IBM Security QRadar SIEM
Versión 7.2.6

Guía de administración

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 369.

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.

© Copyright IBM Corporation 2012, 2015.

Contenido

© Copyright IBM Corp. 2012, 2015

Introducción a la administración de productos de QRadar

Los administradores utilizan IBM® Security QRadar SIEM para gestionar los paneles de control, los delitos, la actividad de registro, la actividad de la red, los activos y los informes.

Público al que se dirige

Esta guía está dirigida a todos los usuarios de QRadar SIEM responsables de investigar y gestionar la seguridad de la red. Esta guía presupone que tiene acceso a QRadar SIEM y que conoce la red corporativa y las tecnologías de red.

Documentación técnica

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

Para obtener información sobre el acceso a más documentación técnica 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?rs=0&uid=swg21612861).

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, y asume toda la responsabilidad en lo que

© Copyright IBM Corp. 2012, 2015

se refiere al cumplimiento de las leyes, normativas y políticas aplicables. El licenciatario declara que obtendrá o ha obtenido los consentimientos, permisos o licencias necesarios para permitir el uso legal de IBM Security QRadar.

Capítulo 1. Novedades para administradores en QRadar V7.2.6

IBM Security QRadar V7.2.6 incorpora las características y mejoras siguientes.

Desplegar y gestionar instancias multiarrendatario de QRadar

Como proveedor de servicios de seguridad gestionados (MSSP) o proveedor de servicios dentro de una organización de varias divisiones, ahora puede desplegar instancias multiarrendatario de IBM Security QRadar. Creando dominios y arrendatarios para cada cliente, puede gestionar cada uno de los ellos de forma independiente y asegurarse de que los datos sólo sean visibles para los usuarios de cada arrendatario. Más información...

Compartición y colaboración de contenido de seguridad de QRadar en el portal de IBM Security App Exchange

IBM Security App Exchange es un nuevo portal web para que los usuarios y business partners aprovechen la potencia y el conocimiento de la comunidad global de QRadar. Utilice IBM Security App Exchange para colaborar con otros y compartir contenido de seguridad en extensiones pequeñas y consumibles para ampliar las funciones existentes en la infraestructura de QRadar. Más información...

Ocultar datos confidenciales directamente desde QRadar

Utilice la nueva herramienta **Gestión de ofuscación de datos** para ocultar datos confidenciales directamente desde QRadar sin utilizar la línea de mandatos.

Las nuevas expresiones basadas en campos predefinidos facilitan el enmascaramiento de elementos de datos comunes tales como nombres de usuario, nombres de grupo, nombres de netBIOS y nombres de host. También puede crear expresiones regulares para ofuscar otros datos en los registro de sucesos y de flujo según sea necesario para las políticas de privacidad corporativas y gubernamentales. Más información...

Importar extensiones y contenido sin utilizar el script de gestión de contenido

Para ampliar las prestaciones de QRadar, utilice la nueva herramienta **Gestión de extensiones** para importar extensiones de seguridad en el despliegue de QRadar. La nueva interfaz facilita la adición e instalación de aplicaciones y contenido de seguridad directamente desde el nuevo IBM Security App Exchange en QRadar. Antes de instalar una extensión, puede revisar el contenido y especificar si el contenido existente debe sobrescribirse o conservarse. Más información...

Visualización de despliegue

Puede abrir una visualización del despliegue en el nivel de host desde la lista **Acciones de despliegue**. En la visualización puede ver la relación entre los hosts y modificar la ubicación relativa de los hosts sin modificar la configuración del

© Copyright IBM Corp. 2012, 2015

despliegue actual. También puede exportar el gráfico en formato PNG o VDX. Más información...

Varias plantillas de notificación de correo electrónico

Ahora puede seleccionar entre una lista de plantillas de correo electrónico de respuesta disponibles al configurar reglas. Ahora puede crear plantillas diferentes para usuarios distintos, plantillas diferentes para tipos de delitos diferentes, etc. Para obtener más información sobre la configuración de reglas, consulte la *Guía del usuario de IBM Security QRadar*. Más información...

Sucesos de caducidad de datos de referencia

Los elementos de Correlaciones de datos de referencia, Correlación de conjuntos, Correlación de correlaciones, Tabla de referencia y Conjuntos de referencia desencadenan ahora un suceso de **Caducidad de datos de referencia** cuando caducan. El suceso de **Caducidad de datos de referencia** contiene el nombre de la recopilación y el elemento que ha caducado.

Puede utilizar la característica, por ejemplo, para hacer un seguimiento de aspectos tales como cuentas de usuario caducadas en la red. Más información...

Scripts de acción personalizada

Puede conectar scripts a reglas personalizadas para realizar acciones personalizadas en respuesta a los sucesos de red. Por ejemplo, puede escribir un script para crear una regla de cortafuegos que bloquee una dirección IP de origen de la red en respuesta a una regla que se desencadena mediante un número definido de intentos de inicio de sesión fallidos. Puede utilizar la ventana Acción personalizada de la pestaña **Admin** para gestionar los scripts de acción personalizada. Más información...

Mayor seguridad para los valores del sistema

Configure los valores del sistema en una interfaz nueva y más segura. Acceda a la nueva ventana **Ver y gestionar el sistema** a través de HTTPS para configurar cortafuegos, interfaces de red y servidores de correo electrónico.

Nota: Para mejorar la seguridad, los cambios de contraseña y hora del sistema se configuran en la consola de QRadar. Más información...

Tiempo de espera de inactividad

La propiedad **Tiempo de espera de inactividad** controla la cantidad máxima de tiempo que una sesión inactiva permanece viva. Si transcurre un tiempo superior al intervalo de tiempo especificado sin actividad, la sesión finaliza y el usuario se desconecta. De forma predeterminada, el intervalo de tiempo máximo es de 30 minutos. Más información...

Capítulo 2. Visión general de la administración de QRadar

Los administradores utilizan la pestaña **Admin** en IBM Security QRadar para gestionar paneles de control, actividad de registro, delitos, actividad de red, activos (si están disponibles) e informes.

Esta visión general incluye información general sobre el acceso a la interfaz de usuario y la pestaña **Admin** y su uso.

Prestaciones de su producto de inteligencia y seguridad

La documentación del producto IBM Security QRadar describe funciones tales como delitos, flujos, activos y correlación histórica, que pueden no estar disponibles en todos los productos de QRadar. Dependiendo del producto que esté utilizando, algunas de las características documentadas podrían no estar disponibles en su despliegue. Revise las prestaciones de cada producto como guía para obtener la información que necesita.

IBM Security QRadar SIEM incluye la gama completa de prestaciones de inteligencia y seguridad para los despliegues locales. QRadar SIEM consolida datos de sucesos de origen de registro de aplicaciones y puntos finales de dispositivo distribuidos por la red, y realiza actividades de normalización y correlación inmediata en los datos en bruto para distinguir hebras reales de falsos positivos.

Utilice IBM Security Intelligence on Cloud para recopilar, analizar, archivar y almacenar grandes volúmenes de registros de sucesos de red y de seguridad en un entorno alojado. Analice los datos para proporcionar visibilidad en el desarrollo de hebras, y cumpla los requisitos de creación de informes y supervisión de la conformidad al tiempo que reduce el coste total de propiedad.

Utilice IBM Security QRadar Log Manager para recopilar, analizar, archivar y almacenar grandes volúmenes de registros de sucesos de red y de seguridad. QRadar Log Manager analiza datos para proporcionar visibilidad en el desarrollo de hebras, y puede ayudar al cumplimiento de los requisitos de creación de informes y supervisión.

Al buscar ayuda, utilice la tabla siguiente, que muestra las prestaciones de los productos:

Tabla 1. Comparación de prestaciones de QRadar

Prestación	QRadar SIEM	IBM Security Intelligence on Cloud	IBM Security QRadar Log Manager
Da soporte a despliegues alojados	No	Sí	No
Paneles de control personalizables	Sí	Sí	Sí
Motor de reglas personalizadas	Sí	Sí	Sí
Gestionar sucesos de red y seguridad	Sí	Sí	Sí
Gestionar registros de aplicación y host	Sí	Sí	Sí
Alertas basadas en umbral	Sí	Sí	Sí
Plantillas de conformidad	Sí	Sí	Sí

© Copyright IBM Corp. 2012, 2015

Tabla 1. Comparación de prestaciones de QRadar (continuación)

Prestación	QRadar SIEM	IBM Security Intelligence on Cloud	IBM Security QRadar Log Manager
Archivado de datos	Sí	Sí	Sí
Integración de canales de información de reputación de IP de IBM Security X-Force Threat Intelligence	Sí	Sí	Sí
Despliegues autónomos de WinCollect	Sí	Sí	Sí
Despliegues gestionados de WinCollect	Sí	No	Sí
Integración de QRadar Vulnerability Manager	Sí	No	Sí
Supervisión de la actividad de red	Sí	No	No
Perfilado de activos	Sí	Sí	No [1]
Gestión de delitos	Sí	Sí	No
Captura y análisis de flujo de red	Sí	No	No
Correlación histórica	Sí	Sí	No
Integración de QRadar Risk Manager	Sí	No	No
Integración de QRadar Incident Forensics	Sí	No	No
[1] QRadar Log Manager solo hace un seguimiento de datos de activos si QRadar Vulnerability Manager está instalado.			

Navegadores web soportados

Para que las características de los productos de IBM Security QRadar funcionen correctamente, debe utilizar un navegador web soportado.

Cuando accede al sistema de QRadar, se le pide el nombre de usuario y la contraseña. El nombre de usuario y la contraseña debe haberlos configurado el administrador de antemano.

En la tabla siguiente se enumeran las versiones soportadas de los navegadores web.

Tabla 2. 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 de navegador habilitada.	10.0
Microsoft Internet Explorer de 64 bits con la modalidad de Microsoft Edge habilitada.	11.0
Google Chrome	Versión 46

Visión general de la pestaña Admin

La pestaña **Admin** proporciona varias opciones de pestaña y de menú que permiten configurar QRadar.

Debe tener privilegios administrativos para acceder a las funciones administrativas. Para acceder a las funciones administrativas, pulse la pestaña **Admin** en la interfaz de usuario.

La pestaña **Admin** también incluye las siguientes opciones de menú:

Tabla 3. Opciones de menú de la pestaña Admin

Opción de menú	Descripción
Editor de despliegue	Abre la ventana Editor de despliegue. Para obtener más información, consulte el Capítulo 11, "Editor de despliegue", en la página 137.
Desplegar cambios	Despliega los cambios de configuración de la sesión actual en su despliegue. Para obtener más información, consulte el apartado "Despliegue de cambios".
Avanzado	El menú **Avanzado** proporciona las opciones siguientes: **Limpiar modelo SIM**: Restablece el módulo SIM. Consulte el apartado "Restablecimiento de SIM" en la página 7. **Desplegar configuración completa**: Despliega todos los cambios de configuración. Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.Para obtener más información, consulte el apartado "Despliegue de cambios".

Despliegue de cambios

Puede actualizar los valores de configuración en la pestaña **Admin**. Los cambios se guardan en un área intermedia donde se almacenan hasta que despliegue manualmente los cambios.

Acerca de esta tarea

Cada vez que acceda a la pestaña **Admin** y cada vez que cierre una ventana en la pestaña **Admin**, un banner en la parte superior de la pestaña **Admin** mostrará el siguiente mensaje: `Buscando cambios no desplegados`. Si se encuentran cambios no desplegados, el banner se actualiza y proporciona información sobre los cambios no desplegados.

Si la lista de cambios no desplegados es larga, se proporciona una barra de desplazamiento. Desplace el contenido de la lista.

El mensaje del banner también indica qué tipo de cambio de despliegue se debe hacer. Elija una de las dos opciones siguientes:

- **Desplegar cambios**: Pulse el icono **Desplegar cambios** de la barra de herramientas de la pestaña **Admin** para desplegar todos los cambios de configuración de la sesión actual en su despliegue.
- **Desplegar configuración completa**: Seleccione **Avanzado** > **Desplegar configuración completa** en el menú de la pestaña **Admin** para desplegar todos los valores de configuración en su despliegue. A continuación todos los cambios desplegados se aplican en el despliegue.

  Importante: Al pulsar **Desplegar configuración completa**, QRadar reinicia todos los servicios, lo que provoca una interrupción en la recopilación de datos hasta que se completa el despliegue.

Después de desplegar los cambios, el banner borra la lista de cambios no desplegados y comprueba el área de transferencia de nuevo para ver si hay nuevos cambios no desplegados. Si no hay ninguno, se visualiza el mensaje siguiente: `No hay ningún cambio por desplegar.`

Procedimiento

1. Pulse **Ver detalles**.
2. Seleccione una de las opciones siguientes:
   a. Para expandir un grupo para visualizar todos los elementos, pulse el signo más (+) situado junto al texto. Cuando haya acabado, puede pulsar el signo menos (-).
   b. Para expandir todos los grupos, pulse **Expandir todo**. Cuando haya acabado, puede pulsar **Contraer todo**.
   c. Pulse **Ocultar detalles** para ocultar los detalles de la vista de nuevo.
3. Realice la tarea sugerida:
   a. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.
   b. En el menú de la pestaña **Admin**, pulse **Avanzado** > **Desplegar configuración completa**.

      Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Actualización de los detalles de usuario

Puede acceder a los detalles del usuario administrativo a través de la interfaz de usuario principal.

Procedimiento

1. Pulse **Preferencias**.
2. Opcional: Actualice los detalles de usuario configurables.

Opción	Descripción
Parámetro	Descripción
Correo electrónico	Escriba una dirección de correo electrónico nueva.
Contraseña	Escriba una contraseña nueva.
Confirmar contraseña	Vuelva a escribir la nueva contraseña.

Opción	Descripción
Habilitar notificaciones emergentes	Los mensajes de notificación emergentes del sistema se muestran en la esquina inferior derecha de la interfaz de usuario. Para inhabilitar las notificaciones emergentes, desmarque esta casilla de verificación. Para obtener más información sobre las notificaciones emergentes, consulte la guía del usuario de su producto.

3. Pulse **Guardar**.

Restablecimiento de SIM

Utilice la pestaña **Admin** para restablecer el módulo SIM. Ahora puede eliminar de la base de datos y del disco toda la información de delitos, dirección IP de origen y dirección IP de destino.

Acerca de esta tarea

Esta opción es útil después de ajustar el despliegue para evitar recibir información adicional de falsos positivos.

El proceso de restablecimiento de SIM puede tardar varios minutos, en función de la cantidad de datos del sistema. Si intenta ir a otras áreas de la interfaz de usuario de QRadar durante el proceso de restablecimiento de SIM, se visualiza un mensaje de error.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú **Avanzado**, seleccione **Limpiar modelo SIM**.
3. Lea la información en la ventana Restablecer módulo de datos SIM.
4. Seleccione una de las siguientes opciones.

Opción	Descripción
Limpieza parcial	Cierra todos los delitos de la base de datos. Si selecciona la opción **Limpieza parcial**, podrá seleccionar también la casilla de verificación **Desactivar todos los delitos**.
Limpieza total	Purga todos los datos de SIM actuales e históricos, incluyendo delitos, direcciones IP de origen y direcciones IP de destino.

5. Si desea continuar, seleccione la casilla de verificación **¿Está seguro de que desea restablecer el modelo de datos?**.
6. Pulse **Continuar**.
7. Cuando haya finalizado el proceso de restablecimiento de SIM, pulse **Cerrar**.
8. Cuando haya finalizado el proceso de restablecimiento de SIM, restablezca el navegador.

Supervisión de sistemas con SNMP

Supervisión de dispositivos a través del sondeo de SNMP.

IBM Security QRadar utiliza el agente de Net-SNMP, que da soporte a diversas MIB de supervisión de recursos del sistema. Se pueden sondear con soluciones de Gestión de red para la supervisión y la generación de alertas de los recursos del sistema. Para obtener más información sobre Net-SNMP, consulte la documentación de Net-SNMP.

Gestión de vistas de datos agregados

Un gran volumen de agregación de datos puede degradar el rendimiento del sistema. Para mejorar el rendimiento del sistema, pueden inhabilitarse, habilitarse o suprimirse vistas de datos agregados. Las gráficas de series temporales, las gráficas de informe y las reglas de anomalía utilizan vistas de datos agregados.

Acerca de esta tarea

Los elementos de la lista desplegable **Visualizar** reordenan los datos visualizados.

La vista de datos agregados debe generar datos para las reglas de ADE, los gráficos de series temporales y los informes.

Inhabilite o suprima vistas si se alcanza el número máximo de vistas.

En la columna **ID de datos agregados** pueden aparecer vistas duplicadas porque una vista de datos agregados puede incluir varias búsquedas.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión de datos agregados**.
4. Para filtrar la lista de vistas de datos agregados, seleccione una de las siguientes opciones:
   - Seleccione una opción de una de las listas siguientes: **Vista**, **Base de datos**, **Mostrar** o **Visualizar**.
   - Escriba un ID de datos agregados, un nombre de informe, un nombre de gráfica o nombre de búsqueda guardada en el campo de búsqueda.
5. Para gestionar una vista de datos agregados, seleccione la vista y luego la acción adecuada en la barra de herramientas.
   - Si se selecciona **Inhabilitar vista** o **Suprimir vista**, una ventana mostrará las dependencias de contenido de la vista de datos agregados. Una vez inhabilitada o suprimida la vista de datos agregados, los componentes dependientes ya no utilizarán datos agregados.
   - Si habilita una vista de datos agregados inhabilitada, los datos agregados de la vista suprimida se restauran.

Tabla 4. Descripciones de las columnas de la vista Gestión de datos agregados

Columna	Descripción
ID de datos agregados	Identificador de los datos agregados
Nombre de búsqueda guardada	Nombre definido para la búsqueda guardada

Tabla 4. Descripciones de las columnas de la vista Gestión de datos agregados (continuación)

Columna	Descripción
Nombre de columna	Identificador de columna
Veces que se ha buscado	Recuento de búsqueda
Datos escritos	Tamaño de los datos escritos
Nombre de base de datos	Base de datos en la que se ha escrito el archivo
Hora de la última modificación	Indicación de fecha y hora de la última modificación de los datos
Recuento exclusivo habilitado	True o False; los resultados de búsqueda mostrarán recuentos de sucesos y flujos exclusivos en lugar de recuentos promedio a lo largo del tiempo.

API RESTful

Utilice la interfaz de programación de aplicaciones (API) Representational State Transfer (REST) para realizar consultas HTTPS e integrar IBM Security QRadar con otras soluciones.

Acceso y permisos del rol de usuario

Debe tener permisos del rol de usuario administrativo en QRadar para acceder y usar las API RESTful. .

Acceso a la interfaz de usuario de la documentación técnica de la API REST

La interfaz de usuario de API proporciona descripciones y funciones para las interfaces de la API REST siguientes:

Tabla 5. Interfaces de la API REST

API REST	Descripción
`/api/ariel`	Consultar bases de datos, búsquedas, ID de búsqueda y resultados de búsqueda.
`/api/asset_model`	Devuelve una lista de todos los activos del modelo. También puede listar todos los tipos de propiedad de activo disponibles y búsquedas guardadas, así como actualizar un activo.
`/api/auth`	Cerrar e invalidar la sesión actual.
`/api/help`	Devuelve una lista de funciones de la API.
`/api/siem`	Devuelve una lista de todos los delitos.
`/api/qvm`	Revisar y gestionar los datos de QRadar Vulnerability Manager.
`/api/reference_data`	Ver y gestionar las recopilaciones de datos de referencia.
`/api/qvm`	Recupera activos, vulnerabilidades, redes, servicios abiertos y filtros. También puede crear o actualizar tíquets de remediación.

Tabla 5. Interfaces de la API REST (continuación)

API REST	Descripción
/api/scanner	Ver, crear o iniciar una exploración remota que está relacionada con un perfil de exploración.

La interfaz de documentación técnica de la API REST proporciona una infraestructura que puede utilizar para recopilar el código que necesita para implementar las funciones de QRadar en otros productos.

1. Especifique el URL siguiente en el navegador para acceder a la interfaz de la documentación técnica: `https://`*`dirección_IP_consola`*`/api_doc`.
2. Pulse la cabecera correspondiente a la API a la que desea acceder; por ejemplo, **/ariel**.
3. Pulse la subcabecera para el punto final al que desea acceder, por ejemplo **/databases**.
4. Pulse la subcabecera Experimental o Provisional.

   Nota:

   Los puntos finales de la API están anotados como *experimentales* o como *estables*.

   Experimental
   Indica que el punto final de la API podría no estar totalmente probado y podría cambiar o eliminarse en el futuro sin previo aviso.

   Estable
   Indica que el punto final de la API está totalmente probado y soportado.
5. Pulse **Try it out** para recibir respuestas HTTPS con el formato correcto.
6. Revise y recopile la información que necesita implementar en la solución de terceros.

Foro de API de QRadar y ejemplos de código

El foro de API proporciona más información acerca de la API REST, que incluye las respuestas a las preguntas más frecuentes y ejemplos de código con anotaciones que puede utilizar en un entorno de prueba. Para obtener más información, consulte el foro de API (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca).

Acciones personalizadas

Puede conectar scripts a reglas personalizadas para realizar acciones personalizadas en respuesta a los sucesos de red. Utilice la ventana Acción personalizada para gestionar los scripts de acción personalizada.

Las acciones personalizadas le ofrecen la posibilidad de seleccionar o definir el valor que se pasa al script y la acción resultante.

Por ejemplo, puede escribir un script para crear una regla de cortafuegos que bloquee una dirección IP de origen de la red en respuesta a una regla que se desencadena mediante un número definido de intentos de inicio de sesión fallidos.

Los ejemplos siguientes son acciones personalizadas resultantes de pasar valores a un script:

- Bloquear usuarios y dominios.
- Iniciar flujos de trabajo y actualizaciones en sistemas externos.
- Actualizar servidores TAXI con una representación STIX de una amenaza.

Nota: esta característica funciona mejor con sucesos de reglas personalizadas de bajo volumen y con reglas personalizadas con un valor limitador de respuesta bajo.

Pulse **Añadir** en la barra de herramientas de la ventana Acción personalizada para abrir el diálogo **Definir acción personalizada**, donde puede cargar scripts que definan acciones personalizadas. Las versiones de lenguajes de programación soportadas por el producto se indican en la lista **Intérprete**.

Nota: Para poder garantizar la seguridad del despliegue, QRadar no da soporte a la gama completa de funciones de script suministradas por los lenguajes Python, Perl o Bash.

Puede definir dos tipos de parámetros que se pasan al script que se carga:

Tabla 6. Parámetros de acción personalizada

Parámetro	Descripción
Propiedad fija	Las propiedades fijas son valores que se pasan al script de acción personalizada. Estas propiedades no se basan en los sucesos o en el flujo en sí mismos, sino que cubren otros valores definidos en los que puede utilizar el script para actuar sobre ellos. Por ejemplo, las propiedades fijas *username* y *password* para un sistema de terceros se pasan a un script que provoca el envío de una alerta SMS u otra acción definida. Puede cifrar propiedades fijas, como por ejemplo contraseñas, marcando el recuadro **Valor de cifrado**.
Propiedad de suceso de red	Las propiedades de suceso de red son propiedades Ariel dinámicas generadas por sucesos. Seleccione una propiedad de suceso de red para pasarla al script en la lista **Propiedad**. Por ejemplo, la propiedad de suceso de red *sourceip* proporciona un parámetro que coincide con la dirección IP de origen del suceso desencadenado. Para obtener más información sobre propiedades de Ariel, consulte *IBM Security QRadar Ariel Query Language Guide*.

Los parámetros se pasan al script por el orden por el que los añade en el diálogo **Definir una acción personalizada**.

Probar la acción personalizada

Puede probar si el script se ejecuta satisfactoriamente antes de asociarlo con una regla. Seleccione una acción personalizada y pulse **Ejecución de prueba** > **Ejecutar** para probar el script. El diálogo Ejecución de acción personalizada de prueba devuelve el resultado de la prueba y cualquier salida generada por el script.

Los scripts de acción personalizada se ejecutan dentro de un entorno de cajón de arena en los hosts gestionados de QRadar. Si tiene que grabar en disco desde un script de acción personalizada, debe utilizar el directorio siguiente: `/home/customactionuser`. Los scripts de acción personalizada se ejecutan en el host gestionado que ejecuta el procesador de sucesos que ha desencadenado la regla.

Después de configurar y probar la acción personalizada, utilice el **Asistente de reglas** para crear una regla de suceso nueva y asociar la acción personalizada con ella.

Para obtener más información sobre reglas de suceso, consulte *IBM Security QRadar SIEM Users Guide*.

Capítulo 3. Gestión de usuarios

Los administradores utilizan la función **Gestión de usuarios** de la pestaña **Admin** en IBM Security QRadar para configurar y gestionar cuentas de usuario.

Al configurar inicialmente QRadar, debe crear cuentas de usuario para todos los usuarios que necesitan acceso a QRadar. Después de la configuración inicial, puede editar las cuentas de usuario para asegurarse de que la información de usuario es actual. También puede añadir y suprimir cuentas de usuario, según sea necesario.

Visión general de la gestión de cuentas de usuario

Una cuenta de usuario define el nombre de usuario, la contraseña predeterminada y la dirección de correo electrónico de un usuario.

Asigne los elementos siguientes para cada nueva cuenta de usuario que cree:

- **Rol de usuario**: Determina los privilegios que se otorgan al usuario para acceder a las funciones y la información de QRadar. Hay dos roles de usuario predeterminados definidos: Admin y Todos. Antes de añadir cuentas de usuario, debe crear más roles de usuario para cumplir los requisitos de permisos específicos de los usuarios.
- **Perfil de seguridad**: Determina las redes, los orígenes de registro y los dominios a los que se otorga acceso al usuario. QRadar contiene un perfil de seguridad predeterminado para los usuarios administrativos. El perfil de seguridad Admin incluye acceso a todas las redes, a todos los orígenes de registro y a todos los dominios. Antes de añadir cuentas de usuario, debe crear más perfiles de seguridad para cumplir los requisitos de acceso específicos de los usuarios.

Gestión de roles

Con la ventana Roles de usuario puede crear roles de usuario y gestionarlos.

Creación de un rol de usuario

Utilice esta tarea para crear los roles de usuario que el despliegue necesita.

Acerca de esta tarea

De forma predeterminada, el sistema proporciona un rol de usuario administrativo predeterminado, que da acceso a todas las áreas de QRadar SIEM. Los usuarios que tienen asignado un rol de usuario administrativo no pueden editar su propia cuenta. Esta restricción se aplica al rol de usuario Admin predeterminado. Otro usuario administrativo debe realizar los cambios en la cuenta.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Roles de usuario**.
4. En la barra de herramientas, pulse **Nuevo**.
5. Configure los siguientes parámetros:

© Copyright IBM Corp. 2012, 2015

a. En el campo **Nombre del rol de usuario**, escriba el nombre exclusivo de este rol de usuario.
b. Seleccione los permisos que desee asignar a este rol de usuario. Consulte el apartado "Acceso y permisos de los roles de usuario" en la página 32.

6. En el área **Paneles de control**, seleccione los paneles de control a los que desea que acceda el rol de usuario y pulse **Añadir**.

   Nota:

   a. Un panel de control no muestra información alguna si el rol de usuario no tiene permiso para ver los datos del panel de control.
   b. Si un usuario modifica los paneles de control visualizados, en el próximo inicio de sesión aparecen los paneles de control definidos correspondientes al rol de usuario.

7. Pulse **Guardar**.
8. Cierre la ventana Gestión de roles de usuario.
9. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Edición de un rol de usuario

Puede editar un rol existente para cambiar los permisos que están asignados al rol.

Acerca de esta tarea

Para localizar rápidamente el rol de usuario que desea editar en la ventana Gestión de roles de usuario, puede escribir un nombre de rol en el cuadro de texto **Tipo por filtrar**. Este cuadro se halla encima del panel izquierdo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Roles de usuario**.
4. En el panel izquierdo de la ventana Gestión de roles de usuario, seleccione el rol de usuario que desea editar.
5. En el panel derecho, actualice los permisos según convenga. Consulte el apartado "Acceso y permisos de los roles de usuario" en la página 32.
6. Modifique las opciones de **Paneles de control** correspondientes al rol de usuario según convenga.
7. Pulse **Guardar**.
8. Cierre la ventana Gestión de roles de usuario.
9. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Supresión de un rol de usuario

Si un rol de usuario ya no es necesario, puede suprimirlo.

Acerca de esta tarea

Si hay cuentas de usuario asignadas al rol de usuario que desea suprimir, debe volver a asignar las cuentas de usuario a otro rol de usuario. El sistema detecta automáticamente esta condición y le solicitará que actualice las cuentas de usuario.

Puede localizar rápidamente el rol de usuario que desea suprimir en la ventana Gestión de roles de usuario. Escriba un nombre de rol en el cuadro de texto **Tipo por filtrar**, que se encuentra encima del panel izquierdo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Roles de usuario**.
4. En el panel izquierdo de la ventana Gestión de roles de usuario, seleccione el rol que desea suprimir.
5. En la barra de herramientas, pulse **Suprimir**.
6. Pulse **Aceptar**.
   - Si hay cuentas de usuario asignadas a este rol de usuario, se abre la ventana Hay usuarios asignados a este rol de usuario. Vaya al paso 7.
   - Si no hay cuentas de usuario asignadas a este rol de usuario, el rol de usuario se suprime satisfactoriamente. Vaya al paso 8.
7. Vuelva a asignar las cuentas de usuario de la lista a otro rol de usuario:
   a. En el cuadro de lista **Rol de usuario para asignar**, seleccione un rol de usuario.
   b. Pulse **Confirmar**.
8. Cierre la ventana Gestión de roles de usuario.
9. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Gestión de perfiles de seguridad

Los perfiles de seguridad definen a qué redes, orígenes de registro y dominios puede acceder un usuario.

Con la ventana Gestión de perfiles de seguridad puede ver, crear, actualizar y suprimir perfiles de seguridad.

Prioridades de los permisos

En este tema se define cada una de las opciones de prioridad de permiso.

La prioridad de permiso determina qué componentes del perfil de seguridad deben tenerse en cuenta cuando el sistema muestra sucesos en la pestaña **Actividad de registro** y flujos en la pestaña **Actividad de red**.

Asegúrese de que comprende las restricciones siguientes:

- **Ninguna restricción**: Esta opción no aplica restricciones sobre qué sucesos se visualizan en la pestaña **Actividad de registro** y qué flujos se visualizan en la pestaña **Actividad de red**.
- **Solo red**: Esta opción hace que el usuario pueda ver solamente los sucesos y los flujos que están asociados con las redes especificadas en este perfil de seguridad.
- **Solo orígenes de registro**: Esta opción hace que el usuario pueda ver solamente los sucesos que están asociados con los orígenes de registro especificados en este perfil de seguridad.
- **Redes y orígenes de registro**: Esta opción hace que el usuario pueda ver solamente los sucesos y flujos que están asociados con los orígenes de registro y las redes especificados en este perfil de seguridad.

Por ejemplo, si el perfil de seguridad permite el acceso a sucesos de un origen de registro pero la red de destino está restringida, el suceso no se visualiza en la pestaña **Actividad de registro**. El suceso debe cumplir ambos requisitos.

- **Redes u orígenes de registro**: Esta opción permite al usuario ver los sucesos y flujos que están asociados con los orígenes de registro o las redes especificados en este perfil de seguridad.

Por ejemplo, si un perfil de seguridad permite el acceso a sucesos de un origen de registro pero la red de destino está restringida, el suceso se visualiza en la pestaña **Actividad de registro** si la prioridad de permiso está establecida en **Redes u orígenes de registro**. Si la prioridad de permiso está establecida en **Redes y orígenes de registro**, el suceso no se visualiza en la pestaña **Actividad de registro** .

Los perfiles de seguridad se deben actualizar con un dominio asociado. Las restricciones de nivel de dominio no se aplican hasta que se actualizan los perfiles de seguridad y se despliegan los cambios.

Creación de un perfil de seguridad

Para añadir cuentas de usuario, primero debe crear perfiles de seguridad para cumplir los requisitos de acceso específicos de los usuarios.

Acerca de esta tarea

QRadar SIEM contiene un perfil de seguridad predeterminado para los usuarios administrativos. El perfil de seguridad Admin incluye acceso a todas las redes, a todos los orígenes de registro y a todos los dominios.

Para seleccionar varios elementos en la ventana Gestión de perfiles de seguridad, mantenga pulsada la tecla Control mientras selecciona cada red o grupo de redes que desea añadir.

Si después de añadir redes, orígenes de registro o dominios quiere eliminar uno o varios de los elementos que ha añadido antes de guardar la configuración, puede seleccionar el elemento y pulsar el icono **Eliminar (<)**. Para eliminar todos los elementos, pulse **Eliminar todo**.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Perfiles de seguridad**.
4. En la barra de herramientas de la ventana Gestión de perfiles de seguridad, pulse **Nuevo**.
5. Configure los siguientes parámetros:
   a. En el campo **Nombre del perfil de seguridad**, escriba un nombre exclusivo para el perfil de seguridad. El nombre del perfil de seguridad debe cumplir los requisitos siguientes: 3 caracteres como mínimo y 30 caracteres como máximo.
   b. `Opcional` Escriba una descripción del perfil de seguridad. El número máximo de caracteres es de 255.
6. Pulse la pestaña **Prioridad de permiso**.

7. En el panel Configuración de prioridades de permiso, seleccione una opción de prioridad de permiso. Consulte el apartado “Prioridades de los permisos” en la página 15.
8. Configure las redes que desee asignar al perfil de seguridad:
   a. Pulse la pestaña **Redes**.
   b. En el árbol de navegación del panel izquierdo de la pestaña **Redes**, seleccione la red a la que desea que este perfil de seguridad tenga acceso.
   c. Pulse el icono **Añadir (>)** para añadir la red al panel Redes asignadas.
   d. Repita este procedimiento por cada red que desee añadir.
9. Configure los orígenes de registro que desee asignar al perfil de seguridad:
   a. Pulse la pestaña **Orígenes de registro**.
   b. En el árbol de navegación del panel izquierdo, seleccione el grupo de orígenes de registro o el origen de registro al que desea que este perfil de seguridad tenga acceso.
   c. Pulse el icono **Añadir (>)** para añadir el origen de registro al panel Orígenes de registro asignados.
   d. Repita este procedimiento por cada origen de registro que desee añadir.
10. Configure los dominios que desee asignar al perfil de seguridad:
    a. Pulse la pestaña **Dominios**.
    b. En el árbol de navegación del panel izquierdo, seleccione el dominio al que desea que este perfil de seguridad tenga acceso.
    c. Pulse el icono **Añadir (>)** para añadir el dominio red al panel Dominios asignados.
    d. Repita este procedimiento para cada dominio que desee añadir.
11. Pulse **Guardar**.
12. Cierre la ventana Gestión de perfiles de seguridad.
13. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Edición de un perfil de seguridad

Puede editar un perfil de seguridad existente para actualizar las redes y los orígenes de registro a los que puede acceder un usuario y la prioridad de permiso.

Acerca de esta tarea

Para localizar rápidamente el perfil de seguridad que desea editar en la ventana Gestión de perfiles de seguridad, escriba el nombre del perfil de seguridad en el cuadro de texto **Tipo por filtrar**. Se halla encima del panel izquierdo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Perfiles de seguridad**.
4. En el panel izquierdo, seleccione el perfil de seguridad que desee editar.
5. En la barra de herramientas, pulse **Editar**.
6. Actualice los parámetros como sea necesario.
7. Pulse **Guardar**.
8. Si se abre la ventana El perfil de seguridad tiene datos de serie temporal, seleccione una de las opciones siguientes:

Opción	Descripción
Conservar datos antiguos y guardar	Seleccione esta opción para conservar los datos de serie temporal acumulados anteriormente. Si elige esta opción, pueden producirse errores cuando los usuarios asociados a este perfil de seguridad vean los gráficos de serie temporal.
Ocultar datos antiguos y guardar	Seleccione esta opción para ocultar los datos de serie temporal. Si elige esta opción, la acumulación de datos de serie temporal se reinicia después de desplegar los cambios de configuración.

9. Cierre la ventana Gestión de perfiles de seguridad.
10. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Duplicación de un perfil de seguridad

Si desea crear un nuevo perfil de seguridad que sea bastante parecido a un perfil de seguridad ya existente, puede duplicar el perfil de seguridad existente y, a continuación, modificar los parámetros.

Acerca de esta tarea

Para localizar rápidamente el perfil de seguridad que desea duplicar en la ventana Gestión de perfiles de seguridad, puede escribir el nombre del perfil de seguridad en el cuadro de texto **Tipo por filtrar**, que se halla encima del panel izquierdo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema Gestión de usuarios**.
3. Pulse el icono **Perfiles de seguridad**.
4. En el panel izquierdo, seleccione el perfil de seguridad que desee duplicar.
5. En la barra de herramientas, pulse **Duplicar**.
6. En la ventana de confirmación, escriba un nombre exclusivo para el perfil de seguridad duplicado.
7. Pulse **Aceptar**.
8. Actualice los parámetros como sea necesario.
9. Cierre la ventana Gestión de perfiles de seguridad.
10. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Supresión de un perfil de seguridad

Si un perfil de seguridad ya no es necesario, puede suprimirlo.

Acerca de esta tarea

Si hay cuentas de usuario asignadas a los perfiles de seguridad que desea suprimir, debe volver a asignar las cuentas de usuario a otro perfil de seguridad. QRadar SIEM detecta automáticamente esta condición y le solicitará que actualice las cuentas de usuario.

Para localizar rápidamente el perfil de seguridad que desea suprimir en la ventana Gestión de perfiles de seguridad, puede escribir el nombre del perfil de seguridad en el cuadro de texto **Tipo por filtrar**. Se halla encima del panel izquierdo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Perfiles de seguridad**.
4. En el panel izquierdo, seleccione el perfil de seguridad que desee suprimir.
5. En la barra de herramientas, pulse **Suprimir**.
6. Pulse **Aceptar**.
   - Si hay cuentas de usuario asignadas a este perfil de seguridad, se abre la ventana Hay usuarios asignados a este perfil de seguridad. Vaya al apartado "Supresión de un rol de usuario" en la página 14.
   - Si no hay cuentas de usuario asignadas a este perfil de seguridad, el perfil de seguridad se suprime satisfactoriamente. Vaya al apartado "Supresión de un rol de usuario" en la página 14.
7. Vuelva a asignar las cuentas de usuario de la lista a otro perfil de seguridad:
   a. En el cuadro de lista **Perfil de seguridad de usuario para asignar**, seleccione un perfil de seguridad.
   b. Pulse **Confirmar**.
8. Cierre la ventana Gestión de perfiles de seguridad.
9. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Gestión de cuentas de usuario

En este tema se proporciona información sobre la gestión de las cuentas de usuario.

Al configurar inicialmente el sistema, debe crear cuentas de usuario para cada uno de los usuarios. Después de la configuración inicial, puede que sea necesario crear más cuentas de usuario y gestionar las cuentas de usuario existentes.

Creación de una cuenta de usuario

Puede crear nuevas cuentas de usuario.

Antes de empezar

Antes de crear una cuenta de usuario, debe asegurarse de que el rol de usuario y el perfil de seguridad necesarios estén creados.

Acerca de esta tarea

Cuando cree una cuenta de usuario, debe asignar credenciales de acceso, un rol de usuario y un perfil de seguridad al usuario. Los roles de usuario definen qué acciones puede realizar el usuario. Los perfiles de seguridad definen a qué datos puede acceder el usuario.

Puede crear varias cuentas de usuario que incluyan privilegios administrativos; sin embargo, cualquier cuenta de usuario que sea gestor administrador puede crear otras cuentas de usuario administrativo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Usuarios**.
4. En la barra de herramientas de **Gestión de usuarios**, pulse **Nuevo**.
5. Especifique los valores de los parámetros siguientes:
   a. En el campo **Nombre de usuario**, escriba un nombre exclusivo para el nuevo usuario. El nombre de usuario debe contener 30 caracteres como máximo.
   b. En el campo **Contraseña**, escriba una contraseña para dar acceso al usuario.

      La contraseña debe cumplir los criterios siguientes:
      - 5 caracteres como mínimo
      - 255 caracteres como máximo
6. Pulse **Guardar**.
7. Cierre la ventana Detalles del usuario.
8. Cierre la ventana Gestión de usuarios.
9. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Supresión de una cuenta de usuario

Si una cuenta de usuario ya no es necesaria, puede suprimirla.

Acerca de esta tarea

Después de suprimir un usuario, el usuario ya no tendrá acceso a la interfaz de usuario. Si el usuario intenta iniciar sesión, se visualiza un mensaje para informar al usuario de que el nombre de usuario y la contraseña ya no son válidos. Los elementos que un usuario suprimido había creado, como las búsquedas guardadas y los informes, permanecen asociados con el usuario suprimido.

Para localizar rápidamente la cuenta de usuario que desea suprimir en la ventana Gestión de usuarios, puede escribir el nombre del usuario en el cuadro de texto **Buscar usuario** de la barra de herramientas.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Usuarios**.
4. Seleccione el usuario que desee suprimir.
5. En la barra de herramientas, pulse **Suprimir**.
6. Pulse **Aceptar**.
7. Cierre la ventana Gestión de usuarios.

Inhabilitación de una cuenta de usuario

Puede inhabilitar una cuenta de usuario para impedir que un usuario acceda a QRadar. La opción de inhabilitar una cuenta de usuario temporalmente revoca el acceso de un usuario sin suprimir la cuenta.

Acerca de esta tarea

Si el usuario con la cuenta inhabilitada intenta iniciar sesión, se visualiza un mensaje para informar al usuario de que el nombre de usuario y la contraseña ya no son válidos. Los elementos creados por el usuario, como por ejemplo las búsquedas y los informes guardados, permanecen asociados al usuario.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Usuarios**.
4. En el panel Gestionar usuarios, pulse la cuenta de usuario que desea inhabilitar.
5. En la ventana Detalles de usuario, seleccione **Inhabilitado** en la lista **Rol de usuario**.
6. Pulse **Guardar**.
7. Cierre la ventana Detalles del usuario.
8. Cierre la ventana Gestión de usuarios.
9. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Gestión de autenticación

Cuando la autenticación está configurada y un usuario especifica una combinación no válida de nombre de usuario y contraseña, se visualiza un mensaje para indicar que el inicio de sesión no es válido.

Si el usuario intenta acceder al sistema varias veces con información no válida, debe esperar la cantidad de tiempo configurado antes de intentar acceder al sistema de nuevo. Puede configurar los valores de la consola para determinar el número máximo de inicios de sesión fallidos y otros valores relacionados. Para obtener más información sobre la configuración de los valores de consola para la autenticación, consulte “Configuración de la hora del sistema de QRadar” en la página 56.

IBM Security QRadar da soporte a los tipos de autenticación siguientes:

- **Autenticación del sistema**: los usuarios se autentican localmente. La autenticación del sistema es el tipo de autenticación predeterminado.
- **Autenticación RADIUS**: los usuarios se autentican mediante un servidor RADIUS (servicio de usuarios de autenticación remota mediante llamada telefónica). Cuando un usuario intenta iniciar sesión, QRadar cifra la contraseña solamente y reenvía el nombre de usuario y la contraseña al servidor RADIUS para su autenticación.
- **Autenticación TACACS**: los usuarios se autentican mediante un servidor TACACS (sistema de control de acceso mediante control del acceso desde terminales). Cuando un usuario intenta iniciar sesión, QRadar cifra el nombre de usuario y la contraseña y reenvía esta información al servidor TACACS para su autenticación. La autenticación de TACACS utiliza Cisco Secure ACS Express como servidor TACACS. QRadar da soporte a Cisco Secure ACS Express hasta la versión 4.3.
- **Microsoft Active Directory**: los usuarios se autentican mediante un servidor LDAP (Lightweight Directory Access Protocol) que utiliza Kerberos.

- **LDAP**: los usuarios se autentican mediante un servidor LDAP nativo.

Lista de comprobación de requisitos previos para proveedores de autenticación externa

Para poder configurar RADIUS, TACACS, Active Directory o LDAP como tipo de autenticación, debe realizar las tareas siguientes:

__ • Configure el servidor de autenticación antes de configurar la autenticación en QRadar. Para obtener más información, consulte la documentación del servidor.

__ • Asegúrese de que el servidor tiene las cuentas de usuario y los niveles de privilegios adecuados para comunicarse con QRadar. Para obtener más información, consulte la documentación del servidor.

__ • Asegúrese de que la hora del servidor de autenticación está sincronizada con la hora del servidor de QRadar. Para obtener más información sobre el establecimiento de la hora, consulte el Capítulo 6, “Configurar QRadar”, en la página 69.

__ • Asegúrese de que todos los usuarios tienen las cuentas de usuario y los roles adecuados para permitir la autenticación con los servidores de proveedor.

Autenticación externa para usuarios administrativos

Los usuarios administrativos deben poder ser capaces de iniciar la sesión en IBM Security QRadar incluso cuando la autenticación externa falla.

Cuando la autenticación externa está configurada, debe establecer la contraseña local para los usuarios administrativos. Cuando el usuario inicia la sesión, el nombre de usuario y la contraseña se validan primero contra la autoridad remota. Si la autoridad remota no está disponible, la contraseña se valida localmente y el usuario puede iniciar la sesión y realizar funciones administrativas.

La contraseña local no está sincronizada con la autorización remota. Para evitar problemas al iniciar la sesión en QRadar cuando la autoridad remota no está disponible, recuerde actualizar la contraseña local al mismo tiempo que actualiza la contraseña en la autoridad remota.

No puede cambiar la contraseña de administración local mientras la autoridad remota está activa. Para cambiar la contraseña de administración, debe inhabilitar temporalmente la autenticación externa, restablecer la contraseña y volver a configurar la autenticación externa.

Cuando crea usuarios no administrativos, no se establece la contraseña local. Los usuarios no administrativos solo autentican contra la autoridad remota. Si la autoridad remota no está disponible o si se rechazan las credenciales de usuario, el usuario no puede iniciar la sesión.

Configuración de la autenticación del sistema

Puede configurar la autenticación local en el sistema de QRadar.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.
3. Pulse el icono **Autenticación**.

4. En el cuadro de lista **Módulo de autenticación**, seleccione **Autenticación del sistema**.
5. Pulse **Guardar**.

Configuración de autenticación de RADIUS

Puede configurar la autenticación de RADIUS en el sistema de QRadar.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema Gestión de usuarios**.
3. Pulse el icono **Autenticación**.
4. En el cuadro de lista **Módulo de autenticación**, seleccione **Autenticación RADIUS**.
5. Configure los parámetros:
   a. En el campo **Servidor RADIUS**, escriba el nombre de host o la dirección IP del servidor RADIUS.
   b. En el campo **Puerto de RADIUS**, escriba el puerto del servidor RADIUS.
   c. En el cuadro de lista **Tipo de autenticación**, seleccione el tipo de autenticación que desee realizar.

