte el Capítulo 8, “Instalación de QRadar Incident Forensics”, en la página 23 y el Capítulo 9, “Adición de un host gestionado de QRadar Incident Forensics aQRadar Console”, en la página 25.

El diagrama interactivo siguiente muestra los pasos principales del proceso de instalación correspondiente a las instalaciones distribuidas. El proceso de instalación es el mismo para los despliegues autónomos, pero sin desplegar un host gestionado.

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

Procedimiento

1. Inicie sesión en QRadar Console como administrador:

   `https://`*`Dirección_IP_QRadar`*

   El nombre de usuario predeterminado es `admin`. La contraseña es la contraseña de la cuenta de usuario root especificada durante la instalación.
2. Pulse la pestaña **Admin**.
3. En el panel **Configuración del sistema**, pulse **Gestión del sistema y licencias**.
4. En la tabla de hosts, seleccione QRadar Incident Forensics Processor (**Tipo de dispositivo** 6000) o el host de QRadar Incident Forensics Standalone (**Tipo de dispositivo** 6100) y pulse **Acciones de despliegue** > **Editar host gestionado**.
5. Pulse **Gestión de componentes**.
6. Para añadir dispositivos de captura de paquetes, pulse el icono de añadir (+) y especifique la información sobre el dispositivo.

   Consejo: El nombre de usuario predeterminado para el dispositivo QRadar Packet Capture es `continuum`.
7. Pulse **Guardar**.

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. El abastecimiento de este documento no confiere ninguna licencia sobre dichas patentes. Puede enviar consultas acerca de las licencias, por escrito, a:

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

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, Japan

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación vigente:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, QUE INCLUYEN, PERO NO SE LIMITAN A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, MERCANTIBILIDAD O ADECUACIÓN A UN FIN DETERMINADO. Algunos países no permiten la renuncia a garantías implícitas o explícitas en determinadas transacciones, por lo que puede que esta declaración no se le aplique.

Esta información podría contener inexactitudes técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; dichos cambios se incorporarán a las 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 de los materiales de este producto de IBM, por lo que la utilización de dichos sitios web será por cuenta y riesgo 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 licenciatarios de este programa que deseen obtener información sobre él con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido este) y (ii) el uso mutuo de información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Esta información puede estar disponible, sujeta a los términos y condiciones adecuados, incluido en algunos casos, el pago de una tasa.

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 contenidos en él se determinaron en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Algunas mediciones se pueden haber realizado en sistemas en nivel de desarrollo y no existen garantías de que estas mediciones sean las mismas en sistemas de disponibilidad general. Es más, es posible que la estimación de algunas medidas se haya realizado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a 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 relacionadas con las funciones de los productos que no son de IBM deberán dirigirse a los proveedores de estos productos.

Todas las sentencias relacionadas con la futura dirección o intención de IBM están sujetas a cambio o retirada sin previo aviso y sólo representan objetivos y metas.

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.

Este manual contiene ejemplos de datos e informes que se utilizan en operaciones comerciales diarias. Para ilustrarlos de la mejor manera posible, los ejemplos incluyen nombres de personas, compañías marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres y direcciones de empresas reales es pura coincidencia.

Si visualiza esta información en una copia software, es posible que no aparezcan las fotografías ni las ilustraciones en color.

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.

Los términos siguientes son marcas registradas de otras empresas:

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

Java y todas las marcas y logotipos basados en Java son marcas comerciales o marcas registradas de Oracle y/o de sus filiales.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

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

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

Consideraciones de 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 la oferta de software utiliza cookies para recopilar información de identificación personal, se establece a continuación información específica sobre el uso de cookies de esta oferta.

Dependiendo de las configuraciones desplegadas, esta oferta de software puede utilizar cookies de sesión que recopilan el ID de sesión de cada usuario a efectos de gestión y autenticación de sesiones. Estas cookies pueden inhabilitarse, pero si se inhabilitan también se eliminará la funcionalidad que 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