      Elija una de las opciones siguientes:

Opción	Descripción
CHAP	El protocolo de autenticación por desafío mutuo (Challenge Handshake Authentication Protocol, CHAP) establece una conexión de protocolo punto a punto (PPP) entre el usuario y el servidor.
MSCHAP	El protocolo de autenticación por desafío mutuo de Microsoft (MSCHAP) autentica estaciones de trabajo remotas de Windows.
ARAP	El protocolo de acceso remoto de Apple (Apple Remote Access Protocol, ARAP) establece autenticación para el tráfico de red de AppleTalk.
PAP	El protocolo de autenticación de contraseñas (PAP) envía texto en claro entre el usuario y el servidor.

   d. En el campo **Secreto compartido**, escriba el secreto compartido que QRadar SIEM utiliza para cifrar las contraseñas RADIUS para la transmisión al servidor RADIUS.
6. Pulse **Guardar**.

Configuración de autenticación de TACACS

Puede configurar la autenticación de TACACS en el sistema de QRadar.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios**.

3. Pulse el icono **Autenticación**.
4. En el cuadro de lista **Módulo de autenticación**, seleccione **Autenticación TACACS**.
5. Configure los parámetros:
   a. En el campo **Servidor TACACS**, escriba el nombre de host o la dirección IP del servidor TACACS.
   b. En el campo **Puerto TACACS**, escriba el puerto del servidor TACACS.
   c. En el cuadro de lista **Tipo de autenticación**, seleccione el tipo de autenticación que desee realizar.

      Elija una de las opciones siguientes:

Opción	Descripción
ASCII	ASCII (American Standard Code for Information Interchange) envía el nombre de usuario y la contraseña en texto simple.
PAP	El protocolo de autenticación de contraseñas (PAP) envía texto en claro entre el usuario y el servidor. PAP es el tipo de autenticación predeterminado.
CHAP	El protocolo de autenticación por desafío mutuo (Challenge Handshake Authentication Protocol, CHAP) establece una conexión de protocolo punto a punto (PPP) entre el usuario y el servidor.
MSCHAP	El protocolo de autenticación por desafío mutuo de Microsoft (MSCHAP) autentica estaciones de trabajo remotas de Windows.
MSCHAP2	La versión 2 del protocolo de autenticación por desafío mutuo de Microsoft (MSCHAP2) autentica estaciones de trabajo remotas de Windows mediante la autenticación mutua.
EAPMD5	Protocolo de autenticación extensible que utiliza el protocolo MD5 (EAPMD5) y establece una conexión PPP.

   d. En el campo **Secreto compartido**, escriba el secreto compartido que QRadar utiliza para cifrar las contraseñas TACACS para la transmisión al servidor TACACS.
6. Pulse **Guardar**.

Configuración de la autenticación de Active Directory

Puede configurar la autenticación de Microsoft Active Directory en el sistema de IBM Security QRadar.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** y a continuación pulse el icono **Autenticación**.
3. En el cuadro de lista **Módulo de autenticación**, seleccione **Active Directory**.

   Configure los siguientes parámetros:

Parámetro	Descripción
URL de servidor	Escriba el URL que se utiliza para conectar con el servidor LDAP; por ejemplo, ldaps://*host*:*puerto*.
Contexto de LDAP	Escriba el contexto de LDAP que desea utilizar; por ejemplo, DC=QRADAR,DC=INC.
Dominio LDAP	Escriba el dominio que desea utilizar; por ejemplo, qradar.inc.

4. Pulse **Guardar**.

Autenticación de LDAP

Puede configurar QRadar para utilizar proveedores LDAP (Lightweight Directory Access Protocol) para la autenticación y autorización de los usuarios.

QRadar lee la información de usuario y rol del servidor LDAP basándose en los criterios de autorización que ha definido.

En entornos dispersos geográficamente, el rendimiento se puede ver negativamente afectado si el servidor LDAP y la consola QRadar no están geográficamente cercanas entre sí. Por ejemplo, los atributos de usuario pueden tardar mucho en llenarse si la consola de QRadar está en Norteamérica y el servidor LDAP está en Europa.

Configuración de la autenticación de LDAP

Puede configurar la autenticación de LDAP en el sistema de IBM Security QRadar.

Antes de empezar

Si tiene previsto utilizar el cifrado SSL o la autenticación TLS con el servidor LDAP, debe importar el certificado SSL o TLS del servidor LDAP al directorio `/opt/qradar/conf/trusted_certificates` en la consola de QRadar. Para obtener más información sobre la configuración de los certificados, consulte el apartado "Configuración de certificados SSL o TLS" en la página 29.

Si utiliza la autorización de grupo, debe configurar un perfil de seguridad o un rol de usuario de QRadar en la consola de QRadar para cada grupo de LDAP utilizado por QRadar. Cada perfil de seguridad o rol de usuario de QRadar debe tener al menos un grupo **Aceptar**. La correlación de nombres de grupo con roles y perfiles de seguridad de usuario es sensible a las mayúsculas y minúsculas.

Acerca de esta tarea

La *Autenticación* establece una prueba de identidad para cualquier usuario que intente iniciar sesión en el servidor de QRadar. Cuando un usuario inicia sesión, el nombre de usuario y la contraseña se envían al directorio LDAP para verificar si las credenciales son correctas. Para enviar esta información de forma segura, configure la conexión del servidor LDAP para utilizar el cifrado SSL (Secure Socket Layer) o TLS (Transport Layer Security).

La *Autorización* es el proceso de determinar qué permisos de acceso tiene un usuario. Los usuarios están autorizados a realizar tareas en función de sus asignaciones de roles. Debe tener una conexión de enlace válida al servidor LDAP para poder seleccionar los valores de autorización.

Los valores de atributo de usuario son sensibles a las mayúsculas y minúsculas. La correlación de nombres de grupo con roles y perfiles de seguridad de usuario también es sensible a las mayúsculas y minúsculas.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema** > **Gestión de usuarios** y pulse el icono **Autenticación**.
3. En el cuadro de lista **Módulo de autenticación**, seleccione **LDAP**.
4. Pulse **Añadir** y rellene los parámetros de configuración básica.

Más información sobre parámetros de configuración básicos de LDAP:

Tabla 7. Parámetros de configuración básicos de LDAP

Parámetro	Descripción
URL de servidor	Nombre de DNS o dirección IP del servidor LDAP. El URL debe incluir un valor de puerto. Por ejemplo, `ldap://<nombre_host>:<puerto>` o `ldap://<dirección_ip>:<puerto>`.
Conexión SSL	Seleccione **Verdadero** o **Falso** para especificar si el cifrado SSL (Secure Sockets Layer) está habilitado. Si se habilita el cifrado SSL, el valor del campo **URL de servidor** debe especificar una conexión segura. Por ejemplo, `ldaps://secureldap.mydomain.com:636` utiliza un URL de servidor seguro.
Autenticación TLS	Seleccione **Verdadero** o **Falso** para especificar si la autenticación TLS (Transport Layer Security) está habilitada. El cifrado TLS (seguridad de la capa de transporte) para conectar con el servidor LDAP se negocia como parte del protocolo LDAP normal y no requiere una designación de protocolo ni un puerto especial en el campo **URL de servidor**.
Examinar base completa	Seleccione **Verdadero** para buscar en todos los subdirectorios del nombre de directorio (DN) especificado. Seleccione **Falso** para buscar en el contenido inmediato del DN base. No se busca en los subdirectorios.
Campo de usuario LDAP	Identificador del campo de usuario en el que desea buscar. Puede especificar una lista de varios campos de usuario separados por comas para autenticar contra varios campos. Por ejemplo, si especifica **uid,mailid**, un usuario se puede autenticar mediante su ID de usuario o mediante su ID de correo.
DN base de usuario	El DN (nombre distinguido) del nodo en el que se iniciará la búsqueda de un usuario. El **DN base de usuario** se convierte en la ubicación inicial para cargar usuarios. Por razones de rendimiento, asegúrese de que el **DN base de usuario** sea tan específico como sea posible. Por ejemplo, si todas las cuentas de usuarios están en el servidor de directorios en la carpeta Usuarios y su nombre de dominio es `ibm.com`, el valor de DN base de usuario sería `cn=Usuarios,dc=ibm,dc=com`.

Tabla 7. Parámetros de configuración básicos de LDAP (continuación)

Parámetro	Descripción
Recomendación	Seleccione **Ignorar** o **Seguir** para especificar qué se hace con las recomendaciones.

5. En **Valores de conexión**, seleccione el tipo de conexión de enlace.

   Más información sobre conexiones de enlace:

Tabla 8. Conexiones de enlace de LDAP

Tipo de conexión de enlace	Descripción
Enlace anónimo	Utilice el enlace anónimo para crear una sesión con el servidor de directorios LDAP que no requiere que se proporcione información de autenticación.
Enlace autenticado	Utilice el enlace autenticado cuando desea que la sesión requiera una combinación de nombre de usuario y contraseña válidos. Un enlace autenticado satisfactoriamente autoriza al usuario autenticado a leer la lista de usuarios y roles del directorio LDAP durante la sesión.Para mayor seguridad, asegúrese de que el ID de usuario que se utiliza para la conexión de enlace no tiene permisos para realizar ninguna tarea que no sea leer el directorio LDAP. Proporcione el **DN de inicio de sesión** y la **Contraseña**. Por ejemplo, si el nombre de inicio de sesión es `admin` y el dominio es `ibm.com`, el valor de **DN de inicio de sesión** sería `cn=admin,dc=ibm,dc=com`.

6. Pulse **Probar conexión** para probar la información de conexión. Debe proporcionar información de usuario para autenticar contra los atributos de usuario especificados en **Campo de usuario LDAP**. Si especificó varios valores en **Campo de usuario LDAP**, debe proporcionar información de usuario para autenticar contra el primer atributo especificado.
7. Seleccione el método de autorización que se utilizará.

   Más información sobre los métodos de autorización:

Tabla 9. Métodos de autorización de LDAP

Parámetro de método de autorización	Descripción
Local	La combinación de nombre de usuario y contraseña se verifica para cada usuario que inicia la sesión, pero no se intercambia información de autorización alguna entre el servidor LDAP y el servidor de QRadar. Si elige la autorización **Local**, debe crear cada usuario en la consola de QRadar.
Atributos de usuario	Seleccione **Atributos de usuario** cuando desee especificar qué atributos de perfil de seguridad y rol de usuario se pueden utilizar para determinar niveles de autorización. Debe especificar un atributo de rol de usuario y también un atributo de perfil de seguridad. Los atributos que puede utilizar se recuperan del servidor LDAP según los valores de conexión.Los valores de atributo de usuario son sensibles a las mayúsculas y minúsculas.

Tabla 9. Métodos de autorización de LDAP (continuación)

Parámetro de método de autorización	Descripción
Basado en grupo	Seleccione **Basado en grupo** cuando desea que los usuarios hereden permisos de acceso según el rol después de su autenticación con el servidor LDAP. La correlación de nombres de grupo con roles y perfiles de seguridad de usuario es sensible a las mayúsculas y minúsculas.
DN base de grupo	Especifica el nodo de inicio del directorio LDAP para cargar grupos. Por ejemplo, si todos los grupos están en en la carpeta `Grupos` del servidor de directorios y su nombre de dominio es `ibm.com`, el valor de **DN base de grupo** sería `cn=Grupos,dc=ibm,dc=com`.
Límite de consulta habilitado	Establece un límite sobre el número de grupos devueltos.
Límite de resultado de consulta	El número máximo de grupos devueltos por la consulta. De forma predeterminada, los resultados de la consulta están limitados a mostrar solo los 1000 primeros resultados de la consulta.
Por miembro	Seleccione **Por miembro** para buscar grupos de acuerdo con los miembros de grupo. En el cuadro **Campo de miembro de grupo**, especifique el atributo LDAP que se utiliza para definir la pertenencia al grupo de usuarios. Por ejemplo, si el grupo utiliza el atributo memberUid para determinar la pertenencia al grupo, especifique `memberUid` en el cuadro **Campo de miembro de grupo**.
Por consulta	Seleccione **Por consulta** para buscar grupos ejecutando una consulta. Proporcione la información de la consulta en los cuadros de texto **Campo de miembro de grupo** y **Campo de consulta de grupo**. Por ejemplo, para buscar todos los grupos que tengan como mínimo un atributo **`memberUid`** y que tengan un valor de **`cn`** que empiece por la letra 's', escriba `memberUid` en **Campo de miembro de grupo** y `cn=s*` en **Campo de consulta de grupo**.

8. Si ha especificado la autorización Basado en grupo, pulse **Cargar grupos** y pulse el icono más (+) o menos (-) para añadir o eliminar grupos de privilegios.

   Las opciones de privilegios de rol de usuario controlan a qué componentes de QRadar tiene acceso el usuario. Las opciones de privilegios de perfil de seguridad controlan los datos de QRadar a los que cada usuario tiene acceso.

   Nota: Los límites de consulta se pueden establecer marcando el recuadro de selección **Límite de consulta habilitado** o se pueden establecer en el servidor LDAP. Si los límites de consulta se establecen en el servidor LDAP, recibirá un mensaje en el que se indica que el límite de consulta está habilitado incluso aunque no haya marcado el recuadro de selección **Límite de consulta habilitado**.
9. Pulse **Guardar**.
10. Pulse **Gestionar sincronización** para intercambiar información de autenticación y autorización entre el servidor LDAP y la consola de QRadar.

a. Si es la primera vez que configura la conexión LDAP, pulse **Ejecutar sincronización ahora** para sincronizar los datos.
b. Especifique la frecuencia de la sincronización automática.
c. Pulse **Cerrar**.

11. Repita los pasos para añadir más servidores LDAP y pulse **Guardar** cuando haya acabado.

Sincronización de datos con un servidor LDAP

Puede sincronizar datos manualmente entre el servidor IBM Security QRadar y el servidor de autenticación LDAP.

Acerca de esta tarea

Si utiliza la autorización que se basa en los atributos o grupos de usuarios, la información de usuario se importa automáticamente del servidor LDAP a la consola de QRadar.

Cada grupo que se configure en el servidor LDAP debe tener un rol de usuario o un perfil de seguridad correspondiente que se configura en la consola de QRadar. Para cada grupo que coincida, los usuarios se importan y se les asignan permisos en función del rol o el perfil de seguridad de cada usuario.

De forma predeterminada, la sincronización se produce cada 24 horas. La temporización de la sincronización se basa en la hora de la última ejecución. Por ejemplo, si ejecuta manualmente la sincronización a las 23:45 horas y establece la sincronización en 8 horas, la siguiente sincronización se producirá a las 07:45 horas. Si cambian los permisos de acceso para un usuario que ha iniciado sesión cuando se llevaba a cabo la sincronización, la sesión deja de ser válida. Se redirige al usuario a la pantalla de inicio de sesión con la solicitud siguiente.

Procedimiento

1. En la pestaña **Admin**, pulse **Configuración del sistema** y, a continuación, pulse **Autenticación**.
2. En la lista **Módulo de autenticación**, seleccione **LDAP**.
3. Pulse **Gestionar sincronización** y después pulse **Ejecutar sincronización ahora**.

Configuración de certificados SSL o TLS

Si utiliza un servidor de directorio LDAP para la autenticación de los usuarios y desea habilitar el cifrado SSL o la autenticación TLS, debe configurar el certificado SSL o TLS.

Procedimiento

1. Inicie, mediante SSH, la sesión en el sistema como usuario root.
   a. Nombre de usuario: `root`
   b. Contraseña: `<contraseña>`
2. Escriba el mandato siguiente para crear el directorio `/opt/qradar/conf/trusted_certificates/`:

   ```
   mkdir -p /opt/qradar/conf/trusted_certificates
   ```

3. Copie el certificado SSL o TLS del servidor LDAP en el directorio `/opt/qradar/conf/trusted_certificates` en el sistema.
4. Verifique que la extensión del archivo de certificado sea `.cert`, que indica que el certificado es de confianza. El sistema QRadar solamente carga archivos `.cert`.

Visualización del texto contextual para la información de LDAP

Puede crear un archivo de configuración de propiedades de LDAP para visualizar la información de usuario LDAP como texto contextual. Este archivo de configuración consulta la base de datos de LDAP para buscar información de usuario LDAP que esté asociada con sucesos, delitos o activos.

Antes de empezar

El servidor web debe reiniciarse una vez creadas las propiedades de LDAP. Considere la posibilidad de planificar esta tarea para que se lleve a cabo durante una ventana de mantenimiento, cuando no hay usuarios activos con sesiones iniciadas en el sistema.

Acerca de esta tarea

En el ejemplo siguiente se indican las propiedades que puede añadir a un archivo de configuración `ldap.properties`.

```
ldap.url=ldap://LDAPserver.example.com:389
ldap.authentication=simple
ldap.userName=nombre.usuario
ldap.password=contraseña.cifrada
ldap.basedn=O=IBM,C=US ldap.filterString=(&(objectclass=user)(samaccountname=%USER%))
ldap.attributes.displayName=Name
ldap.attributes.email=Email
ldap.attributes.employeeID=EmployeeID
ldap.attributes.department=Department
```

Procedimiento

1. Utilice SSH para iniciar la sesión en IBM Security QRadar como usuario root.
2. Para cifrar la contraseña del usuario LDAP, ejecute el script `/opt/qradar/bin/runjava.sh com.q1labs.core.util.PasswordEncrypt [`*`contraseña`*`]`.
3. Utilice un editor de texto para crear el archivo de configuración `/opt/qradar/conf/ldap.properties`.
4. Especifique la ubicación y la información de autenticación para acceder al servidor LDAP remoto.
   a. Especifique el URL del servidor LDAP y el número de puerto.

      Utilice `ldaps://` o `ldap://` para conectar con el servidor remoto; por ejemplo, `ldap.url=ldaps://LDAPserver.example.com:389`.
   b. Escriba el método de autenticación que se utiliza para acceder al servidor LDAP.

      Los administradores pueden utilizar el método de autenticación simple; por ejemplo, `ldap.authentication=simple`.
   c. Teclee el nombre de usuario que tiene permisos para acceder al servidor LDAP. Por ejemplo, `ldap.userName=`*`nombre.usuario`*.
   d. Para autenticarse con el servidor LDAP remoto, escriba la contraseña cifrada del usuario LDAP. Por ejemplo, `ldap.password=`*`contraseña`*.
   e. Escriba el DN base que se utiliza para buscar los usuarios en el servidor LDAP. Por ejemplo, `ldap.basedn=`*`DNbase`*.
   f. Escriba un valor que se utilizará para el filtro de parámetros de búsqueda en LDAP.

      Por ejemplo, en IBM Security QRadar, cuando se pasa el puntero del ratón por encima de `ldap.filterString=(&(objectclass=user)(samaccountname=%USER%))`, el valor `%USER%` se sustituye por el nombre de usuario.

5. Escriba uno o varios atributos para que aparezcan en el texto contextual.

   Debe incluir un atributo LDAP como mínimo. Cada valor debe utilizar este formato: `ldap.attributes.`*`nombre_atributo=Texto descriptivo para mostrar en la interfaz de usuario`*`.`
6. Verifique que se disponga de permiso de lectura para el archivo de configuración `ldap.properties`.
7. Inicie sesión en QRadar como administrador.
8. En la pestaña **Admin**, seleccione **Avanzado** > **Reiniciar el servidor web**.

Resultados

Los administradores pueden pasar el puntero del ratón por encima del campo **Nombre de usuario** en la pestaña **Actividad de registro** y la pestaña **Delitos** o pasar el puntero del ratón sobre el campo **Último usuario** en la pestaña **Activos** (si está disponible) para visualizar más información sobre el usuario LDAP.

Varios repositorios LDAP

Puede configurar IBM Security QRadar para la correlación de entradas de varios repositorios LDAP con un solo repositorio virtual.

Si se configuran varios repositorios, cuando un usuario inicia la sesión, es necesario especificar qué repositorio se debe utilizar para la autenticación. Es necesario especificar la vía de acceso completa del repositorio y el nombre de dominio en el campo de nombre de usuario. Por ejemplo, Repositorio_1 se ha configurado de manera que utilice el dominio `ibm.com` y Repositorio_2 se ha configurado de manera que utilice el dominio `ibm.ca.com`, la información de inicio de sesión puede tener el aspecto siguiente:

- `OU=User Accounts,OU=PHX,DC=qcorpaa,DC=aa,DC=ibm.com\`*`nombre_usuario`*
- `OU=Office,OU=User Accounts,DC=qcorpaa,DC=aa,DC=ibm.ca.com\`*`nombre_usuario`*

La información de usuario se importa automáticamente del servidor LDAP en el caso de los repositorios que utilizan atributos de usuario o autorización de grupo. En el caso de los repositorios que utilizan la autorización local, debe crear los usuarios directamente en el sistema de QRadar.

Ejemplo: Configuración y preparación del acceso con los privilegios mínimos

Otorgue a los usuarios únicamente la cantidad mínima de acceso que necesitan para realizar sus tareas cotidianas.

Puede asignar privilegios diferentes para los datos de QRadar y para las prestaciones de QRadar. Para realizar esta asignación, especifique diferentes grupos de aceptación y denegación para los perfiles de seguridad y los roles de usuario. Los grupos de aceptación asignan privilegios y los grupos de denegación restringen los privilegios.

Veamos un ejemplo. Su empresa ha contratado a un grupo de estudiantes en prácticas. John está en el último año de un programa de ciberseguridad especializado en la universidad de su zona. Se le ha pedido que supervise y revise las vulnerabilidades conocidas de la red y que prepare un plan correctivo en función de lo que averigüe. La información referente a las vulnerabilidades de la red de la empresa es confidencial.

Como administrador de QRadar, debe asegurarse de que los estudiantes en prácticas tengan acceso limitado a los datos y los sistemas. A la mayoría de los

estudiantes en prácticas se les debe denegar el acceso a QRadar Vulnerability Manager, pero la tarea que se ha asignado a John exige que él sí tenga acceso. La política de la organización es que los estudiantes en prácticas nunca tengan acceso a la API de QRadar.

En la tabla siguiente se muestra que John debe ser un miembro de los grupos **company.interns** y **qvm.interns** para tener acceso a QRadar Risk Manager y QRadar Vulnerability Manager.

Tabla 10. Grupos de privilegios de rol de usuario

Rol de usuario	Aceptar	Denegar
Admin	qradar.admin	company.firedemployees
QVM	qradar.qvm qvm.interns	company.firedemployees qradar.qrm company.interns
QRM	qradar.qrm company.interns	company.firedemployees

En la tabla siguiente se muestra que el perfil de seguridad para **qvm.interns** no permite a John acceder a la API de QRadar.

Tabla 11. Grupos de privilegios de perfil de seguridad

Perfil de seguridad	Aceptar	Denegar
QVM	qradar.secprofile.qvm	company.firedemployees
API	qradar.secprofile.qvm.api	company.firedemployees qradar.secprofile.qvm.interns

Acceso y permisos de los roles de usuario

Utilice los parámetros de la ventana Gestión de roles de usuario para restringir el acceso a las funciones de IBM Security QRadar.

En la tabla siguiente se describen los parámetros de la ventana Gestión de roles de usuario. Los parámetros visibles en la ventana Gestión de roles de usuario dependen de qué componentes de QRadar están instalados.

Tabla 12. Descripción de los parámetros de la ventana Gestión de roles de usuario

Parámetro	Descripción
Nombre del rol de usuario	Nombre exclusivo para el rol.

Tabla 12. Descripción de los parámetros de la ventana Gestión de roles de usuario (continuación)

Parámetro	Descripción
Admin	Otorga acceso administrativo a la interfaz de usuario. Puede otorgar permisos administrativos específicos: **Gestor administrador** Otorga acceso administrativo a la interfaz de usuario. Otorgue permisos administrativos específicos. **Configuración de redes remotas y servicios remotos** Otorga permiso para configurar redes y servicios remotos en la pestaña **Admin**. **Administrador del sistema** Otorga permiso para acceder a todas las áreas de la interfaz de usuario. Los usuarios que tienen este acceso no pueden editar otras cuentas de administrador.
Delitos	Otorga acceso a todas las funciones de la pestaña **Delitos**. Puede otorgar permisos específicos: **Asignar delitos a usuarios** Otorga permiso para asignar delitos a otros usuarios. **Mantener reglas personalizadas** Otorga permiso para crear y editar reglas personalizadas. **Gestionar motivos de cierre de delitos** Otorga permiso para gestionar razones de cierre de delitos. **Ver reglas personalizadas** Otorga permiso para ver reglas personalizadas. Si se otorga a un rol de usuario que no tenga asimismo el permiso **Mantener reglas personalizadas**, el rol de usuario no puede crear ni editar reglas personalizadas.

Tabla 12. Descripción de los parámetros de la ventana Gestión de roles de usuario (continuación)

Parámetro	Descripción
Actividad de registro	Otorga acceso a las funciones de la pestaña **Actividad de registro**. También puede otorgar permisos específicos: **Mantener reglas personalizadas** Otorga permiso para crear o editar reglas que se muestran en la pestaña **Actividad de registro**. **Gestionar series temporales** Otorga permiso para configurar y ver gráficas de datos de series temporales. **Propiedades de suceso definidas por el usuario** Otorga permiso para crear propiedades de suceso personalizadas. Para obtener más información sobre las propiedades de sucesos personalizadas, consulte la guía del usuario de su producto. **Ver reglas personalizadas** Otorga permiso para ver reglas personalizadas. Si se otorga a un rol de usuario que no tenga asimismo el permiso **Mantener reglas personalizadas**, el rol de usuario no puede crear ni editar reglas personalizadas.

Tabla 12. Descripción de los parámetros de la ventana Gestión de roles de usuario (continuación)

Parámetro	Descripción
Activos	**Nota:** Este permiso solamente se visualiza si IBM Security QRadar Vulnerability Manager está instalado en el sistema. Otorga acceso a la función de la pestaña **Activos**. Puede otorgar permisos específicos: **Realizar exploraciones de VA** Otorga permiso para realizar exploraciones de evaluación de vulnerabilidades. Para obtener más información sobre la evaluación de vulnerabilidades, consulte la guía de gestión de evaluación de vulnerabilidades. **Eliminar vulnerabilidades** Otorga permiso para eliminar las vulnerabilidades de los activos. **Descubrimiento de servidores** Otorga permiso para descubrir servidores. **Ver datos de VA** Otorga permiso para los datos de evaluación de vulnerabilidades. Para obtener más información sobre la evaluación de vulnerabilidades, consulte la guía de gestión de evaluación de vulnerabilidades.

Tabla 12. Descripción de los parámetros de la ventana Gestión de roles de usuario (continuación)

Parámetro	Descripción
Actividad de red	Otorga acceso a todas las funciones de la pestaña **Actividad de red**. Puede otorgar acceso específico a los permisos siguientes: **Mantener reglas personalizadas** Otorga permiso para crear o editar reglas que se muestran en la pestaña **Actividad de red**. **Gestionar series temporales** Otorga permiso para configurar y ver gráficas de datos de series temporales. **Propiedades de flujo definidas por el usuario** Otorga permiso para crear propiedades de flujo personalizadas. **Ver reglas personalizadas** Otorga permiso para ver reglas personalizadas. Si el rol de usuario no tiene también el permiso **Mantener reglas personalizadas**, el rol de usuario no puede crear ni editar reglas personalizadas. **Ver contenido de flujo** Otorga permiso para acceder a los datos de flujo.
Informes	Otorga permiso para acceder a todas las funciones de la pestaña **Informes**. Puede otorgar permisos específicos del usuario: **Distribuir informes vía correo electrónico** Otorga permiso para distribuir informes a través del correo electrónico. **Mantener plantillas** Otorga permiso para editar las plantillas de informe.
Vulnerability Manager	Otorga permiso para la función QRadar Vulnerability Manager. IBM Security QRadar Vulnerability Manager debe estar activado. Para obtener más información, consulte la publicación *IBM Security QRadar Vulnerability Manager Guía del usuario*.
Análisis forense	Otorga permiso para las prestaciones de QRadar Incident Forensics. **Crear casos en Incident Forensics** Otorga permiso para crear casos para recopilaciones de archivos pcap y de documentos importados.

Tabla 12. Descripción de los parámetros de la ventana Gestión de roles de usuario (continuación)

Parámetro	Descripción
Extensiones de menú contextual de IP	Otorga permiso para las opciones añadidas al menú contextual.
Configuración de plataforma	Otorga permiso para los servicios de **Configuración de plataforma**. **Descartar notificaciones del sistema** Otorga permiso para ocultar las notificaciones del sistema en la pestaña **Mensajes**. **Ver datos de referencia** Otorga permiso para ver datos de referencia cuando está disponible en los resultados de la búsqueda. **Ver notificaciones del sistema** Otorga permiso para ver las notificaciones del sistema en la pestaña **Mensajes**.

Parámetros de perfil de seguridad

En la tabla siguiente se proporcionan descripciones de los parámetros de la ventana Gestión de perfiles de seguridad:

Tabla 13. Parámetros de la ventana Gestión de perfiles de seguridad

Parámetro	Descripción
Nombre del perfil de seguridad	Escriba un nombre exclusivo para el perfil de seguridad. El nombre del perfil de seguridad debe cumplir los requisitos siguientes: • 3 caracteres como mínimo • 30 caracteres como máximo
Descripción	`Opcional.` Escriba una descripción del perfil de seguridad. El número máximo de caracteres es de 255.

Parámetros de la ventana Gestión de usuarios

En la tabla siguiente se proporcionan descripciones de los parámetros de la ventana Gestión de usuarios:

Tabla 14. Parámetros de la ventana Gestión de usuarios

Parámetro	Descripción
Nombre de usuario	Muestra el nombre de usuario de esta cuenta de usuario.
Descripción	Muestra la descripción de la cuenta de usuario.
Correo electrónico	Muestra la dirección de correo electrónico de esta cuenta de usuario.

Tabla 14. Parámetros de la ventana Gestión de usuarios (continuación)

Parámetro	Descripción
Rol de usuario	Muestra el rol de usuario que está asignado a esta cuenta de usuario. Los roles de usuario definen qué acciones puede realizar el usuario.
Perfil de seguridad	Muestra el perfil de seguridad que está asignado a esta cuenta de usuario. Los perfiles de seguridad definen a qué datos puede acceder el usuario.

Barra de herramientas de la ventana Gestión de usuarios

funciones de la barra de herramientas de la ventana Gestión de usuarios

En la tabla siguiente se proporcionan descripciones de las funciones de la barra de herramientas de la ventana Gestión de usuarios:

Tabla 15. Funciones de la barra de herramientas de la ventana Gestión de usuarios

Función	Descripción
Nuevo	Pulse este icono para crear una cuenta de usuario. Para obtener más información sobre la creación de una cuenta de usuario, consulte el apartado "Creación de una cuenta de usuario" en la página 19.
Editar	Pulse este icono para editar la cuenta de usuario seleccionada.
Suprimir	Pulse este icono para suprimir la cuenta de usuario seleccionada.
Buscar usuarios	En este cuadro de texto puede escribir una palabra clave y luego pulsar Intro para localizar una cuenta de usuario específica.

Parámetros de la ventana Detalles del usuario

Parámetros de la ventana Detalles del usuario

En la tabla siguiente se proporcionan descripciones de los parámetros de la ventana Detalles del usuario:

Tabla 16. Parámetros de la ventana Detalles del usuario

Parámetro	Descripción
Nombre de usuario	Escriba un nombre exclusivo para el usuario. El nombre de usuario debe contener 30 caracteres como máximo.
Correo electrónico	Escriba la dirección de correo electrónico del usuario. La dirección de correo electrónico debe cumplir los requisitos siguientes: • Debe ser una dirección de correo electrónico válida • 10 caracteres como mínimo • 255 caracteres como máximo

Tabla 16. Parámetros de la ventana Detalles del usuario (continuación)

Parámetro	Descripción
Contraseña	Escriba una contraseña para dar acceso al usuario. La contraseña debe cumplir los criterios siguientes: • 5 caracteres como mínimo • 255 caracteres como máximo
Confirmar contraseña	Vuelva a escribir la contraseña para confirmarla.
Descripción	`Opcional.` Escriba una descripción de la cuenta de usuario. El número máximo de caracteres es de 2.048.
Rol de usuario	En el cuadro de lista, seleccione el rol de usuario que desea asignar a este usuario. Para añadir, editar o suprimir roles de usuario, puede pulsar el enlace **Gestionar roles de usuario**. Para obtener información sobre los roles de usuario, consulte el apartado “Gestión de roles” en la página 13.
Perfil de seguridad	En el cuadro de lista, seleccione el perfil de seguridad que desea asignar a este usuario. Para añadir, editar o suprimir perfiles de seguridad, puede pulsar el enlace **Gestionar perfiles de seguridad**. Para obtener información sobre los perfiles de seguridad, consulte el apartado “Gestión de perfiles de seguridad” en la página 15.

Capítulo 4. Gestión de sistemas y licencias

Gestionar sistemas y licencias del despliegue de QRadar.

Debe asignar una licencia para cada sistema del despliegue, incluidos los dispositivos de software. QFlow y recopiladores de sucesos de QRadar no necesitan una licencia.

Cuando se instala un sistema de QRadar, una clave de licencia predeterminada le proporciona acceso a la interfaz de usuario durante cinco semanas. Antes de que la licencia predeterminada caduque, debe asignar una clave de licencia al sistema. También puede añadir licencias para habilitar los productos de QRadar, como QRadar Vulnerability Manager.

Hay un periodo de gracia de 14 días para volver a asignar una licencia. Puede desbloquear una licencia si la clave está cargada, después de que se apliquen parches a un host mediante un arreglo o después de que se cargue una clave de desbloqueo. Una vez transcurrido el periodo de gracia, la licencia estará fijada (bloqueada) al sistema.

Si el estado de la licencia es **No válido**, debe sustituirse la licencia. Este estado podría indicar que la licencia se ha modificado sin autorización.

Una licencia permanece sin desplegar hasta que se despliega el cambio de licencia.

Visión general de Gestión del sistema y licencias

Utilice la ventana Gestión del sistema y licencias para gestionar el sistema y las claves de licencia y para reiniciar o concluir el sistema.

La barra de herramientas de la ventana Gestión del sistema y licencias proporciona las funciones siguientes:

Tabla 17. Funciones de la barra de herramientas de Gestión del sistema y licencias

Función	Descripción
Asignar licencia a sistema	Utilice esta función para asignar una licencia a un sistema. Cuando se selecciona **Licencias** en el menú **Visualizar**, la etiqueta de esta función pasa a ser **Asignar sistema a licencia**.
Cargar licencia	Utilice esta función para cargar una licencia a la consola. Para obtener más información, consulte el apartado “Carga de una clave de licencia” en la página 44.
Acciones (Licencia)	Seleccione **Licencias** en el menú **Visualizar** para ver las opciones de menú de licencia. Si selecciona **Acciones** > **Revertir asignación** en una licencia desplegada dentro del periodo de gracia asignado, que es de 14 días después del despliegue, el estado de la licencia pasa a ser **Desbloqueada**. Puede reasignar una licencia desbloqueada a otro sistema.

© Copyright IBM Corp. 2012, 2015

Tabla 17. Funciones de la barra de herramientas de Gestión del sistema y licencias (continuación)

Función	Descripción
Acciones (Sistema)	Seleccione **Sistemas** en el menú **Visualizar** y pulse el menú **Acciones** para ver las opciones siguientes: **Ver y gestionar el sistema**: seleccione un sistema y pulse **Acciones** > **Ver y gestionar el sistema** para ver la ventana Información del sistema. Pulse las pestañas **Licencia**, **Cortafuegos**, **Interfaces de red** y **Servidor de correo electrónico** para configurar estos elementos del sistema. **Añadir host de alta disponibilidad**: Seleccione un sistema y luego seleccione esta opción para añadir un host de alta disponibilidad (HA) al sistema para formar un clúster de alta disponibilidad. Para obtener más información sobre la alta disponibilidad, consulte la guía de alta disponibilidad de su producto. **Revertir asignación**: Seleccione esta opción para deshacer los cambios de licencia por fases. La configuración vuelve a la última asignación de licencia desplegada. **Nota:** Si revierta la asignación de una licencia desplegada dentro del periodo de gracia de la asignación, que es de 14 días después del despliegue, el estado de la licencia pasa a ser **Desbloqueada**. Puede reasignar una licencia **Desbloqueada** a otro sistema. **Reiniciar el servidor web**: Seleccione esta opción para reiniciar la interfaz de usuario, cuando sea necesario. Por ejemplo, podría tener que reiniciar la interfaz de usuario después de instalar un nuevo protocolo que añada componentes de interfaz de usuario nuevos. **Cerrar el sistema**: Seleccione un sistema y luego seleccione esta opción para cerrar el sistema. Para obtener más información, consulte el apartado "Cierre de un sistema" en la página 50. **Reiniciar sistema**: Seleccione un sistema y luego seleccione esta opción para reiniciar el sistema. Para obtener más información, consulte el apartado "Reinicio de un sistema" en la página 49. **Recopilar archivos de registro**: recopilar archivos de registro para el host seleccionado.

Si selecciona **Licencias** en el menú **Visualizar**, en la ventana Gestión del sistema y licencias se muestra la información siguiente:

Tabla 18. Parámetros de la ventana Gestión del sistema y licencias - vista Licencias

Parámetro	Descripción
Nombre de host	Sistema asignado a esta licencia.
IP de host	Sistema asignado a esta licencia.
Tipo de dispositivo de licencia	Tipo de dispositivo asignado a esta licencia.
Identidad de licencia	Nombre del producto de IBM Security QRadar que proporciona esta licencia.

Tabla 18. Parámetros de la ventana Gestión del sistema y licencias - vista Licencias (continuación)

Parámetro	Descripción
Estado de licencia	El estado de la licencia asignada a esta sistema puede ser uno de los siguientes: **No asignada**: la licencia no está asignada a un sistema. **No desplegada**: la licencia está asignada a un sistema pero el cambio de asignación no está desplegado. Esto significa que la licencia no está activa en el despliegue todavía. **Desplegada**: la licencia está asignada y activa en el despliegue. **Desbloqueada**: la licencia está desbloqueada. Las licencias desplegadas en los últimos 10 días se pueden desbloquear. Este es el periodo de gracia predeterminado para volver a asignar una licencia. Una vez transcurrido el periodo de gracia, la licencia estará fijada (bloqueada) al sistema. Si tiene que desbloquear una licencia después de ese periodo, póngase en contacto con el servicio de soporte al cliente. **No válido**: la licencia no es válida y debe sustituirse. Este estado podría indicar que la licencia se ha modificado sin autorización.
Fecha de caducidad de la licencia	Fecha de caducidad.
Límite de velocidad de sucesos	Velocidad máxima de sucesos permitida según los términos de la licencia.
Límite de velocidad de flujo	Velocidad máxima de flujo permitida según los términos de la licencia.

Lista de comprobación de la gestión de licencias

Utilice las opciones disponibles en la ventana Gestión del sistema y licencias para gestionar las claves de licencia.

Una clave de licencia predeterminada le proporciona acceso a la interfaz de usuario durante cinco semanas. Debe asignar una clave de licencia al sistema.

Debe configurar el sistema de QRadar para que los usuarios puedan utilizar las herramientas. Empiece por obtener una clave de licencia. Una vez que disponga de una clave de licencia, debe cargarla a la consola y asignarla a un sistema.

Durante la configuración inicial de un sistema debe llevar a cabo las tareas siguientes:

Procedimiento

1. Obtenga una clave de licencia mediante uno de estos métodos:
   - En el caso de una clave de licencia nueva o actualizada, póngase en contacto con el representante de ventas local.
   - Para cualquier otro problema técnico, póngase en contacto con el servicio de soporte al cliente.
2. Cargue la clave de licencia.

Cuando se carga una clave de licencia, aparece en la lista de la ventana Gestión del sistema y licencias, pero permanece sin asignar. Para obtener más información, consulte el apartado "Carga de una clave de licencia".

3. Asigne la licencia a un sistema o asigne un sistema a una licencia.
4. Para desplegar los cambios, en el menú de la pestaña **Admin**, pulse **Avanzado** > **Desplegar configuración completa**.

   Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Carga de una clave de licencia

Cargue una clave de licencia en consola de QRadar cuando instale un sistema de QRadar nuevo, actualice una licencia caducada o añada un producto de QRadar, como QRadar Vulnerability Manager, al despliegue.

Antes de empezar

Elija una de las opciones siguientes si necesita ayuda con la clave de licencia:

- En el caso de una clave de licencia nueva o actualizada, póngase en contacto con el representante de ventas local.
- Para cualquier otro problema técnico, póngase en contacto con el servicio de soporte al cliente.

Acerca de esta tarea

Si inicia la sesión en su consola de QRadar y encuentra que la clave de licencia ha caducado, se le dirige automáticamente a la ventana Gestión del sistema y licencias. Debe cargar una clave de licencia para poder continuar. Si uno de los sistemas host incluye una clave de licencia caducada, se muestra un mensaje al iniciar la sesión en el que se indica que un sistema necesita una clave de licencia nueva. Debe acceder a la ventana Gestión del sistema y licencias para actualizar esa clave de licencia.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En la barra de herramientas, pulse **Cargar licencia**.
5. En el cuadro de diálogo, pulse **Seleccionar archivo**.
6. En la ventana Carga de archivo, localice y seleccione la clave de licencia.
7. Pulse **Abrir**.
8. Pulse **Cargar**.

Resultados

La licencia se cargará en su consola de QRadar y se mostrará en la ventana Gestión del sistema y licencias. De forma predeterminada, la licencia no está asignada.

Qué hacer a continuación

"Asignación de una licencia a un sistema" en la página 49

Asignación de una licencia a un sistema

Asignar un licencia desde la ventana Gestión del sistema y licencias.

Acerca de esta tarea

Cuando se instala un sistema de QRadar, una clave de licencia predeterminada le proporciona acceso a la interfaz de usuario durante cinco semanas. Antes de que la licencia predeterminada caduque, debe asignar una clave de licencia al sistema. También puede añadir licencias para habilitar los productos de QRadar, como QRadar Vulnerability Manager.

Puede asignar varias licencias a un sistema. Por ejemplo, además de IBM Security QRadar SIEM, puede asignar IBM Security QRadar Risk Manager y IBM Security QRadar Vulnerability Manager a su sistema consola de QRadar.

A continuación se indican los estados de licencia de los sistemas QRadar:

- **No asignada**: la licencia no está asignada a un sistema.
- **No desplegada**: la licencia está asignada a un sistema pero el cambio de asignación no está desplegado. Esto significa que la licencia no está activa en el despliegue todavía.
- **Desplegada**: la licencia está asignada y activa en el despliegue.
- **Desbloqueada**: las licencias desplegadas en los últimos 10 días se pueden desbloquear. Este es el periodo de gracia predeterminado para volver a asignar una licencia. Una vez transcurrido el periodo de gracia, la licencia estará fijada (bloqueada) al sistema. Si tiene que desbloquear una licencia después de ese periodo, póngase en contacto con el servicio de soporte al cliente.
- **No válido**: la licencia no es válida y debe sustituirse. Este estado podría indicar que la licencia se ha modificado sin autorización.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Licencias**.
5. Seleccione una licencia no asignada.
6. Pulse **Asignar sistema a licencia**.
7. Opcional: Para filtrar la lista de licencias, escriba una palabra clave en el cuadro de búsqueda **Cargar licencia**.
8. En la lista de licencias, seleccione una licencia.
9. Seleccione un sistema.
10. Pulse **Asignar licencia a sistema**.

Revertir una asignación

Puede revertir una licencia asignada dentro del periodo de gracia de 14 días.

Acerca de esta tarea

Después de asignar una licencia a un sistema y antes de desplegar los cambios de configuración, puede deshacer la asignación de licencia. Al deshacer la asignación de licencia, se mantiene la última licencia asignada y desplegada en el sistema.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Licencias**.
5. Seleccione la licencia que desee revertir.
6. Pulse **Acciones** > **Revertir asignación**.

Visualización de los detalles de licencia

Una clave de licencia proporciona información y aplica obligatoriamente los límites y las prestaciones en un sistema de IBM Security QRadar.

Acerca de esta tarea

En la ventana Gestión del sistema y licencias puede ver los detalles de las licencias, como, por ejemplo, el número de orígenes de registro permitidos y las fechas de caducidad.

Nota: Si excede el límite de orígenes de anotaciones configurados, se visualiza un mensaje de error. Si los orígenes de registro se han descubierto de forma automática y se excede el límite, se inhabilitan automáticamente. Para ampliar el número de orígenes de registro, póngase en contacto con su representante de ventas.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Licencias**.
5. Para ver información de licencia para un host, seleccione el host y pulse **Acciones** > **Ver licencia**.

Qué hacer a continuación

En la ventana Licencias puede realizar las tareas siguientes:

- Pulse **Cargar licencia** para cargar una licencia. Consulte el apartado Carga de una clave de licencia.
- Pulse **Asignar licencia a sistema** en la barra de herramientas para asignar una licencia. Consulte Asignación de una licencia a un sistema.

Exportación de una licencia

Exporte la información de clave de licencias a un archivo externo en un sistema de escritorio.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Licencias**.
5. En el menú **Acciones**, seleccione **Exportar licencias**.

6. Seleccione una de las opciones siguientes:

   Abrir con
   Abre los datos de clave de licencia con la aplicación seleccionada.

   Guardar archivo
   Guarda el archivo en el escritorio.

7. Pulse **Aceptar**.

Gestión de sistemas

Utilice la ventana Gestión del sistema y licencias para gestionar los sistemas del despliegue.

Ver información del sistema, gestionar licencias, gestionar sistemas, reiniciar y concluir un sistema, añadir un host de alta disponibilidad, recopilar archivos de registro y completar otras actividades de gestión en el sistema.

Visualización de detalles del sistema y de licencia

Vea información sobre el sistema, incluidas las licencias de la ventana Detalles del sistema.

Acerca de esta tarea

Abra la ventana Detalles del sistema para ver información acerca del sistema y las licencias que se han asignado al sistema.

El panel Licencia visualiza los detalles siguientes para cada licencia asignada al sistema seleccionado:

Tabla 19. Parámetros de licencia

Parámetro	Descripción
Identidad de licencia	Nombre del producto de IBM Security QRadar que proporciona esta licencia.

Tabla 19. Parámetros de licencia (continuación)

Parámetro	Descripción
Estado de licencia	El estado de la licencia asignada a esta sistema puede ser uno de los siguientes: **No asignada**: la licencia no está asignada a un sistema. **No desplegada**: la licencia está asignada a un sistema pero el cambio de asignación no está desplegado. Esto significa que la licencia no está activa en el despliegue todavía. **Desplegada**: la licencia está asignada y activa en el despliegue. **Desbloqueada**: la licencia está desbloqueada. Las licencias desplegadas en los últimos 10 días se pueden desbloquear. Este es el periodo de gracia predeterminado para volver a asignar una licencia. Una vez transcurrido el periodo de gracia, la licencia estará fijada (bloqueada) al sistema. Si tiene que desbloquear una licencia después de ese periodo, póngase en contacto con el servicio de soporte al cliente. **No válido**: la licencia no es válida y debe sustituirse. Este estado podría indicar que la licencia se ha modificado sin autorización.
Tipo de dispositivo de licencia	Tipo de dispositivo asignado a esta licencia.
Fecha de caducidad de la licencia	Fecha de caducidad.
Límite de velocidad de sucesos	Velocidad máxima de sucesos permitida según los términos de la licencia.
Límite de velocidad de flujo	Velocidad máxima de flujo permitida según los términos de la licencia.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. Para visualizar los detalles del sistema, seleccione un host y pulse **Acciones** > **Ver y gestionar el sistema** o efectúe una doble pulsación sobre el host.
6. Pulse la pestaña **Licencia**.

Qué hacer a continuación

En el panel Licencia, puede completar las tareas siguientes:

- Seleccione una licencia y pulse **Ver licencia**. Consulte el apartado "Visualización de los detalles de licencia" en la página 46.
- Pulse **Cargar licencia** para cargar una licencia. Consulte el apartado "Carga de una clave de licencia" en la página 44.

- Pulse **Asignar licencia a sistema** en la barra de herramientas para asignar una licencia. Consulte Asignación de una licencia a un sistema.

Estado del sistema

En la vista Estado del sistema se muestran las notificaciones del sistema y la información de salud del host de IBM Security QRadar.

Seleccione el icono **Admin** > **Configuración del sistema** > **Estado del sistema** del área Configuración del sistema en la pestaña Admin para ver el uso de la CPU, las lecturas y escrituras de la red, las lecturas y escrituras de disco, el uso de memoria, los flujos por segundo (FPS) y los sucesos por segundo (EPS).

Pase el ratón sobre un gráfico para ver más información y la medida que se representa gráficamente.

Asignación de una licencia a un sistema

Después de obtener una licencia y cargarla, utilice los menús disponibles en la ventana Gestión del sistema y licencias para asignar una licencia.

Puede asignar varias licencias a un sistema. Por ejemplo, además de IBM Security QRadar SIEM, puede asignar IBM Security QRadar Risk Manager y IBM Security QRadar Vulnerability Manager a su sistema consola de QRadar.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. Seleccione un sistema disponible.
6. Pulse **Asignar licencia a sistema**.
7. Opcional: Para filtrar la lista de licencias, escriba una palabra clave en el cuadro de búsqueda **Cargar licencia**.
8. En la lista de licencias, seleccione una licencia.
9. Seleccione un sistema.
10. Pulse **Asignar licencia a sistema**.

Reinicio de un sistema

En el menú **Acciones** en la ventana Gestión del sistema y licencias puede reiniciar un sistema en su despliegue.

Acerca de esta tarea

La recopilación de datos se detiene mientras el sistema se está cerrando y reiniciando.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. Seleccione el sistema que desee reiniciar.

6. En el menú **Acciones**, seleccione **Reiniciar sistema**.

Cierre de un sistema

En el menú **Acciones** en la ventana Gestión del sistema y licencias puede concluir un sistema en su despliegue.

Acerca de esta tarea

La recopilación de datos se detiene mientras el sistema se está cerrando.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. Seleccione el sistema que desee cerrar.
6. En el menú **Acciones**, seleccione **Cerrar**.

Exportación de detalles del sistema

En el menú **Acciones** en la ventana Gestión del sistema y licencias puede exportar información de sistemas a un archivo externo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. En el menú **Acciones**, seleccione **Exportar sistemas**.
6. Seleccione una de las opciones siguientes:

   Abrir con
   Abre los datos de clave de licencia con la aplicación seleccionada.

   Guardar archivo
   Guarda el archivo en el escritorio.
7. Pulse **Aceptar**.

Recopilación de archivos de registro

Los archivos de registro de QRadar contienen información detallada sobre el despliegue, como nombres de host, direcciones IP y direcciones de correo electrónico. Si necesita ayuda para resolver problemas, puede recopilar los archivos de registro y enviarlos al servicio de soporte de IBM.

Acerca de esta tarea

Puede recopilar los archivos de registro de uno o más sistemas host al mismo tiempo. El tiempo que se necesita para recopilar los archivos de registro depende del tamaño del despliegue y del número de hosts que desee incluir en la recopilación de archivos de registro. Los archivos de registro de la consola de QRadar se incluyen automáticamente en cada recopilación de archivos de registro.

Puede seguir utilizando la consola de QRadar mientras se ejecuta la recopilación de archivos de registro. Si el sistema está recopilando activamente archivos de registro, no puede iniciar una solicitud de recopilación nueva. Debe cancelar el proceso de recopilación activo e iniciar otra recopilación.

Cuando el proceso de recopilación de archivos de registro finaliza, aparece una notificación del sistema en el panel de control **Supervisión del sistema**.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En la ventana de navegación, pulse **Configuración del sistema** y pulse el icono **Gestión del sistema y licencias**.
3. Pulse Control en el teclado y pulse cada host que desee incluir en la recopilación de archivos de registro.
4. Pulse **Acciones** > **Recopilar archivos de registro**.
5. Pulse **Opciones avanzadas** y elija las opciones para la recopilación de archivos de registro. Las recopilaciones de archivos de registro cifrados solamente las pueden descifrar el servicio de soporte de IBM. Si desea acceder a la recopilación de archivos de registro, no cifre el archivo.
6. Pulse **Recopilar archivos de registro**.
7. En **Mensajes de actividades de soporte del sistema**, un mensaje indica el estado del proceso de recopilación.

   Para cancelar un proceso de recopilación de archivos de registro activo, pulse la **X** del mensaje de notificación.
8. Para descargar la recopilación de archivos de registro, pulse **pulse aquí para descargar el archivo** en la notificación **La recopilación de archivos de registro se ha completado satisfactoriamente**.

Comprobación de la integridad de los registros de sucesos y flujo

Cuando el hashing de registro está habilitado, cualquier sistema que graba datos de sucesos y flujo crea archivos hash. Utilice estos archivos hash para verificar que los registros de suceso y flujo no se han modificado desde que se grabaron originalmente en el disco.

Los archivos hash se generan en la memoria antes de que los archivos se graben en el disco de modo que los registros de sucesos y flujo no se pueden alterar antes de que se generen los archivos hash

Antes de empezar

Asegúrese de que el hashing de registro está habilitado para el sistema QRadar. Para obtener información sobre la habilitación de los parámetros de hashing de registro de flujo o de hashing de registro de sucesos, consulte Configuración de los valores del sistema.

Acerca de esta tarea

Debe iniciar la sesión en el sistema que tiene el almacén de datos de sucesos y flujos y ejecutar un programa de utilidad para comprobar los registros. No puede comprobar la integridad del registro en la interfaz del visor de sucesos y flujo.

Esta tabla describe los parámetros utilizados con el programa de utilidad **check_ariel_integrity.sh**.

Tabla 20. Parámetros para el programa de utilidad **check_ariel_integrity.sh**

Parámetro	Descripción
-d	Duración en minutos de los datos del archivo de registro a explorar. El periodo de tiempo precede inmediatamente a la hora final especificada mediante el parámetro **-t**. Por ejemplo, si se especifica **-d 5**, se exploran todos los datos de registro recopilados cinco minutos antes de la hora final **-t**.
-n	La base de datos de QRadar a explorar. Las opciones válidas son `sucesos` y `flujos`.
-t	La hora final de la exploración. El formato de la hora final es `"aaaa/mm/dd hh:mm"` donde `hh` se especifica en formato de 24 horas. Si no se especifica ninguna hora final, se utiliza la hora actual.
-a	Algoritmo hash a utilizar. Este algoritmo debe ser el mismo que se utilizó para crear las claves de hash. Si no se especifica ningún algoritmo, se utiliza SHA-1.
-r	La ubicación del hashing de registro. Este argumento solo es necesario cuando el hashing de registro no está en la ubicación especificada en el archivo de configuración `/opt/qradar/conf/arielConfig.xml`.
-k	La clave utilizada para el cifrado Hash-based Message Authentication Code (HMAC). Si no especifica ninguna clave HMAC y el sistema está habilitado para el cifrado HMAC, el script **check_ariel_integrity.sh** toma de forma predeterminada la clave especificada en los valores del sistema.
-h	Muestra el mensaje de ayuda para el programa de utilidad de **check_ariel_integrity.sh**.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Para ejecutar el programa de utilidad, teclee el mandato siguiente:

   ```
   /opt/qradar/bin/check_ariel_integrity.sh -d <duración> -n <nombre de base de datos>
   [-t <hora final>] [-a <algoritmo hash>] [-r <directorio raíz de hash>] [-k <clave hmac>]
   ```

   Por ejemplo, para validar los últimos 10 minutos de datos de suceso, teclee el mandato siguiente:

   ```
   /opt/qradar/bin/check_ariel_integrity.sh -n events -d 10
   ```

Resultados

Si se devuelve un mensaje `ERROR` o `ANÓMALO`, la clave hash generada a partir de los datos actuales del disco no coincide con la clave hash creada cuando los datos se grabaron en el disco. O bien la clave, o bien los datos se han modificado.

Consideraciones de ancho de banda para hosts gestionados

Planifique el uso del ancho de banda para hosts gestionados en el despliegue de IBM Security QRadar.

Para replicar datos de estado y configuración, asegúrese de tener un ancho de banda mínimo de 100 Mbps entre la consola de QRadar y todos los hosts gestionados.

Es necesario un ancho de banda mayor cuando realiza búsquedas en la actividad de registro y de red, y si tiene más de 10.000 sucesos por segundo (Events Per Second, EPS). El rendimiento del sistema y de la red afectan a la velocidad de búsqueda de datos. Los Recopiladores de sucesos de QRadar, mediante la configuración de almacén y reenvío, reenvían todos los datos de acuerdo con la planificación definida por el usuario. Debe asignar ancho de banda suficiente para los datos que desee recopilar, de lo contrario, el dispositivo de almacén y reenvío no podrá mantener el ritmo planificado.

Puede utilizar los métodos siguientes para mitigar las limitaciones de ancho de banda entre centros de datos:

Procese y envíe los datos a hosts situados en el centro de datos primario
Diseñe el despliegue para procesar y enviar datos a hosts situados en el centro de datos primario, donde reside la consola, a medida que se recopilan los datos. En este diseño, todas las búsquedas basadas en el usuario buscan los datos en el centro de datos local, en lugar de esperar a que sitios remotos devuelvan datos. Puede desplegar un recopilador de sucesos de almacén y reenvío, como por ejemplo un dispositivo QRadar 15XX físico o virtual, en ubicaciones remotas para controlar ráfagas de datos en la red. El ancho de banda se utiliza en las ubicaciones remotas, y las búsquedas de datos tienen lugar en el centro de datos primario, y no en una ubicación remota.

No ejecute búsquedas de larga duración a través de conexiones con un ancho de banda limitado
Asegúrese de que los usuarios no ejecuten búsquedas de larga duración a través de enlaces que tienen un ancho de banda limitado. Las búsquedas que tienen filtros precisos limitan la cantidad de datos que se recuperan de las ubicaciones remotas y reducen la cantidad de ancho de banda que es necesaria para devolver los datos resultantes.

Despliegue de hosts gestionados y componentes después de la instalación

Después de la instalación puede añadir hosts gestionados al despliegue. Para facilitar la distribución de los procesos, puede añadir recopiladores de sucesos de QRadar, QRadar Procesadores de flujos u otros dispositivos al despliegue.

Acerca de esta tarea

Puede configurar los componentes, como los exploradores de vulnerabilidades, en un host gestionado.

Si ha configurado IBM Security QRadar Incident Forensics en el despliegue, puede añadir un host gestionado de QRadar Incident Forensics. Para obtener más información, consulte la publicación *IBM Security QRadar Incident Forensics Guía de instalación*.

Si ha configurado IBM Security QRadar Vulnerability Manager en el despliegue, puede añadir exploradores de vulnerabilidades y un procesador de vulnerabilidades. Para obtener más información, consulte la publicación *IBM Security QRadar Vulnerability Manager Guía del usuario*.

Si ha configurado IBM Security QRadar Risk Manager en el despliegue, puede añadir un host gestionado. Para obtener más información, consulte la publicación *IBM Security QRadar Risk Manager Installation Guide*.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel **Configuración del sistema**, pulse **Gestión del sistema y licencias**.
3. En la tabla de hosts, seleccione uno de los siguientes dispositivos que desee gestionar.
   - consola de QRadar
   - Host gestionado de QRadar
4. Opcional: Utilice el menú **Acciones de despliegue** para añadir y configurar los componentes de la instalación de software. Puede ver visualizaciones de su despliegue seleccionando **Acciones de despliegue** > **Ver despliegue** .

   Puede descargar una imagen `PNG` o un archivo `VDX` de Microsoft Visio (2010) de la visualización de despliegue desde la ventana **Vista de despliegue**.
5. En el menú **Acciones de despliegue**, seleccione una acción.
6. Especifique la información necesaria y seleccione las opciones adecuadas.
7. Cierre la ventana Gestión del sistema y licencias.
8. Pulse la pestaña **Admin**.
9. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Configuración de información del sistema

Para poner en funcionamiento el sistema de seguridad de QRadar o realizar el mantenimiento del sistema, debe configurar la consola de QRadar y los valores de sistema de los hosts gestionados desde la ventana Información del sistema.

Acerca de esta tarea

Puede asignar roles para las interfaces de red, gestionar licencias, configurar el servidor de correo electrónico que QRadar debe utilizar, y utilizar el cortafuegos local para gestionar el acceso de los dispositivos externos a QRadar.

Si necesita realizar cambios en la configuración de red, como por ejemplo un cambio de dirección IP, en la consola de QRadar y los sistemas host gestionados después de la instalación del despliegue de QRadar, utilice el programa de utilidad **qchange_netsetup**. Para obtener más información sobre los valores de red, consulte la guía del usuario de su producto.

Si cambia el parámetro **`External Flow Source Monitoring Port`** en la configuración de QFlow, también debe actualizar la configuración del acceso de cortafuegos.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Gestión del sistema y licencias**.
4. En el menú **Visualizar**, seleccione **Sistemas**.
5. Seleccione el host para el que desea configurar los valores de acceso de cortafuegos.
6. En el menú **Acciones**, pulse **Ver y gestionar el sistema**.

   Nota: Puede pulsar con el botón derecho sobre el host seleccionado para acceder a esta opción de menú o puede efectuar una doble pulsación sobre el host para abrir la ventana Información del sistema.

7. Para configurar el cortafuegos local para permitir el acceso a este host desde los dispositivos especificados externos al despliegue de QRadar, pulse la pestaña **Cortafuegos**.
   a. Configure el acceso para dispositivos que están fuera del despliegue y necesitan conectarse a este host.
   b. Acceda a esta regla pulsando la flecha.
8. Para configurar las interfaces de red en el sistema de QRadar, pulse la pestaña **Interfaces de red** .
   a. Seleccione una interfaz de red en la columna **Dispositivo**.
   b. Pulse **Editar**.
   c. Configure los parámetros.

   No puede editar una interfaz de red con un rol de gestión, cruce de alta disponibilidad o esclavo.
9. Para configurar un servidor de correo electrónico para la distribución de alertas, informes, notificaciones y mensajes de suceso, pulse la pestaña **Servidor de correo electrónico**.
   a. En el campo **Dirección de servidor de correo electrónico**, teclee el nombre host o la dirección IP del servidor de correo electrónico que desea utilizar.

      Si no tiene un servidor de correo electrónico y desea utilizar el servidor de correo electrónico proporcionado por QRadar, teclee `localhost` para utilizar proceso de correo electrónico local.

      Al configurar QRadar, éste busca un servidor de retransmisión de correo, que utiliza para enviar mensajes de correo electrónico. Por ejemplo, si desea enviar correo a *de@YourCompany.com*, debe configurar el valor **Servidor de correo electrónico** con un servidor de retransmisión de correo, que sabe cómo acceder a *YourCompany.com*.

      Si configura el valor del servidor de correo como `localhost`, los mensajes de correo no salen del marco de QRadar. Si desea entrega de correo externo, utilice un servidor de retransmisión de correo válido.

      Nota: es recomendable utilizar el puerto 25 para la conexión de servidor de correo electrónico.
10. Pulse **Guardar**.

Cambio de la contraseña de usuario root en la consola de QRadar

Como procedimiento de seguridad recomendado, cambie la contraseña de usuario root en consola de QRadar a intervalos regulares.

Procedimiento

1. Utilice SSH para iniciar la sesión en consola de QRadar como usuario root.
2. Escriba el nombre de usuario y la contraseña para el usuario root.

   El nombre de usuario y la contraseña son sensibles a las mayúsculas y minúsculas.
3. Utilice el mandato **`passwd`** para cambiar la contraseña.

Configuración de la hora del sistema de QRadar

Cuando ejecute un sistema que abarca varias zonas horarias, configure todos los dispositivos para que utilicen la misma zona horaria que la consola de IBM Security QRadar. Como alternativa, puede configurar todos los dispositivos, incluida la consola de QRadar, para que utilicen la hora media de Greenwich (GMT).

Utilice uno de los métodos siguientes para configurar la hora del sistema de IBM Security QRadar:

- Configure un servidor NTP (Network Time Protocol) para mantener la hora del sistema.

  La hora se sincroniza automáticamente entre la consola de QRadar y los hosts gestionados.
- Configure manualmente la hora del sistema.

Problemas ocasionados por discrepancia de zona horaria

Para asegurarse de que las búsquedas y las funciones relacionadas con datos funcionan adecuadamente, todos los dispositivos deben sincronizar los valores de hora con el dispositivo de consola de QRadar. Cuando los valores de zona horaria son discrepantes, verá resultados incoherentes entre las búsquedas de QRadar y los datos de informes.

El servicio de acumulador se ejecuta en todos los dispositivos con almacenamiento local para crear acumulaciones minuto a minuto y resúmenes cada hora y cada día. QRadar utiliza los datos acumulados en informes y en gráficos de series temporales. Cuando las zonas horarias son discrepantes en un despliegue distribuido, los gráficos de informe y de series temporales muestran resultados incoherentes cuando se comparan con los resultados de consultas de AQL debido a la forma en que se agregan los datos acumulados.

Las búsquedas de QRadar se ejecutan contra datos que se almacenan en las bases de datos de Ariel, que utilizan una estructura de fecha (AAAA/MM/DD/HH/MM) para almacenar archivos en el disco. Si la zona horaria cambia después de que los datos se hayan escrito en el disco, se interrumpe la secuencia de denominación de archivos en las bases de datos de Ariel, lo que puede provocar problemas de integridad.

Configuración manual de la hora del sistema en la IBM Security QRadar SIEM Console

Establezca manualmente la *hora del sistema* en la consola de QRadar y sincronícela con los hosts gestionados.

Acerca de esta tarea

Antes de ajustar manualmente la hora del sistema, detenga los servicios de QRadar y, a continuación utilice el mandato **date** para cambiar la hora y la fecha del sistema.

Procedimiento

1. Detenga los servicios de QRadar.

   ```
   service hostcontext stop
   service tomcat stop
   ```

```
service hostservices stop
```

2. Teclee el mandato **date** con los parámetros de hora.

   ```
   date <MMddhhmm><AAAA>
   ```

   Por ejemplo, si desea establecer la hora en 13 de diciembre, 2018, 17:24, teclee el mandato siguiente:

   ```
   date 121317242018
   ```

3. Sincronice el reloj del hardware para la hora actual.

   ```
   /sbin/hwclock --systohc
   ```

4. Reinicie los servicios de QRadar.

   ```
   service hostservices start
   service tomcat start
   service hostcontext start
   ```

5. Sincronice la hora de consola de QRadar con sus hosts gestionados de QRadar tecleando el mandato siguiente.

   ```
   /opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh
   ```

6. En la pestaña **Admin**, pulse **Avanzado** > **Desplegar configuración completa**, para reiniciar servicios en todos los hosts gestionados de QRadar.

   La hora queda sincronizada entre la consola de QRadar y los hosts gestionados.

   Para sincronizar su hora de consola de QRadar con un servidor de hora, debe habilitar los servicios de sincronización en su consola de QRadar.

Configuración del servidor de horas en la IBM Security QRadar SIEM Console

Habilite los servicios de sincronización horaria en la consola de QRadar y sincronice la hora con los hosts gestionados.

Procedimiento

1. Utilice SSH para iniciar la sesión en consola de QRadar como el usuario root.
2. Edite el archivo ntp.conf.

   ```
   vi /etc/ntp.conf
   ```

3. En la sección server del archivo ntp.conf, deje las entradas del servidor existentes o sustituirlas por su propio servidor NTP (protocolo de hora en red). Las entradas de servidor del archivo ntp.conf empiezan por 'server'.

   Puede utilizar servidores públicos de Proyecto NTP en (http://www.ntp.org/).

   ```
   server 0.rhel.pool.ntp.org iburst
   server 1.rhel.pool.ntp.org iburst
   server 2.rhel.pool.ntp.org iburst
   server 3.rhel.pool.ntp.org iburst
   ```

   Si utiliza servidores NTP públicos, compruebe que el cortafuegos permite las solicitudes NTP salientes.

4. Guarde los cambios y cierre el archivo.
5. Habilite el servicio ntpd para ejecutar en el nivel de ejecución 3.

   ```
   chkconfig --level 3 ntpd on
   ```

6. Verifique que el servicio ntpd está habilitado para ejecutarse durante el reinicio.

   ```
   chkconfig --list ntpd
   ```

   Verifique que 3:on se visualice en la salida.

```
ntpd 0:off 1:off 2:off 3:on 4:off 5:off 6:off
```

7. Para evitar que se produzcan errores de recopilación de datos cuando cambie la hora del sistema, detenga los servicios de QRadar.

   ```
   service hostcontext stop
   service tomcat stop
   service hostservices stop
   ```

8. Sincronice la hora con su servidor NTP.

   ```
   ntpdate <ntp.server.address>
   ```

9. Inicie el servicio `ntpd`.

   ```
   service ntpd start
   ```

10. Reinicie los servicios de QRadar.

    ```
    service hostservices start
    service tomcat start
    service hostcontext start
    ```

11. Sincronice la hora en todos los hosts gestionados con su consola de QRadar tecleando el mandato siguiente:

    ```
    /opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh
    ```

12. En la pestaña **Admin**, pulse **Avanzado** > **Desplegar configuración completa**, para reiniciar servicios en todos los hosts gestionados de QRadar.

    La hora queda sincronizada entre consola de QRadar y los hosts gestionados.

Capítulo 5. Configuración del origen de información de usuario

Configure el sistema de IBM Security QRadar para recopilar información de usuarios y grupos de los puntos finales de gestión de acceso e identidad.

IBM Security QRadar SIEM utiliza la información que se recopila de los puntos finales para enriquecer la información del usuario que está asociada con el tráfico y los sucesos que se producen en la red.

Visión general de los orígenes de información de usuario

Puede configurar un origen de información de usuario para habilitar la recopilación de información de usuario de un punto final de gestión de acceso e identidad.

Un punto final de gestión de acceso e identidad es un producto que recopila y gestiona las identidades de usuarios electrónicos, las pertenencias a grupo y los permisos de acceso. Estos puntos finales se denominan orígenes de información de usuario.

Utilice los programas de utilidad siguientes para configurar y gestionar los orígenes de información de usuario:

- **Tivoli Directory Integrator**: Debe instalar y configurar Tivoli Directory Integrator en un host que no sea de QRadar.
- **UISConfigUtil.sh**: Utilice este programa de utilidad para crear, recuperar, actualizar o suprimir orígenes de información de usuario. Puede utilizar orígenes de información de usuario para integrar QRadar SIEM utilizando un servidor de Tivoli Directory Integrator.
- **GetUserInfo.sh**: Utilice este programa de utilidad para recopilar información de usuario de un origen de información de usuario y almacenar la información en una recopilación de datos de referencia. Puede utilizar este programa de utilidad para recopilar información de usuario bajo demanda o según una planificación.

Orígenes de información de usuario

Un origen de información de usuario es un componente configurable que permite la comunicación con un punto final para recuperar información de usuarios y de grupos.

Los sistemas de QRadar dan soporte a los siguientes orígenes de información de usuario:

© Copyright IBM Corp. 2012, 2015

Tabla 21. Orígenes de información soportados.

Origen de información	Información que se recopila
Microsoft Windows Active Directory (AD), versión 2008: Microsoft Windows AD es un servicio de directorio que autentica y autoriza a todos los usuarios y sistemas que utilizan la red de Windows.	• full_name • user_name • user_principal_name • family_name • given_name • account_is_disabled • account_is_locked • password_is_expired • password_can_not_be_changed • no_password_expired • password_does_not_expire
IBM Security Access Manager (ISAM), versión 7.0: ISAM es una solución de autenticación y autorización para aplicaciones existentes, aplicaciones web corporativas y aplicaciones de cliente/servidor. Para obtener más información, consulte la documentación de IBM Security Access Manager (ISAM).	• name_in_rgy • first-name • last-name • account_valid • password_valid
IBM Security Identity Manager (ISIM), versión 6.0: ISIM proporciona el software y los servicios necesarios para desplegar soluciones de suministro basadas en políticas. Este producto automatiza el proceso de suministro de empleados, contratistas y Business Partners de IBM con derechos de acceso a las aplicaciones que necesitan, ya sea en un entorno empresarial cerrado o a través de una empresa virtual o ampliada. Para obtener más información, consulte la documentación de IBM Security Integration Manager (ISIM).	• Nombre completo • DN

Recopilaciones de datos de referencia para la información de usuario

En este tema se proporciona información sobre cómo las recopilaciones de datos de referencia almacenan los datos recopilados de los orígenes de información de usuario.

Cuando QRadar SIEM recopila información de un origen de información de usuario, crea de forma automática una recopilación de datos de referencia para almacenar la información. El nombre de la recopilación de datos de referencia se deriva del nombre del grupo de origen de información de usuario. Por ejemplo, una recopilación de datos de referencia que se recopile desde Microsoft Windows AD puede llamarse Domain Admins.

El tipo de recopilación de datos de referencia es un correlación de correlaciones. En una correlación de referencia de correlaciones, los datos se almacenan en registros que correlacionan una clave con otra clave, que a su vez se correlaciona con un solo valor.

Por ejemplo:

- `#`
- `# Domain Admins`
- `# key1,key2,data`
- `smith_j,Full Name,John Smith`
- `smith_j,account_is_disabled,0`
- `smith_j,account_is_locked`
- `smith_j,password_does_not_expire,1`

Para obtener más información sobre las recopilaciones de datos de referencia, consulte la nota técnica referente a las recopilaciones de datos de referencia (*Reference Data Collections Technical Note*).

Ejemplo de flujo de trabajo de integración

Después de que la información de usuarios y grupos se haya recopilado y almacenado en una recopilación de datos de referencia, hay muchas formas en las que puede utilizar los datos en IBM Security QRadar SIEM.

Puede crear alertas e informes significativos que muestren el cumplimiento de las políticas de seguridad de la compañía por parte del usuario.

Observe el ejemplo siguiente:

Para asegurarse de que las actividades realizadas por usuarios de ISIM con privilegios cumplen las políticas de seguridad, puede realizar las tareas siguientes:

Cree un origen de registro para recopilar y analizar los datos de auditoría correspondientes a cada servidor de ISIM cuyos registros se han recopilado. Para obtener más información sobre la creación de un origen de registro, consulte la publicación *Managing Log Sources Guide*.

1. Cree un origen de información de usuario para el servidor de ISIM y recopile la información del grupo de usuarios ISIM Administrators. Este paso crea una recopilación de datos de referencia que se llama ISIM Administrators. Consulte el apartado "Creación de un origen de información de usuario" en la página 65.
2. Configure un componente básico para comprobar si hay sucesos en los que la dirección IP de origen es el servidor de ISIM y el nombre de usuario figura en la recopilación de datos de referencia de administrador de ISIM. Para obtener más información sobre los componentes básicos, consulte la guía del usuario de su producto.
3. Cree una búsqueda de sucesos que utilice el componente básico personalizado como filtro. Para obtener más información sobre las búsquedas de sucesos, consulte la guía del usuario de su producto.
4. Cree un informe personalizado que utilice la búsqueda de sucesos personalizada para generar informes diarios sobre la actividad de auditoría de los usuarios de ISIM con privilegios. Estos informes generados indican si alguna actividad de administrador de ISIM infringe la política de seguridad. Para obtener más información sobre los informes, consulte la guía del usuario de su producto.

Nota: Si desea recopilar registros de seguridad de aplicaciones, debe crear un módulo de soporte de dispositivo (DSM). Para obtener más información, consulte la publicación *IBM Security QRadar DSM Configuration Guide*.

Visión general de las tareas de gestión y configuración del origen de información de usuario

Para integrar inicialmente los orígenes de información de usuario, debe realizar las tareas siguientes:

1. Configure un servidor de Tivoli Directory Integrator. Consulte el apartado "Configuración del servidor de Tivoli Directory Integrator".
2. Cree y gestione los orígenes de información de usuario. Consulte el apartado "Creación y gestión de un origen de información de usuario" en la página 64.
3. Recopile la información de usuario. Consulte el apartado "Recopilación de información de usuario" en la página 67.

Configuración del servidor de Tivoli Directory Integrator

Para que IBM Security QRadar se integre con los orígenes de información de usuario, debe instalar y configurar Tivoli Directory Integrator en un host que no sea de QRadar.

Acerca de esta tarea

No se necesita configuración alguna en el sistema; sin embargo, debe acceder a la consola para obtener el archivo `QRadarIAM_TDI.zip`. A continuación, instale y configure un servidor de Tivoli Directory Integrator en un host independiente. Si es necesario, también debe crear e importar un certificado autofirmado.

Cuando se extrae el archivo `QRadarIAM_TDI.zip` en el servidor de Tivoli Directory Integrator, el directorio TDI se crea automáticamente. El directorio TDI incluye los siguientes archivos:

- QradarIAM.sh, que es el script de inicio de TDI para Linux
- QradarIAM.bat, que es el script de inicio de TDI para Microsoft Windows
- QradarIAM.xml, que es el script xml de TDI y se debe almacenar en la misma ubicación que el archivo QradarIAM.properties
- QradarIAM.properties, que es el archivo de propiedades del script xml de TDI

Cuando instale Tivoli Directory Integrator, debe configurar un nombre para el directorio de soluciones. Esta tarea requiere que acceda al directorio de soluciones. Por lo tanto, en los pasos de la tarea, `<directorio_soluciones>` hace referencia al nombre que ha dado al directorio.

Se utilizan los parámetros siguientes para crear e importar certificados:

Tabla 22. Parámetros de configuración de certificación

Parámetro	Descripción
<dirección_ip_servidor>	Define la dirección IP del servidor de Tivoli Directory Integrator.
<días_validez>	Define el número de días que el certificado es válido.
<archivo_almacén_claves>	Define el nombre del archivo de almacén de claves.
-storepass <contraseña>	Define la contraseña del almacén de claves.
- keypass <contraseña>	Define la contraseña para el par de claves pública/privada.

Tabla 22. Parámetros de configuración de certificación (continuación)

Parámetro	Descripción
<alias>	Define el alias para un certificado exportado.
<archivo_certificado>	Define el nombre de archivo del certificado.

Procedimiento

1. Instale Tivoli Directory Integrator en un host que no sea de QRadar. Para obtener más información sobre cómo instalar y configurar Tivoli Directory Integrator, consulte la documentación de Tivoli Directory Integrator (TDI).
2. Inicie, mediante SSH, la sesión en la consola como usuario root.
   a. Nombre de usuario: `root`
   b. Contraseña: `<contraseña>`
3. Copie el archivo `QRadarIAM_TDI.zip` en el servidor de Tivoli Directory Integrator.
4. En el servidor de Tivoli Directory Integrator, extraiga el archivo `QRadarIAM_TDI.zip` en el directorio de soluciones.
5. Configure el servidor de Tivoli Directory Integrator para la integración con QRadar.
   a. Abra el archivo `<directorio_soluciones>/solution.properties` de Tivoli Directory Integrator.
   b. Quite la marca de comentario de la propiedad com.ibm.di.server.autoload. Si ya se ha quitado la marca de comentario de esta propiedad, anote el valor de la propiedad.
   c. Seleccione una de las opciones siguientes:
      - Cambie los directorios por el directorio autoload.tdi, que contiene la propiedad com.ibm.di.server.autoload de forma predeterminada.
      - Cree un directorio autoload.tdi en el <directorio_soluciones> para almacenar la propiedad com.ibm.di.server.autoload.
   d. Mueva los archivos TDI/QRadarIAM.xml y TDI/QRadarIAM.property del directorio de Tivoli Directory Integrator al directorio <directorio_soluciones>/autoload.tdi o al directorio que ha creado en el paso anterior.
   e. Mueva los scripts `QradarIAM.bat` y `QradarIAM.sh` del directorio de Tivoli Directory Integrator a la ubicación desde la que desea iniciar Tivoli Directory Integrator.
6. Si se requiere la autenticación basada en certificados para que el sistema se autentique en el servidor de Tivoli Directory Integrator, seleccione una de las opciones siguientes:
   - Para crear e importar un certificado autofirmado, consulte el paso 7.
   - Para importar un certificado de autoridad emisora de certificados, consulte el paso 8.
7. Cree el certificado autofirmado e impórtelo al almacén de confianza de Tivoli Directory Integrator.
   a. Para generar un almacén de claves y un par de claves privada/pública, escriba el mandato siguiente:
      - `keytool -genkey -dname cn=<dirección_ip_servidor> -validity <días_validez> -keystore <archivo_almacén_claves> -storepass <contraseña> - keypass <contraseña>`

- Por ejemplo, `keytool -genkey -dname cn=192.168.1.1 -validity 365 -keystore server.jks -storepass secret -keypass secret`

b. Para exportar el certificado del almacén de claves, escriba el mandato siguiente:
   - `keytool -export -alias <alias> -file <archivo_certificado> -keystore <archivo_almacén_claves> - storepass <contraseña>`
   - Por ejemplo, `keytool -export -alias mykey -file server.cert -keystore server.jks -storepass secret`

c. Para importar el certificado primario al almacén de claves como certificado de autoridad emisora de certificados, escriba el mandato siguiente:
   - `keytool -import -trustcacerts -file <archivo_certificado> -keystore <archivo_almacén_claves> -storepass <contraseña> -alias <alias>.`
   - Por ejemplo, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`

d. Copie el archivo de certificado en `/opt/qradar/conf/trusted_certificates`, en consola de QRadar.

8. Importe el certificado de autoridad emisora de certificados al almacén de confianza de Tivoli Directory Integrator.

   a. Para importar el certificado de autoridad emisora de certificados al almacén de claves como certificado de autoridad emisora de certificados autofirmado, escriba el mandato siguiente:
      - `keytool -import -trustcacerts -file <archivo_certificado> -keystore <archivo_almacén_claves> -storepass <contraseña> -alias <alias>.`
      - Por ejemplo, `keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey`

   b. Copie el archivo de certificado de autoridad emisora de certificados en `/opt/qradar/conf/trusted_certificates`, en consola de QRadar.

9. Edite el archivo <directorio_soluciones>/solution.properties para quitar la marca de comentario de las propiedades siguientes y configurarlas:
   - javax.net.ssl.trustStore=<archivo_almacén_claves>
   - {protect}-javax.net.ssl.trustStorePassword=<contraseña>
   - javax.net.ssl.keyStore=<archivo_almacén_claves>
   - {protect}-javax.net.ssl.keyStorePassword=<contraseña>

   Nota: La contraseña actual no modificada predeterminada podría visualizarse en el formato siguiente: {encr}EyHbak. Escriba la contraseña como texto sin formato. La contraseña se cifra la primera vez que se inicia Tivoli Directory Integrator.

10. Utilice uno de los siguientes scripts para iniciar Tivoli Directory Integrator:
    - QradarIAM.sh para Linux
    - QradarIAM.bat para Microsoft Windows

Creación y gestión de un origen de información de usuario

Utilice el programa de utilidad UISConfigUtil para crear, recuperar, actualizar o suprimir orígenes de información de usuario.

Creación de un origen de información de usuario

Utilice el programa de utilidad UISConfigUtil para crear un origen de información de usuario.

Antes de empezar

Antes de crear un origen de información de usuario, debe instalar y configurar el servidor de Tivoli Directory Integrator. Para obtener más información, consulte el apartado "Configuración del servidor de Tivoli Directory Integrator" en la página 62.

Acerca de esta tarea

Cuando cree un origen de información de usuario, debe identificar los valores de propiedad necesarios para configurar el origen de información de usuario. En la tabla siguiente se describen los valores de propiedad soportados:

Tabla 23. Valores de propiedad de interfaz de usuario soportados

Propiedad	Descripción
tdiserver	Define el nombre de host del servidor de Tivoli Directory Integrator.
tdiport	Define el puerto de escucha del conector HTTP en el servidor de Tivoli Directory Integrator.
hostname	Define el nombre del host de origen de información de usuario.
port	Define el puerto de escucha para el registro de gestión de acceso e identidad en el host de información de usuario.
username	Define el nombre de usuario que QRadar SIEM utiliza para la autenticación con el registro de gestión de acceso e identidad.
password	Define la contraseña que se necesita para la autenticación con el registro de gestión de acceso e identidad.
searchbase	Define el DN base.
searchfilter	Define el filtro de búsqueda que se necesita para filtrar la información de usuario que se recupera del registro de gestión de acceso e identidad.

Procedimiento

1. Inicie, mediante SSH, la sesión en la consola como usuario root.
   a. Nombre de usuario: `root`
   b. Contraseña: `<contraseña>`
2. Para añadir un origen de información de usuario, escriba el mandato siguiente:
   `UISConfigUtil.sh add <nombre> -t <AD|ISAM|ISIM|ISFIM> [-d descripción] [-p prop1=valor1,prop2=valor2...,propn=valorn]`

   Donde:

   - `<nombre>` es el nombre del origen de información de usuario que desea añadir.

- <AD|ISAM|ISIM|ISFIM> indica el tipo de origen de información de usuario.
- [-d descripción] es una descripción del origen de información de usuario. Este parámetro es opcional.
- [-p prop1=valor1,prop2=valor2,...,propn=valorn] identifica los valores de propiedad necesarios para el origen de información de usuario. Para obtener más información sobre los parámetros soportados, consulte el apartado "Creación de un origen de información de usuario" en la página 65.

Por ejemplo:

- /UISConfigUtil.sh add "UIS_ISIM" -t ISIM -d "UIS for ISIM" -p "tdiserver=nc9053113023.tivlab.austin.ibm.com,tdiport=8080, hostname=vmibm7094.ottawa.ibm.com,port=389, username=cn=root,password=password,\"searchbase=ou=org,DC=COM\",\ "searchfilter=(|(objectClass=erPersonItem)(objectClass=erBPPersonItem) (objectClass=erSystemUser))\""

Recuperación de orígenes de información de usuario

Utilice el programa de utilidad UISConfigUtil para recuperar orígenes de información de usuario.

Procedimiento

1. Inicie, mediante SSH, la sesión en la consola como usuario root.
   a. Nombre de usuario: root
   b. Contraseña: <contraseña>
2. Seleccione una de las opciones siguientes:
   a. Escriba el mandato siguiente para recuperar todos los orígenes de información de usuario: UISConfigUtil.sh get <nombre>
   b. Escriba el mandato siguiente para recuperar un origen de información de usuario determinado:UISConfigUtil.sh get <nombre>

      Siendo <nombre> el nombre del origen de información de usuario que desea recuperar.

      Por ejemplo:

      [root@vmibm7089 bin]# .UISConfigUtil.sh get "UIS_AD"

Edición de un origen de información de usuario

Utilice el programa de utilidad UISConfigUtil para editar un origen de información de usuario.

Procedimiento

1. Inicie, mediante SSH, la sesión en la consola como usuario root.
   a. Nombre de usuario: root
   b. Contraseña: <contraseña>
2. Escriba el mandato siguiente para editar un origen de información de usuario: UISConfigUtil.sh update <nombre> -t <AD|ISAM|ISIM|ISFIM> [-d descripción] [-p prop1=valor1,prop2=valor2...,propn=valorn]

   Donde:

   - <nombre> es el nombre del origen de información de usuario que desea editar.
   - <AD|ISAM|ISIM|ISFIM> indica el tipo de origen de información de usuario. Para actualizar este parámetro, escriba un nuevo valor.

- `[-d descripción]` es una descripción del origen de información de usuario. Este parámetro es opcional. Para actualizar este parámetro, escriba una nueva descripción.
- `[-p prop1=valor1,prop2=valor2,...,propn=valorn]` identifica los valores de propiedad necesarios para el origen de información de usuario. Para actualizar este parámetro, especifique `propiedades nuevas`. Para obtener más información sobre los parámetros soportados, consulte el apartado "Creación de un origen de información de usuario" en la página 65.

Por ejemplo:

```
./UISConfigUtil.sh update "UIS_AD_update" -t AD -d "UIS for AD" -p
"searchbase=DC=local"
```

Supresión de un origen de información de usuario

Utilice el programa de utilidad UISConfigUtil para suprimir un origen de información de usuario.

Procedimiento

1. Inicie, mediante SSH, la sesión en la consola como usuario root.
   a. Nombre de usuario: `root`
   b. Contraseña: `<contraseña>`
2. Escriba el mandato siguiente para suprimir un origen de información de usuario:

   ```
   UISConfigUtil.sh delete <nombre>
   ```

   Siendo `<nombre>` el nombre del origen de información de usuario que desea suprimir.

Qué hacer a continuación

La información de usuario recopilada se almacena en una recopilación de datos de referencia en la base de datos de IBM Security QRadar. Si no existe ninguna recopilación de datos de referencia, se crea una nueva. Si ya se había creado anteriormente una recopilación de datos para este origen de información de usuario, se borran los datos anteriores de la correlación de referencia y se almacena la nueva información de usuario. Para obtener más información sobre las recopilaciones de datos de referencia, consulte el apartado Recopilaciones de datos de referencia.

Recopilación de información de usuario

Utilice el programa de utilidad GetUserInfo para recopilar información de usuario de los orígenes de información de usuario y almacenar los datos en una recopilación de datos de referencia.

Acerca de esta tarea

Utilice esta tarea para recopilar información de usuario bajo demanda. Si desea crear la recopilación de información de usuario automática según una planificación, cree una entrada de trabajo cron. Para obtener más información sobre los trabajos cron, consulte la documentación de Linux.

Procedimiento

1. Inicie, mediante SSH, la sesión en la consola como usuario root.
   a. Nombre de usuario: `root`

b. <contraseña>

2. Escriba el mandato siguiente para recopilar información de usuario bajo demanda:

   GetUserInfo.sh <nombre_OIU>

   Siendo <nombre_OIU> el nombre del origen de información de usuario del que desea recopilar información.

Qué hacer a continuación

La información de usuario recopilada se almacena en una recopilación de datos de referencia en la base de datos. Si no existe ninguna recopilación de datos de referencia, se crea una nueva. Si ya se había creado anteriormente una recopilación de datos para este origen de información de usuario, se borran los datos anteriores de la correlación de referencia y se almacena la nueva información de usuario. Para obtener más información sobre las recopilaciones de datos de referencia, consulte el apartado "Recopilaciones de datos de referencia para la información de usuario" en la página 60.

Capítulo 6. Configurar QRadar

Utilice las características de la pestaña **Admin** para configurar IBM Security QRadar SIEM.

Puede configurar la jerarquía de red, las actualizaciones automáticas, los valores del sistema, los grupos de retención de sucesos y flujos, las notificaciones del sistema, los valores de la consola, las razones de cierre de los delitos y la gestión de índices.

Jerarquía de red

QRadar utiliza la jerarquía de red para comprender el tráfico de red y proporcionarle la capacidad de ver la actividad de todo el despliegue.

Cuando cree la jerarquía de red, considere el método más eficaz para ver la actividad de red. No es necesario que la jerarquía de red se parezca al despliegue físico de la red. QRadar da soporte a cualquier jerarquía de red que pueda definirse mediante un rango de direcciones IP. Puede basar la red en muchas variables diferentes, incluidas las unidades de negocio o geográficas.

Al definir la jerarquía de red, debe tener en cuenta los sistemas, los usuarios y los servidores que se pueden agrupar.

Puede agrupar sistemas y grupos de usuarios que tienen un comportamiento similar. Sin embargo, no debe agrupar con otros servidores en la red un servidor que tenga un comportamiento exclusivo. La colocación de un servidor exclusivo sin otros servidores le da mayor visibilidad en QRadar, y se puede gestionar políticas específicas.

Dentro de un grupo, puede colocar servidores con grandes volúmenes de tráfico, como los servidores de correo, en la parte superior del grupo. Esta jerarquía le proporciona una representación visual cuando se produce una discrepancia.

Si el despliegue procesa más de 600.000 flujos, puede crear varios grupos de nivel superior.

Puede organizar los sistemas y las redes por rol o por patrones de tráfico similares. Por ejemplo, los servidores de correo, los usuarios de los departamentos, los laboratorios o los grupos de desarrollo. Con esta organización, puede diferenciar el comportamiento de red y aplicar políticas de seguridad de gestión de red.

Los grupos de red grandes pueden provocar problemas cuando se ve la información detallada de cada objeto. No configure un grupo de red con más de 15 objetos.

Combine varios CIDR (direccionamiento entre dominios sin uso de clases) o varias subredes en un solo grupo de red para ahorrar espacio en disco. Por ejemplo:

Tabla 24. Ejemplo de varios CIDR y subredes en un solo grupo de red

Grupo	Descripción	Direcciones IP
1	Marketing	10.10.5.0/24

© Copyright IBM Corp. 2012, 2015

Tabla 24. Ejemplo de varios CIDR y subredes en un solo grupo de red (continuación)

Grupo	Descripción	Direcciones IP
2	Ventas	10.10.8.0/21
3	Clúster de base de datos	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32

Añada los servidores clave como objetos individuales y agrupe otros servidores importantes pero relacionados en objetos de varios CIDR.

Defina un grupo integral que lo incluya todo para que, cuando defina nuevas redes, se apliquen las políticas adecuadas y los supervisores de comportamiento. Por ejemplo:

Tabla 25. Ejemplo de un grupo integral

Grupo	Subgrupo	Dirección IP
Cleveland	Varios - Cleveland	10.10.0.0/16
Cleveland	Ventas - Cleveland	10.10.8.0/21
Cleveland	Marketing - Cleveland	10.10.1.0/24

Si añade una red al ejemplo, como 10.10.50.0/24, que es un departamento de recursos humanos, el tráfico se visualiza como basado en Cleveland y se aplican de forma predeterminada las reglas que se aplican al grupo Cleveland.

Conceptos relacionados:

"Actualizaciones de la jerarquía de red en un despliegue multiarrendatario" en la página 207

Los administradores de arrendatarios que tienen el permiso **Definir jerarquía de red** pueden cambiar la jerarquía de red dentro de su propio arrendatario, pero para desplegar los cambios, deben ponerse en contacto con el administrador de proveedor de servicios de seguridad gestionados (MSSP). Los administradores de MSSP pueden planificar el despliegue durante una interrupción planificada, e informar a todos los administradores de arrendatarios de antemano.

Valores de CIDR aceptables

QRadar acepta valores de CIDR específicos.

En la tabla siguiente se proporciona una lista de los valores de CIDR que QRadar acepta:

Tabla 26. Valores de CIDR aceptables

Longitud de CIDR	Máscara	Número de redes	Hosts
/1	128.0.0.0	128 A	2,147,483,392
/2	192.0.0.0	64 A	1,073,741,696
/3	224.0.0.0	32 A	536,870,848
/4	240.0.0.0	16 A	268,435,424
/5	248.0.0.0	8 A	134,217,712
/6	252.0.0.0	4 A	67,108,856

Tabla 26. Valores de CIDR aceptables (continuación)

Longitud de CIDR	Máscara	Número de redes	Hosts
/7	254.0.0.0	2 A	33,554,428
/8	255.0.0.0	1 A	16,777,214
/9	255.128.0.0	128 B	8,388,352
/10	255.192.0.0	64 B	4,194,176
/11	255.224.0.0	32 B	2,097,088
/12	255.240.0.0	16 B	1,048,544
/13	255.248.0.0	8 B	524,272
/14	255.252.0.0	4 B	262,136
/15	255.254.0.0	2 B	131,068
/16	255.255.0.0	1 B	65,534
/17	255.255.128.0	128 C	32,512
/18	255.255.192.0	64 C	16,256
/19	255.255.224.0	32 C	8,128
/20	255.255.240.0	16 C	4,064
/21	255.255.248.0	8 C	2,032
/22	255.255.252.0	4 C	1,016
/23	255.255.254.0	2 C	508
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 subredes	124
/26	255.255.255.192	4 subredes	62
/27	255.255.255.224	8 subredes	30
/28	255.255.255.240	16 subredes	14
/29	255.255.255.248	32 subredes	6
/30	255.255.255.252	64 subredes	2
/31	255.255.255.254	ninguno	ninguno
/32	255.255.255.255	1/256 C	1

Por ejemplo, una red se llama superred cuando el límite de prefijo contiene menos bits que la máscara natural (o con clases, "classful") de la red. Por ejemplo, una red se llama subred cuando el límite de prefijo contiene más bits que la máscara natural de la red:

- 209.60.128.0 es una dirección de red de clase C con una máscara de /24.
- 209.60.128.0 /22 es un superred que produce:
  - 209.60.128.0 /24
  - 209.60.129.0 /24
  - 209.60.130.0 /24
  - 209.60.131.0 /24
- 192.0.0.0 /25

  Rango de hosts de subred

  0 192.0.0.1-192.0.0.126

  1 192.0.0.129-192.0.0.254

- 192.0.0.0 /26

  Rango de hosts de subred

  0 192.0.0.1 - 192.0.0.62

  1 192.0.0.65 - 192.0.0.126

  2 192.0.0.129 - 192.0.0.190

  3 192.0.0.193 - 192.0.0.254
- 192.0.0.0 /27

  Rango de hosts de subred

  0 192.0.0.1 - 192.0.0.30

  1 192.0.0.33 - 192.0.0.62

  2 192.0.0.65 - 192.0.0.94

  3 192.0.0.97 - 192.0.0.126

  4 192.0.0.129 - 192.0.0.158

  5 192.0.0.161 - 192.0.0.190

  6 192.0.0.193 - 192.0.0.222

  7 192.0.0.225 - 192.0.0.254

Tareas relacionadas:

"Definición de la jerarquía de red"
QRadar considera todas las redes de la jerarquía de red como locales. Mantenga actualizada la jerarquía de red para evitar falsos delitos.

Definición de la jerarquía de red

QRadar considera todas las redes de la jerarquía de red como locales. Mantenga actualizada la jerarquía de red para evitar falsos delitos.

Acerca de esta tarea

Los objetos de red son un contenedor para direcciones CIDR. Cualquier dirección IP cubierta por un rango CIDR en la jerarquía de red se considera una dirección local. Cualquier dirección IP que no está definida en un rango CIDR de objetos de red se considera una dirección IP remota. Un CIDR solo puede pertenecer a un objeto de red aunque subconjuntos de un rango de CIDR pueden pertenecer a otro objeto de red. El tráfico de red coincide con el CIDR más exacto. Un objeto de red puede tener varios rangos de CIDR asignados.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Jerarquía de red**.
4. En el árbol de menús de la ventana Vistas de red, seleccione el área de la red en la que desea trabajar.
5. Para añadir objetos de red, siga estos pasos:
   a. Pulse **Añadir** y escriba un nombre exclusivo y una descripción para el objeto.
   b. En la lista **Grupo**, seleccione el grupo en el que desea añadir el nuevo objeto de red.
   c. Para añadir un grupo, pulse el icono situado junto a la lista **Grupo** y escriba un nombre para el grupo.
   d. Escriba el rango CIDR de este objeto y pulse **Añadir**.

e. Pulse **Crear**.

f. Repita los pasos para todos los objetos de red.

6. Pulse **Editar** o **Suprimir** para trabajar con los objetos de red existentes.

Conceptos relacionados:

"Valores de CIDR aceptables" en la página 70
QRadar acepta valores de CIDR específicos.

Actualizaciones automáticas

Puede actualizar automática o manualmente los archivos de configuración para asegurarse de que los archivos de configuración contienen la información de seguridad de red más reciente.

QRadar utiliza archivos de configuración del sistema para proporcionar caracterizaciones útiles de los flujos de datos de red.

Requisitos de actualización automática

La consola debe estar conectada a Internet para recibir actualizaciones. Si la consola no está conectada a Internet, debe configurar un servidor de actualizaciones interno para que la consola descargue los archivos de él.

Hay archivos de actualización disponibles para su descarga manual en el sitio web siguiente:

IBM Fix Central (http://www.ibm.com/support/fixcentral).

Para mantener la integridad de la información y la configuración actual, sustituya los archivos de configuración existentes o integre los archivos actualizados con los archivos existentes.

Después de instalar actualizaciones en la consola y desplegar los cambios, la consola actualiza sus hosts gestionados si el despliegue está definido en el editor de despliegue. Para obtener más información sobre el editor de despliegue, consulte el Capítulo 11, "Editor de despliegue", en la página 137.

Descripción de las actualizaciones

Los archivos de actualización pueden incluir las actualizaciones siguientes:

- Actualizaciones de configuración, que incluyen cambios en el archivo de configuración, vulnerabilidad, correlación QID, y actualizaciones de información sobre amenazas de seguridad.
- Actualizaciones de DSM, que incluyen correcciones para problemas de análisis, cambios de escáner y actualizaciones de protocolo.
- Actualizaciones importantes, que incluyen elementos tales como archivos JAR actualizados.
- Actualizaciones secundarias, que incluyen elementos tales como contenido adicional de la ayuda en línea o scripts actualizados.

Frecuencia de las actualizaciones automáticas para las instalaciones nuevas y las actualizaciones

La frecuencia predeterminada de la actualización automática está determinada por el tipo de instalación y la versión de QRadar.

- Si actualiza desde versiones de QRadaranteriores a la versión 7.2, el valor de la frecuencia de actualización seguirá siendo el mismo después de la actualización. De forma predeterminada, la actualización se establece en semanal, pero puede cambiar manualmente la frecuencia.
- Si instala una instalación nueva de QRadar V7.2 o versiones posteriores, la frecuencia predeterminada de la actualización es diaria. Puede cambiar manualmente la frecuencia.

Conceptos relacionados:

"Configurar un servidor de actualizaciones de QRadar" en la página 79
Si el despliegue incluye una consola de QRadar que no puede acceder a Internet o si desea gestionar manualmente las actualizaciones del sistema, puede configurar un servidor de actualizaciones de QRadar para gestionar el proceso de actualización.

Visualización de actualizaciones pendientes

El sistema está preconfigurado para las actualizaciones automáticas semanales. Puede ver las actualizaciones pendientes en la ventana Actualizaciones.

Acerca de esta tarea

El sistema tiene que estar operativo durante suficiente tiempo para recuperar las actualizaciones semanales. Si no aparece ninguna actualización en la ventana Actualizaciones, el sistema no ha estado en funcionamiento el tiempo suficiente para recuperar las actualizaciones semanales o bien no se han emitido actualizaciones. Si esto ocurre, puede comprobar manualmente si hay actualizaciones nuevas. Para obtener más información sobre la comprobación de la existencia de actualizaciones nuevas, consulte el apartado "Cómo comprobar si hay nuevas actualizaciones" en la página 78.

La barra de herramientas **Comprobar si hay actualizaciones** proporciona las funciones siguientes:

Tabla 27. Funciones de la barra de herramientas Comprobar si hay actualizaciones

Función	Descripción
Ocultar	Seleccione una o varias actualizaciones y luego pulse **Ocultar** para eliminar las actualizaciones seleccionadas de la página Comprobar si hay actualizaciones. En la página Restaurar actualizaciones ocultas pueden verse y restaurarse las actualizaciones ocultas. Para obtener más información, consulte el apartado "Restauración de actualizaciones ocultas" en la página 79.
Instalar	Puede instalar las actualizaciones manualmente. Cuando instale las actualizaciones manualmente, el proceso de instalación se inicia al cabo de un minuto. Para obtener más información, consulte el apartado "Instalación manual de actualizaciones automáticas" en la página 78.

Tabla 27. Funciones de la barra de herramientas Comprobar si hay actualizaciones (continuación)

Función	Descripción
Planificar	Puede configurar una fecha y hora específicas para instalar manualmente las actualizaciones seleccionadas en la consola. La planificación es útil cuando desea planificar la instalación de las actualizaciones durante las horas de menor actividad. Para obtener más información, consulte el apartado "Planificación de una actualización" en la página 77.
Anular planificación	Puede eliminar las planificaciones preconfiguradas para instalar manualmente las actualizaciones en la consola. Para obtener más información, consulte el apartado "Planificación de una actualización" en la página 77.
Buscar por nombre	Puede localizar una actualización concreta por nombre.
Renovación siguiente	Este contador muestra la cantidad de tiempo que falta hasta la próxima renovación automática. La lista de las actualizaciones en la página Comprobar si hay actualizaciones se renueva automáticamente cada 60 segundos. El temporizador se pone en pausa automáticamente cuando se seleccionan una o más actualizaciones.
Pausa	Hace una pausa en el proceso de renovación automática. Para reanudar la renovación automática, pulse **Reproducir**.
Renovar	Renueva la lista de actualizaciones.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Actualización automática**.
4. Para ver los detalles sobre una actualización, seleccione la actualización.

Configuración de los valores de actualización automática

Los valores de actualización automática pueden personalizarse para cambiar la frecuencia, el tipo de actualización, la configuración del servidor y la copia de seguridad.

Acerca de esta tarea

Puede seleccionar **Desplegar automáticamente** para desplegar las actualizaciones automáticamente. Si no se selecciona **Desplegar automáticamente**, debe desplegar los cambios manualmente, en la pestaña **Panel de control**, después de que las actualizaciones se hayan instalado.

Restricción: En un entorno de alta disponibilidad (HA), las actualizaciones automáticas no se instalan cuando un host secundario está activo. Las actualizaciones se instalarán solamente después de que el host primario se convierta en el nodo activo.

Puede seleccionar **Reiniciar servicio automáticamente** para permitir las actualizaciones automáticas que requieren que se reinicie la interfaz de usuario. Se produce una interrupción en la interfaz de usuario cuando el servicio se reinicia. Como alternativa, puede instalar manualmente la actualización desde la ventana Comprobar si hay actualizaciones.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Actualización automática**.
4. En el menú de navegación, pulse **Cambiar valores**.
5. En la pestaña **Básico**, seleccione la planificación de las actualizaciones.
6. En la sección **Actualizaciones de configuración**, seleccione el método que desea utilizar para actualizar los archivos de configuración.
7. En la sección **Actualizaciones de DSM, Explorador, Protocolo**, seleccione una opción para instalar las actualizaciones.
8. En la sección **Actualizaciones principales**, seleccione una opción para recibir las actualizaciones más importantes para los nuevos releases.
9. En la sección **Actualizaciones secundarias**, seleccione una opción para recibir los parches correspondientes a problemas menores del sistema.
10. Seleccione la casilla de verificación **Desplegar automáticamente** si desea desplegar los cambios de actualización automáticamente después de instalar las actualizaciones.
11. Seleccione la casilla de verificación **Reiniciar servicio automáticamente** si desea reiniciar la interfaz de usuario automáticamente después de instalar las actualizaciones.
12. Pulse la pestaña **Avanzado**.
13. En el campo **Servidor web**, escriba el servidor web del cual desea obtener las actualizaciones. El servidor web predeterminado es https://qmmunity.q1labs.com/.
14. En el campo **Directorio**, escriba la ubicación del directorio en el que el servidor web almacena las actualizaciones. El directorio predeterminado es `autoupdates/`.
15. Opcional: En el campo **Servidor proxy**, escriba el URL del servidor proxy. El servidor proxy es necesario si el servidor de aplicaciones utiliza un servidor proxy para conectarse a Internet.
16. Opcional: En el campo **Nombre de usuario de proxy**, escriba el nombre de usuario para el servidor proxy. Se necesita un nombre de usuario si se utiliza un proxy autenticado.
17. En el campo **Contraseña de proxy**, escriba la contraseña para el servidor proxy. Se necesita una contraseña si se utiliza un proxy autenticado.
18. Seleccione la casilla de verificación **Enviar comentarios** si desea enviar comentarios a IBM acerca de la actualización. Si se producen errores durante una actualización, se envía información automáticamente a través de un formulario web.

19. En la lista **Periodo de retención de copia de seguridad**, escriba o seleccione el número de días que desea almacenar los archivos que se sustituyen durante el proceso de actualización. Los archivos se almacenan en la ubicación que se especifica en **Ubicación de copia de seguridad**. El mínimo es un día y el máximo es 65535 años.
20. En el campo **Ubicación de copia de seguridad**, escriba la ubicación en la que desea almacenar los archivos de copia de seguridad.
21. En el campo **Vía de descarga**, escriba la vía de acceso de directorio en la que desea almacenar las actualizaciones de DSM, secundarias y principales. La vía de acceso de directorio predeterminada es `/store/configservices/staging/updates`.
22. Pulse **Guardar**.

Planificación de una actualización

Las actualizaciones automáticas se producen en una planificación recurrente de acuerdo con los valores de la página Actualizar configuración. También puede planificar una actualización o un conjunto de actualizaciones para que se ejecute a una hora determinada.

Acerca de esta tarea

Para reducir el impacto sobre el rendimiento del sistema, planifique una actualización grande para que se ejecute durante las horas de menor actividad.

Para obtener información detallada sobre cada actualización, selecciónela. En el panel derecho de la ventana se muestran una descripción y los mensajes de error, si los hubiera.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Actualización automática**.
4. Opcional: Si desea planificar actualizaciones específicas, seleccione las actualizaciones que desea planificar.
5. En el cuadro de lista **Planificar**, seleccione el tipo de actualización que desee planificar.
6. Seleccione en el calendario la fecha de inicio y la hora en la que desea que se inicien las actualizaciones planificadas.

Borrado de las actualizaciones planificadas

Puede cancelar cualquier actualización planificada.

Acerca de esta tarea

Las actualizaciones planificadas muestran el estado **Planificado** en el campo **Estado**. Después de borrar la planificación, el estado de la actualización aparece como **Nuevo**.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Actualización automática**.

4. En el menú de navegación, pulse **Comprobar si hay actualizaciones**.
5. Opcional: Si desea borrar actualizaciones planificadas concretas, seleccione las actualizaciones que desea borrar.
6. En el cuadro de lista **Anular planificación**, seleccione el tipo de actualización planificada que desee borrar.

Cómo comprobar si hay nuevas actualizaciones

IBM proporciona actualizaciones regularmente. De forma predeterminada, la característica Actualización automática está planificada para descargar e instalar automáticamente las actualizaciones. Si necesita una actualización en un momento distinto de la planificación preconfigurada, puede descargar nuevas actualizaciones.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Actualización automática**.
4. En el menú de navegación, pulse **Comprobar si hay actualizaciones**.
5. Pulse **Obtener nuevas actualizaciones**.

Instalación manual de actualizaciones automáticas

IBM proporciona actualizaciones regularmente. De forma predeterminada, las actualizaciones se descargan y se instalan automáticamente en el sistema. Sin embargo, puede instalar una actualización en un momento distinto de la planificación preconfigurada.

Acerca de esta tarea

El sistema recupera las actualizaciones nuevas desde Fix Central. Este proceso puede tardar bastante tiempo. Cuando haya terminado, las actualizaciones nuevas estarán listadas en la ventana Actualizaciones.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Actualización automática**.
4. En el menú de navegación, pulse **Comprobar si hay actualizaciones**.
5. Opcional: Si desea instalar actualizaciones específicas, seleccione las actualizaciones que desea planificar.
6. En el cuadro de lista **Instalar**, seleccione el tipo de actualización que desee instalar.

Visualización del historial de actualizaciones

Tras una instalación de actualización, sea satisfactoria o fallida, dicha actualización se visualiza en la página Ver historial de actualizaciones.

Acerca de esta tarea

En el panel derecho de la página Ver historial de actualizaciones se muestran una descripción de la actualización y los posibles mensajes de error de instalación. La página Ver historial de actualizaciones proporciona la siguiente información:

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Actualización automática**.
4. En el menú de navegación, pulse **Ver historial de actualizaciones**.
5. Opcional: En el cuadro de texto **Buscar por nombre** puede escribir una palabra clave y luego pulsar Intro para localizar una actualización concreta por nombre.
6. Para investigar una actualización específica, seleccione dicha actualización.

Restauración de actualizaciones ocultas

En la página Comprobar actualizaciones pueden eliminarse actualizaciones. En la página Restaurar actualizaciones ocultas pueden verse y restaurarse las actualizaciones ocultas.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Actualización automática**.
4. En el menú de navegación, pulse **Restaurar actualizaciones ocultas**.
5. Opcional: Para localizar una actualización por nombre, escriba una palabra clave en el cuadro de texto **Buscar por nombre** y pulse Intro.
6. Seleccione la actualización oculta que desee restaurar.
7. Pulse **Restaurar**.

Visualización del registro de actualización automática

El registro de actualización automática contiene la actualización automática más reciente ejecutada en el sistema.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Actualización automática**.
4. En el menú de navegación, pulse **Ver archivo de registro**.

Configurar un servidor de actualizaciones de QRadar

Si el despliegue incluye una consola de QRadar que no puede acceder a Internet o si desea gestionar manualmente las actualizaciones del sistema, puede configurar un servidor de actualizaciones de QRadar para gestionar el proceso de actualización.

El paquete de actualización automática incluye todos los archivos necesarios para configurar manualmente un servidor de actualizaciones, además de los archivos de configuración del sistema necesarios para cada actualización. Después de la configuración inicial, solamente tiene que descargar y descomprimir el paquete de actualización automática más reciente para actualizar la configuración manualmente.

Puede suscribirse a las notificaciones en Fix Central para recibir una notificación cuando haya actualizaciones nuevas.

Conceptos relacionados:

"Actualizaciones automáticas" en la página 73
Puede actualizar automática o manualmente los archivos de configuración para asegurarse de que los archivos de configuración contienen la información de seguridad de red más reciente.

Configuración del servidor de actualizaciones

Utilice esta tarea para configurar un servidor Apache. Debe crear un directorio de actualización y descargar el paquete de actualización automática de Fix Central.

Acerca de esta tarea

Las actualizaciones automáticas están disponibles en Fix Central.

Procedimiento

1. Acceda al servidor Apache. De forma predeterminada, el directorio de actualización se encuentra en el directorio raíz web del servidor Apache. Puede colocar el directorio en otra ubicación si configura QRadar en consecuencia.
2. Cree un directorio de actualización llamado `autoupdates/`.
3. Opcional: Cree una cuenta de usuario y una contraseña de Apache para utilizarlas en el proceso de actualización.
4. Descargue el paquete de actualización automática de Fix Central: http://www.ibm.com/support/fixcentral Encontrará los productos de QRadar en la lista **Grupo de productos** de Security Systems de Fix Central.
5. Guarde el archivo de paquete de actualización automática en el servidor Apache en el directorio `autoupdates/` que ha creado.
6. En el servidor Apache, escriba el mandato siguiente para descomprimir el paquete de actualización automática: **`tar -zxf updatepackage-[timestamp].tgz`**
7. Pulse la pestaña **Admin**.
8. En el menú de navegación, pulse **Configuración del sistema**.
9. Pulse **Actualización automática**.
10. Pulse **Cambiar valores**.
11. Seleccione la ficha **Avanzado**.
12. Para dirigir el proceso de actualización al servidor Apache, configure los parámetros siguientes en el panel **Configuración de servidor**:
    a. En el campo **Servidor web**, escriba la dirección o la vía de acceso del directorio del servidor Apache. Si el servidor Apache se ejecuta en puertos no estándar, añada `:<número_puerto>` al final de la dirección. `https://qmmunity.q1labs.com/:8080`
    b. En el campo **Directorio**, escriba la ubicación del directorio en el que el servidor web almacena las actualizaciones. El directorio predeterminado es `autoupdates/`.
    c. Opcional: En el campo **Servidor proxy**, escriba el URL del servidor proxy. El servidor proxy es necesario si el servidor de aplicaciones utiliza un servidor proxy para conectarse a Internet.
    d. Opcional: En el campo **Nombre de usuario de proxy**, escriba el nombre de usuario para el servidor proxy. Se necesita un nombre de usuario si se utiliza un proxy autenticado.

e. Opcional: En el campo **Contraseña de proxy**, escriba la contraseña para el servidor proxy. Se necesita una contraseña si se utiliza un proxy autenticado.

13. Seleccione **Desplegar cambios**.
14. Pulse **Guardar**.
15. Inicie, mediante SSH, la sesión en QRadar como usuario root.
16. Escriba el mandato siguiente para configurar el nombre de usuario que ha establecido para el servidor Apache: **/opt/qradar/bin/UpdateConfs.pl -change_username <nombre_usuario>**
17. Escriba el mandato siguiente para configurar la contraseña que ha establecido para el servidor Apache: **/opt/qradar/bin/UpdateConfs.pl -change_password <contraseña>**
18. Pruebe el servidor de actualizaciones con este mandato: **lynx https://<servidor de actualizaciones>/<directorio de actualizaciones>/manifest_list**
19. Escriba el nombre de usuario y la contraseña.

Configuración de la consola de QRadar como servidor de actualizaciones

Puede configurar la consola de QRadar para que sea el servidor de actualizaciones.

Acerca de esta tarea

Para configurar la consola de QRadar para que sea el servidor de actualizaciones, tiene que realizar tres tareas:

- Cree un directorio de actualización automática.
- Descargue el paquete de actualización automática de Fix Central.
- Configure QRadar para que acepte las actualizaciones automáticas.

Procedimiento

1. Inicie la sesión en QRadar como usuario root.
2. Escriba el mandato siguiente para crear el directorio de actualizaciones automáticas: **mkdir /opt/qradar/www/autoupdates/**
3. Descargue el paquete de actualización automática de Fix Central: http://www.ibm.com/support/fixcentral Encontrará los productos de QRadar en la lista **Grupo de productos** de Security Systems de Fix Central.
4. Guarde el archivo de paquete de actualización automática en el servidor Apache en el directorio `autoupdates/` que ha creado.
5. En la consola de QRadar, escriba el mandato siguiente para descomprimir el paquete de actualización automática: **tar -zxf updatepackage-[timestamp].tgz**
6. Inicie la sesión en la interfaz de usuario de QRadar.
7. En el menú de navegación, pulse **Configuración del sistema**.
8. Pulse **Actualización automática**.
9. Pulse **Cambiar valores**.
10. Seleccione la ficha **Avanzado**.
11. En el campo **Servidor web**, escriba `https://localhost/`.
12. Deseleccione la casilla de verificación **Enviar comentarios**.

Adición de nuevas actualizaciones

Puede descargar actualizaciones desde Fix Central al servidor de actualizaciones.

Antes de empezar

Debe configurar el servidor de actualizaciones y configurar QRadar para que reciba las actualizaciones procedentes del servidor de actualizaciones.

Procedimiento

1. Descargue el paquete de actualización automática de Fix Central: http://www.ibm.com/support/fixcentral Encontrará los productos de QRadar en la lista **Grupo de productos** de Security Systems de Fix Central.
2. Guarde el archivo de paquete de actualización automática en el servidor de actualizaciones en el directorio `autoupdates/` que ha creado.
3. Escriba el mandato siguiente para descomprimir el paquete de actualización automática: **`tar -zxf autoupdate-[timestamp].tgz`**.
4. Inicie la sesión en QRadar como usuario root.
5. Escriba el mandato siguiente para probar el servidor de actualizaciones: **`lynx https://<servidor de actualizaciones>/<directorio de actualizaciones>/manifest_list`**.
6. Escriba el nombre de usuario y la contraseña del servidor de actualizaciones.

Configuración de los valores del sistema

Puede configurar los valores del sistema comunes en la ventana Valores del sistema.

Acerca de esta tarea

La ventana Valores del sistema incluye parámetros configurables para los valores del sistema siguientes:

- Valores del sistema
- Valores de base de datos
- Valores de base de datos Ariel
- Valores de SNMP
- Valores de daemon SNMP incluidos
- Valores de perfil de activo
- Valores de la consola
- Valores de autenticación
- Configuración de DNS
- Valores de WINS
- Valores de creación de informes
- Valores de exportación de datos

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Valores del sistema**.
4. Configure los valores del sistema.
5. Pulse **Guardar**.

6. En el menú de pestaña **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.

   Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Personalización del menú contextual

Para proporcionar acceso rápido a las funciones, personalice las opciones de menú utilizando una interfaz de programación de aplicaciones (API) de tipo plug-in. Por ejemplo, puede añadir más elementos de menú, como podría ser una opción para explorar el NetBIOS.

Acerca de esta tarea

El archivo `ip_context_menu.xml` acepta nodos XML `menuEntry` para personalizar el menú contextual.

```
<menuEntry name="{Nombre}" description="{Descripción}" exec="{Mandato}"
url="{URL}" requiredCapabilities="{Capacidades necesarias}"/>
```

En la lista siguiente se describen los atributos del elemento `menuEntry`:

Nombre
Texto que se visualiza en el menú contextual.

Descripción
Descripción de la entrada. El texto descriptivo se visualiza en la ayuda contextual correspondiente a la opción de menú. La descripción es opcional.

URL Especifica la dirección Web que se abre en una ventana nueva.

Puede utilizar el marcador de posición `%IP%` para representar la dirección IP. El carácter de ampersand (&), el signo de menor que (<) y el signo de mayor que (>) necesitan los caracteres de escape `&`, `<` y `>` respectivamente.

Por ejemplo, para pasar un URL con varios parámetros que incluyen un marcador para la dirección IP, puede utilizar esta sintaxis: `url="/lookup?&ip=%IP%;force=true"`

Mandato
Mandato que desea ejecutar en la consola. La salida del mandato se visualiza en una ventana nueva. Utilice el marcador de posición %IP% para representar la dirección IP seleccionada.

Capacidades necesarias
Capacidades, como, por ejemplo, "ADMIN", que el usuario debe tener antes de seleccionar esta opción (delimitada por comas). Por ejemplo, "ADMIN". Si el usuario no tiene todas las capacidades que figuran en la lista, las entradas no se visualizan. Las capacidades necesarias es un campo opcional.

El archivo editado debe ser similar al ejemplo siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>
<!- Este es un archivo de configuración para añadir acciones personalizadas al
menú que aparece al pulsar el botón derecho del ratón en la dirección IP. Las
entradas deben tener uno de
los formatos siguientes: -->
<contextMenu>
```

```
<menuEntry name="Traceroute" exec="/usr/sbin/traceroute %IP%" />
<menuEntry name="External ARIN Lookup"
url="http://ws.arin.net/whois/?queryinput=%IP%" />
</contextMenu>
```

Procedimiento

1. Inicie, mediante SSH, la sesión en IBM Security QRadar como usuario root.
2. En el servidor de QRadar, copie el archivo `ip_context_menu.xml` del directorio `/opt/qradar/conf/templates` en el directorio `/opt/qradar/conf`.
3. Abra el archivo `/opt/qradar/conf/ip_context_menu.xml` para su edición.
4. Edite los atributos en el elemento `menuEntry`.
5. Guarde y cierre el archivo.
6. Para reiniciar los servicios, escriba el mandato siguiente:

   ```
   service tomcat restart
   ```

Mejora del menú contextual para las columnas de sucesos y flujos

Puede añadir más acciones a las opciones del menú contextual que están disponibles en las columnas de la tabla **Actividad de registro** o la tabla **Actividad de red**. Por ejemplo, puede añadir una opción para ver más información acerca de la IP de origen o la IP de destino.

Puede pasar al URL o al script cualquier dato que esté en el suceso o en el flujo.

Restricción: Puede añadir opciones al menú contextual solamente en el dispositivo consola de QRadar y solamente a algunos campos de base de datos Ariel.

Procedimiento

1. Inicie, mediante SSH, la sesión en el dispositivo QRadar Console como usuario root.
2. Vaya al directorio `/opt/qradar/conf` y cree un archivo que se llame `arielRightClick.properties`.
3. Edite el archivo `/opt/qradar/conf/arielRightClick.properties`. Utilice la tabla siguiente para especificar los parámetros que determinan las opciones del menú contextual.

Tabla 28. Descripción de los parámetros de archivo `arielRightClick.properties`.

Parámetro	Requisito	Descripción	Ejemplo
`pluginActions`	Obligatorio	Indica una acción de script o URL.	
`arielProperty`	Obligatorio	Especifica la columna, o nombre de campo de Ariel, para la cual está habilitado el menú contextual.	**sourceIP** **sourcePort** **destinationIP** **qid**
`text`	Obligatorio	Especifica el texto que se visualiza en el menú contextual.	Búsqueda de Google

Tabla 28. Descripción de los parámetros de archivo `arielRightClick.properties` (continuación).

Parámetro	Requisito	Descripción	Ejemplo
`useFormattedValue`	Opcional	Especifica si los valores con formato se pasan al script. Se establece en `true` para garantizar que se pase el valor con formato de los atributos, como `username` y `payload`. Los valores con formato son más fáciles de leer para los administradores que los valores sin formato.	Si el parámetro está establecido en true para la propiedad de nombre de suceso (QID), el nombre de suceso del QID se pasa al script. Si el parámetro está establecido en false, se pasa al script el valor del QID sin formato (en bruto).
`url`	Necesario para acceder a un URL	Especifica el URL, que se abre en una ventana nueva, y los parámetros que se pasan al URL. Utilice este formato: `$nombre_campo_Ariel$`	`sourceIPwebUrlAction.url= http://www.mywebsite.com? q=$sourceIP$`
`command`	Necesario si la acción es un mandato	Especifica la vía de acceso absoluta del archivo de script o mandato.	`destinationPortScript Action.command=/bin/echo`
`arguments`	Necesario si la acción es un mandato	Especifica los datos que se pasan al script. Utilice el formato siguiente: `$nombre_campo_Ariel$`	`destinationPortScript Action.arguments=$qid$`

Para cada uno de los nombres de clave que se especifican en la lista *pluginActions*, defina la acción mediante el uso de una clave con el formato *nombre de clave*, *propiedad*.

4. Guarde y cierre el archivo.
5. Inicie la sesión en la interfaz de usuario de QRadar.
6. Pulse la pestaña **Admin**.
7. Seleccione **Avanzado** > **Reiniciar el servidor web**.

Ejemplo

En el ejemplo siguiente se muestra cómo añadir *Probar URL* como una opción del menú contextual para las direcciones IP de origen.

```
pluginActions=sourceIPwebUrlAction

sourceIPwebUrlAction.arielProperty=sourceIP
sourceIPwebUrlAction.text=Probar URL
sourceIPwebUrlAction.url=http://www.mywebsite.com?q=$sourceIP$
```

En el ejemplo siguiente se muestra cómo habilitar la acción de script para los puertos de destino.

```
pluginActions=destinationPortScriptAction

destinationPortScriptAction.arielProperty=destinationPort
destinationPortScriptAction.text=Probar mandato sin formato
destinationPortScriptAction.useFormattedValue=false
destinationPortScriptAction.command=/bin/echo
destinationPortScriptAction.arguments=$qid$
```

En el ejemplo siguiente se muestra la adición de varios parámetros a una acción de script o URL.

```
pluginActions=qidwebUrlAction,sourcePortScriptAction

qidwebUrlAction.arielProperty=qid,device,eventCount
qidwebUrlAction.text=Búsqueda de Google
qidwebUrlAction.url=http://www.google.com?q=$qid$-$device$-$eventCount$

sourcePortScriptAction.arielProperty=sourcePort
sourcePortScriptAction.text=Mandato sin formato de puerto
sourcePortScriptAction.useFormattedValue=true
sourcePortScriptAction.command=/bin/echo
sourcePortScriptAction.arguments=$qid$-$sourcePort$-$device$-$CONTEXT$
```

Visión general de los valores de retención de activos

Información adicional sobre el periodo, en días, durante el cual desea almacenar la información de perfil de activo.

- Se efectúan comprobaciones de los umbrales de retención para los activos a intervalos regulares. De forma predeterminada, el intervalo de limpieza es de 12 horas.
- Todos los periodos de retención especificados son relativos a la última fecha de visualización de la información, independientemente de si la información fue vista por última vez por un explorador u observada de forma pasiva por el sistema.
- La información de activos se suprime a medida que caduca, lo que significa que, tras un intervalo de limpieza, se conserva toda la información de activos que está dentro de su umbral de retención correspondiente.
- De forma predeterminada, se conservan los activos que están asociados con las vulnerabilidades no remediadas (tal como las detecta QVM u otro explorador).
- Los activos siempre pueden suprimirse manualmente a través de la interfaz de usuario.

Tabla 29. Componentes de activo

Componente de activo	Retención predeterminada (en días)	Notas
Dirección IP	120 días	De forma predeterminada, las direcciones IP proporcionadas por el usuario se conservan hasta que se suprimen manualmente.
Direcciones MAC (interfaces)	120 días	De forma predeterminada, las interfaces proporcionadas por el usuario se conservan hasta que se suprimen manualmente.
Nombres de host de DNS y NetBIOS	120 días	De forma predeterminada, los nombres de host proporcionados por el usuario se conservan hasta que se suprimen manualmente.

Tabla 29. Componentes de activo (continuación)

Componente de activo	Retención predeterminada (en días)	Notas
Propiedades de activos	120 días	De forma predeterminada, las direcciones IP proporcionadas por el usuario se conservan hasta que se suprimen manualmente. Las propiedades de activos a las que este valor puede afectar son: • Nombre • Nombre unificado • Peso • Descripción • Propietario del negocio • Contacto profesional • Propietario técnico • Contacto técnico • Ubicación • Fiabilidad de detección • AP inalámbrico • SSID inalámbrico • ID de conmutador • ID de puerto de conmutador • Requisito de confidencialidad de CVSS • Requisito de integridad de CVSS • Requisito de disponibilidad de CVSS • Potencial de daños colaterales de CVSS • Usuario técnico • SO proporcionado por el usuario • Tipo de alteración temporal de SO • ID de alteración temporal de SO • Ampliado • Riesgo de CVSS heredado (anterior a la versión 7.2) • VLAN • Tipo de activo

Tabla 29. Componentes de activo (continuación)

Componente de activo	Retención predeterminada (en días)	Notas
Productos de activo	120 días	De forma predeterminada, los productos proporcionados por el usuario se conservan hasta que se suprimen manualmente. Los productos de activo son los siguientes: • SO de activo • Aplicaciones instaladas de activo • Productos que están asociados a los puertos de activo abiertos
Puertos abiertos de activo	120 días	
Grupo de NetBIOS de activo	120 días	Los grupos de NetBIOS raramente se utilizan, y muchos clientes desconocen su existencia. En los casos en los que se utilizan, se suprimen transcurridos 120 días.
Aplicación de cliente de activo	120 días	Las aplicaciones cliente todavía no se han incluido en la interfaz de usuario. Este valor se puede pasar por alto.
Usuarios de activo	30 días	

Creación de un archivo de mensaje de inicio de sesión de QRadar

Puede añadir y personalizar un mensaje de inicio de sesión en la consola de QRadar.

Antes de empezar

Debe tener acceso de usuario root a la interfaz de línea de mandatos para crear un archivo de mensaje de inicio de sesión.

Procedimiento

1. Inicie la sesión en QRadar como usuario root.
2. En el archivo `/etc/`, escriba el mandato siguiente:

   ```
   vim loginMSG
   ```

   El editor Vim creará un archivo `loginMsg`. No especifique el nombre de archivo utilizando caracteres especiales.
3. Pulse `i` para escribir el mensaje.
4. Para guardar el mensaje, pulse ESC.
5. Para volver a la línea de mandatos, escriba el mandato siguiente:

```
:wq
```

6. Pulse Intro.
7. Para habilitar el mensaje de inicio de sesión, acceda a **Admin** > **Valores del sistema**.
8. Pulse **Valores de autenticación**.
9. En el campo **Archivo de mensaje de inicio de sesión**, escriba la vía de acceso de archivo siguiente:

   ```
   /etc/loginMsg
   ```

10. Pulse **Guardar**.
11. Cierre la sesión de QRadar para ver el nuevo mensaje de inicio de sesión.

Configuración de los certificados de servidor IF-MAP

Para poder configurar la autenticación de IF-MAP en la ventana Valores del sistema, debe configurar el certificado de servidor IF-MAP.

Configuración del certificado del servidor IF-MAP para la autenticación básica

Esta tarea proporciona instrucciones para la configuración del certificado de IF-MAP para la autenticación básica.

Antes de empezar

Póngase en contacto con el administrador del servidor IF-MAP para obtener una copia del certificado público del servidor IF-MAP. El certificado debe tener la extensión de archivo `.cert`; por ejemplo, ifmapserver.cert.

Procedimiento

1. Inicie, mediante SSH, la sesión en QRadar como usuario root.
2. Copie el certificado en el directorio `/opt/qradar/conf/trusted_certificates`.

Configuración del certificado del servidor IF-MAP para la autenticación mutua

Esta tarea proporciona instrucciones para la configuración del certificado de IF-MAP para la autenticación mutua.

Antes de empezar

Póngase en contacto con el administrador del servidor IF-MAP para obtener una copia del certificado público del servidor IF-MAP. El certificado debe tener la extensión de archivo `.cert`; por ejemplo, ifmapserver.cert.

La autenticación mutua requiere la configuración del certificado en la consola y en el servidor IF-MAP. Para obtener ayuda para configurar el certificado en el servidor IF-MAP, póngase en contacto con el administrador del servidor IF-MAP.

Procedimiento

1. Inicie, mediante SSH, la sesión en QRadar como usuario root.
2. Acceda al certificado en el directorio `/opt/qradar/conf/trusted_certificates`.

3. Copie el certificado intermedio SSL y el certificado raíz Verisign SSL en el servidor IF-MAP como certificados de entidad emisora de certificados. Para obtener ayuda, póngase en contacto con el administrador del servidor IF-MAP.
4. Escriba el mandato siguiente para crear el archivo de estándares de criptografía de claves públicas con la extensión .pkcs12: `openssl pkcs12 -export -inkey <clave_privada> -in <certificado> -out <nombre_archivo_pkcs12.pkcs12> -name "Cliente IFMAP"`
5. Escriba el mandato siguiente para copiar el archivo pkcs12 en el directorio /opt/qradar/conf/key_certificates: `cp <nombre_archivo_pkcs12.pkcs12> /opt/qradar/conf/key_certificates`
6. Cree un cliente en el servidor IF-MAP con la autenticación de certificado y cargue el certificado SSL. Para obtener ayuda, póngase en contacto con el administrador del servidor IF-MAP.
7. Cambie los permisos del directorio con los mandatos siguientes: `chmod 755 /opt/qradar/conf/trusted_certificateschmod 644 /opt/qradar/conf/trusted_certificates/*.cert`
8. Escriba el mandato siguiente para reiniciar el servicio de Tomcat: `service tomcat restart`

Sustitución de los certificados SSL en productos QRadar

De forma predeterminada, IBM Security QRadar se configura con un certificado SSL (Security Sockets Layer) autofirmado. Cuando utiliza un certificado autofirmado para acceder a la web, se le indica con un mensaje de aviso que no se reconoce el certificado. Puede sustituir este certificado SSL por un certificado actualizado autofirmado, firmado por una entidad emisora de certificados internos (CA) o firmado por una entidad emisora de certificados (CA) pública.

Visión general de los certificados SSL

SSL es un protocolo de privacidad de comunicaciones que permite a las aplicaciones de cliente/servidor comunicarse de una forma diseñada para impedir las escuchas no deseadas, la manipulación indebida y la falsificación de mensajes.

SSL es un estándar del sector que se utiliza en los sitios web para proteger las transacciones en línea. Para generar un enlace SSL, un servidor web necesita un certificado SSL. Los certificados SSL los emiten las entidades de certificación de terceros de confianza.

Raíz de confianza

Los navegadores y los sistemas operativos incluyen una lista preinstalada de certificados de confianza, que se instala en el almacén de entidades de certificación de raíz de confianza.

Tabla 30. Certificados soportados por QRadar

Certificado	Descripción
Autofirmado	Un certificado autofirmado proporciona una seguridad básica, permitiendo el cifrado de datos entre el usuario y la aplicación. Debido a que los certificados autofirmados no pueden ser autenticados por ninguna entidad emisora de certificados raíz conocida, se avisa a los usuarios sobre este certificado desconocido y deben aceptarlo para poder continuar.
Firmado de CA interna	Las organizaciones que tienen su propia CA raíz interna pueden crear un certificado utilizando dicha CA interna. Este certificado está soportado por QRadar y la CA raíz interna se importa también al entorno de QRadar.
Firmado de CA pública/CA intermedia	Los certificados firmados por las CA públicas conocidas y los certificados intermedios están soportados por QRadar. Los certificados firmados públicos se pueden utilizar directamente en QRadar y los certificados firmados por una CA intermedia se instalan utilizando el certificado firmado y el certificado intermedio para proporcionar funciones de certificado válidas. **Nota:** Normalmente, las organizaciones utilizan un certificado intermedio para crear varias claves SSL en su entorno que desean que estén firmadas por un proveedor de certificados conocido o comercial. Cuando utilizan la clave intermedia pueden crear subclaves a partir de esta clave intermedia. Cuando se utiliza esta configuración, se debe configurar QRadar con el certificado intermedio y con el certificado SSL de host, de modo que las conexiones con el host puedan verificar la vía de acceso completa del certificado.

Conexiones SSL entre los componentes de QRadar

Para establecer todas las conexiones SSL internas entre los componentes, QRadar utiliza el certificado de servidor web que está preinstalado en la consola de QRadar. Cuando se sustituye el certificado preinstalado, el proceso de instalación copia el certificado en todos los hosts gestionados en el despliegue, excepto en los dispositivos de QRadar Incident Forensics.

Todos los certificados de confianza para QRadar deben cumplir los requisitos siguientes:

- El certificado debe ser un certificado X.509 y tener una codificación PEM base64.
- El certificado debe tener una extensión de archivo `.cert`, `.crt`, `.pem` o `.der`.
- Los archivos de almacén de claves que contienen certificados deben tener la extensión `.truststore`.

- El archivo de certificado debe estar almacenado en el directorio `/opt/qradar/conf/trusted_certificates`.

Importante: Si es cliente de IBM Security QRadar Incident Forensics, póngase en contacto con el servicio de Soporte al cliente (www.ibm.com/support/) para obtener asistencia para instalar o actualizar su certificado SSL personalizado en el almacén de claves de QRadar Incident Forensics.

Si se configura la clave SSL con una contraseña, se debe especificar manualmente cada vez que se reinicia el servicio. Con esta configuración, el servicio de la interfaz de usuario web no estará disponible hasta que se especifique la contraseña, por ejemplo, durante la instalación de un parche de QRadar, una migración tras error de alta disponibilidad o un reinicio del sistema. En este caso, los usuarios no pueden iniciar sesión y los hosts gestionados por QRadar no pueden recuperar las actualizaciones de la configuración, el origen del registro de informes y los mensajes de estado del almacenamiento de datos y las reglas hasta que el servicio web esté disponible.

Creación de una solicitud de firma de certificado SSL con claves RSA de 2048 bits

1. Utilice SSH para iniciar la sesión en la consola de QRadar.
2. Genere un archivo de claves privadas utilizando el mandato siguiente:

   ```
   openssl genrsa -out qradar.key 2048
   ```

   Nota: No utilice las opciones de cifrado privadas porque pueden generar problemas de compatibilidad.
   El archivo `qradar.key` se crea en el directorio actual. Conserve este archivo para utilizarlo cuando instale el certificado.
3. Genere el archivo de solicitud de solicitud de firma de certificado (CSR). El archivo `qradar.csr` se utiliza para crear el certificado SSL con una entidad emisora de certificados (CA) interna o comercial. Ejecute el mandato siguiente y proporcione la información necesaria, como se le solicite:

   ```
   openssl req -new -key qradar.key -out qradar.csr
   ```

   Resultado de ejemplo:

   ```
   Proporcione la información siguiente solicitada en la línea de mandatos:
   [root@qradar ~]# openssl genrsa -out qradar.key 2048
   Generando clave privada de RSA, módulo de 2048 bits
   .....................................+++
   .......................+++
   e is 65537 (0x10001)
   [root@bluecar ~]# openssl req -new -key qradar.key -out qradar.csr
   Se le solicitará información que se incorporará
   a su solicitud de certificado.
   Está a punto de entrar un nombre distinguido o DN.
   Puede dejar en blanco algunos campos
   Algunos campos tendrán un valor predeterminado,
   Si escribe '.', el campo se deja en blanco.
   -----
   Nombre de país (código de dos 2 letras) [XX]:US
   Estado o provincia (nombre completo) []:MyState
   Localidad (por ejemplo, city) [Predeterminado City]:MyCity
   Nombre de organización (por ejemplo, company) [Predeterminado Company Ltd]:MyCompany
   Nombre unidad organizativa (por ejemplo, departamento) []:MyCompanyOrg
   Nombre común (por ejemplo, su nombre o el host del servidor) []:qradar.mycompany.com
   Dirección de correo electrónico []:email@mycompany.com

   Escriba los siguientes atributos adicionales
   ```

```
que se enviarán con su solicitud de certificado
Una contraseña de desafío []:
Un nombre de empresa opcional []:
[root@bluecar ~]#
```

4. Si desea verificar la información del CSR antes de enviarlo, puede escribir el mandato siguiente:

   ```
   openssl req -noout -text -in qradar.csr
   ```

   Si se ha especificado información incorrecta, vuelva a ejecutar el mandato OpenSSL para crear de nuevo el archivo CSR.
5. Utilice el SFTP (Secure File Transfer Protocol) u otro programa para copiar de forma segura el archivo CSR en su sistema.
6. Envíe el CSR a su entidad emisora de certificados interna o comercial para que lo firme según sus instrucciones.

   Nota: El CSR se identifica como un certificado en formato Apache.

Certificados firmados por una entidad emisora de certificados interna

Si el certificado lo emite una entidad emisora de certificados y no un proveedor de certificados comercial, se debe actualizar QRadar para que incluya el certificado raíz interno en el almacén de certificados, de modo que se pueda validar correctamente el certificado. Los certificados de verificación raíz se incluyen automáticamente con el sistema operativo.

Para actualizar el almacén de certificados raíz de anclas de confianza en RedHat:

1. Copie el certificado raíz de la CA en `/etc/pki/ca-trust/source/anchors/`.
2. Ejecute el mandato siguiente en la línea de mandatos SSH:

   ```
   update-ca-trust
   ```

Instalación de un nuevo certificado SSL en la consola de QRadar

Antes de empezar

Debe tener lo siguiente:

- El certificado recién firmado emitido por la CA interna, o un certificado público.
- La clave privada `qradar.key` para generar el archivo CSR.
- Un certificado intermedio, si lo utiliza su proveedor de certificados.

  Nota: Si se utiliza un certificado intermedio, ejecute el mandato "install_ssl_cert.sh" con el distintivo `-b` para instalar tanto el certificado nuevo como el certificado intermedio. Cuando se utiliza ese mandato, solicita 3 vías de acceso de archivo:

  – `SSLCertifficateFile`
  – `SSLIntermediateCertificateFile`
  – `SSLCertificateKeyFile`

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Instale el certificado escribiendo el mandato siguiente:

```
[root@csd2-primary ssl]# ls
cert.cert cert.key
[root@qradar ssl]# /opt/qradar/bin/install_ssl_cert.sh -b
Vía de acceso del archivo de clave privada (SSLCertificateKeyFile): /root/ssl/cert.key
Vía de acceso del archivo de clave pública (SSLCertificateFile): /root/ssl/cert.cert
```

Resultado de ejemplo:

```
Ha especificado lo siguiente:
SSLCertificateKeyFile of '/root/ssl/cert.key'
SSLCertificateFile of '/root/ssl/cert.cert'
Continuar y reconfigurar Apache ahora (incluye el reinicio del daemon httpd)
(Y/[N])? y
Reiniciando Apache
Deteniendo httpd: [ OK ]
Iniciando httpd: [ OK ]
En espera de que se ejecute Apache. Terminado.
Deteniendo hostcontext
[Q] Concluyendo el servicio de hostcontext: enviando SIGQUIT a h[ OK ]xt
[Q] Concluyendo el servicio de hostcontext: [ OK ]
Reiniciando Tomcat
Enviando SIGQUIT a tomcat [ OK ]
Deteniendo httpd: [ OK ]
Concluyendo tomcat: [ OK ]
Iniciando tomcat: [ OK ]
Iniciando httpd: [ OK ]
Reiniciando hostcontext
[Q] Reiniciando servicio de hostcontext: [ OK ]
Reiniciando hostcontext en 172.16.77.105
OK: Certificado SSL personalizado aplicado satisfactoriamente.
[root@qradar ssl]#
```

3. En la pestaña **Admin**, pulse **Avanzado** > **Desplegar configuración completa**

   Nota: Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Resolución de problemas

Si tiene problemas con el certificado, tal como un nombre o dirección IP incorrectos, o si ha transcurrido la fecha de caducidad o existe un cambio de IP o nombre de host en su consola, puede optar por revertir a un certificado autofirmado.

Para generar un certificado autofirmado, siga estos pasos en la consola de QRadar:

1. Realice una copia de seguridad de los certificados instalados previamente que no funcionan. Cuando ejecuta la generación de certificados, se detectan los certificados existentes y se informa acerca de los mismos, lo que hace que se detenga el proceso de generación.

   ```
   mkdir /root/backup.certs/
   mv /etc/httpd/conf/certs/cert.* /root/backup.certs/
   ```

2. Ejecute el mandato **/opt/qradar/bin/install_ssl_cert.sh -generate** para generar nuevos certificados. Este proceso también se utiliza durante la instalación de QRadar para generar el certificado SSL inicial.

   ```
   [root@qavm215 certs]# /opt/qradar/bin/install_ssl_cert.sh --generate
   Generando certificado SSL autofirmado ... (OK)
   Instalando certificado SSL autofirmado ... (OK)
   Martes 19 set 14:00:42 ADT 2017 [install_ssl_cert.sh] OK:
   El certificado SSL generado se ha instalado correctamente
   [root@qavm215 certs]#
   ```

3. Mueva los certificados recién generados a un directorio nuevo. Utilice el script `install_ssl_cert.sh` en la modalidad de instalación para instalar y distribuir los nuevos certificados SSL.

```
[root@qavm215 ~]# mkdir /root/updated.certs/
[root@qavm215 ~]# mv /etc/httpd/conf/certs/cert.* /root/updated.certs/
[root@qavm215 ~]# /opt/qradar/bin/install_ssl_cert.sh
Vía de acceso del archivo de clave pública (SSLCertificateFile):
/root/updated.certs/cert.cert
Vía de acceso del archivo de clave privada (SSLCertificateKeyFile):
/root/updated.certs/cert.key

Ha especificado lo siguiente:

       SSLCertificateFile of /root/updated.certs/cert.cert
    SSLCertificateKeyFile of /root/updated.certs/cert.key

Reconfigurar Apache ahora (incluye el reinicio de httpd) (Y/[N])? y
Copia de seguridad de configuración SSL actual ... (OK)
Instalando certificado SSL de usuario... (OK)
Recargando configuración httpd:
 - Reiniciando servicio httpd ... (OK)
Reiniciando servicios:
 - Deteniendo contexto de host ... (OK)
 - Reiniciando Tomcat ... (OK)
 - Iniciando contexto de host ... (OK)
Martes 19 set 14:45:57 ADT 2017 [install_ssl_cert.sh] OK:
Se ha completado la instalación del certificado SSL
[root@qavm215 ~]#
```

Direccionamiento IPv6 en los despliegues de QRadar

El direccionamiento IPv4 e IPv6 está soportado para la conectividad de red y la gestión de los dispositivos y el software de IBM Security QRadar. Cuando se instala QRadar, se solicita que especifique si el protocolo Internet es IPv4 o IPv6.

Lea la información siguiente sobre el direccionamiento IPv6.

"Componentes de QRadar que dan soporte al direccionamiento IPv6"

"Despliegue de QRadar en entornos IPv6 o mixtos" en la página 96

"Limitaciones del direccionamiento IPv6 " en la página 97

Componentes de QRadar que dan soporte al direccionamiento IPv6

Los componentes de QRadar siguientes dan soporte al direccionamiento IPv6.

Pestaña Actividad de red

Puesto que **Dirección de origen - IPv6** y **Dirección de destino - IPv6** no son columnas predeterminadas, no se visualizan de forma automática. Para visualizar estas columnas, debe seleccionarlas al configurar los parámetros de búsqueda (definición de columna).

Para ahorrar espacio y reducir la indexación en un entorno de origen IPv4 o IPv6, los campos de dirección IP adicionales no se almacenan ni se visualizan. En un entorno mixto IPv4 e IPv6, un registro de flujo contiene las direcciones IPv4 e IPv6.

Las direcciones IPv6 están soportadas tanto para los datos de paquete, incluido sFlow, como para los datos de NetFlow V9. Sin embargo, las versiones anteriores de NetFlow podrían no dar soporte a IPv6.

Pestaña Actividad de registro

Puesto que **Dirección de origen - IPv6** y **Dirección de destino - IPv6** no son columnas predeterminadas, no se visualizan de forma automática. Para visualizar estas columnas, debe seleccionarlas al configurar los parámetros de búsqueda (definición de columna).

Cuando una dirección no existe, se utilizan registros basados en plantillas para evitar malgastar el espacio. Los DSM pueden analizar las direcciones IPv6 a partir de la carga útil de suceso. Si algún DSM no puede analizar las direcciones IPv6, puede analizarlas una extensión de origen de registro. Para obtener más información sobre las extensiones de origen de registro, consulte la publicación *Guía del usuario de orígenes de registro*.

Búsqueda, agrupación y creación de informes sobre los campos de IPv6

Puede buscar sucesos y flujos mediante los parámetros de IPv6 en los criterios de búsqueda.

También puede agrupar y ordenar registros de sucesos y flujos que están basados en parámetros de IPv6.

Puede crear informes que se basen en datos procedentes de las búsquedas basadas en IPv6.

Reglas personalizadas

Se ha añadido la regla personalizada siguiente para dar soporte al direccionamiento IPv6: **SRC/DST IP = Dirección IPv6**

Los componentes básicos basados en IPv6 están disponibles en otras reglas.

Editor de despliegue

El editor de despliegue da soporte a las direcciones IPv6.

Módulos de soporte de dispositivos (DSM)

Los DSM pueden analizar la dirección IPv6 de origen y de destino de las cargas útiles de sucesos.

Despliegue de QRadar en entornos IPv6 o mixtos

Para iniciar la sesión en QRadar en un entorno IPv6 o mixto, escriba la dirección IP entre corchetes:

```
https://[<dirección IP>]
```

Ambos entornos IPv4 e IPv6 pueden utilizar un archivo hosts para la conversión de direcciones. En un entorno IPv6 o mixto, el cliente resuelve la dirección de la consola por su nombre de host. Debe añadir la dirección IP de la consola IPv6 al archivo `/etc/hosts` en el cliente.

Se aceptan los orígenes de flujo, como NetFlow y sFlow, desde direcciones IPv4 e IPv6. Se aceptan los orígenes de sucesos, como syslog y SNMP, desde direcciones IPv4 e IPv6. Puede inhabilitar los superflujos y el empaquetado de flujos en un entorno IPv6.

Restricción:
De forma predeterminada, no puede añadir un host gestionado solo IPv4 a una consola IPv6 y de modalidad mixta IPv4. Debe ejecutar un script para habilitar un host gestionado solo IPv4.

Limitaciones del direccionamiento IPv6

Cuando QRadar se despliega en un entorno IPv6, existen las limitaciones siguientes:

- La jerarquía de red no se actualiza para dar soporte a IPv6.

  Algunas partes del despliegue de QRadar, incluidos la vigilancia, la búsqueda y el análisis, no hacen uso de la jerarquía de red. Por ejemplo, en la pestaña Actividad de registro, no puede buscar ni agregar sucesos Por red.
- No hay perfiles de activo basados en IPv6.
- Los perfiles de activo se crean solamente si QRadar recibe sucesos, flujos y datos de vulnerabilidad para los hosts IPv4.
- No se comprueban los perfiles de host en las reglas personalizadas de las direcciones IPv6.
- No hay optimización ni indexación especializada de las direcciones IPv6.
- No hay orígenes y destinos basados en IPv6 para los delitos.

Instalación de un host gestionado solo IPv4 en un entorno mixto

De forma predeterminada, en los productos de IBM Security QRadar no puede añadir un host gestionado solo IPv4 a una consola IPv6 y de modalidad mixta IPv4. Debe ejecutar un script para habilitar un host gestionado solo IPv4.

Procedimiento

1. Instale consola de QRadar seleccionando el direccionamiento IPv6.
2. Después de la instalación, en consola de QRadar, escriba el mandato siguiente:
   `/opt/qradar/bin/setup_v6v4_console.sh`
3. Para añadir un host gestionado IPv4, escriba el mandato siguiente:
   `/opt/qradar/bin/add_v6v4_host.sh`
4. Añada el host gestionado mediante el editor de despliegue.

Retención de datos

Configure periodos de retención personalizados para datos concretos.

Los grupos de retención definen las políticas de retención para los sucesos y flujos que cumplen los requisitos de los filtros personalizados. A medida que QRadar recibe sucesos y flujos, cada suceso y flujo se compara con los criterios de filtro de grupo de retención. Cuando un suceso o un flujo coincide con un filtro de grupo de retención, se almacena en ese grupo de retención hasta se agota el periodo de tiempo de la política de retención. Esta característica permite configurar varios grupos de retención.

Los grupos de retención se ordenan por prioridad de la fila superior a la fila inferior en las ventanas Retención de sucesos y Retención de flujos. En el grupo se almacena un registro que se corresponde con los criterios de filtro con la prioridad más alta. Si el registro no coincide con ninguno de los grupos de retención

configurados, el registro se almacena en el grupo de retención predeterminado, que siempre se encuentra bajo la lista de los grupos de retención configurables.

Configuración de los grupos de retención

De forma predeterminada, las ventanas Retención de sucesos y Retención de flujos proporcionan un grupo de retención predeterminado y 10 grupos de retención sin configurar. Hasta que configure un grupo de retención, todos los sucesos o flujos se almacenan en el grupo de retención predeterminado.

Acerca de esta tarea

Las ventanas Retención de sucesos y Retención de flujos proporcionan la información siguiente para cada grupo de retención:

Tabla 31. Parámetros de la ventana de retención

Parámetro	Descripción
Orden	Orden de prioridad de los grupos de retención.
Nombre	Nombre del grupo de retención.
Retención	Periodo de retención del grupo de retención.
Compresión	Política de compresión del grupo de retención.
Política de supresión	Política de supresión del grupo de retención.
Filtros	Filtros aplicados al grupo de retención. Mueva el puntero de ratón sobre el parámetro **Filtros** para obtener más información sobre los filtros aplicados.
Distribución	Uso del grupo de retención en forma de porcentaje del total de retención de datos en todos los grupos de retención.
Habilitado	Especifica si el grupo de retención está habilitado (verdadero) o inhabilitado (falso).
Fecha de creación	Fecha y hora en que se creó el grupo de retención.
Fecha de modificación	Fecha y hora en que el grupo de retención se modificó por última vez.

La barra de herramientas proporciona las funciones siguientes:

Tabla 32. Barra de herramientas de la ventana de retención

Función	Descripción
Editar	Editar un grupo de retención.
Habilitar/inhabilitar	Habilitar o inhabilitar un grupo de retención. Cuando se inhabilita un grupo, todos los datos nuevos que coincidan con los requisitos del grupo inhabilitado se almacenan en el siguiente grupo que coincida con las propiedades.

Tabla 32. Barra de herramientas de la ventana de retención (continuación)

Función	**Descripción**
Suprimir	Suprimir un grupo de retención. Cuando se suprime un grupo de retención, los datos contenidos en el grupo de retención no se eliminan del sistema; solamente se suprimen los criterios que definen el grupo. Todos los datos se conservan en el almacenamiento.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. Pulse el icono **Retención de sucesos** o **Retención de flujos**.
4. Efectúe una doble pulsación en el primer grupo de retención disponible.
5. Configure los siguientes parámetros:

Parámetro	*Descripción*
Nombre	Escriba un nombre exclusivo para el grupo de retención.
Conservar los datos colocados en este grupo durante	Seleccione un periodo de retención. Cuando el periodo de retención se acaba, los datos se suprimen según el parámetro *Suprimir datos en este grupo*.
Permitir la compresión de los datos de este grupo	Marque la casilla de verificación para habilitar la compresión de datos y luego seleccione un intervalo de tiempo en el cuadro de lista. Cuando el intervalo de tiempo se agota, todos los datos del grupo de retención son candidatos para la compresión. Esto aumenta el rendimiento del sistema, ya que garantiza que no se comprimen datos durante el período de tiempo especificado. La compresión solo tiene lugar cuando el espacio de disco utilizado alcanza el 83% para cargas útiles y el 85% para registros.

Parámetro	*Descripción*
Suprimir datos en este grupo	Seleccione una política de supresión. Seleccione **Cuando se necesite espacio de almacenamiento** si desea que los datos que coincidan con el parámetro *Conservar los datos colocados en este grupo durante* permanezcan en el almacenamiento hasta que el sistema de supervisión de discos detecte que se necesita almacenamiento. Si el espacio de disco alcanza el 85% para los registros y el 83% para las cargas útiles, se suprimirán datos. La supresión continúa hasta que el espacio de disco utilizado llegue al 82% para los registros y al 81% para las cargas útiles. Seleccione **Inmediatamente después de transcurrir el periodo de retención** si desea que los datos se supriman inmediatamente después de comprobar que coinciden con el parámetro **Conservar los datos colocados en este grupo durante**. Los datos se suprimen en el siguiente proceso de mantenimiento de disco planificado, independientemente de las necesidades de compresión o de espacio de disco libre. Cuando se requiere almacenamiento, solo se suprimen los datos que coincidan con el parámetro **Conservar los datos colocados en este grupo durante**.
Descripción	Escriba una descripción para el grupo.
Filtros actuales	Configure los filtros. En la primera lista, seleccione un parámetro por el que desea filtrar. Por ejemplo, Dispositivo, Puerto de origen o Nombre de suceso. En la segunda lista, seleccione el modificador que desea utilizar para el filtro. La lista de modificadores depende del atributo seleccionado en la primera lista. En el campo de texto, escriba información específica relacionada con el filtro y luego pulse **Añadir filtro**. Los filtros se muestran en el cuadro de texto **Filtros actuales**. Puede seleccionar un filtro y pulsar **Eliminar filtro** para eliminar un filtro del cuadro de texto **Filtros actuales**.

6. Pulse **Guardar**.
7. Pulse **Guardar** de nuevo.

   El grupo de retención comienza a almacenar datos que coinciden con los parámetros de retención inmediatamente.

Gestión de la secuencia de los grupos de retención

Puede cambiar el orden de los grupos de retención para asegurarse de que los datos se comparan con los grupos de retención en el orden exigido por sus requisitos.

Acerca de esta tarea

Los grupos de retención se ordenan por prioridad de la fila superior a la fila inferior en las ventanas Retención de sucesos y Retención de flujos. Se almacena un registro en el primer grupo de retención que se corresponde con los parámetros de registro.

No puede mover el grupo de retención predeterminado. Siempre se encuentra al final de la lista.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. Pulse el icono **Retención de sucesos** o **Retención de flujos**.
4. Pulse el icono.
5. Seleccione y mueva el grupo de retención necesario a la ubicación correcta.

Edición de un grupo de retención

Si es necesario, puede editar los parámetros de un grupo de retención.

Acerca de esta tarea

En la ventana de parámetros de retención, el panel Filtros actuales no se visualiza cuando se edita un grupo de retención predeterminado.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. Seleccione una de las opciones siguientes:
4. Pulse el icono **Retención de sucesos**.
5. Pulse el icono **Retención de flujos**.
6. Seleccione el grupo de retención que desee editar y, a continuación, pulse **Editar**.
7. Edite los parámetros. Para obtener más información, consulte el apartado "Configuración de los grupos de retención" en la página 98.
8. Pulse **Guardar**.

Habilitación e inhabilitación de un grupo de retención

Al configurar y guardar un grupo de retención, está habilitado de forma predeterminada. Puede inhabilitar un grupo de retención para ajustar la retención de sucesos o flujos.

Acerca de esta tarea

Cuando se inhabilita un grupo, todos los sucesos o flujos nuevos que coincidan con los requisitos del grupo inhabilitado se almacenan en el siguiente grupo que

coincida con las propiedades de sucesos o flujos.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. Seleccione una de las opciones siguientes:
4. Pulse el icono **Retención de sucesos**.
5. Pulse el icono **Retención de flujos**.
6. Seleccione el grupo de retención que desee inhabilitar y, a continuación, pulse **Habilitar/inhabilitar**.

Supresión de un grupo de retención

Cuando se suprime un grupo de retención, los sucesos o los flujos contenidos en el grupo de retención no se eliminan del sistema; solamente se suprimen los criterios que definen el grupo. Todos los sucesos o flujos se conservan en el almacenamiento.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. Pulse el icono **Retención de sucesos** o el icono **Retención de flujos**.
4. Seleccione el grupo de retención que desee suprimir y, a continuación, pulse **Suprimir**.

Configuración de notificaciones de sistema

Puede configurar alertas de rendimiento del sistema para los umbrales. En esta sección se proporciona información sobre la configuración de los umbrales del sistema.

Acerca de esta tarea

En la tabla siguiente se describen los parámetros de la ventana Notificaciones globales del sistema.

Tabla 33. Parámetros de la ventana Notificaciones globales del sistema

Parámetro	Descripción
Carga del sistema durante 1 minuto	Escriba el promedio de carga del sistema del umbral durante el último minuto.
Carga del sistema durante 5 minutos	Escriba el promedio de carga del sistema del umbral durante los 5 últimos minutos.
Carga del sistema durante 15 minutos	Escriba el promedio de carga del sistema del umbral durante los 15 últimos minutos.
Porcentaje de paginación utilizado	Escriba el porcentaje del umbral de espacio de paginación utilizado.
Paquetes recibidos por segundo	Escriba el número para el umbral de paquetes recibidos por segundo.
Paquetes transmitidos por segundo	Escriba el número para el umbral de paquetes transmitidos por segundo.
Bytes recibidos por segundo	Escriba el número para el umbral de bytes recibidos por segundo.

Tabla 33. Parámetros de la ventana Notificaciones globales del sistema (continuación)

Parámetro	Descripción
Bytes transmitidos por segundo	Escriba el número para el umbral de bytes transmitidos por segundo.
Errores de recepción	Escriba el número para el umbral de paquetes dañados recibidos por segundo.
Errores de transmisión	Escriba el número para el umbral de paquetes dañados transmitidos por segundo.
Colisiones de paquetes	Escriba el número para el umbral de colisiones que se producen por segundo al transmitir paquetes.
Paquetes recibidos descartados	Escriba el número para el umbral de paquetes recibidos que se han descartado por segundo debido a falta de espacio en los almacenamientos intermedios.
Paquetes transmitidos descartados	Escriba el número para el umbral de paquetes transmitidos que se han descartado por segundo debido a falta de espacio en los almacenamientos intermedios.
Errores de portadora en transmisión	Escriba el número para el umbral de errores de portadora que se producen por segundo al transmitir paquetes.
Errores de trama de recepción	Escriba el número para el umbral de errores de alineación de tramas que se producen por segundo en los paquetes recibidos.
Desbordamientos FIFO de recepción	Escriba el número para el umbral de errores de desbordamiento FIFO (primero en entrar, primero en salir) que se producen por segundo en los paquetes recibidos.
Desbordamientos FIFO de transmisión	Escriba el número para el umbral de errores de desbordamiento FIFO (primero en entrar, primero en salir) que se producen por segundo en los paquetes transmitidos.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Notificaciones globales del sistema**.
4. Escriba valores para cada parámetro que desee configurar.
5. Por cada parámetro, seleccione **Habilitado** y **Responder si el valor es** y luego seleccione una de las opciones siguientes:

Opción	Descripción
Mayor que	Se genera una alerta si el valor del parámetro sobrepasa el valor configurado.
Menor que	Se genera una alerta si el valor del parámetro es inferior al valor configurado.

6. Escriba una descripción de la resolución preferida a la alerta.
7. Pulse **Guardar**.
8. En el menú de la pestaña, pulse **Desplegar cambios**.

Configuración de las notificaciones por correo electrónico personalizadas

Cuando configure reglas en QRadar, especifique que cada vez que la regla genere una respuesta, se envíe una notificación por correo electrónico a los destinatarios. La notificación por correo electrónico proporciona información útil, como las propiedades de sucesos o flujos.

Acerca de esta tarea

Puede personalizar el contenido de las notificaciones por correo electrónico acerca de las respuestas de las reglas; para ello, edite el archivo `alert-config.xml`.

Nota: Las referencias a los flujos no se aplican a QRadar Log Manager.

Debe crear un directorio temporal en el que pueda editar con seguridad las copias de los archivos, sin peligro de sobrescribir los archivos predeterminados. Después de editar y guardar el archivo `alert-config.xml`, debe ejecutar un script que valide los cambios. El script de validación aplica automáticamente los cambios en un área intermedia, en la que puede realizar un despliegue mediante el editor de despliegue de QRadar.

Procedimiento

1. Inicie, mediante SSH, la sesión en la consola de QRadar como usuario root.
2. Cree un nuevo directorio temporal que se utilizará para editar de forma segura las copias de los archivos predeterminados.
3. Para copiar los archivos que están almacenados en el directorio `custom_alerts` en el directorio temporal, escriba el mandato siguiente:

   ```
   cp /store/configservices/staging/globalconfig/templates/
   custom_alerts/*.* <nombre_directorio>
   ```

   La opción <nombre_directorio> es el nombre del directorio temporal que ha creado.
4. Confirme que los archivos se han copiado satisfactoriamente:
   a. Para obtener una lista de los archivos del directorio, escriba el mandato siguiente:

      ```
      ls -lah
      ```

   b. Verifique que el archivo siguiente aparece en la lista:

      ```
      alert-config.xml
      ```
5. Abra el archivo `alert-config.xml` para su edición.
6. Para crear varios elementos de plantilla, copie el elemento `<template></template>`, incluidos las etiquetas y el contenido y, a continuación, péguelo debajo del elemento `<template></template>` existente.

   Importante: Establezca la `Propiedad activa` en `Verdadero` para cada tipo de plantilla de suceso y flujo que desea que aparezca como una opción en QRadar.
7. Edite el contenido del elemento `<template></template>`.
   a. Especifique el tipo de plantilla utilizando la siguiente propiedad XML:

      ```
      <templatetype></templatetype>
      ```

      Los valores posibles son suceso (event) o flujo (flow). Este valor es obligatorio.
   b. Especifique el nombre de la plantilla utilizando el siguiente elemento XML:

```
<templatename></templatename>
```

c. Establezca el elemento active en True:

```
<active>true</active>
```

d. Edite el elemento subject, si es necesario.

e. Añada o elimine parámetros del elemento body. Para ver los parámetros válidos, consulte la tabla Parámetros de notificación aceptados.

f. Repita estos pasos para cada plantilla que añada.

8. Guarde y cierre el archivo.
9. Para validar los cambios, escriba el mandato siguiente:

```
/opt/qradar/bin/runCustAlertValidator.sh
                                    <nombre_directorio>
```

La opción *<nombre_directorio>* es el nombre del directorio temporal que ha creado.

Si el script valida el cambio satisfactoriamente, se visualiza el mensaje siguiente:

```
File alert-config.xml was deployed successfully to staging!
```

10. Iniciar sesión en QRadar.
11. Pulse la pestaña **Admin**.
12. Seleccione **Avanzado** > **Desplegar configuración completa**.

Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Ejemplo

Tabla 34. Parámetros de notificación aceptados

Parámetros comunes	Parámetros de suceso	Parámetros de flujo
AppName	EventCollectorID	Type
RuleName	DeviceId	CompoundAppID
RuleDescription	DeviceName	FlowSourceIDs
EventName	DeviceTime	SourceASNList
EventDescription	DstPostNATPort	DestinationASNList
EventProcessorId	SrcPostNATPort	InputIFIndexList
Qid	DstMACAddress	OutputIFIndexList
Category	DstPostNATIPAddress	AppId
RemoteDestinationIP	DstPreNATIPAddress	Host
Payload	SrcMACAddress	Port
Credibility	SrcPostNATIPAddress	SourceBytes
Relevance	SrcPreNATIPAddress	SourcePackets
Source	SrcPreNATPor	Direction
SourcePort	DstPreNATPort	SourceTOS
SourceIP		SourceDSCP
Destination		SourcePrecedence
DestinationPort		DestinationTOS
DestinationIP		DestinationDSCP
DestinationUserName		SourceASN

Tabla 34. Parámetros de notificación aceptados (continuación)

Parámetros comunes	Parámetros de suceso	Parámetros de flujo
Protocol		DestinationASN
StartTime		InputIFIndex
Duration		OutputIFIndex
StopTime		FirstPacketTime
EventCount		LastPacketTime
SourceV6		TotalSourceBytes
DestinationV6		TotalDestinationBytes
UserName		TotalSourcePackets
DestinationNetwork		TotalDestinationPackets
SourceNetwork		SourceQOS
Severity		DestinationQOS
CustomPropertiesList		SourcePayload

Razones de cierre de delito personalizadas

Puede gestionar las opciones que figuran en el cuadro de lista **Razón del cierre** de la pestaña **Delitos**.

Cuando un usuario cierra un delito en la pestaña **Delitos**, se visualiza la ventana Cerrar delito. Se solicita al usuario que seleccione una razón en el cuadro de lista **Razón del cierre**. Aparecen en la lista tres opciones predeterminadas:

- Ajuste de falsos positivos
- Irrelevante
- Violación de política

Los administradores pueden añadir, editar y suprimir razones de cierre de delito en la pestaña **Admin**.

Adición de una razón de cierre de delito personalizada

Cuando se añade una razón de cierre de delito personalizada, la razón nueva aparece listada en la ventana Razones de cierre de delito personalizado y en el cuadro de lista **Razón del cierre** en la ventana Cerrar delito de la pestaña **Delitos**.

Acerca de esta tarea

La ventana Razones de cierre de delito personalizado proporciona los parámetros siguientes.

Tabla 35. Parámetros de la ventana Razones de cierre de delito personalizado

Parámetro	Descripción
Razón	Razón que se muestra en el cuadro de lista **Razón del cierre** de la pestaña **Delitos** de la ventana Cerrar delito.
Creado por	Usuario que ha creado esta razón de cierre de delito personalizada.

Tabla 35. Parámetros de la ventana Razones de cierre de delito personalizado (continuación)

Parámetro	Descripción
Fecha de creación	Fecha y hora en que el usuario ha creado esta razón de cierre de delito personalizada.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Razones de cierre de delito personalizado**.
4. Pulse **Añadir**.
5. Escriba una razón exclusiva del cierre de los delitos. Las razones deben tener entre 5 y 60 caracteres de longitud.
6. Pulse **Aceptar**. La nueva razón de cierre de delito personalizada aparece ahora listada en la ventana Razones de cierre de delito personalizado. En el cuadro de lista **Razón del cierre** de la pestaña **Delitos** de la ventana Cerrar delito también se muestra la razón personalizada.

Edición de una razón de cierre de delito personalizada

La edición de una razón de cierre de delito personalizada actualiza la razón en la ventana Razones de cierre de delito personalizado y en el cuadro de lista **Razón del cierre** de la ventana Cerrar delito, pestaña **Delitos**.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Razones de cierre de delito personalizado**.
4. Seleccione la razón de que desea editar.
5. Pulse **Editar**.
6. Escriba una razón exclusiva del cierre de los delitos. Las razones deben tener entre 5 y 60 caracteres de longitud.
7. Pulse **Aceptar**.

Supresión de una razón de cierre de delito personalizada

La supresión de una razón de cierre de delito personalizada elimina la razón de la ventana Razones de cierre de delito personalizado y del cuadro de lista *Razón del cierre* de la ventana Cerrar delito, pestaña **Delitos**.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Razones de cierre de delito personalizado**.
4. Seleccione la razón de que desea suprimir.
5. Pulse **Suprimir**.
6. Pulse **Aceptar**.

Configuración de una propiedad de activo personalizada

Defina propiedades de activo para facilitar las consultas de activos. Las propiedades personalizadas proporcionan más opciones de consulta.

Procedimiento

1. Pulse la pestaña **Admin**.
2. Pulse **Propiedades de activos personalizadas**.
3. En el campo **Nombre**, escriba un descriptor para la propiedad de activo personalizada.
4. En el menú desplegable **Tipo**, seleccione **Numérico** o **Texto** para definir el tipo de información para la propiedad de activo personalizada.
5. Pulse **Aceptar**.
6. Pulse la pestaña **Activos**.
7. Pulse **Editar activo** > **Propiedades de activos personalizadas**.
8. Especifique la información necesaria en el campo de valor.
9. Pulse **Aceptar**.

Gestión de índices

La característica Gestión de índices le permite controlar la indexación de base de datos en las propiedades de sucesos y flujos.

La indexación de las propiedades de sucesos y flujos permite optimizar las búsquedas. Puede habilitar la indexación en cualquier propiedad que aparezca listada en la ventana Gestión de índices y puede habilitar la indexación en más de una propiedad.

La característica Gestión de índices también proporciona estadísticas, como por ejemplo:

- El porcentaje de búsquedas guardadas en ejecución en el despliegue que incluyen la propiedad indexada
- El volumen de los datos que el índice escribe en el disco durante el periodo de tiempo seleccionado

Para habilitar la indexación de carga útil, debe habilitar la indexación en la propiedad Filtro rápido.

Habilitación de índices

La ventana Gestión de índices lista todas las propiedades de sucesos y flujos que se pueden indexar y proporciona estadísticas para las propiedades. Las opciones de la barra de herramientas permiten habilitar e inhabilitar la indexación en las propiedades de sucesos y flujos seleccionadas.

Acerca de esta tarea

La modificación de la indexación de base de datos puede disminuir el rendimiento del sistema. No olvide supervisar las estadísticas de índice después de habilitar la indexación en varias propiedades.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse *Configuración del sistema*.
3. Pulse el icono **Gestión de índices**.
4. Seleccione una o más propiedades en la lista de Gestión de índices.
5. Seleccione una de las opciones siguientes:
   - Pulse **Habilitar índice**.
   - Pulse **Inhabilitar índice**.
6. Pulse **Guardar**.
7. Pulse **Aceptar**.

Resultados

En las listas que incluyen propiedades de sucesos y flujos, los nombres de las propiedades indexadas se añaden con el texto siguiente: *[Indexado]*. Como ejemplos de estas listas cabe citar los parámetros de búsqueda en las páginas de criterios de búsqueda de las pestañas *Actividad de registro* y *Actividad de red* y la ventana Añadir filtro.

Habilitación de la indexación de carga útil para optimizar los tiempos de búsqueda

Para optimizar los tiempos de búsqueda de sucesos y flujos, habilite la indexación de carga útil en la propiedad **Filtro rápido**.

Restricción:

Utilice la característica **Filtro rápido** de la pestaña **Actividad de registro** y la pestaña **Actividad de red** para buscar cargas útiles de suceso y flujo mediante una serie de texto. La indexación de carga útil aumenta los requisitos de almacenamiento en disco y puede afectar al rendimiento del sistema. Habilite la indexación de carga útil si el despliegue cumple las condiciones siguientes:

- Los procesadores de sucesos y flujos tienen una utilización de disco inferior al 70%.
- Los procesadores de sucesos y flujos están por debajo del 70% de la velocidad máxima de sucesos por segundo (EPS) o flujos por interfaz (FPI).

Procedimiento

1. En el panel de navegación de la pestaña **Admin** del producto QRadar, pulse **Configuración del sistema**.
2. Pulse **Gestión de índices**.
3. En el campo **Búsqueda rápida**, escriba `Filtro rápido`.

   Se muestra la propiedad **Filtro rápido**.
4. Seleccione la propiedad **Filtro rápido** que desea indexar.

   En la tabla de resultados, utilice el valor de la columna **Base de datos** para identificar la propiedad **Filtro rápido** de los sucesos o los flujos.
5. En la barra de herramientas, pulse **Habilitar índice**.

   Un punto verde indica que el índice de carga útil está habilitado.

   Si una lista incluye propiedades de sucesos o flujos que están indexadas, se añaden a los nombres de propiedad el texto siguiente: `[Indexado]`.
6. Pulse **Guardar**.

Qué hacer a continuación

Para gestionar los índices de carga útil, consulte el apartado "Configuración del periodo de retención para los índices de carga útil".

Configuración del periodo de retención para los índices de carga útil

Puede configurar el periodo de tiempo durante el cual los productos de IBM Security QRadar almacenan los índices de carga útil.

De forma predeterminada, los índices de carga útil se conservan durante una semana. El periodo de retención mínimo es un día y el máximo es dos años.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Valores del sistema**.
4. En la sección **Valores de base de datos**, seleccione un periodo de tiempo de retención de la lista **Retención de índice de carga útil**.
5. Pulse **Guardar**.
6. Cierre la ventana Valores del sistema.
7. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Capítulo 7. Gestión de conjuntos de referencia

Con la ventana Gestión de conjuntos de referencia puede crear y gestionar conjuntos de referencia. También pueden importarse elementos en un conjunto de referencia de un archivo externo.

Un conjunto de referencia es un conjunto de elementos que se derivan de sucesos y flujos que se producen en la red. Como ejemplos de elementos que se derivan de sucesos, cabe citar las direcciones IP y los nombres de usuario.

Después de crear un conjunto de referencia, puede crear reglas para detectar la actividad de registro o la actividad de red que está asociada con el conjunto de referencia. Por ejemplo, puede crear una regla para detectar cuándo intenta un usuario no autorizado acceder a los recursos de la red. También puede configurar una regla para añadir un elemento a un conjunto de referencia cuando la actividad de registro o la actividad de red cumple las condiciones de la regla. Por ejemplo, puede crear una regla para detectar cuándo accede un empleado a un sitio web prohibido y añadir la dirección IP de ese empleado a un conjunto de referencia. Para obtener más información sobre la configuración de reglas, consulte la guía del usuario de su producto.

Adición de un conjunto de referencia

En la pestaña **Admin** puede añadir un conjunto de referencia que puede incluir en las pruebas de las reglas.

Acerca de esta tarea

Después de crear un conjunto de referencia, el conjunto de referencia aparece listado en la ventana Gestión de conjuntos de referencia. En el asistente de reglas, este conjunto de referencia aparece como una opción en la página **Respuesta de regla**. Después de configurar una o varias reglas para enviar elementos a este conjunto de referencia, los parámetros **Número de elementos**, **Reglas asociadas** y **Capacidad** se actualizan automáticamente.

Procedimiento

1. En la ventana Gestión de conjuntos de referencia, pulse **Añadir**.
2. Configure los parámetros:

Tabla 36. Parámetros de conjunto de referencia

Parámetro	Descripción
Nombre	Nombre exclusivo para este conjunto de referencia.

© Copyright IBM Corp. 2012, 2015

Tabla 36. Parámetros de conjunto de referencia (continuación)

Parámetro	Descripción
Tipo	Existen 5 tipos de elementos de conjunto de referencia que puede elegir: • **Alfanumérico**: una colección de valores alfanuméricos • **Numérico**: una colección de valores numéricos • **IP** - una colección de direcciones IP • **Puerto**: una colección de números de puerto • **Alfanumérico (sin distinción de mayúsculas/minúsculas)**: una colección de valores alfanuméricos, pero las prueba pasan por alto la combinación de mayúsculas y minúsculas. No se puede editar el parámetro **Tipo** después de crear un conjunto de referencia.
Tiempo de vida de elementos	Utilice este parámetro para indicar si el intervalo **time_to_live** se basa en la primera o la última visualización de los datos. • **Desde el primero visto** - desde el momento en que el elemento se ha insertado por primera vez en el conjunto de referencia • **Desde el último visto** - desde el momento en que el elemento se ha insertado por última vez en el conjunto de referencia Un suceso de **caducidad de datos de referencia** que contiene el nombre del conjunto de referencia y el valor del elemento se desencadena cuando caduca un elemento de conjunto de referencia. De forma predeterminada, todos los elementos se conservan indefinidamente. Si no deselecciona el recuadro **Vive para siempre**, el elemento nunca caduca.

3. Pulse **Crear**.

Sucesos de caducidad de elemento

Puede utilizar los sucesos creados cuando caducan elementos en un conjunto de referencia para hacer un seguimiento de aspectos tales como cuentas de usuario caducadas en la red.

De forma predeterminada, todos los elementos de conjunto de referencia se conservan indefinidamente, lo que significa que existen en el conjunto de referencia hasta que se eliminan. Sin embargo, puede establecer el tiempo de vida del elemento para que se cree un suceso que contenga el nombre del conjunto de referencia y el valor del elemento cuando caduque el elemento.

Puede utilizar estos sucesos para detectar, por ejemplo, la no utilización de las cuentas de red:

1. Cree un conjunto de referencia para realizar el seguimiento de usuarios caducados. Establezca el tiempo de vida de los elementos para reflejar un periodo razonable de inactividad de cuenta.
2. Cree una regla de suceso personalizado para añadir datos de inicio de sesión (como **username**) como elementos al conjunto de referencia.
3. Si no se han añadido datos para un usuario concreto dentro del periodo de tiempo de vida, el elemento del conjunto de referencia caduca y se desencadena un suceso de **Caducidad de datos de referencia**.
4. A continuación, puede utilizar la pestaña **Actividad de registro** para realizar un seguimiento de los sucesos.

Edición de un conjunto de referencia

Utilice la ventana Gestión de conjuntos de referencia para editar un conjunto de referencia.

Procedimiento

1. En la ventana **Gestión de conjuntos de referencia**, seleccione un conjunto de referencia.
2. Pulse **Editar**.
3. Edite los parámetros.

Tabla 37. Parámetros de conjunto de referencia

Parámetro	Descripción
Nombre	Nombre exclusivo para este conjunto de referencia. La longitud máxima es de 255 caracteres.
Tipo	No se puede editar el parámetro **Tipo** después de crear un conjunto de referencia.
Tiempo de vida de elementos	Cantidad de tiempo que desea conservar cada elemento en el conjunto de referencia. Si especifica una cantidad de tiempo, también debe indicar cuándo desea empezar a contar el tiempo para un elemento. **Vive para siempre** es el valor predeterminado.

4. Pulse **Enviar**.

Supresión de conjuntos de referencia

Puede suprimir un conjunto de referencia en la ventana Gestión de conjuntos de referencia.

Acerca de esta tarea

Cuando se suprimen conjuntos de referencia, una ventana de confirmación indica si los conjuntos de referencia que desea suprimir tienen reglas que están asociadas

con ellos. Después de suprimir un conjunto de referencia, el valor de configuración **Añadir a un conjunto de referencia** se borra de las reglas asociadas.

Consejo: Antes de suprimir un conjunto de referencia, puede ver las reglas asociadas en la pestaña **Referencia**.

Procedimiento

Seleccione una de las opciones siguientes:

- En la ventana Gestión de conjuntos de referencia, seleccione un conjunto de referencia y luego pulse **Suprimir**.
- En la ventana Gestión de conjuntos de referencia, utilice el cuadro de texto **Búsqueda rápida** para visualizar solamente los conjuntos de referencia que desee suprimir y luego pulse **Suprimir listados**.

Visualización del contenido de un conjunto de referencia

La pestaña **Contenido** proporciona una lista de los elementos que están incluidos en este conjunto de referencia.

Procedimiento

1. En la ventana Gestión de conjuntos de referencia, seleccione un conjunto de referencia.
2. Pulse **Ver contenido**.
3. Para ver el contenido, pulse la pestaña **Contenido**.

   Consejo: Utilice el campo **Búsqueda rápida** para filtrar elementos específicos. Todos los elementos que coinciden con la palabra clave se muestran en la lista **Contenido**. A continuación, puede seleccionar la acción en la barra de herramientas.

Tabla 38. Parámetros de la pestaña Contenido

Parámetro	Descripción
Valor	Valor del elemento. Por ejemplo, si la referencia contiene una lista de direcciones IP, el valor es la dirección IP.
Origen	Se coloca ***nombre_regla*** en el conjunto de referencia como respuesta a una regla. El **Usuario** se importa de un archivo externo o se añade manualmente al conjunto de referencia.
Tiempo de vida	Tiempo que queda hasta que este elemento se elimine del conjunto de referencia.
Fecha de última aparición	Fecha y hora en que este elemento se ha detectado por última vez en la red.

4. Pulse la pestaña **Referencias** y vea las referencias.

Consejo: Utilice el campo **Búsqueda rápida** para filtrar elementos específicos. Todos los elementos que coinciden con la palabra clave se muestran en la lista **Contenido**. A continuación, puede seleccionar la acción en la barra de herramientas.

Tabla 39. Parámetros de la pestaña Contenido

Parámetro	Descripción
Nombre de regla	Nombre de esta regla.
Grupo	Nombre del grupo al que pertenece esta regla.
Categoría	Categoría de la regla. Las opciones disponibles son **Regla personalizada** y **Regla de detección de anomalías**.
Tipo	Tipo de esta regla.
Habilitado	Indica si la regla está habilitada o inhabilitada.
Respuesta	Respuestas que se han configurado para esta regla.
Origen	**Sistema** indica que se trata de una regla predeterminada. **Modificado** indica que una regla predeterminada se ha personalizado. **Usuario** indica que se trata de una regla creada por el usuario.

5. Para ver o editar una regla asociada, efectúe una doble pulsación en la regla en la lista **Referencias**.

   En el asistente de reglas puede editar los valores de configuración de las reglas.

Adición de un elemento a un conjunto de referencia

Puede añadir un elemento a un conjunto de referencia mediante la ventana Gestión de conjuntos de referencia.

Procedimiento

1. En la ventana Gestión de conjuntos de referencia, seleccione un conjunto de referencia.
2. Pulse **Ver contenido**.
3. Pulse la pestaña **Contenido**.
4. En la barra de herramientas, pulse **Nuevo**.
5. Configure los siguientes parámetros:

Parámetro	Descripción
Valor(es)	Si desea escribir varios valores, incluya un carácter separador entre cada valor y luego especifique el carácter de separador en el campo **Carácter separador**.
Carácter separador	Escriba el carácter separador que ha utilizado en el campo **Valor(es)**.

6. Pulse **Añadir**.

Supresión de elementos de un conjunto de referencia

Puede suprimir elementos de un conjunto de referencia.

Procedimiento

1. En la ventana Gestión de conjuntos de referencia, seleccione un conjunto de referencia.
2. Pulse **Ver contenido**.
3. Pulse la pestaña **Contenido**.
4. Seleccione una de las opciones siguientes:
   - Seleccione un elemento y después pulse **Suprimir**.
   - Utilice el cuadro de texto **Búsqueda rápida** para visualizar solamente los elementos que desee suprimir y luego pulse **Suprimir listados**.
5. Pulse **Suprimir**.

Importación de elementos a un conjunto de referencia

Puede importar elementos de un archivo de texto o CSV externo.

Antes de empezar

Asegúrese de que el archivo de texto o CSV que desea importar está almacenado en su sistema local.

Procedimiento

1. En la ventana Gestión de conjuntos de referencia, seleccione un conjunto de referencia.
2. Pulse **Ver contenido**.
3. Pulse la pestaña **Contenido**.
4. En la barra de herramientas, pulse **Importar**.
5. Pulse **Examinar**.
6. Seleccione el archivo de texto o CSV que desea importar.
7. Pulse **Importar**.

Exportación de elementos de un conjunto de referencia

Puede exportar elementos a un archivo de texto o CSV externo.

Procedimiento

1. En la ventana Gestión de conjuntos de referencia, seleccione un conjunto de referencia.
2. Pulse **Ver contenido**.
3. Pulse la pestaña **Contenido**.
4. En la barra de herramientas, pulse **Exportar**.
5. Seleccione una de las opciones siguientes:
6. Si desea abrir la lista para visualizarla de inmediato, seleccione la opción **Open with** y seleccione una aplicación en el cuadro de lista.
7. Si desea guardar la lista, seleccione la opción **Save File**.
8. Pulse **Aceptar**.

Capítulo 8. Gestionar recopilaciones de datos de referencia con el programa de utilidad de datos de referencia

Utilice el programa de utilidad `ReferenceDataUtil.sh` para realizar recopilaciones de datos de referencia complejos.

Utilice el programa de utilidad de datos de referencia para gestionar recopilaciones de datos de referencia de la línea de mandatos. Puede utilizar `ReferenceDataUtil.sh` para crear los tipos de recopilación de datos de referencia siguientes:

- Correlación de referencia
- Correlación de referencia de conjuntos
- Correlación de referencia de correlaciones
- Tabla de referencia

Creación de una recopilación de datos de referencia

Utilice el programa de utilidad `ReferenceDataUtil.sh` para crear una recopilación de datos de referencia.

Procedimiento

1. Inicie, mediante SSH, la sesión en QRadar como usuario root.
2. Vaya al directorio /opt/qradar/bin.
3. Para crear la recopilación de datos de referencia, escriba el mandato siguiente:

   ```
   ./ReferenceDataUtil.sh create name [MAP | MAPOFSETS | MAPOFMAPS |
   REFTABLE] [ALN | NUM | IP | PORT | ALNIC | DATE]
   [-timeoutType=[FIRST_SEEN | LAST_SEEN]] [-timeToLive=]
   ```

4. Para llenar la correlación con los datos de un archivo externo, escriba el mandato siguiente:

   ```
   ./ReferenceDataUtil.sh load nombre nombre_archivo [-encoding=...]
   [-sdf=" ... "]
   ```

Ejemplo

```
Crear una correlación alfanumérica
 ./ReferenceDataUtil.sh create testALN MAP ALN

Crear una correlación de conjuntos de valores PORT que caducará 3 horas después
de que se haya visto por última vez
 ./ReferenceDataUtil.sh create testPORT MAPOFSETS PORT -timeoutType=LAST_SEEN
-timeToLive='3 hours'

Crear una correlación de correlaciones de valores numéricos que caducará 3 horas y 15
minutos después de que haya visto por primera vez
 ./ReferenceDataUtil.sh create testNUM MAPOFMAPS NUM -timeoutType=FIRST_SEEN
-timeToLive='3 hours 15 minutes'

Crear una tabla de referencia con un valor predeterminado de valores alfanuméricos
 ./ReferenceDataUtil.sh create testTable REFTABLE ALN
-keyType=ipKey:IP,portKey:PORT,numKey:NUM,dateKey:DATE
```

© Copyright IBM Corp. 2012, 2015

Qué hacer a continuación

Inicie la sesión en la interfaz de usuario para crear reglas que añadan datos a las recopilaciones de datos de referencia. También puede crear pruebas de reglas que detecten si hay actividad por parte de los elementos que se encuentran en la recopilación de datos de referencia. Para obtener más información sobre la creación de reglas y las pruebas de las reglas, consulte la guía del usuario de su producto.

Referencia de mandatos de ReferenceDataUtil.sh

Puede gestionar las recopilaciones de datos de referencia con el programa de utilidad `ReferenceDataUtil.sh`.

create

Crea una recopilación de datos de referencia.

nombre
Nombre de la recopilación de datos de referencia.

[MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]
Tipo de la recopilación de datos de referencia.

[ALN | ALNIC | NUM | IP | PORT | DATE]
Tipo de datos del conjunto de referencia:

- **ALN** especifica una recopilación de datos de referencia de valores alfanuméricos. Este tipo de datos da soporte a las direcciones IPv4 e IPv6.
- **ALNIC** especifica una recopilación de datos de referencia de valores alfanuméricos, pero las prueba pasan por alto la combinación de mayúsculas y minúsculas. Este tipo de datos da soporte a las direcciones IPv4 e IPv6.
- **NUM** especifica una recopilación de datos de referencia de valores numéricos.
- **IP** especifica una recopilación de datos de referencia de direcciones IP. Este tipo de datos solamente da soporte a la dirección IPv4.
- **PORT** especifica una recopilación de datos de referencia de direcciones de puerto.
- **DATE** especifica una recopilación de datos de referencia de valores de fecha.

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]
Especifica si la cantidad de tiempo que los elementos de datos permanecen en la recopilación de datos de referencia se calcula desde el momento en que el elemento se ha visto por primera vez o por última vez.

[-TimeToLive='']
Cantidad de tiempo que los elementos de datos permanecen en la recopilación de datos de referencia.

[-keyType=name:elementType,name:elementType,...]
Parámetro **REFTABLE** obligatorio que consta de pares de nombre de clave y **ELEMENTTYPE**.

[-key1Label='']
Etiqueta opcional para key1, o la clave primaria. Una clave es un tipo de información, como por ejemplo una dirección IP.

[-valueLabel='']
Etiqueta opcional para los valores de la recopilación.

update

Actualiza una recopilación de datos de referencia.

nombre
Nombre de la recopilación de datos de referencia.

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]
Especifica si la cantidad de tiempo que los elementos de datos permanecen en la recopilación de datos de referencia se calcula desde el momento en que el elemento se ha visto por primera vez o por última vez.

[-timeToLive='']
Cantidad de tiempo que los elementos de datos permanecen en la recopilación de datos de referencia.

[-keyType=name:elementType,name:elementType,...]
Parámetro **REFTABLE** obligatorio que consta de pares de nombre de clave y **elementType**.

[-key1Label='']
Etiqueta opcional para key1.

[-valueLabel='']
Etiqueta opcional para los valores de la recopilación.

add

Añade un elemento de datos a una recopilación de datos de referencia.

nombre
Nombre de la recopilación de datos de referencia.

<valor> <clave1> [clave2]
Par de clave-valor que desea añadir. MAP y MAPOFSETS requieren la clave 1. MAPOFMAPS y REFTABLE requieren la clave 1 y la clave 2. Las claves son series alfanuméricas. La clave 2 es la clave de segundo nivel y es necesaria cuando se realiza una adición o una supresión en una recopilación MAPOFMAPS o REFTABLE.

[-sdf=" ... "]
Serie de formato de fecha simple que se utiliza para analizar los datos de fecha.

delete

Suprime un elemento de una recopilación de datos de referencia.

nombre
Nombre de la recopilación de datos de referencia.

<valor> <clave1> [clave2]
Par de clave-valor que desea suprimir. MAP y MAPOFSETS requieren la clave 1. MAPOFMAPS y REFTABLE requieren la clave 1 y la clave 2. Las claves son series alfanuméricas.

[-sdf=" ... "]
Serie de formato de fecha simple que se utiliza para analizar los datos de fecha.

remove

Elimina una recopilación de datos de referencia.

nombre
Nombre de la recopilación de datos de referencia.

purge

Purga todos los elementos de una recopilación de datos de referencia.

nombre
Nombre de la recopilación de datos de referencia.

list

Lista los elementos de una recopilación de datos de referencia.

nombre
Nombre de la recopilación de datos de referencia.

[displayContents]
Lista todos los elementos de una recopilación de datos de referencia.

listall

Lista todos los elementos de todas las recopilaciones de datos de referencia.

[displayContents]
Lista todos los elementos de todas las recopilaciones de datos de referencia.

load

Llena una recopilación de datos de referencia con datos de un archivo CSV externo.

nombre
Nombre de la recopilación de datos de referencia.

nombre_archivo
Nombre de archivo completo que se cargará. Cada línea del archivo representa un registro que se añadirá a la recopilación de datos de referencia.

[-encoding=...]
Codificación que se utiliza para leer el archivo.

[-sdf=" ... "]
Serie de formato de fecha simple que se utiliza para analizar los datos de fecha.

Capítulo 9. Gestión de servicios autorizados

En la pestaña **Admin** pueden configurarse servicios autorizados para autenticarun servicio de soporte al cliente o una llamada de API para el despliegue de QRadar.

La autenticación de un servicio de soporte al cliente permite al servicio conectarse con su interfaz de usuario de QRadar y rechazar o actualizar las notas de un delito mediante un servicio web. Un servicio autorizado puede añadirse o revocarse en cualquier momento.

La API RESTful de QRadar utiliza servicios autorizados para autenticar las llamadas de API a la consola de QRadar. Para obtener más información sobre la API RESTful, consulte la publicación *IBM Security QRadar API Guide*.

La ventana Gestionar servicios autorizados proporciona la información siguiente:

Tabla 40. Parámetros de servicios autorizados

Parámetro	Descripción
Nombre del servicio	Nombre del servicio autorizado.
Autorizado por	Nombre del usuario o administrador que autorizó la adición del servicio.
Señal de autenticación	Señal que está asociada con este servicio autorizado.
Rol de usuario	Rol de usuario que está asociado con este servicio autorizado.
Perfil de seguridad	Perfil de seguridad que está asociado con este servicio autorizado.
Creado	Fecha en que se ha creado este servicio autorizado.
Caduca	Fecha y hora en que el servicio autorizado caduca. De forma predeterminada, el servicio autorizado es válido durante 30 días.

Visualización de servicios autorizados

La ventana Servicios autorizados muestra una lista de servicios autorizados, desde la que puede copiar la señal correspondiente al servicio.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Servicios autorizados**.
4. En la ventana Gestionar servicios autorizados, seleccione el servicio autorizado adecuado.

   La señal se visualiza en el campo **Señal seleccionada** de la barra superior. Puede copiar la señal en el software del proveedor para su autenticación con QRadar.

© Copyright IBM Corp. 2012, 2015

Adición de un servicio autorizado

Utilice la ventana Añadir servicio autorizado para añadir un nuevo servicio autorizado.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Servicios autorizados**.
4. Pulse **Añadir servicio autorizado**.
5. En el campo **Nombre del servicio**, escriba el nombre de este servicio autorizado. El nombre puede tener una longitud máxima de 255 caracteres.
6. En la lista **Rol de usuario**, seleccione el rol de usuario que desee asignar a este servicio autorizado. Los roles de usuario asignados a un servicio autorizado determinan las funciones a las que dicho servicio puede acceder en la interfaz de usuario de QRadar.
7. En la lista **Perfil de seguridad**, seleccione el perfil de seguridad que desee asignar a este servicio autorizado. El perfil de seguridad determina las redes y los orígenes de registro a los que este servicio puede acceder en la interfaz de QRadar.
8. En la lista **Fecha de caducidad**, escriba o seleccione la fecha en la que desea que caduque este servicio. Si no hace falta una fecha de caducidad, seleccione **Sin caducidad**.
9. Pulse **Crear servicio**.

   El mensaje de confirmación contendrá un campo de señal que tendrá que copiar en el software del proveedor para la autenticación con IBM Security QRadar.

Revocación de servicios autorizados

Utilice la ventana Añadir servicio autorizado para revocar un servicio autorizado.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Servicios autorizados**.
4. En la ventana Gestionar servicios autorizados, seleccione el servicio que desea revocar.
5. Pulse **Revocar autorización**.

Capítulo 10. Gestionar la copia de seguridad y la recuperación

Puede realizar operaciones de copia de seguridad y recuperación de los datos y la información de QRadar.

Puede utilizar la funcionalidad de copia de seguridad y recuperación para hacer una copia de seguridad de los datos de sucesos y flujos; sin embargo, los datos de sucesos y flujos deberán restaurarse de forma manual. Para obtener ayuda para restaurar los datos de sucesos y flujos, consulte la nota técnica referente a la restauración de los datos (*Restoring Your Data Technical Note*).

De forma predeterminada, QRadar crea un archivo de copia de seguridad de la información de configuración a diario a media noche. El archivo de copia de seguridad contiene la información de configuración, los datos o ambas cosas correspondientes al día anterior.

Puede utilizar dos tipos de copias de seguridad: las copias de seguridad de la configuración y las copias de seguridad de datos.

Las copias de seguridad de la configuración incluyen los siguientes componentes:

- Activos
- Certificados
- Logotipos personalizados
- Reglas personalizadas
- Módulos de soporte de dispositivos (DSM)
- Categorías de sucesos
- Orígenes de flujo
- Búsquedas de flujos y sucesos
- Grupos
- Información de gestión de índices
- Información de clave de licencia
- Orígenes de registro
- Delitos
- Elementos de conjuntos de referencia
- Planificación de almacenamiento y reenvío
- Información de usuarios y roles de usuarios
- Datos de vulnerabilidad (si QRadar Vulnerability Manager está instalado)

Las copias de seguridad de los datos incluyen la siguiente información:

- Información del registro de auditoría
- Datos de sucesos
- Datos de flujo
- Datos de informe
- Índices

© Copyright IBM Corp. 2012, 2015

Gestión de los archivos de copia de seguridad

Vea y gestione los archivos de copia de seguridad.

En la ventana Gestión de archivos de copia de seguridad, puede ver y gestionar todos los archivos de copia de seguridad creados satisfactoriamente.

Visualización de los archivos de copia de seguridad

Utilice la ventana Archivos de copia de seguridad para ver una lista de los archivos de copia de seguridad.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Copia de seguridad y recuperación**.

Importación de un archivo de copia de seguridad

La importación de un archivo de copia de seguridad es útil si desea restaurar un archivo de copia de seguridad que se ha creado en otro host de QRadar.

Acerca de esta tarea

Si coloca un archivo de copia de seguridad de QRadar en el directorio `/store/backupHost/inbound` del servidor de la consola, el archivo de copia de seguridad se importa automáticamente.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Copia de seguridad y recuperación**.
4. En el campo **Cargar archivo**, pulse **Examinar**.
5. Localice y seleccione el archivo que desea cargar. El archivo debe tener la extensión .tgz.
6. Pulse **Abrir**.
7. Pulse **Cargar**.

Supresión de un archivo de copia de seguridad

Para suprimir un archivo de copia de seguridad, el archivo de copia de seguridad y el componente de contexto de host deben hallarse en el mismo sistema. El sistema también debe estar en comunicación con la consola y no puede haber otra copia de seguridad en curso.

Acerca de esta tarea

Si se suprime un archivo de copia de seguridad, se elimina del disco y de la base de datos. Asimismo, se elimina la entrada correspondiente en esta lista y se genera un suceso de auditoría para informar de la eliminación.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.

3. Pulse **Copia de seguridad y recuperación**.
4. En la sección **Copias de seguridad existentes**, seleccione el archivo que desea suprimir.
5. Pulse **Suprimir**.

Creación de un archivo de copia de seguridad

De forma predeterminada, QRadar crea un archivo de copia de seguridad de la información de configuración a diario a media noche. El archivo de copia de seguridad contiene la información de configuración, los datos o ambas cosas correspondientes al día anterior. Puede personalizar esta copia de seguridad nocturna y crear una copia de seguridad de la configuración bajo demanda, según sea necesario.

Planificación de la copia de seguridad nocturna

Utilice la ventana Configuración de la recuperación de copias de seguridad para configurar un proceso nocturno de copia de seguridad.

Acerca de esta tarea

De forma predeterminada, el proceso de copia de seguridad nocturna solamente incluye los archivos de configuración. Puede personalizar el proceso de copia de seguridad nocturna para que incluya datos de la consola y de determinados hosts gestionados. También puede personalizar el periodo de retención de copia de seguridad, la ubicación del archivo de copia de seguridad, el límite de tiempo para que se procese una copia de seguridad antes de que se produzca un tiempo de espera excedido y la prioridad de copia de seguridad en relación con otros procesos de QRadar.

Nota: Para garantizar un rendimiento óptimo, es aconsejable no planificar la ejecución de la copia de seguridad nocturna a la misma hora que las actualizaciones automáticas de QRadar.

La ventana Configuración de la recuperación de copias de seguridad proporciona los siguientes parámetros:

Tabla 41. Parámetros de Configuración de la recuperación de copias de seguridad

Parámetro	Descripción
Configuración general de la copia de seguridad	

Tabla 41. Parámetros de Configuración de la recuperación de copias de seguridad (continuación)

Parámetro	Descripción
Vía de acceso del repositorio de seguridad	Escriba la ubicación en la que desea almacenar el archivo de copia de seguridad. La ubicación predeterminada es `/store/backup`. Esta vía de acceso debe existir antes de que se inicie el proceso de copia de seguridad. Si esta vía de acceso no existe, el proceso de copia termina anormalmente. Si modifica esta vía de acceso, asegúrese de que la nueva vía de acceso sea válida en todos los sistemas del despliegue. • Los datos activos se almacenan en el directorio `/store`. Si tiene tanto datos activos como archivos de copia de seguridad almacenados en el mismo directorio, podría alcanzarse con facilidad la capacidad de almacenamiento de datos y las copias de seguridad planificadas podrían fallar. Le recomendamos que especifique una ubicación de almacenamiento en otro sistema o que copie los archivos de copia de seguridad a otro sistema una vez finalizado el proceso de copia de seguridad. Puede utilizar una solución de almacenamiento de Network File System (NFS) en el despliegue de QRadar. Para obtener más información sobre el uso de NFS, consulte la publicación *Offboard Storage Guide*.
Periodo de retención de copia de seguridad (días)	Escriba o seleccione el periodo de tiempo, en días, que desea almacenar los archivos de copia de seguridad. El valor por omisión es de 2 días. Este periodo de tiempo solamente afecta a los archivos de copia generados como resultado de un proceso planificado. No se ven afectados por este valor las copias de seguridad bajo demanda ni los archivos de copia de seguridad importados.
Plan de copia de seguridad nocturna	Seleccione una opción de copia de seguridad.

Tabla 41. Parámetros de Configuración de la recuperación de copias de seguridad (continuación)

Parámetro	Descripción
Seleccione los hosts gestionados que desee que ejecuten copias de seguridad de datos:	Esta opción solamente se visualiza si selecciona la opción **Copias de seguridad de la configuración y datos**. Se listan todos los hosts del despliegue. El primer host de la lista es la consola; de forma predeterminada está habilitada para copia de seguridad de datos y por tanto no aparece una casilla de verificación. Si tiene hosts gestionados en el despliegue, los hosts gestionados aparecen en la lista debajo de la consola y cada host gestionado incluye una casilla de verificación. Seleccione la casilla de verificación de los hosts gestionados en los que desee ejecutar las copias de seguridad de datos. En cada host (de la consola o gestionado), puede borrar opcionalmente los elementos de datos que desea excluir del archivo de copia de seguridad.
Copia de seguridad de la configuración sólo	
Límite de tiempo de copia de seguridad (min)	Escriba o seleccione el periodo de tiempo, en minutos, que desea permitir que se ejecute la copia de seguridad. El valor predeterminado es de 180 minutos. Si el proceso de copia de seguridad sobrepasa el límite de tiempo configurado, el proceso de copia de seguridad se cancela de forma automática.
Prioridad de copia de seguridad	Seleccione en este cuadro de lista el nivel de importancia que desea que el sistema dé al proceso de copia de seguridad de la configuración en comparación con otros procesos. Una prioridad media o alta tiene mayor impacto sobre el rendimiento del sistema.
Copia de seguridad de datos	
Límite de tiempo de copia de seguridad (min)	Escriba o seleccione el periodo de tiempo, en minutos, que desea permitir que se ejecute la copia de seguridad. El valor predeterminado es de 1020 minutos. Si el proceso de copia de seguridad sobrepasa el límite de tiempo configurado, la copia de seguridad se cancela de forma automática.

Tabla 41. Parámetros de Configuración de la recuperación de copias de seguridad (continuación)

Parámetro	Descripción
Prioridad de copia de seguridad	Seleccione en la lista el nivel de importancia que desea que el sistema dé al proceso de copia de seguridad de los datos en comparación con otros procesos. Una prioridad media o alta tiene mayor impacto sobre el rendimiento del sistema.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Copia de seguridad y recuperación**.
4. En la barra de herramientas, pulse **Configurar**.
5. En la ventana Configuración de la recuperación de copias de seguridad, personalice la copia de seguridad nocturna.
6. Pulse **Guardar**.
7. Cierre la ventana Archivos de copia de seguridad.
8. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Creación de un archivo de copia de seguridad de la configuración bajo demanda

Si tiene que hacer una copia de seguridad de los archivos de configuración en un momento distinto del de la copia de seguridad nocturna planificada, puede crear un archivo de copia de seguridad bajo demanda. Los archivos de copia de seguridad bajo demanda solo incluyen información de configuración.

Acerca de esta tarea

Inicie un archivo de copia de seguridad bajo demanda durante un periodo en el que QRadar tenga poca carga de proceso, como puede ser fuera del horario de oficina habitual. Durante el proceso de copia de seguridad, el rendimiento del sistema se ve afectado.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Copia de seguridad y recuperación**.
4. En la barra de herramientas, pulse **Copia de seguridad a petición**.
5. Especifique los valores de los parámetros siguientes:

Opción	Descripción
Nombre	Escriba un nombre exclusivo que desee asignar a este archivo de copia de seguridad. El nombre puede tener una longitud máxima de 100 caracteres alfanuméricos. El nombre puede contener los caracteres siguientes: signo de subrayado (_), guión (-) o punto (.).
Descripción	Escriba una descripción para este archivo de copia de seguridad de la configuración. La descripción puede tener como máximo 255 caracteres.

6. Pulse **Ejecutar copia de seguridad**.

   No puede iniciar un nuevo proceso de copia de seguridad o de restauración mientras no haya acabado la copia de seguridad bajo demanda. Puede supervisar el proceso del archivo de copia de seguridad en la ventana Archivos de copia de seguridad. Consulte el apartado "Visualización de los archivos de copia de seguridad" en la página 124.

Restauración de los archivos de copia de seguridad

La restauración de un archivo de copia de seguridad es útil cuando se desea restaurar en el sistema QRadar archivos de configuración, datos de delitos y datos de activos previamente archivados.

Antes de restaurar un archivo de copia de seguridad, tenga en cuenta las siguientes consideraciones:

- Solo puede restaurar un archivo de copia de seguridad creado en el mismo release de software, incluido el nivel de parche. Por ejemplo, si ejecuta IBM Security QRadar 7.1.0 (MR2), el archivo de copia de seguridad debe haberse creado en IBM Security QRadar.
- El proceso de restauración solamente restaura la información de configuración, los datos de delitos y los datos de activos. Para obtener ayuda para restaurar los datos de sucesos o flujos, consulte la nota técnica *Restoring Your Data*.
- Si el archivo de copia de seguridad se ha originado en un sistema de consola habilitado para NAT, solamente podrá restaurar ese archivo de copia de seguridad en un sistema habilitado para NAT.

Durante el proceso de restauración, se efectúan los pasos siguientes en la consola:

1. Se hace copia de seguridad de los archivos y las tablas de base de datos existentes.
2. Tomcat se cierra.
3. Todos los procesos del sistema se cierran.
4. Los archivos se extraen del archivo de copia de seguridad y se restauran en disco.
5. Las tablas de base de datos se restauran.
6. Todos los procesos del sistema se reinician.
7. Tomcat se reinicia.

Restauración de un archivo de copia de seguridad

Puede restaurar un archivo de copia de seguridad. La restauración de un archivo de copia de seguridad es útil si se produce una anomalía de hardware del sistema o si desea almacenar un archivo de copia de seguridad en un dispositivo sustituto.

Acerca de esta tarea

Puede reiniciar la consola solamente después de que el proceso de restauración se haya completado.

El proceso de restauración puede durar hasta varias horas dependiendo del tamaño del archivo de copia de seguridad que deba restaurarse. Cuando haya finalizado, se visualizará un mensaje de confirmación.

Una ventana proporciona el estado del proceso de restauración. Esta ventana proporciona los errores para cada host y las instrucciones para resolver los errores.

Los parámetros siguientes están disponibles en la ventana Restaurar una copia de seguridad:

Tabla 42. Parámetros de Restaurar una copia de seguridad

Parámetro	Descripción
Nombre	Nombre del archivo de copia de seguridad.
Descripción	Descripción, si procede, del archivo de copia de seguridad.
Tipo	Tipo de copia de seguridad. Solamente se pueden restaurar las copias de seguridad de la configuración; por lo tanto, este parámetro muestra **config**.
Seleccionar todos los elementos de configuración	Cuando se selecciona, esta opción indica que todos los elementos de configuración se incluyen en la restauración del archivo de copia de seguridad.
Restaurar configuración	Lista los elementos de configuración que se incluirán en la restauración del archivo de copia de seguridad. Para eliminar elementos, puede deseleccionar las casillas de verificación de cada elemento que desee eliminar o deseleccionar la casilla de verificación **Seleccionar todos los elementos de configuración**.
Seleccionar todos los elementos de datos	Cuando se selecciona, esta opción indica que todos los elementos de datos se incluyen en la restauración del archivo de copia de seguridad.
Restaurar datos	Lista los elementos de configuración que se incluirán en la restauración del archivo de copia de seguridad. Todos los elementos están deseleccionados de forma predeterminada. Para restaurar elementos de datos, puede seleccionar las casillas de verificación de cada elemento que desee restaurar.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Copia de seguridad y recuperación**.
4. Seleccione el archivo que desee restaurar.
5. Pulse **Restaurar**.
6. En la ventana Restaurar una copia de seguridad, configure los parámetros.
7. Pulse **Restaurar**.
8. Pulse **Aceptar**.
9. Pulse **Aceptar**.
10. Seleccione una de las opciones siguientes:
    - Si la interfaz de usuario se ha cerrado durante el proceso de restauración, abra un navegador web e inicie sesión en QRadar.
    - Si no se ha cerrado la interfaz de usuario, se mostrará la ventana de inicio de sesión. Inicie la sesión en QRadar.
11. Siga las instrucciones en la ventana de estado.

Qué hacer a continuación

Una vez comprobado que los datos se han restaurado en el sistema, asegúrese de que también se hayan restaurado los DSM, los exploradores de evaluaciones de vulnerabilidad (VA) y los protocolos de origen de registro.

Si el archivo de la copia de seguridad se ha originado en un clúster de alta disponibilidad, debe pulsar **Desplegar cambios** para restaurar la configuración del clúster de alta disponibilidad una vez finalizada la restauración. Si la replicación de disco está habilitada, el host secundario sincroniza inmediatamente los datos una vez restaurado el sistema. Si el host secundario se ha eliminado del despliegue después de una copia de seguridad, el host secundario muestra un estado anómalo en la ventana Gestión del sistema y licencias.

Restauración de un archivo de copia de seguridad creado en otro sistema de QRadar

Cada archivo de copia de seguridad incluye la información de dirección IP del sistema en el que se ha creado. Cuando se restaura un archivo de copia de seguridad de un sistema de QRadar distinto, la dirección IP del archivo de copia de seguridad y la del sistema que está restaurando no coinciden. Puede corregir las direcciones IP no coincidentes.

Acerca de esta tarea

Puede reiniciar la consola solamente después de que el proceso de restauración se haya completado.

El proceso de restauración puede durar hasta varias horas dependiendo del tamaño del archivo de copia de seguridad que deba restaurarse. Cuando haya finalizado, se visualizará un mensaje de confirmación.

Una ventana proporciona el estado del proceso de restauración. Esta ventana proporciona los errores para cada host y las instrucciones para resolver los errores.

Debe detener el servicio iptables en cada host gestionado del despliegue. El servicio Iptables es un cortafuegos basado en Linux.

La ventana Restaurar una copia de seguridad (accesibilidad de hosts gestionados) proporciona la información siguiente:

Tabla 43. Parámetros de Restaurar una copia de seguridad (accesibilidad de hosts gestionados)

Parámetro	Descripción
Nombre de host	Nombre del host gestionado.
Dirección IP	Dirección IP del host gestionado.
Estado de acceso	Estado de acceso al host gestionado.

La ventana Restaurar una copia de seguridad proporciona los siguientes parámetros:

Tabla 44. Parámetros de Restaurar una copia de seguridad

Parámetro	Descripción
Nombre	Nombre del archivo de copia de seguridad.
Descripción	Descripción, si procede, del archivo de copia de seguridad.
Tipo	Tipo de copia de seguridad. Solamente se pueden restaurar las copias de seguridad de la configuración; por lo tanto, este parámetro muestra **config**.
Seleccionar todos los elementos de configuración	Cuando se selecciona, esta opción indica que todos los elementos de configuración se incluyen en la restauración del archivo de copia de seguridad. Esta casilla de verificación está seleccionada de forma predeterminada. Para borrar todos los elementos de configuración, desmarque la casilla de verificación.
Restaurar configuración	Lista los elementos de configuración que se incluirán en la restauración del archivo de copia de seguridad. Todos los elementos están seleccionados de forma predeterminada. Para eliminar elementos, puede deseleccionar las casillas de verificación de cada elemento que desee eliminar o deseleccionar la casilla de verificación **Seleccionar todos los elementos de configuración**.
Seleccionar todos los elementos de datos	Cuando se selecciona, esta opción indica que todos los elementos de datos se incluyen en la restauración del archivo de copia de seguridad. Esta casilla de verificación está seleccionada de forma predeterminada. Para borrar todos los elementos de datos, desmarque esta casilla de verificación.

Tabla 44. Parámetros de Restaurar una copia de seguridad (continuación)

Parámetro	Descripción
Restaurar datos	Lista los elementos de configuración que se incluirán en la restauración del archivo de copia de seguridad. Todos los elementos están deseleccionados de forma predeterminada. Para restaurar elementos de datos, puede seleccionar las casillas de verificación de cada elemento que desee restaurar.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Copia de seguridad y recuperación**.
4. Seleccione el archivo que desee restaurar.
5. Pulse **Restaurar**.
6. En la ventana Restaurar una copia de seguridad, configure los parámetros.
7. Pulse **Restaurar**.
8. Detenga las tablas IP:
   a. Inicie, mediante SSH, la sesión en el host gestionado como usuario root.
   b. Escriba el mandato **`service iptables stop`**.
   c. Repita esta acción para todos los hosts gestionados del despliegue.
9. En la ventana Restaurar una copia de seguridad, pulse **Probar acceso a hosts**.
10. Cuando la prueba se haya realizado con todos los hosts gestionados, verifique que en la columna **Estado de acceso** se indica que el estado es **Correcto**.
11. Si en la columna **Estado de acceso** aparece el estado **Sin acceso** para un host, detenga iptables de nuevo y, a continuación, pulse **Probar acceso a hosts** otra vez para intentar establecer conexión.
12. En la ventana Restaurar una copia de seguridad, configure los parámetros.
13. Pulse **Restaurar**.
14. Pulse **Aceptar**.
15. Pulse **Aceptar** para iniciar sesión.
16. Seleccione una de las opciones siguientes:
    - Si la interfaz de usuario se ha cerrado durante el proceso de restauración, abra un navegador web e inicie sesión en QRadar.
    - Si no se ha cerrado la interfaz de usuario, se mostrará la ventana de inicio de sesión. Inicie la sesión en QRadar.
17. Vea el resultado del proceso de restauración y siga las instrucciones para resolver los errores que puedan haberse producido.
18. Renueve la ventana del navegador web.
19. En la pestaña **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.

    Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Qué hacer a continuación

Una vez comprobado que los datos se han restaurado en el sistema, debe volver a aplicar los RPM para los DSM, los exploradores de evaluaciones de vulnerabilidad (VA) o los protocolos de origen de registro.

Si el archivo de la copia de seguridad se ha originado en un clúster de alta disponibilidad, debe pulsar **Desplegar cambios** para restaurar la configuración del clúster de alta disponibilidad una vez finalizada la restauración. Si la replicación de disco está habilitada, el host secundario sincroniza inmediatamente los datos una vez restaurado el sistema. Si el host secundario se ha eliminado del despliegue después de una copia de seguridad, el host secundario muestra un estado anómalo en la ventana Gestión del sistema y licencias.

Restauración de datos

Puede restaurar los datos en consola de QRadar y los hosts gestionados a partir de los archivos de copia de seguridad. La parte de datos de los archivos de copia de seguridad incluye información como por ejemplo información de dirección IP de destino, datos de activo, información de categoría de suceso, datos de vulnerabilidad,datos de flujo y datos de suceso.

Cada host gestionado del despliegue, incluido consola de QRadar, crea todos los archivos de copia de seguridad en el directorio `/store/backup/`. El sistema podría incluir un montaje `/store/backup` de un servicio de SAN o NAS externo. Los servicios externos proporcionan retención de datos fuera de línea a largo plazo, que suele ser necesaria para las regulaciones de conformidad, como PCI.

Restricción: Debe restaurar la copia de seguridad de la configuración antes de restaurar la copia de seguridad de los datos.

Antes de empezar

Asegúrese de que se cumplen las condiciones siguientes:

- Si va a restaurar datos en un consola de QRadar nuevo, se ha restaurado la copia de seguridad de la configuración.
- Sabe la ubicación del host gestionado en el que se ha hecho la copia de seguridad de los datos.
- Si el despliegue incluye un punto de montaje diferente para ese volumen, el directorio `/store` o `/store/ariel` tiene espacio suficiente para los datos que desea recuperar.
- Sabe la fecha y la hora de los datos que desea recuperar.

Procedimiento

1. Inicie, mediante SSH, la sesión en QRadar como usuario root.
2. Vaya al directorio `/store/backup`.
3. Para obtener una lista de los archivos de copia de seguridad, escriba `ls -l`.
4. Si aparece una lista de archivos de copia de seguridad, escriba `cd /` para ir al directorio raíz.

   Importante: Los archivos restaurados deben estar en el directorio `/store`. Si escribe `cd` en lugar de `cd /`, los archivos se restauran en el directorio `/root/store`.

5. Para extraer los archivos de copia de seguridad a su directorio original, escriba el mandato siguiente:

   ```
   tar -zxpvPf /store/backup/backup.<nombre>.<ID_host_nombre_host>
   .<fecha destino>.<tipo de copia de seguridad>.<indicación de fecha y hora>.tgz
   ```

Tabla 45. Descripción de las variables de nombre de archivo

Variable de nombre de archivo	Descripción
ID_host_nombre_host	Nombre del sistema de QRadar en el que se aloja el archivo de copia de seguridad seguido del identificador del sistema de QRadar
fecha destino	Fecha en que se ha creado el archivo de copia de seguridad. El formato de la fecha de destino es *<día>_<mes>_<año>*.
tipo de copia de seguridad	Las opciones son `data` o `config`.
indicación de fecha y hora	Hora en que se ha creado el archivo de copia de seguridad.

Resultados

La copia de seguridad diaria captura todos los datos de cada host. Si desea restaurar datos en un host gestionado que contiene solamente datos de suceso o flujo, únicamente se restauran esos datos en ese host.

Verificación de los datos restaurados

Verifique que los datos se hayan restaurado correctamente en IBM Security QRadar.

Procedimiento

1. Para verificar que los archivos se han restaurado, revise el contenido de uno de los directorios restaurados con el mandato siguiente:

   ```
   cd /store/ariel/flows/payloads/<aaaa/mm/dd>
   ```

   ```
   cd /store/ariel/events/payloads/<aaaa/mm/dd>
   ```

   Puede ver los directorios restaurados que se crean para cada hora del día. Si faltan directorios, puede que no se hayan capturado los datos correspondientes a ese periodo de tiempo.
2. Verifique que los datos restaurados están disponibles.
   a. Inicie la sesión en la interfaz de QRadar.
   b. Pulse la pestaña **Actividad de registro** o **Actividad de red**.
   c. Seleccione **Editar búsqueda** en la lista **Buscar** de la barra de herramientas.
   d. En el panel Rango de tiempo de la ventana Buscar, seleccione **Intervalo específico**.
   e. Seleccione el rango de tiempo de los datos que ha restaurado y luego pulse **Filtro**.
   f. Vea el resultado para verificar los datos restaurados.
   g. Si los datos restaurados no están disponibles en la interfaz de QRadar, verifique que se hayan restaurado en la ubicación correcta y que los permisos de archivo estén bien configurados.

      Los archivos restaurados deben estar en el directorio `/store`. Si ha escrito `cd` en lugar de `cd /` al extraer los archivos restaurados, compruebe si en el directorio `/root/store` están los archivos restaurados. Si no ha cambiado de

directorios antes de extraer los archivos restaurados, compruebe si los archivos restaurados están en el directorio `/store/backup/store`.

Normalmente, los archivos se restauran con los permisos originales. Sin embargo, si los archivos son propiedad de la cuenta de usuario root, pueden producirse problemas. Si los archivos son propiedad de la cuenta de usuario root, cambie los permisos mediante los mandatos **chown** y **chmod**.

Qué hacer a continuación

Una vez comprobado que los datos se han restaurado, debe volver a aplicar los RPM para los DSM, los exploradores de evaluaciones de vulnerabilidad (VA) y los protocolos de origen de registro.

Capítulo 11. Editor de despliegue

Utilice el editor de despliegue para gestionar los componentes individuales de QRadar. Después de configurar el despliegue, puede acceder a los componentes individuales de cada host gestionado del despliegue y configurarlo.

Requisitos del editor de despliegue

Antes de utilizar el editor de despliegue, asegúrese de que cumple los requisitos mínimos del sistema.

El editor de despliegue requiere Java™ Runtime Environment (JRE). Puede descargar Java 1.6 ó 1.7 del sitio web de Java (www.java.com). Si utiliza el navegador web Mozilla Firefox, debe configurarlo para aceptar los archivos JNLP (Java Network Protocol Language).

Muchos navegadores web que utilizan el motor de Microsoft Internet Explorer, como Maxthon, instalan componentes que pueden ser incompatibles con la pestaña **Admin**. Puede que tenga que inhabilitar los navegadores web que están instalados en el sistema.

Para acceder al editor de despliegue desde detrás de un servidor proxy o un cortafuegos, debe configurar los valores de proxy adecuados en el escritorio. El software entonces podrá detectar automáticamente los valores de proxy desde el navegador.

Para configurar los valores de proxy, abra la configuración de Java en el Panel de control y configure la dirección IP del servidor proxy. Para obtener más información, consulte la documentación de Microsoft.

Vistas del editor de despliegue

El editor de despliegue proporciona las diferentes vistas del despliegue.

Puede acceder al editor de despliegue mediante la pestaña **Admin**. Puede utilizar el editor de despliegue para crear el despliegue, asignar conexiones y configurar cada componente.

Después de actualizar los valores de configuración con el editor de despliegue, debe guardar los cambios en el área de transferencia. Debe desplegar manualmente todos los cambios mediante la opción de menú de la pestaña **Admin**. A continuación todos los cambios desplegados se aplican en el despliegue.

El editor de despliegue proporciona las vistas siguientes:

Vista de sistema

Utilice la página System View para asignar un componente de software a los hosts gestionados del despliegue. La página System View incluye todos los hosts gestionados del despliegue. Un host gestionado es un sistema del despliegue que tiene software de QRadar instalado.

© Copyright IBM Corp. 2012, 2015

De forma predeterminada, la página System View también incluye los componentes siguientes:

- **Contexto de host**, que supervisa todos los componentes de QRadar para garantizar que el funcionamiento de cada componentes es el previsto.
- **Acumulador**, que analiza los flujos, los sucesos, la creación de informes, la escritura de datos de base de datos y las alertas a un módulo de soporte de dispositivo (DSM).

  Un acumulador se halla en cualquier host que contenga un Procesador de sucesos.

En la página System View, el panel de la izquierda proporciona una lista de hosts gestionados, que puede ver y configurar. El editor de despliegue sondea el despliegue para comprobar si hay actualizaciones de los hosts gestionados. Si el editor de despliegue detecta un cambio en un host gestionado del despliegue, se visualiza un mensaje en el que se le informa del cambio. Por ejemplo, si se elimina un host gestionado, se visualiza un mensaje que indica que los componentes asignados a ese host deben reasignarse a otro host.

Asimismo, si añade un host gestionado al despliegue, el editor de despliegue muestra un mensaje que indica que el host gestionado se ha añadido.

Vista de sucesos

Utilice la página Event View para crear una vista de los componentes:

- Componentes de QRadar QFlow Collector
- Procesadores de sucesos
- recopiladores de sucesos de QRadar
- Orígenes externos
- Destinos externos
- Componentes de Magistrado
- Nodos de datos

En la página Event View, el panel de la izquierda proporciona una lista de los componentes que puede añadir a la vista. El panel de la derecha proporciona una vista del despliegue.

Vista de vulnerabilidades

Utilice la página Vulnerability View para crear una vista de los componentes de IBM Security QRadar Vulnerability Manager. Debe instalar IBM Security QRadar Vulnerability Manager para ver esta vista. Para obtener más información, consulte la publicación *IBM Security QRadar Vulnerability Manager Guía del usuario*.

Configuración de preferencias del editor de despliegue

Puede configurar las preferencias del editor de despliegue para modificar los incrementos del zoom y la frecuencia de sondeo de presencia.

Procedimiento

1. Seleccione **Archivo** > **Edit Preferences**.
2. Para configurar el parámetro **Presence Poll Frequency**, escriba la frecuencia, en milisegundos, con la que desea que el host gestionado supervise el despliegue para comprobar si hay actualizaciones.

3. Para configurar el parámetro **Zoom Increment**, escriba el valor de incremento cuando la opción de zoom esté seleccionada.

   Por ejemplo, 0,1 indica el 10%.

Creación del despliegue mediante el Editor de despliegue

Utilice el Editor de despliegue en la pestaña **Admin** para añadir y configurar componentes en el despliegue de IBM Security QRadar. También puede utilizar el Editor de despliegue para visualizar el despliegue.

Antes de empezar

Para añadir hosts gestionados a un despliegue existente o para añadir recopiladores de sucesos de QRadar,Procesadores de flujos, u otros dispositivos a su despliegue, utilice **Acciones de despliegue** en el **Gestión del sistema y licencias** en la pestaña **Admin**.

Para poder utilizar el editor de despliegue, asegúrese de que se cumplen las condiciones siguientes:

- Instale Java Runtime Environment (JRE). Puede descargar Java 1.6 ó 1.7 del sitio web de Java (www.java.com).
- Si utiliza el navegador Firefox, debe configurarlo para aceptar los archivos JNLP (Java Network Protocol Language).
- Planifique el despliegue de QRadar, incluidas las direcciones IP y la información de inicio de sesión para todos los dispositivos del despliegue.

Procedimiento

1. Pulse la pestaña **Admin** y pulse **Editor de despliegue**.
2. Pulse la pestaña **Vista de sucesos** y añada componentes de suceso al despliegue.
3. Pulse la pestaña **Vista de sistema** y construya el sistema.
4. Configure los componentes.
5. Para dividir el despliegue en fases, en el Editor de despliegue, pulse **File** > **Save to Staging**.
6. Despliegue la configuración eligiendo una de las opciones siguientes en la pestaña **Admin**, en consola de QRadar.
   - Pulse **Desplegar cambios**.
   - Pulse **Avanzado** > **Desplegar configuración completa**.

   Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Tareas relacionadas:

"Despliegue de hosts gestionados y componentes después de la instalación" en la página 53

Después de la instalación puede añadir hosts gestionados al despliegue. Para facilitar la distribución de los procesos, puede añadir recopiladores de sucesos de QRadar, QRadar Procesadores de flujos u otros dispositivos al despliegue.

Generación de claves públicas para los productos de QRadar

Para reenviar sucesos normalizados en el editor de despliegue de IBM Security QRadar, debe copiar el archivo de clave pública, `/root/.ssh/id_rsa.pub`, del origen externo al destino externo.

Si el origen externo y el destino externo están en sistemas distintos, la clave pública se genera automáticamente. Si el origen y el destino externos están en un sistema "all-in-one", la clave pública no se genera automáticamente. Debe generar la clave pública de forma manual.

Procedimiento

Para generar manualmente la clave pública, siga estos pasos:

1. Utilice SSH para iniciar la sesión en el sistema como usuario root.
2. Para generar la clave pública, escriba el mandato siguiente:

   ```
   opt/qradar/bin/ssh-key-generating
   ```
3. Pulse Intro.

   El par de clave pública y clave privada se genera y se guarda en la carpeta `/root/.ssh/id_rsa`.

Gestión de la vista de sucesos

Utilice la página Event View para crear y gestionar los componentes del despliegue.

Creación de la vista de sucesos

Para crear la vista de sucesos, siga estos pasos:

1. Añada componentes a la vista.
2. Conecte los componentes.
3. Conecte los despliegues.
4. Cambie el nombre de los componentes de modo que cada componente tenga un nombre exclusivo.

Vistas de sucesos de componentes de QRadar en el despliegue

Utilice la página Vista de sucesos para crear una vista de los componentes de IBM Security QRadar, incluidos los componentes QRadar QFlow Collectors, Procesadores de sucesos, recopiladores de sucesos de QRadar, orígenes externos, destinos externos y Magistrado.

QRadar QFlow Collector

QRadar VFlow Collector recopila los flujos de red procedentes de los dispositivos de la red. Se incluyen los canales de información en directo y grabados, como los registros de flujo de TAP de red, puertos SPAN, NetFlow y QRadar.

QRadar QFlow Collector agrupa en un flujo los paquetes individuales relacionados. Un flujo se inicia cuando QRadar QFlow Collector detecta el primer paquete que tiene una dirección IP de origen, un puerto de origen y un puerto de destino únicos, así como otras opciones de protocolo específicas.

Cada paquete nuevo se evalúa. Los recuentos de bytes y paquetes se añaden a los contadores estadísticos del registro de flujo. Al final de un intervalo, se envía un registro de estado del flujo a un Recopilador de sucesos y los contadores estadísticos del flujo se restablecen. Un flujo finaliza cuando no se detecta actividad para el flujo dentro del periodo de tiempo configurado.

Si el protocolo no da soporte a las conexiones de puerto, QRadar combina todos los paquetes entre los dos hosts en un único registro de flujo. Sin embargo, QRadar QFlow Collector no registra los flujos hasta que se establece una conexión con otro componente de QRadar y los datos se recuperan.

Recopilador de sucesos

Recopila sucesos de seguridad procedentes de los dispositivos de seguridad, que se conocen como orígenes de registro, de la red.

El Recopilador de sucesos normaliza los sucesos recopilados y envía la información al Procesador de sucesos.

Puede conectar un Procesador de sucesos no de consola a un Procesador de sucesos en consola de QRadar o a otro Procesador de sucesos del despliegue. El acumulador recopila la información de flujos y sucesos del Procesador de sucesos.

El Procesador de sucesos de consola de QRadar siempre está conectado a Magistrado. Esta conexión no puede suprimirse.

Nodo de datos

El Nodo de datos recibe flujos y sucesos de seguridad de los procesadores de sucesos y flujos.

El Nodo de datos almacena estos datos de seguridad en disco.

El Nodo de datos está siempre conectado a componentes de Procesador de sucesos o Procesador de flujos.

Origen externo

Origen de datos externo que reenvía datos normalizados a un Recopilador de sucesos. Puede configurar un origen externo para recibir los datos y cifrarlos antes de reenviarlos.

Las últimas versiones de los sistemas de QRadar pueden recibir datos de las versiones anteriores de los sistemas de QRadar. Sin embargo, las versiones anteriores no pueden recibir datos de las versiones más recientes. Para evitarlo, actualice todos los receptores antes de actualizar los remitentes.

Destino externo

Indica un dispositivo externo que recibe datos de sucesos o flujos. Un destino externo puede recibir datos procedentes solamente de un Recopilador de sucesos.

Las últimas versiones de los sistemas de QRadar pueden recibir datos de las versiones anteriores de los sistemas de QRadar. Sin embargo, las versiones anteriores no pueden recibir datos de las versiones más recientes. Para evitarlo, actualice todos los receptores antes de actualizar los remitentes.

Magistrado

Puede añadir un componente Magistrado para cada despliegue. Magistrado proporciona vistas, informes, alertas y análisis del tráfico de red y de los sucesos de seguridad. Magistrado procesa los sucesos o flujos utilizando las reglas personalizadas que están configuradas para crear una respuesta. Si no existen reglas personalizadas, Magistrado utiliza el conjunto de reglas predeterminado para procesar el suceso o flujo problemático.

Magistrado da prioridad a la respuesta y asigna un valor de magnitud que se basa en varios factores, que incluyen el número de respuestas, la gravedad, la relevancia y la credibilidad.

Una vez que Magistrado establezca la magnitud, proporcionará varias opciones para la resolución.

Adición de componentes

Cuando configure el despliegue, debe utilizar la página Event View del editor de despliegue para añadir los componentes.

Puede añadir los siguientes componentes de QRadar a la página Event View:

- Recopilador de sucesos
- Procesador de sucesos
- Origen externo
- Destino externo
- QRadar QFlow Collector
- Nodo de datos

Procedimiento

1. En la pestaña **Admin**, pulse **Editor de despliegue**.
2. En el panel Event Components, seleccione el componente que desee añadir al despliegue.
3. Escriba un nombre exclusivo para el componente que desea añadir y pulse **Siguiente**.

   Restricción: El nombre puede tener una longitud máxima de 20 caracteres y puede incluir signos de subrayado y guiones.
4. En el cuadro de lista **Select a host to assign to**, seleccione un host gestionado y pulse **Siguiente**.
5. Pulse **Finalizar**.
6. Repita los pasos del 3 al 5 para cada uno de los componentes que desea añadir a la vista.
7. En el menú del editor de despliegue, seleccione **File > Save to Staging**.

   El editor de despliegue guarda los cambios en el área de transferencia y se cierra automáticamente.
8. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Conexión de componentes

Después de añadir todos los componentes necesarios en la página Event View, debe conectarlos.

Acerca de esta tarea

Utilice la página Event View para conectar los componentes entre sí. Se aplican algunas restricciones. Por ejemplo, puede conectar un Recopilador de sucesos a un Procesador de sucesos, pero no a un componente Magistrado.

En la tabla siguiente se describen los componentes que se pueden conectar.

Tabla 46. Descripción de las conexiones de componentes soportadas

Conexión de origen	Conexión de destino	Descripción
QRadar QFlow Collector	Recopilador de sucesos	QRadar QFlow Collector puede conectarse solamente a un Recopilador de sucesos. QRadar QFlow Collector no puede conectarse a un Recopilador de sucesos de un dispositivo 15xx. El número de conexiones no está restringido.
Recopilador de sucesos	Procesador de sucesos	Un Recopilador de sucesos solamente se puede conectar a un único Procesador de sucesos. Un Recopilador de sucesos de consola se puede conectar solamente a un Procesador de sucesos de consola. Esta conexión no puede eliminarse. Un recopilador de sucesos no de consola puede conectarse a un Procesador de sucesos en el mismo sistema. Un Recopilador de sucesos no de consola puede conectarse a un Procesador de sucesos remoto, pero solamente si el Procesador de sucesos no existe en la consola.
Recopilador de sucesos	Destino externo	El número de conexiones no está restringido.
Origen externo	Recopilador de sucesos	El número de conexiones no está restringido. Un Recopilador de sucesos conectado a un dispositivo de solo sucesos no puede recibir una conexión externa desde hardware del sistema que tenga habilitada la característica **Receive Flows**. Un Recopilador de sucesos conectado a un dispositivo de solo QFlow no puede recibir una conexión externa desde un sistema remoto si el sistema tiene habilitada la característica **Receive Events**.

Tabla 46. Descripción de las conexiones de componentes soportadas (continuación)

Conexión de origen	Conexión de destino	Descripción
Procesador de sucesos	Magistrado (MPC)	Solamente se puede conectar un Procesador de sucesos a Magistrado.
Procesador de sucesos	Procesador de sucesos	Un Procesador de sucesos de consola no se puede conectar a un Procesador de sucesos no de consola. Un Procesador de sucesos no de consola se puede conectar a otro Procesador de sucesos de consola o no de consola, pero no a ambos al mismo tiempo. Un Procesador de sucesos no de consola se conecta a un Procesador de sucesos de consola cuando se añade un host gestionado no de consola.
Nodo de datos	Procesador de sucesos	Solo se puede conectar un nodo de datos a un procesador de sucesos o flujos. Puede conectar varios Nodos de datos al mismo procesador de sucesos para crear un clúster de almacenamiento.

Procedimiento

1. En la página Event View, seleccione el componente para el que desea establecer una conexión.
2. Pulse **Acciones** > **Add Connection**.

   Se visualiza una flecha en la correlación. La flecha representa una conexión entre dos componentes.
3. Arrastre el final de la flecha al componente con el que desea establecer una conexión.
4. Opcional: Configure el filtrado del flujo en una conexión entre QRadar QFlow Collector y un Recopilador de sucesos.
   a. Pulse el botón derecho del ratón en la flecha que hay entre QRadar QFlow Collector y el Recopilador de sucesos; a continuación, pulse **Configurar**.
   b. En el campo correspondiente al parámetro **Filtros de flujos**, escriba las direcciones IP o las direcciones CIDR de los recopiladores de sucesos de QRadar a los que desea que QRadar QFlow Collector envíe los flujos.
5. Pulse **Guardar**.
6. Repita estos pasos para todos los componentes restantes que requieran conexiones.

Reenvío de sucesos y flujos normalizados

Para reenviar sucesos y flujos normalizados, configure un Recopilador de sucesos externo en el despliegue actual para recibir sucesos y flujos de un Recopilador de sucesos externo asociado en el despliegue receptor.

Acerca de esta tarea

Puede añadir los siguientes componentes a la página Event View:

- **Off-site Source** es un Recopilador de sucesos externo del que desea recibir datos de suceso y flujos.

  Restricción: El origen externo debe estar configurado con los permisos adecuados para enviar datos de sucesos y flujos al destino externo.
- **Off-site Target** es un Recopilador de sucesos externo al que desea enviar datos de suceso y flujos.

Ejemplo:

Para reenviar sucesos y flujos normalizados entre dos despliegues (A y B), donde el despliegue B desea recibir sucesos y flujos del despliegue A:

1. Configure el despliegue A con un destino externo para proporcionar la dirección IP del host gestionado que contiene el recopilador de sucesos B.
2. Conecte el recopilador de sucesos A al destino externo.
3. En el despliegue B, configure un origen externo con la dirección IP del host gestionado que incluye el Recopilador de sucesos A y el puerto que el Recopilador de sucesos está supervisando.

Si desea desconectar el origen externo, debe eliminar las conexiones de ambos despliegues. En el despliegue A, elimine el destino externo y, en el despliegue B, elimine el origen externo.

Para habilitar el cifrado entre los despliegues, debe habilitar el cifrado tanto en el origen externo como en el destino externo. Además, debe asegurarse de que la clave pública SSH para el origen externo (cliente) está disponible para el destino (servidor) para garantizar el acceso adecuado. Por ejemplo, para habilitar el cifrado entre el origen externo y el Recopilador de sucesos B:

1. Cree claves SSH con el mandato **ssh-keygen -1 -t rsa** y pulse Intro cuando se le pregunte sobre el directorio y la frase de contraseña. Esta acción coloca el archivo en el directorio `//root/.ssh` de forma predeterminada.
2. Copie el archivo `id_rsa.pub` en el directorio `/root/.ssh` del Recopilador de sucesos y la consola de origen. Cambie el nombre del archivo por `authorized_keys`.

   Si no se le han asignado privilegios de propietario rw (chmod 600 authorized_keys) sobre el archivo y el directorio padre, puede utilizar el mandato **ssh-copy-id**. Por ejemplo, **ssh-copy-id -i nombre_usuario_host@IP_host**. Con **-i** se especifica que se utilizará el archivo de identidad `/root/.ssh/id_rsa.pub`. Por ejemplo, `ssh-copy-id -i root@10.100.133.80`. Este mandato añadirá todas las entradas o creará un archivo `authorized_keys` en la consola de destino con los privilegios adecuados. No comprueba si hay entradas duplicadas. El archivo `authorized_keys` también debe estar presente en la consola en la que se utilizan otras características. Si un host gestionado se añade a una consola que reenvía sucesos, también debe haber un archivo `authorized_keys` en el directorio `/root/.ssh` correspondiente. Si no es así, la adición de un host gestionado fallará. Esto es necesario independientemente de si se utiliza o no el cifrado entre el host gestionado y la consola.
3. En la consola de origen, cree un archivo llamado `ssh_keys_created` en `/opt/qradar/conf`. Este archivo debe crearse para que el reenvío de sucesos y flujos no se interrumpa cuando otras características (tales como la adición de

un host gestionado a una de las consolas) se utilicen juntas. Cambie el propietario y el grupo por **nobody** y el permiso por **775** si es necesario. Ejecute `chown nobody:nobody /opt/qradar/conf/ssh_keys_created` y `chmod 775 /opt/qradar/conf/ssh_keys_created` para asegurarse de que se puede hacer una copia de seguridad y una restauración del archivo correctamente.

4. Siga el paso de origen y destino externos para dos consolas. Programe la consola de destino primero y luego despliegue los cambios. Programe la consola de origen a continuación y luego despliegue los cambios.

El diagrama siguiente muestra el reenvío de sucesos y flujos entre los despliegues.

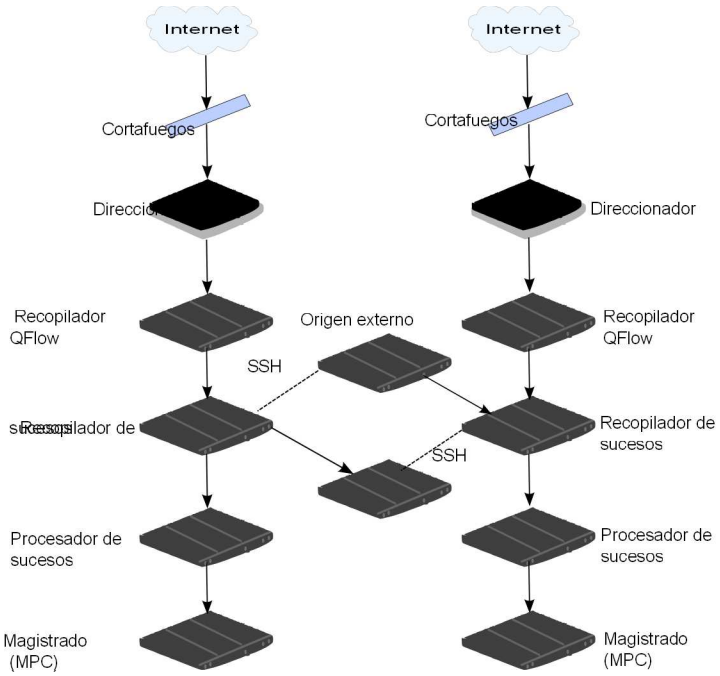

Figura 1. Reenvío de sucesos entre los despliegues con SSH

Si el origen o el destino externos están en un sistema "all-in-one", la clave pública no se genera automáticamente; por lo tanto, debe generarla manualmente. Para obtener más información sobre la generación de claves públicas, consulte la documentación de Linux.

Si actualiza la configuración de Recopilador de sucesos o los puertos de supervisión, debe actualizar manualmente las configuraciones de origen y de destino para mantener la conexión entre los despliegues.

Procedimiento

1. En la pestaña **Admin**, pulse **Editor de despliegue**.
2. En el panel Event Components, seleccione **Off-site Source** o bien **Off-site Target**.
3. Escriba un nombre exclusivo para el origen externo o el destino externo. El nombre puede tener una longitud máxima de 20 caracteres y puede incluir signos de subrayado y guiones. Pulse **Siguiente**.
4. Especifique los valores para los parámetros y pulse **Finalizar**.

El nombre de host del campo **Enter a name for the off-site host** puede contener un máximo de 20 caracteres y puede incluir caracteres de subrayado o guiones.

Si selecciona la casilla **Encrypt traffic from off-site source**, también debe seleccionar la casilla de cifrado en el origen y el destino externos asociados.

5. Repita la acción para todos los orígenes y destinos externos restantes.
6. En el menú del editor de despliegue, pulse **File** > **Save to Staging**.
7. En el menú de pestaña **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.

   Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Reenvío de flujos de filtrado

Puede configurar el reenvío de flujos de filtrado. Puede utilizar flujos filtrados para dividir el reenvío de flujos en varios recuadros y para reenviar flujos específicos para determinadas investigaciones.

Procedimiento

1. En el sistema de destino, configure el sistema de origen como un origen fuera de sitio.
   a. En la pestaña **Admin**, pulse **Gestión del sistema y licencias** > **Acciones de despliegue** > **Gestionar orígenes externos**.
   b. Añada la dirección IP del sistema de origen y seleccione **Recibir sucesos** o **Recibir flujos**.
   c. Seleccione **Gestionar conexiones** y elija el host que se espera que reciba la conexión fuera del sitio.
   d. Pulse **Guardar**.
   e. Seleccione **Despliegue de configuración completa** en el menú **Avanzado** para que los cambios surtan efecto.
2. En el sistema de origen, configure el destino del reenvío, la dirección IP y el número de puerto.
   a. Pulse **Menú principal** > **Admin**.
   b. Pulse **Destinos de reenvío** > **Añadir**.
   c. Configure la dirección IP del sistema de destino y el puerto de destino.
   d. Introduzca 32000 para el número de puerto en el sistema de origen. El puerto 32000 se utiliza para el reenvío de flujos.
   e. Seleccione **Normalizado** en la lista **Formato de suceso**.
3. Configuración de reglas de direccionamiento.
   a. Pulse **Menú principal** > **Admin**.
   b. Pulse **Reglas de direccionamiento** > **Añadir**.
   c. Seleccione las reglas que desee añadir.

      Nota: Las reglas solamente reenvían correctamente los flujos basados en delitos, o información de CRE, si **Reenvío fuera de linea** está seleccionado en la pantalla Reglas de direccionamiento.

   Se reenvían los flujos que se han filtrado en la pantalla **Reglas de direccionamiento**.

Cambio de nombre de componentes

Debe cambiar el nombre de un componente en la vista para identificarlo de forma exclusiva en el despliegue.

Procedimiento

1. En el panel Event Components, seleccione el componente cuyo nombre desea cambiar.
2. Pulse **Actions** > **Rename Component**.
3. Escriba un nombre nuevo para el componente.

   El nombre debe ser alfanumérico sin caracteres especiales.
4. Pulse **Aceptar**.

Visualización del progreso del reequilibrado de datos

Después de instalar un Nodo de datos en el despliegue, consulte el progreso de los datos que se mueven entre el procesador de sucesos y el Nodo de datos. Si el reequilibrado de datos se ha completado, puede ver información adicional sobre los nodos de datos desplegados.

Procedimiento

1. En consola de QRadar pulse la pestaña **Admin** para ver el estado de los nodos de datos del despliegue en la parte superior de la ventana.
2. Pulse **Ver** en la columna **Detalle** para abrir la ventana **Detalles de sistema y licencia**.
3. Consulte el progreso de cualquier operación de reequilibrado de datos y la capacidad del dispositivo del Nodo de datos en el panel **Distribución de datos de seguridad**.

Archivado del contenido de los nodos de datos

Cuando se establece un dispositivo de nodo de datos en la modalidad de archivo, no se escriben datos en el dispositivo. Los datos existentes se guardan.

Procedimiento

1. En el editor de despliegue, pulse el botón derecho del ratón en el nodo de datos que desea establecer en la modalidad de archivo y pulse **Configurar**.
2. Pulse **Archivar**.
3. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.
4. Si desea reanudar el equilibrado de datos en un nodo de datos que se encuentra en modalidad de archivado, pulse **Configurar** > **Activo**.

Guardar datos del procesador de sucesos en un dispositivo de nodo de datos

Mejore el rendimiento del procesador de sucesos guardando todos los datos en un dispositivo de nodo de datos en lugar de guardarlos en el procesador de sucesos. Si no hay ningún dispositivo de nodo de datos activo disponible en el mismo clúster que el procesador de sucesos, el procesador de sucesos guarda los datos localmente. Cuando haya un dispositivo de nodo de datos disponible, transfiere tantos datos como sea posible desde el procesador de sucesos. Los nodos de datos equilibran los datos de manera que todos los nodos de datos de un clúster tengan el mismo porcentaje de espacio libre.

Procedimiento

1. En el editor de despliegue, pulse el botón derecho del ratón en el procesador de sucesos que tiene datos que desea transferir a un dispositivo de nodo de datos que y pulse **Configurar**.
2. Pulse **Activo** y seleccione **Processing-Only** en la lista.
3. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Gestión de la vista de sistema

Utilice la página System View para seleccionar los componentes que desea ejecutar en cada host gestionado del despliegue.

Visión general de la página System View

Utilice la página System View para gestionar todos los hosts gestionados de la red.

Un host gestionado es un componente de la red que contiene software de QRadar. Si va a utilizar un dispositivo QRadar, los componentes de ese modelo de dispositivo se visualizan en la página System View. Si el software de QRadar está instalado en su hardware, la página System View incluye un componente de contexto de host.

Utilice la página System View para realizar las tareas siguientes:

- Añadir hosts gestionados al despliegue
- Utilizar redes NAT en el despliegue
- Actualizar la configuración de puertos de los hosts gestionados
- Asignar un componente a un host gestionado
- Configurar un contexto de host
- Configurar un acumulador

Requisitos de compatibilidad de software para los hosts de consola y no de consola

No puede añadir, asignar ni configurar componentes en un host gestionado no de consola si la versión de QRadar es incompatible con la versión que hay en la consola. Si a un host gestionado se le habían asignado anteriormente componentes y está ejecutando una versión incompatible, puede ver los componentes igualmente. Sin embargo, no puede actualizar ni suprimir los componentes.

Cifrado

El cifrado proporciona mayor seguridad para todo el tráfico entre los hosts gestionados. Para proporcionar más seguridad, QRadar también incorpora soporte integrado para OpenSSH. Cuando se integra con QRadar, OpenSSH proporciona una comunicación segura entre los componentes.

El cifrado se produce entre los hosts gestionados del despliegue; por lo tanto, el despliegue debe constar de más de un host gestionado para que se pueda utilizar el cifrado. El cifrado se habilita mediante el uso de túneles SSH (reenvío de puertos) iniciados desde el cliente. Un cliente es el sistema que inicia una conexión en una relación cliente/servidor. Cuando el cifrado está habilitado para un host gestionado, se crean túneles de cifrado para todas las aplicaciones de cliente de un host gestionado. Los túneles de cifrado proporcionan un acceso protegido a los servidores respectivos. Si se habilita el cifrado en un host gestionado no de

consola, se crean túneles de cifrado automáticamente para las bases de datos y otras conexiones de servicio de soporte a la consola.

Cuando se habilita el cifrado en un host gestionado, se crea el túnel SSH de cifrado en el host de cliente. Por ejemplo, la conexión entre el Procesador de sucesos y el Recopilador de sucesos y la conexión entre el Procesador de sucesos y Magistrado están cifradas. Cuando se habilita el cifrado en consola de QRadar, se utiliza un túnel cifrado cuando se buscan sucesos mediante la pestaña **Delitos**.

Consejo: Puede pulsar el botón derecho del ratón en un componente para habilitar el cifrado entre los componentes.

Importante: La habilitación del cifrado reduce el rendimiento de un host gestionado en un 50% como mínimo.

Adición de un host gestionado

Utilice la página System View del editor de despliegue para añadir un host gestionado.

Antes de empezar

Asegúrese de que ha instalado QRadar en el host gestionado.

Si desea habilitar la conversión de direcciones de red (NAT) para un host gestionado, la red debe utilizar la conversión NAT estática. Para obtener más información, consulte el apartado "Redes habilitado para NAT" en la página 156.

Si desea añadir un host gestionado habilitado para NAT a una consola que no está configurada para dar soporte a NAT, debe inhabilitar NAT en la consola. Para obtener más información, consulte el apartado "Cambio del estado de NAT para un host gestionado" en la página 158.

Procedimiento

1. Pulse **Acciones** > **Añadir host gestionado**.
2. Pulse **Siguiente**.
3. Especifique valores para los parámetros.
   Utilice la tabla siguiente como ayuda para configurar los parámetros.

Tabla 47. Parámetros para el host gestionado

Cabecera	Cabecera
Host is NATed	Seleccione la casilla para utilizar una conversión de direcciones de red (NAT) existente en este host gestionado.
Enable Encryption	Seleccione la casilla para crear un túnel del cifrado SSH para el host.
	Marque la casilla de verificación para habilitar la compresión de datos entre dos hosts gestionados.

4. Si ha seleccionado la casilla de verificación **Host is NATed**, configure los parámetros.

Tabla 48. Parámetros para una red habilitado para NAT

Parámetro	Descripción
Enter public IP of the server or appliance to add	El host gestionado utiliza esta dirección IP para comunicarse con otros hosts gestionados en redes diferentes utilizando NAT.
Select NATed network	Si el host gestionado se encuentra en la misma subred que la consola, seleccione la consola de la red habilitada para NAT. Si el host gestionado no se encuentra en la misma subred que la consola, seleccione el host gestionado de la red habilitada para NAT.

5. Pulse **Siguiente**.
6. Pulse **Finalizar**.
7. Despliegue los cambios.

Conceptos relacionados:

"Redes habilitado para NAT" en la página 156
La conversión de direcciones de red (NAT) convierte una dirección IP perteneciente a una red en una dirección IP perteneciente a otra red. NAT proporciona una mayor seguridad para el despliegue de IBM Security QRadar pues las solicitudes se gestionan mediante el proceso de conversión y las direcciones IP internas están ocultas. Cuando se utiliza NAT, los sistemas que residen en una red interna privada se convierten mediante un dispositivo de red, normalmente un cortafuegos, y se pueden comunicar con la red Internet pública mediante esa red. Utilice NAT para correlacionar una dirección IP interna con una dirección IP externa.

Edición de un host gestionado

Utilice la página System View del editor de despliegue para editar un host gestionado.

Antes de empezar

Si desea habilitar la conversión de direcciones de red (NAT) para un host gestionado, la red debe utilizar la conversión NAT estática. Para obtener más información, consulte el apartado "Redes habilitado para NAT" en la página 156.

Si desea añadir un host gestionado habilitado para NAT a una consola que no está configurada para dar soporte a NAT, debe inhabilitar NAT en la consola. Para obtener más información, consulte el apartado "Cambio del estado de NAT para un host gestionado" en la página 158.

Procedimiento

1. Pulse el icono **System View**.
2. Pulse el botón derecho del ratón en el host gestionado que desea editar y seleccione **Editar host gestionado**.

   Esta opción está disponible solamente cuando el componente seleccionado tiene un host gestionado en el que se está ejecutando una versión compatible de QRadar.
3. Pulse **Siguiente**.

4. Edite los valores de los parámetros según convenga.
   Utilice la tabla siguiente como ayuda para configurar los parámetros.

Tabla 49. Parámetros para el host gestionado

Cabecera	Cabecera
Host is NATed	Seleccione la casilla para utilizar una conversión de direcciones de red (NAT) existente en este host gestionado.
Enable Encryption	Seleccione la casilla para crear un túnel del cifrado SSH para el host.
	Marque la casilla de verificación para habilitar la compresión de datos entre dos hosts gestionados.

5. Si ha seleccionado la casilla de verificación **Host is NATed**, configure los parámetros.

Tabla 50. Parámetros para una red habilitado para NAT

Parámetro	Descripción
Enter public IP of the server or appliance to add	El host gestionado utiliza esta dirección IP para comunicarse con otros hosts gestionados en redes diferentes utilizando NAT.
Select NATed network	Si el host gestionado se encuentra en la misma subred que la consola, seleccione la consola de la red habilitada para NAT. Si el host gestionado no se encuentra en la misma subred que la consola, seleccione el host gestionado de la red habilitada para NAT.

6. Pulse **Siguiente**.
7. Pulse **Finalizar**.

Eliminación de un host gestionado

Puede eliminar los hosts gestionados no de consola del despliegue. No se puede eliminar un host gestionado que aloje la consola de QRadar.

Consejo: La opción **Eliminar host** está disponible solamente cuando el componente seleccionado tiene un host gestionado en el que se está ejecutando una versión compatible de QRadar.

Procedimiento

1. Pulse el icono **System View**.
2. Pulse el botón derecho del ratón en el host gestionado que desea suprimir y seleccione **Eliminar host**.
3. Pulse **Aceptar**.
4. En el menú de pestaña **Admin**, pulse **Avanzado** > **Desplegar configuración completa**.
   Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Configuración de un host gestionado

Utilice la página System View del editor de despliegue para configurar un host gestionado.

Procedimiento

1. En la página System View, pulse el botón derecho del ratón en el host gestionado que desea configurar y pulse **Configurar**.
2. Especifique los valores de los parámetros:

   En el campo **Ports to exclude**, utilice una coma para separar varios puertos.
3. Pulse **Guardar**.

Asignación de un componente a un host

Utilice la página System View para asignar a los hosts gestionados del despliegue los componentes de QRadar que ha añadido en la página Event View.

Consejo: El cuadro de lista muestra solamente los hosts gestionados en los que se ejecuta una versión compatible de QRadar.

Procedimiento

1. Pulse el icono **System View**.
2. En la lista **Host gestionado**, seleccione el host gestionado al que desea asignar un componente de QRadar.
3. Seleccione el componente que desea asignar a un host gestionado.
4. En el menú, seleccione **Acciones > Asignar**.
5. En el cuadro de lista **Seleccione un host**, seleccione el host que desee asignar a este componente. Pulse **Siguiente**.
6. Pulse **Finalizar**.

Configuración de Contexto de host

Utilice la página System View del editor de despliegue para configurar el componente Contexto de host en un host gestionado.

El componente Contexto de host supervisa todos los componentes de QRadar para garantizar que el funcionamiento de cada componentes es el previsto.

Procedimiento

1. En el editor de despliegue, pulse la pestaña **System View**.
2. Seleccione el host gestionado que incluye el contexto de host que desea configurar.
3. Seleccione el componente Contexto de host.
4. Pulse **Acciones** > **Configurar**.
5. Especifique valores para los parámetros.

Tabla 51. Parámetros de Contexto de host

Parámetro	Descripción
Warning Threshold	Cuando se sobrepasa el umbral configurado de uso de disco, se envía un correo electrónico al administrador que indica el estado actual de uso de disco. El umbral de aviso predeterminado es 0,75. Por lo tanto, cuando el uso de disco supera el 75%, se envía un correo electrónico en el que se informa de ello. Si el uso de disco sigue aumentando por encima del umbral configurado, se envía un nuevo correo electrónico después de cada incremento del uso del 5%. De forma predeterminada, Contexto de host supervisa el uso de disco en las particiones siguientes: • `/` • `/store` • `/store/tmp` **Nota:** Se envían mensajes de correo electrónico de notificación desde la dirección de correo electrónico que está especificada en el parámetro **Dirección de origen de alertas de correo electrónico** a la dirección de correo electrónico que está especificada en el parámetro **Dirección de correo electrónico administrativa**. Estos parámetros se configuran en la ventana Valores del sistema. Para obtener más información, consulte el apartado Capítulo 6, “Configurar QRadar”, en la página 69.
Recovery Threshold	Cuando el sistema sobrepasa el umbral de conclusión, el uso de disco debe estar por debajo del umbral de recuperación antes de que se reinicien los procesos. El valor predeterminado es 0,90. Por lo tanto, los procesos no se reinician hasta que el uso de disco está por debajo del 90%. **Nota:** Se envían mensajes de correo electrónico de notificación desde la dirección de correo electrónico que está especificada en el parámetro **Dirección de origen de alertas de correo electrónico** a la dirección de correo electrónico que está especificada en el parámetro **Dirección de correo electrónico administrativa**. Estos parámetros se configuran en la ventana Valores del sistema. Para obtener más información, consulte el apartado Capítulo 6, “Configurar QRadar”, en la página 69.

Tabla 51. Parámetros de Contexto de host (continuación)

Parámetro	Descripción
Shutdown Threshold	Cuando el sistema sobrepasa el umbral de conclusión, se detienen todos los procesos. Se envía un correo electrónico al administrador en el que se indica el estado actual del sistema. El valor predeterminado es 0,95; por lo tanto, cuando el uso de disco supera el 95%, todos los procesos se detienen. **Nota:** Se envían mensajes de correo electrónico de notificación desde la dirección de correo electrónico que está especificada en el parámetro **Dirección de origen de alertas de correo electrónico** a la dirección de correo electrónico que está especificada en el parámetro **Dirección de correo electrónico administrativa**. Estos parámetros se configuran en la ventana Valores del sistema. **Nota:** Para obtener más información, consulte el apartado Capítulo 6, "Configurar QRadar", en la página 69.
Inspection Interval	Frecuencia, en milisegundos, con la que desea que se compruebe el uso de disco.
Inspection Interval	Frecuencia, en milisegundos, con la que desea que se inspeccione la salida de SAR.
Alert Interval	Frecuencia, en milisegundos, con la que desea que se le notifique que el umbral se ha sobrepasado.
Time Resolution	Tiempo, en segundos, que desea que la inspección de SAR esté en marcha.
Inspection Interval	Frecuencia, en milisegundos, con la que desea supervisar los archivos de registro.
Monitored SYSLOG File Name	Nombre del archivo SYSLOG.
Alert Size	Número máximo de líneas que desea supervisar en el archivo de registro.

6. Pulse **Guardar**.

Configuración de un acumulador

Utilice la página System View del editor de despliegue para configurar el componente acumulador en un host gestionado.

El componente acumulador ayuda en la recopilación de datos y la detección de anomalías para el Procesador de sucesos en un host gestionado. El componente acumulador es responsable de recibir corrientes de sucesos y flujos desde el Procesador de sucesos local y de escribir datos de base de datos; también contiene el motor de detección de anomalías (ADE).

Procedimiento

1. En el editor de despliegue, pulse la pestaña **System View**.
2. Seleccione el host gestionado que desea configurar.

3. Seleccione el componente acumulador.
4. Pulse **Acciones** > **Configurar**.
5. Configure los parámetros.

Tabla 52. Parámetros del acumulador

Parámetro	Descripción
Central Accumulator	Especifica si el componente actual es un acumulador central. Un acumulador central solo existe en un sistema de consola.
Motor de detección de anomalías	El motor de detección de anomalías (ADE) es responsable de analizar los datos de la red y de reenviar los datos al sistema de reglas para su resolución. Para el acumulador central, escriba la dirección y el puerto con la sintaxis siguiente: *<consola>:<puerto>* Para un acumulador que no sea central, escriba la dirección y el puerto con la sintaxis siguiente: *<dirección IP no de consola>:<puerto>*
Streamer Accumulator Listen Port	Puerto de escucha responsable de recibir corrientes de flujos del Procesador de sucesos. El valor predeterminado es 7802.
Alerts DSM Address	Dirección del módulo de soporte de dispositivo (DSM) que se utiliza para el reenvío de alertas desde el acumulador. Utilice la sintaxis siguiente: *<dirección IP DSM>:<número puerto DSM>*.

6. Pulse **Guardar**.

Redes habilitado para NAT

La conversión de direcciones de red (NAT) convierte una dirección IP perteneciente a una red en una dirección IP perteneciente a otra red. NAT proporciona una mayor seguridad para el despliegue de IBM Security QRadar pues las solicitudes se gestionan mediante el proceso de conversión y las direcciones IP internas están ocultas. Cuando se utiliza NAT, los sistemas que residen en una red interna privada se convierten mediante un dispositivo de red, normalmente un cortafuegos, y se pueden comunicar con la red Internet pública mediante esa red. Utilice NAT para correlacionar una dirección IP interna con una dirección IP externa.

La configuración de NAT para QRadar exige utilizar NAT estático y permite una sola dirección IP pública por cada host gestionado.

Cualquier host de QRadar que no esté en el mismo grupo NAT que su homólogo, o que esté en un grupo NAT distinto, se configura para que utilice la dirección IP pública de ese host para acceder a él. Por ejemplo, cuando configura una dirección IP pública en la consola de QRadar, cualquier host que resida en el mismo grupo NAT utiliza la dirección IP privada de la consola de QRadar para comunicarse.

Cualquier host gestionado que resida en un grupo NAT distinto utiliza la dirección IP pública de la consola de QRadar para comunicarse.

Si tiene un host en una de estas ubicaciones de grupo NAT, pero el host no necesita una conversión externa, escriba la dirección IP privada en los campos **IP privada** e **IP pública**. Los sistemas situados en ubicaciones remotas con un grupo NAT diferente que la consola, todavía necesitan una dirección IP externa y NAT, pues necesitan poder establecer conexiones con la consola. Solamente los hosts que residen en el mismo grupo NAT que la consola pueden utilizar las mismas direcciones IP pública y privada.

Adición de una red habilitado para NAT a QRadar

Utilice el editor de despliegue para añadir una red habilitado para NAT al despliegue de QRadar.

Antes de empezar

Asegúrese de que ha configurado las redes habilitado para NAT mediante la conversión NAT estática. Esta configuración garantiza las comunicaciones entre los hosts gestionados que existen en diferentes redes habilitado para NAT.

Procedimiento

1. En el editor de despliegue, pulse la pestaña **NATed Networks**.
2. Pulse **Añadir**.
3. Escriba un nombre para una red que desea utilizar para NAT.
4. Pulse **Aceptar**.

   Se visualiza la ventana Manage NATed Networks, en la que se incluye la red habilitado para NAT añadida.
5. Pulse **Aceptar**.
6. Pulse **Sí**.

Edición de una red habilitado para NAT

Con el editor de despliegue puede editar una red habilitado para NAT.

Procedimiento

1. En el editor de despliegue, pulse la pestaña **NATed Networks**.
2. Seleccione la red habilitado para NAT network que desee editar y, a continuación, pulse **Editar**.
3. Escriba un nombre nuevo para la red habilitado para NAT de red y pulse **Aceptar**.

   La ventana Manage NATed Networks muestra las redes habilitado para NAT actualizadas.
4. Pulse **Aceptar**.
5. Pulse **Sí**.

Supresión de una red habilitado para NAT de QRadar

Utilice el editor de despliegue para suprimir una red habilitado para NAT del despliegue:

Procedimiento

1. En el editor de despliegue, pulse la pestaña **NATed Networks**.
2. Seleccione la red habilitado para NAT que desee suprimir.
3. Pulse **Suprimir**.
4. Pulse **Aceptar**.
5. Pulse **Sí**.

Cambio del estado de NAT para un host gestionado

Utilice el editor de despliegue para cambiar el estado de NAT de un host gestionado en el despliegue.

Antes de empezar

Si desea habilitar NAT para un host gestionado, la red habilitado para NAT debe utilizar la conversión NAT estática.

Para cambiar el estado de NAT para un host gestionado, asegúrese de actualizar la configuración del host gestionado en QRadar antes de actualizar el dispositivo. La actualización de la configuración en primer lugar impide que no se pueda acceder al host y permite desplegar los cambios en ese host.

Procedimiento

1. En el editor de despliegue, pulse la pestaña **System View**.
2. Pulse el botón derecho del ratón en el host gestionado que desea editar y seleccione **Editar host gestionado**.
3. Pulse **Siguiente**.
4. Seleccione una de las opciones siguientes:
   - Si desea habilitar NAT para el host gestionado, seleccione la casilla de verificación **Host is NATed** y pulse **Siguiente**.
   - Si desea inhabilitar NAT para el host gestionado, deseleccione la casilla de verificación **Host is NATed**.

   Importante: Cuando cambie el estado de NAT de un host gestionado existente, podrían visualizarse mensajes de error. Pase por alto estos mensajes de error.
5. Si ha habilitado NAT, seleccione una red habilitado para NAT y especifique los valores de los parámetros:

Tabla 53. Parámetros para una red habilitado para NAT

Parámetro	Descripción
Change public IP of the server or appliance to add	El host gestionado utiliza esta dirección IP para comunicarse con otro host gestionado que pertenece a otra red diferente utilizando NAT.
Select NATed network	Actualice la configuración de red habilitado para NAT.

Tabla 53. Parámetros para una red habilitado para NAT (continuación)

Parámetro	Descripción
Manage NATs List -	NAT (conversión de direcciones de red) convierte una dirección IP en una red a una dirección IP diferente en otra red. NAT proporciona una mayor seguridad para su despliegue, ya que las solicitudes se gestionan mediante el proceso de conversión y se ocultan las direcciones IP internas. Para obtener más información, consulte el apartado "Redes habilitado para NAT" en la página 156.

6. Pulse **Siguiente**.
7. Pulse **Finalizar**.
8. Actualice la configuración del dispositivo (cortafuegos) con el que el host gestionado se comunica.
9. En el menú de pestaña **Admin**, pulse **Avanzado** > **Desplegar configuración completa**.

   Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Configuración de componentes

Utilice el editor de despliegue para configurar cada componente del despliegue.

Configuración de QRadar QFlow Collector

Utilice el editor de despliegue para configurar QRadar QFlow Collector.

Acerca de esta tarea

Puede configurar un filtro de flujo en la conexión desde un QRadar QFlow Collector y varios recopiladores de sucesos de QRadar. Un filtro de flujo controla qué flujo recibe un componente. El parámetro **Flow Filter** está disponible en la ventana Flow Connection Configuration.

Pulse el botón derecho del ratón en la flecha entre el componente que desea configurar para el filtrado de flujo y seleccione **Configurar**.

En la tabla siguiente se describen los parámetros avanzados de QRadar QFlow Collector:

Procedimiento

1. En la página Event View o System View, seleccione el QRadar QFlow Collector que desea configurar.
2. Pulse **Acciones** > **Configurar**.
3. Especifique los valores de los parámetros siguientes:

Parámetro	Descripción
Event Collector Connections	Componente Recopilador de sucesos que está conectado a este QRadar QFlow Collector. La conexión se visualiza en el formato siguiente: *<dirección IP host>:<puerto>*. Si QRadar QFlow Collector no está conectado a un Recopilador de sucesos, el parámetro está vacío.
QFlow CollectorID	ID exclusivo de QRadar QFlow Collector.
Maximum Content Capture	Tamaño de la captura, en bytes, que se adjuntará a un flujo. Puede estar comprendido entre 0 y 65535. El valor 0 inhabilita la captura de contenido. El valor predeterminado es 64 bytes. Los QRadar QFlow Collectors capturan un número configurable de bytes al principio de cada flujo. La transferencia de grandes cantidades de contenido a través de la red podría afectar a la red y al rendimiento. En los hosts gestionados en los que los QRadar QFlow Collectors están en enlaces de alta velocidad cercanos, puede aumentar el tamaño de la captura de contenido. **Importante:** El incremento del tamaño de la captura de contenido aumenta los requisitos de almacenamiento en disco para la asignación de disco sugerida.
Alias Autodetection	La opción **Yes** permite que QRadar QFlow Collector detecte los alias de los orígenes de flujo externos. Cuando QRadar QFlow Collector recibe el tráfico de un dispositivo con una dirección IP, pero sin alias actual, QRadar QFlow Collector intenta una búsqueda DNS inversa para determinar el nombre de host del dispositivo. Si la búsqueda es satisfactoria, QRadar QFlow Collector añade esta información a la base de datos y notifica esta información a todo el despliegue. La opción **No** impide que QRadar QFlow Collector detecte los alias de los orígenes de flujo externos.

4. En la barra de herramientas, pulse **Avanzado** para mostrar los parámetros avanzados.
5. Especifique valores para los parámetros avanzados, según sea necesario.

Tabla 54. Parámetros avanzados de QRadar QFlow Collector:

Parámetro	Descripción
Event Collector Connections	Recopilador de sucesos conectado a este QRadar QFlow Collector. La conexión se visualiza en el formato siguiente: *<dirección IP host>:<puerto>*. Si QRadar QFlow Collector no está conectado a un Recopilador de sucesos, el parámetro está vacío.
Flow Routing Mode	La opción **0** habilita **Distributor Mode**, lo que permite que QRadar QFlow Collector agrupe los flujos que tienen propiedades similares. La opción **1** habilita **Flow Mode**, que impide el empaquetado de los flujos.
Maximum Data Capture/Packet	Número de bytes por paquete que desea que QRadar QFlow Collector analice.
Time Synchronization Server IP Address	Dirección IP o nombre de host del servidor de hora.
Time Synchronization Timeout Period	Cantidad de tiempo que desea que el host gestionado continúe intentando sincronizar la hora antes de exceder el tiempo de espera. El valor predeterminado es de 15 minutos.
Endace DAG Interface Card Configuration	Parámetros de tarjeta de interfaz de supervisión de red Endace. Para obtener más información sobre la entrada necesaria para este parámetro, consulte el sitio web de soporte de IBM (www.ibm.com/support).
Flow Buffer Size	Cantidad de memoria, en MB, que desea reservar para el almacenamiento de flujo. El valor predeterminado es 400 MB.
Maximum Number of Flows	Número máximo de flujos desea enviar desde QRadar QFlow Collector a un Recopilador de sucesos.
Remove duplicate flows	La opción **Yes** permite que QRadar QFlow Collector elimine los flujos duplicados. La opción **No** impide que QRadar QFlow Collector elimine los flujos duplicados.
Verify NetFlow Sequence Numbers	El valor **Yes** permite a QRadar QFlow Collector comprobar los números de secuencia de NetFlow entrantes para asegurarse de que todos los paquetes están presentes y son correctos. Se visualiza una notificación si un paquete falta o se ha recibido dañado.

Tabla 54. Parámetros avanzados de QRadar QFlow Collector: (continuación)

Parámetro	Descripción
External Flow De-duplication method	Método que desea utilizar para eliminar los orígenes de flujo externos duplicados (deduplicación): • **Source** permite que QRadar QFlow Collector compare los orígenes de flujo iniciales. Este método compara la dirección IP del dispositivo que ha exportado el registro de flujo externo actual con la dirección IP del dispositivo que ha exportado el primer registro externo de ese flujo en particular. Si las direcciones IP no coinciden, el registro de flujo externo actual se descarta. • La opción **Record** permite que QRadar QFlow Collector compare los registros de flujos externos individuales. Este método registra una lista de cada registro de flujo externo detectado por un dispositivo determinado y compara cada registro posterior con esa lista. Si el registro actual se encuentra en la lista, dicho registro se descarta.
Flow Carry-over Window	Número de segundos antes del final de un intervalo que desea que se conserven los flujos unilaterales hasta el siguiente intervalo. Este valor deja tiempo para que el lado inverso del flujo llegue antes de que se notifique.

Tabla 54. Parámetros avanzados de QRadar QFlow Collector: (continuación)

Parámetro	Descripción
External flow record comparison mask	• Este parámetro solamente es válido si se ha especificado **Record** en el parámetro **External Flow De-duplication method**. Los campos de registro de flujo externo que desea utilizar para eliminar flujos duplicados incluyen las opciones siguientes: • **D** (dirección) • **B** (recuento de bytes) • **P** (recuento de paquetes) Puede combinar estas opciones. Las combinaciones posibles de las opciones son las siguientes: • La opción **DBP** utiliza la dirección, el recuento de bytes y el recuento de paquetes cuando se comparan los registros de flujos. • La opción **XBP** utiliza el recuento de bytes y el recuento de paquetes cuando se comparan los registros de flujos. • La opción **DXP** utiliza la dirección y el recuento de paquetes cuando se comparan los registros de flujos. • La opción **DBX** utiliza la dirección y el recuento de bytes cuando se comparan los registros de flujos. • La opción **DXX** utiliza la dirección cuando se comparan los registros de flujos. • La opción **XBX** utiliza el recuento de bytes cuando se comparan los registros de flujos. • La opción **XXP** utiliza el recuento de paquetes cuando se comparan los registros de flujos.
Create Superflows	La opción **Yes** permite que QRadar QFlow Collector cree superflujos a partir de los flujos de grupo que tienen propiedades similares. La opción **No** impide la creación de superflujos.

Tabla 54. Parámetros avanzados de QRadar QFlow Collector: (continuación)

Parámetro	Descripción
Type A Superflows	Umbral para los superflujos de tipo A. Un superflujo de tipo A es un grupo de flujos que va de un host a varios hosts. Este flujo es un flujo unidireccional que es un agregado de todos los flujos que tienen hosts de destino diferentes, pero que tienen estos parámetros iguales: • Protocolo • Bytes de origen • Hosts de origen • Red de destino • Puerto de destino (flujos TCP y UDP solamente) • Distintivos TCP (flujos TCP solamente) • Tipo y código de ICMP (flujos ICMP solamente)
Type B Superflows	Umbral para los superflujos de tipo B. Un superflujo de tipo B es un grupo de flujos que va de varios hosts a un host. Este flujo es un flujo unidireccional que es un agregado de todos los flujos que tienen hosts de origen diferentes, pero que tienen estos parámetros iguales: • Protocolo • Bytes de origen • Paquetes de origen • Host de destino • Red de origen • Puerto de destino (flujos TCP y UDP solamente) • Distintivos TCP (flujos TCP solamente) • Tipo y código de ICMP (flujos ICMP solamente)

Tabla 54. Parámetros avanzados de QRadar QFlow Collector: (continuación)

Parámetro	Descripción
Type C Superflows	Umbral para los superflujos de tipo C. Un superflujo de tipo C es un grupo de flujos que va de un host a otro host. Este flujo es un flujo unidireccional que es un agregado de todos los flujos no ICMP que tienen puertos de origen o de destino diferentes, pero que tienen estos parámetros iguales: • Protocolo • Host de origen • Host de destino • Bytes de origen • Bytes de destino • Paquetes de origen • Paquetes de destino
Recombine Asymmetric Superflows	En algunas redes, el tráfico está configurado para tomar rutas alternativas para el tráfico de entrada y de salida. Este direccionamiento se denomina direccionamiento asimétrico. Puede combinar los flujos que se reciben de uno o de varios QRadar QFlow Collector. Sin embargo, si desea combinar varios flujos de varios componentes QRadar QFlow Collector, debe configurar los orígenes de flujo en el parámetro **Asymmetric Flow Source Interface(s)** en la configuración de QRadar QFlow Collector. • La opción **Yes** permite que QRadar QFlow Collector combine de nuevo los flujos asimétricos. • La opción **No** impide que QRadar QFlow Collector combine de nuevo los flujos asimétricos.
Ignore Asymmetric Superflows	La opción **Yes** permite que QRadar QFlow Collector cree superflujos mientras los flujos asimétricos están habilitados. La opción **No** impide que QRadar QFlow Collector cree superflujos mientras los flujos asimétricos están habilitados.
Minimum Buffer Data	Cantidad mínima de datos, en bytes, que desea que la tarjeta de interfaz de supervisión de red Endace reciba antes de que los datos capturados se devuelvan al proceso de QRadar QFlow Collector. Si este parámetro es 0 y no hay datos disponibles, la tarjeta de interfaz de supervisión de red Endace permite un comportamiento no de bloqueo.

Tabla 54. Parámetros avanzados de QRadar QFlow Collector: (continuación)

Parámetro	Descripción
Maximum Wait Time	Cantidad máxima de tiempo, en microsegundos, que desea que la tarjeta de interfaz de supervisión de red Endace espere la cantidad mínima de datos. La cantidad mínima de datos se especifica en el parámetro **Minimum Buffer Data**.
Polling Interval	Intervalo, en microsegundos, que desea que la tarjeta de interfaz de supervisión de red Endace espere antes de comprobar si hay más datos. Un intervalo de sondeo evita el tráfico de sondeo excesivo hacia la tarjeta y, por lo tanto, ahorra ancho de banda y tiempo de proceso.

6. Pulse **Guardar**.
7. Repita esta acción para todos los QRadar QFlow Collectors del despliegue que desee configurar.

Conceptos relacionados:

"Vistas de sucesos de componentes de QRadar en el despliegue" en la página 140

Configuración de un Recopilador de sucesos

Utilice el editor de despliegue para configurar un Recopilador de sucesos.

Procedimiento

1. En la página Event View o System View, seleccione el Recopilador de sucesos que desea configurar.
2. Pulse **Acciones** > **Configurar**.
3. Especifique los valores de los parámetros siguientes:

Parámetro	Descripción
Destination Event Processor	Especifica el componente Procesador de sucesos que está conectado a este Recopilador de sucesos. La conexión se visualiza en el formato siguiente: *<dirección IP host>:<puerto>*.
Flow Listen Port	Puerto de escucha de los flujos.
Event Forwarding Listen Port	Puerto de reenvío de sucesos del Recopilador de sucesos.
Flow Forwarding Listen Port	Puerto de reenvío de flujos del Recopilador de sucesos.

4. En la barra de herramientas, pulse **Avanzado** para mostrar los parámetros avanzados.
5. Configure los parámetros avanzados, según sea necesario.

Tabla 55. Parámetros avanzados del Recopilador de sucesos

Parámetro	Descripción
Primary Collector	**True** especifica que el Recopilador de sucesos está en un sistema de consola. **False** especifica que el Recopilador de sucesos está en un sistema no de consola.
Autodetection Enabled	**Yes** permite que el Recopilador de sucesos analice y acepte automáticamente el tráfico procedente de orígenes de registro desconocidos anteriormente. Los puertos de cortafuegos adecuados se abren para permitir que la detección automática reciba sucesos. Esta es la opción predeterminada. **No** impide que el Recopilador de sucesos analice y acepte automáticamente el tráfico procedente de orígenes de registro desconocidos anteriormente. Para obtener más información, consulte la publicación *Managing Log Sources Guide*.
Flow Deduplication Filter	Cantidad de tiempo, en segundos, que los flujos están en el almacenamiento intermedio antes de que se reenvíen.
Asymmetric Flow Filter	Cantidad de tiempo, en segundos, que el flujo asimétrico está en el almacenamiento intermedio antes de que se reenvíe.
Forward Events Already Seen	**True** permite que el Recopilador de sucesos reenvíe los sucesos que se han detectado en el sistema. **False** impide que el Recopilador de sucesos reenvíe los sucesos que se han detectado en el sistema. Esta opción evita los bucles de sucesos en el sistema.

6. Pulse **Guardar**.
7. Repita esta acción para todos los recopiladores de sucesos de QRadar del despliegue que desee configurar.

Conceptos relacionados:

"Vistas de sucesos de componentes de QRadar en el despliegue" en la página 140

Configuración de un Procesador de sucesos

Utilice el editor de despliegue para configurar un Procesador de sucesos.

Procedimiento

1. En la página Event View o System View, seleccione el Procesador de sucesos que desea configurar.
2. Pulse **Acciones** > **Configurar**.
3. Especifique los valores de los parámetros:

Tabla 56. Valores de los parámetros del Procesador de sucesos

Parámetro	Descripción
Event Collector Connections Listen Port	Puerto que el Procesador de sucesos supervisa para las conexiones de entrada del Recopilador de sucesos. El valor predeterminado es el puerto 32005.
Event Processor Connections Listen Port	Puerto que el Procesador de sucesos supervisa para las conexiones de entrada del Procesador de sucesos. El valor predeterminado es el puerto 32007.

4. En la barra de herramientas, pulse **Avanzado** para mostrar los parámetros avanzados.
5. Especifique valores para los parámetros, según sea necesario.

Tabla 57. Parámetros avanzados del Procesador de sucesos

Parámetro	Descripción
Test Rules	La lista de reglas para comprobar **Test Rules** está disponible solamente para el Procesadores de sucesos no de consola. Si una regla está configurada para comprobarla localmente, la opción **Globally** no altera temporalmente el valor de la regla. Si selecciona **Locally**, las reglas se comprueban en el Procesador de sucesos y no se comparten con el sistema. Si selecciona **Globally**, las reglas individuales de cada Procesador de sucesos se comparten y se comprueban en todo el sistema. Cada regla se puede cambiar a **Global** para su detección por parte de cualquier Procesador de sucesos del sistema. Por ejemplo,puede crear una regla que le avise cuando haya cinco intentos de inicio de sesión fallidos en un periodo de 5 minutos. Cuando el Procesador de sucesos que contiene la regla local detecta cinco intentos de inicio de sesión fallidos, la regla genera una respuesta. Si la regla del ejemplo se ha establecido en Global, cuando se detecten cinco intentos de inicio de sesión fallidos en un intervalo de 5 minutos en cualquier Procesador de sucesos, la regla genera una respuesta. Cuando las reglas se comparten globalmente, la regla puede detectar cuándo un intento de inicio de sesión fallido proviene de cinco procesadores de sucesos. Comprobar las reglas globalmente es el valor predeterminado para el Procesador de sucesos no de consola, y cada regla del Procesador de sucesos está establecida para comprobarse localmente.

Tabla 57. Parámetros avanzados del Procesador de sucesos (continuación)

Parámetro	Descripción
Overflow Event Routing Threshold	Escriba el umbral de sucesos por segundo que el Procesador de sucesos puede gestionar. Los sucesos por encima de este umbral se colocan en la memoria caché.
Overflow Flow Routing Threshold	Escriba el umbral de flujos por minuto que el Procesador de sucesos puede gestionar. Los flujos por encima de este umbral se colocan en la memoria caché.
Events database path	Escriba la ubicación en la que desea almacenar los sucesos. El valor predeterminado es **/store/ariel/events**.
Payloads database length	Ubicación en la que desea almacenar la información de carga útil. El valor predeterminado es **/store/ariel/payloads** .

6. Pulse **Guardar**.
7. Repita esta acción para todos los Procesadores de sucesos del despliegue que desee configurar.

Conceptos relacionados:

"Vistas de sucesos de componentes de QRadar en el despliegue" en la página 140

Configuración del magistrado

Utilice el editor de despliegue para configurar un componente Magistrado.

Procedimiento

1. En la página Event View o System View, seleccione el Magistrado que desea configurar.
2. Pulse **Acciones** > **Configurar**.
3. En la barra de herramientas, pulse **Avanzado** para mostrar los parámetros avanzados.
4. En el campo **Overflow Routing Threshold**, escriba el umbral de sucesos por segundo que el Magistrado puede gestionar.

   Los sucesos por encima de este umbral se colocan en la memoria caché.

   El valor predeterminado es 20.000.
5. Pulse **Guardar**.

Conceptos relacionados:

"Vistas de sucesos de componentes de QRadar en el despliegue" en la página 140

Configuración de un origen externo

Utilice el editor de despliegue para configurar un origen externo.

Acerca de esta tarea

Para evitar los errores de conexión, cuando configure los componentes de origen y de destino externos, despliegue consola de QRadar con el origen externo en primer lugar. A continuación, despliegue consola de QRadar con el destino externo.

Procedimiento

1. En la página Event View o System View, seleccione el Recopilador de sucesos que desea configurar.
2. Pulse **Acciones** > **Configurar**.
3. Especifique los valores de los parámetros.

Parámetro	Descripción
Receive Events	**True** permite que el sistema reciba sucesos del host de origen externo. **False** impide que el sistema reciba sucesos del host de origen externo.
Receive Flows	**True** permite que el sistema reciba flujos del host de origen externo. **False** impide que el sistema reciba flujos del host de origen externo.

4. Pulse **Guardar**.
5. Repita esta acción para todos los orígenes externos del despliegue que desee configurar.

Conceptos relacionados:

"Vistas de sucesos de componentes de QRadar en el despliegue" en la página 140

Configuración de un destino externo

Utilice el editor de despliegue para configurar un destino externo.

Acerca de esta tarea

Para evitar los errores de conexión, cuando configure los componentes de origen y de destino externos, despliegue consola de QRadar con el origen externo en primer lugar. A continuación, despliegue consola de QRadar con el destino externo.

Procedimiento

1. En la página Event View o System View, seleccione el Recopilador de sucesos que desea configurar.
2. Pulse **Acciones** > **Configurar**.
3. Especifique los valores de los parámetros:

Parámetro	Descripción
Event Collector Listen Port	Puerto de escucha del Recopilador de sucesospara recibir datos de sucesos. El puerto predeterminado para los sucesos es 32004.
Flow Collector Listen Port	Puerto de escucha del Recopilador de sucesos para recibir datos de flujos. El puerto predeterminado para los flujos es 32000.

4. Pulse **Guardar**.

Conceptos relacionados:

"Vistas de sucesos de componentes de QRadar en el despliegue" en la página 140

Capítulo 12. Gestión de orígenes de flujo

Utilice la ventana Orígenes de flujo para gestionar los orígenes de flujo en el despliegue.

Se pueden añadir, habilitar, inhabilitar o suprimir orígenes de flujo.

Conceptos relacionados:

Capítulo 12, "Gestión de orígenes de flujo"
Utilice la ventana Orígenes de flujo para gestionar los orígenes de flujo en el despliegue.

Orígenes de flujo

Para los dispositivos IBM Security QRadar, IBM Security QRadar SIEM añade de forma automática orígenes de flujo para los puertos físicos de los dispositivos. QRadar SIEM también incluye un origen de flujo de NetFlow predeterminado.

Si ha instalado QRadar SIEM en su hardware, QRadar SIEM intenta detectar y añadir automáticamente los orígenes de flujo predeterminados para todos los dispositivos físicos, como, por ejemplo, una tarjeta de interfaz de red (NIC). Además, cuando se asigna un QRadar QFlow Collector, QRadar SIEM incluye un origen de flujo de NetFlow predeterminado.

Con QRadar SIEM puede integrar orígenes de flujo.

Los orígenes de flujo pueden ser internos o externos:

Orígenes de flujo internos
Incluye el hardware adicional que se instala en un host gestionado, como una tarjeta de interfaz de red (NIC). En función de la configuración de hardware del host gestionado, los orígenes de flujo internos podrían incluir los orígenes siguientes:

- Tarjeta de interfaz de red
- Interfaz de Napatech

Orígenes de flujo externos
Incluye cualquier origen de flujo externo que envíe a QRadar QFlow Collector. Si QRadar QFlow Collector recibe varios orígenes de flujo, puede asignar a cada origen de flujo un nombre diferenciado. Cuando los datos de flujo externos son recibidos por un mismo QRadar QFlow Collector, un nombre diferenciado ayuda a distinguir los datos de origen de flujo externos entre sí.

Los orígenes de flujo externos pueden incluir los orígenes siguientes:

- NetFlow
- IPFIX
- sFlow
- J-Flow
- Packeteer
- Archivo de registro de flujos

© Copyright IBM Corp. 2012, 2015

QRadar SIEM puede reenviar datos de origen de flujo externo con el método de suplantación o de no suplantación:

Suplantación
Reenvía los datos de entrada recibidos de los orígenes de flujo a un destino secundario. Para garantizar que los datos de origen de flujo se envían a un destino secundario, configure el parámetro **Interfaz de supervisión** en la configuración del origen de flujo con el puerto en el que se reciben los datos (puerto de gestión). Cuando se utiliza una interfaz específica, QRadar QFlow Collector utiliza una captura de modalidad promiscua para obtener datos de origen de flujo, en lugar del puerto de escucha UDP predeterminado en el puerto 2055. Como resultado, QRadar QFlow Collector puede capturar paquetes de origen de flujo y reenviar los datos.

No suplantación
Para el método de no suplantación, configure el parámetro **Interfaz de supervisión** en la configuración del origen de flujo como `Cualquiera`. QRadar QFlow Collector abre el puerto de escucha, que es el puerto que está configurado como **Puerto de supervisión** para aceptar datos de origen de flujo. Los datos se procesan y se reenvían a otro destino de origen de flujo. La dirección IP de origen de los datos de origen de flujo se convierte en la dirección IP del sistema de QRadar SIEM, no en el direccionador original que envió los datos.

NetFlow

NetFlow es una tecnología propietaria de contabilidad desarrollada por Cisco Systems. NetFlow supervisa el tráfico de flujos a través de un conmutador o un direccionador, interpreta el cliente, el servidor, el protocolo y el puerto que se utiliza, cuenta el número de bytes y paquetes, y envía los datos a un recopilador de NetFlow.

Al proceso de enviar datos desde NetFlow se le suele llamar NDE (exportación de datos de NetFlow). Puede configurar IBM Security QRadar SIEM para aceptar las NDE y así convertirse en un recopilador de NetFlow. QRadar SIEM da soporte a NetFlow versiones 1, 5, 7 y 9. Para obtener más información sobre NetFlow, consulte el sitio web de Cisco (http://www.cisco.com).

Mientras NetFlow amplía la cantidad de red que se supervisa, NetFlow utiliza un protocolo sin conexión (UDP) para ofrecer las NDE. Después de que una NDE se envíe desde un conmutador o un direccionador, el registro de NetFlow se purga. Como se utiliza UDP para enviar esta información y no se garantiza la entrega de los datos, NetFlow registra los registros inexactos y las funciones de alerta reducidas. El resultado podría ser presentaciones inexactas de ambos volúmenes de tránsito y flujos bidireccionales.

Cuando configure un origen de flujo externo para NetFlow, debe realizar las tareas siguientes:

- Asegúrese de que las reglas del cortafuegos pertinentes estén configuradas. Si cambia el parámetro **External Flow Source Monitoring Port** en la configuración de QRadar QFlow Collector, también debe actualizar la configuración del acceso de cortafuegos.
- Asegúrese de que estén configurados los puertos adecuados para QRadar QFlow Collector.

Si utiliza NetFlow versión 9, asegúrese de que la plantilla de NetFlow del origen de NetFlow contenga los campos siguientes:

- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES o OUT_BYTES
- IN_PKTS o OUT_PKTS
- TCP_FLAGS (flujos TCP solamente)

Conceptos relacionados:

Capítulo 11, “Editor de despliegue”, en la página 137
Utilice el editor de despliegue para gestionar los componentes individuales de QRadar. Después de configurar el despliegue, puede acceder a los componentes individuales de cada host gestionado del despliegue y configurarlo.

IPFIX

Internet Protocol Flow Information Export (IPFIX) es una tecnología de contabilidad. IPFIX supervisa el tráfico de flujos a través de un conmutador o un direccionador, interpreta el cliente, el servidor, el protocolo y el puerto que se utiliza, cuenta el número de bytes y paquetes y envía los datos a un recopilador de IPFIX.

IBM Security Network Protection XGS 5000, un sistema de protección frente a intrusiones (IPS) de próxima generación, es un ejemplo de dispositivo que envía tráfico de flujo en formato de flujo IPFIX.

Al proceso de enviar datos de IPFIX se le suele llamar NDE (exportación de datos de NetFlow). IPFIX proporciona más información de flujo y una información más exhaustiva que NetFlow v9. Puede configurar IBM Security QRadar SIEM para que acepte las NDE y así convertirse en un recopilador de IPFIX. IPFIX utiliza UPD (User Datagram Protocol) para distribuir las NDE. Después de que una NDE se envíe desde el dispositivo de reenvío de IPFIX, el registro de IPFIX podría purgarse.

Para configurar QRadar SIEM para que acepte tráfico de flujo de IPFIX, debe añadir un origen de flujo de NetFlow. El origen de flujo de NetFlow procesa los flujos de IPFIX utilizando el mismo proceso.

El sistema de QRadar SIEM podría incluir un origen de flujo de NetFlow predeterminado; por lo tanto, no tendría que configurar un origen de flujo de NetFlow. Para confirmar que el sistema incluye un origen de flujo de NetFlow predeterminado, seleccione **Admin** > **Orígenes de flujo**. Si en la lista de orígenes de flujo aparece **default_Netflow**, IPFIX ya está configurado.

Cuando configure un origen de flujo externo para IPFIX, debe realizar las tareas siguientes:

- Asegúrese de que las reglas del cortafuegos pertinentes estén configuradas. Si cambia el parámetro **External Flow Source Monitoring Port** en la configuración de QRadar QFlow Collector, también debe actualizar la configuración del acceso

de cortafuegos. Para obtener más información sobre la configuración de QRadar QFlow Collector, consulte la publicación *IBM Security QRadar SIEM Guía de administración*.

- Asegúrese de que estén configurados los puertos adecuados para QRadar QFlow Collector.
- Asegúrese de que la plantilla de IPFIX del origen de IPFIX incluye los campos siguientes:
- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES o OUT_BYTES
- IN_PKTS o OUT_PKTS
- TCP_FLAGS (flujos TCP solamente)

sFlow

sFlow es un estándar de múltiples proveedores y usuarios de la tecnología de muestreo que proporciona una supervisión continua de los flujos de tráfico en el nivel de aplicación en todas las interfaces simultáneamente.

sFlow combina las muestras de flujos y los contadores de interfaz en datagramas sFlow que se envían a través de la red a un recopilador de sFlow. IBM Security QRadar SIEM da soporte a las versiones 2, 4 y 5 de sFlow. El tráfico de sFlow se basa en datos de muestreo y, por lo tanto, podría no representar todo el tráfico de la red. Para obtener más información, consulte el sitio web de sflow (www.sflow.org).

sFlow utiliza un protocolo sin conexión (UDP). Cuando se envían datos desde un conmutador o un direccionador, el registro de sFlow se purga. Como se utiliza UDP para enviar esta información y no se garantiza la entrega de los datos, sFlow registra los registros inexactos y las funciones de alerta reducidas. El resultado podría ser presentaciones inexactas de ambos volúmenes de tránsito y flujos bidireccionales.

Cuando configure un origen de flujo externo para sFlow, debe realizar las tareas siguientes:

- Asegúrese de que las reglas del cortafuegos pertinentes estén configuradas.
- Asegúrese de que estén configurados los puertos adecuados para QRadar VFlow Collector.

J-Flow

Tecnología de contabilidad propietaria utilizada por Juniper Networks que permite recopilar estadísticas de los flujos de tráfico de IP. J-Flow permite exportar datos a un puerto UDP en un recopilador J-Flow. También puede habilitar J-Flow en un direccionador o una interfaz para recopilar estadísticas de red de ubicaciones específicas de la red. Tenga en cuenta que el tráfico de J-Flow se basa en datos de

muestreo y, por lo tanto, podría no representar todo el tráfico de la red. Para obtener más información sobre J-Flow, consulte el sitio web de Juniper Networks (www.juniper.net).

J-Flow utiliza un protocolo sin conexión (UDP). Cuando se envían datos desde un conmutador o un direccionador, el registro de J-Flow se purga. Como se utiliza UDP para enviar esta información y no se garantiza la entrega de los datos, J-Flow registra los registros inexactos y las funciones de alerta reducidas. El resultado podría ser presentaciones inexactas de ambos volúmenes de tránsito y flujos bidireccionales.

Cuando configure un origen de flujo externo para J-Flow, debe realizar las tareas siguientes:

- Asegúrese de que las reglas del cortafuegos pertinentes estén configuradas.
- Asegúrese de que estén configurados los puertos adecuados para QFlow Collector.

Packeteer

Los dispositivos Packeteer recopilan, agregan y almacenan los datos de rendimiento de la red. Después de configurar un origen de flujo externo para Packeteer, puede enviar información de flujo desde un dispositivo Packeteer a IBM Security QRadar SIEM.

Packeteer utiliza un protocolo sin conexión (UDP). Cuando se envían datos desde un conmutador o un direccionador, el registro de Packeteer se purga. Como se utiliza UDP para enviar esta información y no se garantiza la entrega de los datos, Packeteer registra los registros inexactos y las funciones de alerta reducidas. Podrían darse presentaciones inexactas de ambos volúmenes de tránsito y flujos bidireccionales.

Para configurar Packeteer como un origen de flujo externo, debe realizar las tareas siguientes:

- Asegúrese de que las reglas del cortafuegos pertinentes estén configuradas.
- Asegúrese de configurar los dispositivos Packeteer para exportar los registros de detalle de flujo y de configurar QRadar QFlow Collector como destino de la exportación de datos.
- Asegúrese de que estén configurados los puertos adecuados para QRadar QFlow Collector.
- Asegúrese de que los ID de clase de los dispositivos Packeteer pueden ser detectados automáticamente por QRadar QFlow Collector.
- Para obtener más información, consulte *Mapping Packeteer Applications into QRadar Technical Note*.

Archivo de registro de flujos

Un archivo de registro de flujos se genera a partir de los registros de flujos de IBM Security QRadar SIEM.

Interfaz de Napatech

Si ha instalado un adaptador de red Napatech en el sistema de IBM Security QRadar SIEM, la opción **Interfaz Napatech** se muestra como origen de flujo basado en paquetes configurable en QRadar SIEM. El adaptador de red Napatech es un adaptador de red inteligente y programable de próxima generación para la red. Para obtener más información, consulte la documentación de Napatech .

Adición o edición de un origen de flujo

Utilice la ventana Origen de flujo para añadir un origen de flujo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. En el menú de navegación, pulse **Flujos**.
4. Pulse **Orígenes de flujo**.
5. Realice una de estas acciones:
   - Para añadir un origen de flujo, pulse **Añadir**.
   - Para editar un origen de flujo, seleccione el origen de flujo y pulse **Editar**.
6. Para crear este origen de flujo a partir de un origen de flujo existente, seleccione la casilla de verificación **Crear a partir de origen de flujo existente** y seleccione un origen de flujo de la lista **Utilizar como plantilla**.
7. Especifique el nombre en **Nombre de origen de flujo**.

   Consejo: Si el origen de flujo externo también es un dispositivo físico, utilice el nombre de dispositivo como nombre del origen de flujo. Si el origen de flujo no es un dispositivo físico, utilice un nombre reconocible.
   Por ejemplo, si desea utilizar tráfico de IPFIX, especifique **ipf1**. Si desea utilizar tráfico de NetFlow, especifique **nf1**.
8. Seleccione un origen de flujo de la lista **Tipo de origen de flujo** y configure las propiedades.
   - Si selecciona la opción **Archivo de registro de flujos**, asegúrese de configurar la ubicación del archivo de registro de flujos en el parámetro **Vía de acceso de archivo de origen**.
   - Si selecciona las opciones **JFlow**, **NetFlow**, **Packeteer FDR** o **sFlow** en el parámetro **Tipo de origen de flujo**, asegúrese de configurar un puerto disponible en el parámetro **Puerto de supervisión**.

     El puerto predeterminado del primer origen de flujo de NetFlow configurado en la red es 2055. Por cada origen de flujo de NetFlow adicional, el número de puerto predeterminado se incrementa en 1. Por ejemplo, el origen de flujo de NetFlow predeterminado del segundo origen de flujo de NetFlow es 2056.
   - Si selecciona la opción **Interfaz Napatech**, especifique en **Interfaz de flujo** la interfaz de flujo que desee asignar al origen de flujo.

     Restricción: La opción **Interfaz Napatech** se visualiza solamente si ha instalado el adaptador de red Napatech en el sistema.
   - Si selecciona la opción **Interfaz de red**, en **Interfaz de flujo** configure solamente un origen de registro para cada interfaz Ethernet.

     Restricción: No se pueden enviar distintos tipos de flujo al mismo puerto.
9. Si el tráfico de la red está configurado para seguir rutas alternativas para el tráficos de entrada y el de salida, seleccione la casilla de verificación **Habilitar flujos asimétricos**.
10. Pulse **Guardar**.
11. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Reenvío de paquetes a QRadar Packet Capture

Puede supervisar el tráfico de red mediante el envío de paquetes de datos en bruto a un dispositivo QRadar QFlow Collector 1310. QRadar QFlow Collector utiliza una tarjeta de supervisión Napatech dedicada para copiar los paquetes entrantes de un puerto de la tarjeta en un segundo puerto que se conecta a un dispositivo QRadar Packet Capture.

Si ya tiene un dispositivo QRadar QFlow Collector 1310 con una tarjeta de red Napatech 10G, puede duplicar el tráfico a QRadar Packet Capture.

Como se muestra en el diagrama siguiente, si ya tiene un dispositivo QRadar QFlow Collector 1310 con una tarjeta de red Napatech 10G, puede duplicar el tráfico a QRadar Packet Capture.

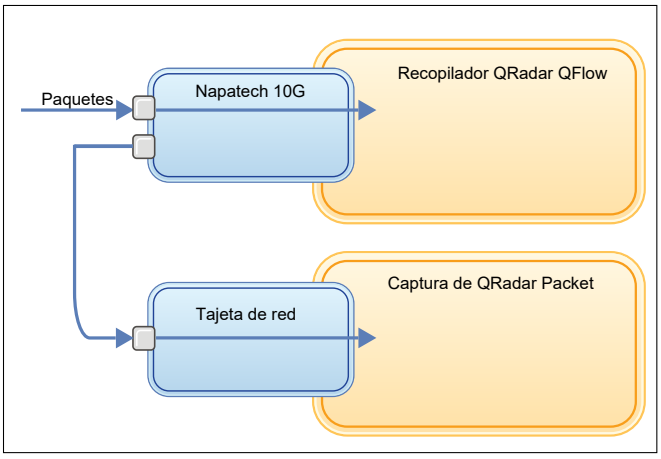

Figura 2. Reenvío de datos de paquete desde un QRadar QFlow Collector a QRadar Packet Capture mediante la tarjeta Napatech

Antes de empezar

Asegúrese de que haber configurado el hardware siguiente en su entorno:

- Haber conectado el cable al puerto 1 de la tarjeta Napatech del dispositivo QRadar QFlow Collector 1310.
- Haber conectado el cable que está conectado al puerto 2 de la tarjeta Napatech, que es el puerto de reenvío, al dispositivo QRadar Packet Capture.
- Haber verificado la conectividad de capa 2 comprobando las luces de enlace en ambos dispositivos.

Procedimiento

1. Utilizando SSH desde la consola de QRadar, inicie la sesión en QRadar QFlow Collector como usuario root. En el dispositivo QRadar QFlow Collector, edite el archivo siguiente.

   `/opt/qradar/init/apply_tunings`

   a. Busque la línea siguiente, cerca de la línea 137.

```
apply_multithread_qflow_changes()
{
     APPLIANCEID=`$NVABIN/myver -a`
     if [ "$APPLIANCEID" == "1310" ]; then
          MODELNUM=$(/opt/napatech/bin/AdapterInfo 2>&1 | grep "Active FPGA Image" | cut -d'-' -f2)
          if [ "$MODELNUM" == "9220" ]; then..
```

b. En las líneas AppendToConf que siguen al código del paso anterior, añada estas líneas:

```
AppendToConf SV_NAPATECH_FORWARD YES
AppendToConf SV_NAPATECH_FORWARD_INTERFACE_SRCDST "0:1"
```

Estas sentencias habilitan el reenvío de paquetes y reenvían paquetes desde el puerto 0 al puerto 1.

c. Asegúrese de que la *multihebra* está habilitada, verificando que la línea siguiente se encuentra en el archivo /opt/qradar/conf/nva.conf .

```
MULTI_THREAD_ON=YES
```

2. Ejecute el script apply_tunings para actualizar los archivos de configuración en QRadar QFlow Collector, escribiendo el mandato siguiente:

```
./apply_tunings restart
```

3. Reinicie los servicios de QRadar especificando el mandato siguiente:

```
service hostcontext restart
```

4. Opcional: Verifique que la tarjeta Napatech esté recibiendo y transmitiendo datos.
   a. Para comprobar que la tarjeta Napatech está recibiendo datos, escriba el mandato siguiente:

      ```
      /opt/napatech/bin/Statistics -dec -interactive
      ```

      Las estadísticas de byte y paquete "RX" se incrementan si la tarjeta está recibiendo datos.
   b. Para comprobar que la tarjeta Napatech está transmitiendo datos, escriba el mandato siguiente:

      ```
      /opt/napatech/bin/Statistics -dec -interactive
      ```

      Las estadísticas "TX" se incrementan si la tarjeta está transmitiendo datos.
5. Opcional: Verifique que QRadar Packet Capture esté recibiendo paquetes del dispositivo QRadar QFlow Collector.
   a. Utilizando SSH desde la consola de QRadar, inicie la sesión en el dispositivo QRadar Packet Capture como usuario root en el puerto 4477.
   b. Verifique que el dispositivo QRadar Packet Capture esté recibiendo paquetes escribiendo el mandato siguiente:

      ```
      watch -d cat /var/www/html/statisdata/int0.txt
      ```

      El archivo int0.txt se actualiza a medida que los datos fluyen al dispositivo QRadar Packet Capture.

   Para obtener más información sobre la captura de paquetes, consulte QRadar Packet Capture.

Habilitación e inhabilitación de un origen de flujo

Con la ventana Origen de flujo puede habilitar o inhabilitar un origen de flujo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. En el menú de navegación, pulse **Flujos**.
4. Pulse el icono **Orígenes de flujo**.
5. Seleccione el origen de flujo que desee habilitar o inhabilitar.

   La columna **Habilitado** indica si el origen de flujo está habilitado o inhabilitado.

Se visualizan los estados siguientes:

- Verdadero indica que el origen de flujo está habilitado.
- Falso indica que el origen de flujo está inhabilitado en ese momento.

6. Pulse **Habilitar/inhabilitar**.
7. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Supresión de un origen de flujo

Utilice la ventana Origen de flujo para suprimir un origen de flujo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. En el menú de navegación, pulse **Flujos**.
4. Pulse **Orígenes de flujo**.
5. Seleccione el origen de flujo que desee suprimir.
6. Pulse **Suprimir**.
7. Pulse **Aceptar**.
8. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Gestión de alias de origen de flujo

Puede utilizar la ventana Alias de origen de flujo para configurar nombres virtuales, o alias, para los orígenes de flujo.

Puede identificar varios orígenes que se envían al mismo QRadar QFlow Collector mediante la dirección IP de origen y el nombre virtual. Con un alias, QRadar QFlow Collector puede identificar de forma exclusiva los orígenes de datos que se envían al mismo puerto y procesarlos.

Cuando QRadar QFlow Collector recibe el tráfico de un dispositivo que tiene una dirección IP, pero no tiene un alias actual, QRadar QFlow Collector intenta una búsqueda DNS inversa. La búsqueda se utiliza para determinar el nombre de host del dispositivo. Si la búsqueda es satisfactoria, QRadar QFlow Collector añade esta información a la base de datos y notifica la información a todos los componentes QRadar QFlow Collector del despliegue.

Utilice el editor de despliegue para configurar QRadar QFlow Collector para que detecte automáticamente los alias de origen de flujo.

Adición de un alias de origen de flujo

Utilice la ventana Alias de origen de flujo para añadir un alias de origen de flujo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. En el menú de navegación, pulse **Flujos**.
4. Pulse el icono **Alias de origen de flujo**.
5. Realice una de estas acciones:
   - Para añadir un alias de origen de flujo, pulse **Añadir** y especifique los valores de los parámetros.

- Para editar un alias existente de origen de flujo, seleccione el alias del origen de flujo, pulse **Editar** y actualice los parámetros.

6. Pulse **Guardar**.
7. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Supresión de un alias de origen de flujo

Utilice la ventana Alias de origen de flujo para suprimir un alias de origen de flujo.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos**.
3. En el menú de navegación, pulse **Flujos**.
4. Pulse el icono **Alias de origen de flujo**.
5. Seleccione el alias de origen de flujo que desee suprimir.
6. Pulse **Suprimir**.
7. Pulse **Aceptar**.
8. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Capítulo 13. Configuración de redes remotas y servicios remotos

Utilice los grupos de redes remotas y servicios remotos para representar la actividad de tráfico en la red para un perfil específico. Los grupos de redes remotas muestran el tráfico de usuario que se origina en las redes remotas denominadas.

Todos los grupos de redes remotas y servicios remotos tienen niveles de grupo y niveles de objeto de hoja. Puede editar los grupos de redes remotas y servicios remotos añadiendo objetos a los grupos existentes o cambiando las propiedades ya existentes para adaptarlas a su entorno.

Si mueve un objeto existente a otro grupo, el nombre del objeto se mueve desde el grupo existente hasta el grupo recién seleccionado. Sin embargo, cuando los cambios de configuración se despliegan, los datos del objeto que están almacenados en la base de datos se pierden y el objeto deja de funcionar. Para resolver este problema, cree una vista nueva y vuelva a crear el objeto que existe con otro grupo.

En la pestaña **Admin**, puede agrupar las redes remotas y los servicios remotos para su uso en las búsquedas de sucesos, flujos y el motor de reglas personalizadas. Puede también agrupar las redes y los servicios en IBM Security QRadar Risk Manager, si está disponible.

Grupos de redes remotas predeterminados

IBM Security QRadar SIEM incluye grupos de redes remotas predeterminados:

En la tabla siguiente se describen los grupos de redes remotas predeterminados.

Tabla 58. Grupos de redes remotas predeterminados

Grupo	Descripción
BOT	Especifica el tráfico que se origina en las aplicaciones BOT.
Bogon	Especifica el tráfico que se origina en direcciones IP no asignadas. Para obtener más información, consulte el material de referencia de bogon en el sitio web de Team CYMRU (http://www.team-cymru.org/Services/Bogons).
RedesHostiles	Especifica el tráfico que se origina en redes hostiles conocidas. RedesHostiles tiene un conjunto de 20 rangos de CIDR configurables (del rango 1 al 20, ambos inclusive).
Neighbours	Este grupo está en blanco de forma predeterminada. Debe configurar este grupo para clasificar el tráfico que se origina en las redes vecinas.

© Copyright IBM Corp. 2012, 2015

Tabla 58. Grupos de redes remotas predeterminados (continuación)

Grupo	Descripción
Smurfs	Especifica el tráfico que se origina en los ataques smurf. Un ataque smurf es un tipo de ataque de denegación de servicio que colapsa un sistema de destino con mensajes ping de difusión con suplantación.
Superflows	Este grupo no es configurable. Un superflujo es un flujo que es un agregado de un número de flujos que tienen un conjunto de elementos similar predeterminado.
RedesDeConfianza	Este grupo está en blanco de forma predeterminada. Debe configurar este grupo para clasificar el tráfico que se origina en las redes de confianza.
Listas de supervisión	Este grupo está en blanco de forma predeterminada. Puede configurar este grupo para clasificar el tráfico que se origina en las redes que desea supervisar.

Los grupos y objetos que incluyen superflujos son solamente para fines informativos y no se pueden editar. Los grupos y los objetos que incluyen bogons se configuran mediante la función de actualización automática.

Grupos de servicios remotos predeterminados

IBM Security QRadar SIEM incluye los grupos de servicios remotos predeterminados.

En la tabla siguiente se describen los grupos de servicios remotos predeterminados.

Tabla 59. Grupos de redes remotas predeterminados

Parámetro	Descripción
Servidores_IRC	Especifica el tráfico que se origina en direcciones comúnmente conocidas como servidores de chat.
Servicios_Enlinea	Especifica el tráfico que se origina en direcciones conocidas comúnmente como servicios en línea que podrían implicar la pérdida de datos.
Porno	Especifica el tráfico que se origina en direcciones comúnmente conocidas por contener material pornográfico explícito.
Proxys	Especifica el tráfico que se origina en servidores proxy abiertos comúnmente conocidos.

Tabla 59. Grupos de redes remotas predeterminados (continuación)

Parámetro	Descripción
Rangos_IP_Reservados	Especifica el tráfico que se origina en los rangos de direcciones IP reservadas.
Spam	Especifica el tráfico que se origina en direcciones comúnmente conocidas por generar correo no deseado (spam).
Spy_Adware	Especifica el tráfico que se origina en direcciones comúnmente conocidas por contener spyware o adware.
Superflows	Especifica el tráfico que se origina en direcciones comúnmente conocidas por generar superflujos.
Warez	Especifica el tráfico que se origina en direcciones comúnmente conocidas por contener software pirateado.

Directrices para los recursos de red

Dados la complejidad y los recursos de red que se necesitan para IBM Security QRadar SIEM en las grandes redes estructuradas, siga las directrices sugeridas.

En la lista siguiente se describen algunas de las prácticas sugeridas que puede seguir:

- Empaquete los objetos y utilice las pestañas **Actividad de red** y **Actividad de registro** para analizar los datos de la red.

  Un número menor de objetos crea menos entrada y menos salida en el disco.
- Normalmente, para los requisitos estándares del sistema, no supere los 200 objetos por grupo.

  Más objetos pueden afectar a la potencia de proceso cuando se investigue el tráfico.

Gestión de objetos de redes remotas

Después de crear grupos de redes remotas, puede agregar resultados de búsqueda de flujos y sucesos en los grupos de redes remotas. También puede crear reglas que comprueben la actividad en los grupos de redes remotas.

Utilice la ventana Redes remotas para añadir o editar un objeto de redes remotas.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración de redes remotas y servicios remotos**.
3. Pulse el icono **Redes remotas**.
4. Para añadir un objeto de redes remotas, pulse **Añadir** y especifique los valores de los parámetros.
5. Para editar un objeto de redes remotas, pulse el grupo que desea visualizar, pulse **Editar** y luego cambie los valores.
6. Pulse **Guardar**.
7. Pulse **Volver**.

8. Cierre la ventana Redes remotas.
9. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Gestión de objetos de servicios remotos

Los grupos de servicios remotos organizan el tráfico que se origina en los rangos de red definidos por el usuario o en el servidor de actualizaciones automáticas de IBM. Después de crear grupos de redes remotas, puede agregar resultados de búsqueda de flujos y sucesos y crear reglas que comprueben la actividad en los grupos de servicios remotos.

Utilice la ventana Servicios remotos para añadir o editar un objeto de servicios remotos.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración de redes remotas y servicios remotos**.
3. Pulse el icono **Servicios remotos**.
4. Para añadir un objeto de servicios remotos, pulse **Añadir** y especifique los valores de los parámetros.
5. Para editar un objeto de servicios remotos, pulse el grupo que desea visualizar, pulse el icono **Editar** y cambie los valores.
6. Pulse **Guardar**.
7. Pulse **Volver**.
8. Cierre la ventana Servicios remotos.
9. En el menú de la pestaña **Admin**, pulse **Desplegar cambios**.

Visión general de las correlaciones de QID

Utilice el programa de utilidad QID (QRadar Identifier) para crear, exportar, importar o modificar entradas de correlaciones de QID definidas por el usuario.

La correlación de QID asocia un suceso de un dispositivo externo a un (QID).

Consulte las tareas siguientes para la gestión de QID:

- "Creación de una entrada de correlación de QID" en la página 185
- "Modificación de una entrada de correlación de QID" en la página 186
- "Importación de entradas de correlaciones de QID" en la página 186
- "Exportación de entradas de correlaciones de QID" en la página 187

Para ejecutar el programa de utilidad, utilice la sintaxis siguiente:

```
qidmap_cli.sh [-l|-c|-m|-i[-f <nombre_archivo>]|-e[-f
<nombre_archivo>]|-d]
```

En la tabla siguiente se describen las opciones de línea de mandatos para el programa de utilidad de correlación QID.

Tabla 60. Opciones del programa de utilidad de correlación QID

Opciones	Descripción
-l	Lista la categoría de nivel bajo.

Tabla 60. Opciones del programa de utilidad de correlación QID (continuación)

Opciones	Descripción
-c	Crea una entrada de correlación de QID.
-m	Modifica una entrada de correlación de QID definida por el usuario ya existente.
-i	Importa las entradas de correlaciones de QID.
-e	Exporta las entradas de correlaciones de QID definidas por el usuario ya existentes.
-f <nombre_archivo>	Si incluye la opción -i o -e, especifique un nombre de archivo para importar o exportar las entradas de correlaciones de QID.
-d	Si incluye la opción -i o -e, especifique un delimitador para el archivo de importación o exportación. El valor predeterminado es una coma.
-h	Muestra las opciones de ayuda.

Creación de una entrada de correlación de QID

Cree una entrada de correlación QID (QRadar Identifier) para correlacionar un suceso de un dispositivo externo a QID.

Procedimiento

1. Inicie, mediante SSH, la sesión en QRadar como usuario root.
2. Para localizar la categoría de nivel bajo para la entrada de correlación de QID que desea crear, escriba el mandato siguiente:

   ```
   /opt/qradar/bin/qidmap_cli.sh -l
   ```

   Si desea buscar una categoría de nivel bajo determinada, puede utilizar el mandato `grep` para filtrar los resultados:

   ```
   /opt/qradar/bin/qidmap_cli.sh -l | grep <texto>
   ```

3. Escriba el mandato siguiente:

   ```
   qidmap_cli.sh -c --qname <nombre> --qdescription <descripción>
   --severity <gravedad> --lowlevelcategoryid <ID>
   ```

   En la tabla siguiente se describen las opciones de línea de mandatos para el programa de utilidad de correlación QID:

Opciones	Descripción
-c	Crea una entrada de correlación de QID.
--qname <nombre>	Nombre que desea asociar con esta entrada de correlación de QID. El nombre puede tener una longitud de hasta 255 caracteres y no debe tener espacios.
--qdescription <descripción>	Descripción de esta entrada de correlación de QID. La descripción puede tener una longitud de hasta 2048 caracteres y no debe tener espacios.
--severity <gravedad>	Nivel de gravedad que desea asignar a esta entrada de correlación de QID. El rango válido va de 1 a 10.
--lowlevelcategoryid <ID>	ID de categoría de nivel bajo que desea asignar a esta entrada de correlación de QID. Para obtener más información, consulte la guía de administración de QRadar.

Modificación de una entrada de correlación de QID

Modifique una entrada de correlación de QID (QRadar Identifier) definida por el usuario existente.

Procedimiento

1. Inicie, mediante SSH, la sesión en QRadar como usuario root.
2. Escriba el mandato siguiente:

   ```
   qidmap_cli.sh -m --qid<QID> --qname <nombre> --qdescription <descripción>
   --severity <gravedad>
   ```

   En la tabla siguiente se describen las opciones de línea de mandatos para el programa de utilidad de correlación QID:

Opciones	Descripción
-m	Modifica una entrada de correlación de QID definida por el usuario ya existente.
--qid<QID>	QID que desea modificar.
--qname <nombre>	Nombre que desea asociar con esta entrada de correlación de QID. El nombre puede tener una longitud de hasta 255 caracteres y no debe tener espacios.
--qdescription <descripción>	Descripción de esta entrada de correlación de QID. La descripción puede tener una longitud de hasta 2048 caracteres y no debe tener espacios.
--severity <gravedad>	Nivel de gravedad que desea asignar a esta entrada de correlación de QID. El rango válido va de 0 a 10.

Importación de entradas de correlaciones de QID

Con el programa de utilidad QID (QRadar Identifier) puede importar entradas de correlaciones de QID de un archivo .txt.

Procedimiento

1. Cree un archivo `.txt` que incluya las entradas de correlaciones de QID definidas por el usuario que desea importar. Asegúrese de que cada entrada del archivo esté separada mediante una coma. Seleccione una de las opciones siguientes:
   - Si desea importar una nueva lista de entradas de correlaciones de QID definidas por el usuario, cree el archivo con el formato siguiente para cada entrada:

     ```
     ,<nombre>,<descripción>,<gravedad>,<categoría>
     ```

     Ejemplo:

     ```
     ,buffer,buffer_QID,7,18401 ,malware,malware_misc,8,18403
     ```

   - Si desea importar una lista existente de entradas de correlaciones de QID definidas por el usuario, cree el archivo con el formato siguiente para cada entrada:

     ```
     <qid>,<nombre>,<descripción>,<gravedad>
     ```

     Ejemplo: `2000002,buffer,buffer_QID,7 2000001,malware,malware_misc`

En la tabla siguiente se describen las opciones de línea de mandatos para el programa de utilidad QID.

Opciones	Descripción
<qid>	QID existente para la entrada. Esta opción es obligatoria si desea importar una lista exportada existente de entradas de QID. Para importar entradas de QID nuevas, no utilice esta opción. El programa de utilidad de correlación QID asigna un identificador (QID) para cada entrada del archivo.
--qname <nombre>	Nombre que desea asociar con esta entrada de correlación de QID. El nombre puede tener una longitud de hasta 255 caracteres y no debe tener espacios.
--qdescription <descripción>	Descripción de esta entrada de correlación de QID. La descripción puede tener una longitud de hasta 2048 caracteres y no debe tener espacios.
--severity <gravedad>	Nivel de gravedad que desea asignar a esta entrada de correlación de QID. El rango válido va de 0 a 10.
--lowlevelcategoryid <ID>	ID de categoría de nivel bajo que desea asignar a esta entrada de correlación de QID. Esta opción solamente es obligatoria si desea importar una lista nueva de entradas de QID.

2. Guarde y cierre el archivo.
3. Inicie, mediante SSH, la sesión en QRadar como usuario root:
4. Para importar el archivo de correlación QID, escriba el mandato siguiente:

   ```
   /opt/qradar/bin/qidmap_cli.sh -i -f
   <nombre_archivo.txt>
   ```

   La opción *<nombre_archivo.txt>* es la vía de acceso del directorio y el nombre del archivo que contiene las entradas de correlaciones de QID. Si alguna de las entradas del archivo provoca un error, no se aplica ninguna entrada del archivo.

Exportación de entradas de correlaciones de QID

Con el programa de utilidad QID (QRadar Identifier) puede exportar entradas de correlaciones de QID de un archivo `.txt`.

Procedimiento

1. Inicie, mediante SSH, la sesión en QRadar como usuario root.
2. Para exportar el archivo de correlación QID, escriba el mandato siguiente:

   ```
   /opt/qradar/bin/qidmap_cli.sh -e -f
   <nombre_archivo.txt>
   ```

   La opción *<nombre_archivo.txt>* es la vía de acceso del directorio y el nombre del archivo que desea que contenga las entradas de correlaciones de QID.

Capítulo 14. Descubrimiento de servidores

La función **Descubrimiento de servidores** utiliza la base de datos de perfiles de activos para descubrir los distintos tipos de servidor que están basados en definiciones de puerto. A continuación, puede seleccionar los servidores para añadirlos a un componente básico de tipo servidor para las reglas.

La función **Descubrimiento de servidores** está basada en componentes básicos de tipo servidor. Se utilizan puertos para definir el tipo de servidor. Así, el componente básico de tipo servidor funciona como un filtro basado en puertos cuando se realiza una búsqueda en la base de datos de perfiles de activo.

Para obtener más información sobre los componentes básicos, consulte la publicación *IBM Security QRadar SIEM Users Guide*.

Descubrimiento de servidores

Utilice la pestaña **Activos** para descubrir servidores en la red.

Procedimiento

1. Pulse la pestaña **Activos**.
2. En el menú de navegación, pulse **Descubrimiento de servidores**.
3. En la lista **Tipo de servidor**, seleccione el tipo de servidor que desee descubrir.
4. Seleccione una de las opciones siguientes para determinar los servidores que desea descubrir:
   - Para utilizar el tipo seleccionado actualmente en **Tipo de servidor** para buscar en todos los servidores del despliegue, seleccione **Todos**.
   - Para buscar en los servidores del despliegue que estaban asignados al tipo seleccionado actualmente en **Tipo de servidor**, seleccione **Asignados**.
   - Para buscar en los servidores del despliegue que no están asignados, seleccione **Sin asignar**.
5. En la lista **Red**, seleccione la red en la que desea buscar.
6. Pulse **Descubrir servidores**.
7. En la tabla **Servidores coincidentes**, seleccione las casillas de verificación de todos los servidores que desee asignar al rol de servidor.
8. Pulse **Aprobar servidores seleccionados**.

© Copyright IBM Corp. 2012, 2015

Capítulo 15. Segmentación en dominios

La segmentación de la red en diferentes dominios permite garantizar que la información relevante está a disposición solamente de aquellos usuarios que la necesitan.

Puede crear perfiles de seguridad para limitar la información que está disponible para un grupo de usuarios dentro de ese dominio. Los perfiles de seguridad proporcionan a los usuarios acceso únicamente a la información que se necesita para completar sus tareas diarias. Se modifica solamente el perfil de seguridad de los usuarios afectados, no cada usuario de forma individual.

También puede utilizar dominios para gestionar los rangos de direcciones IP solapados. Este método es útil cuando se utiliza una infraestructura de IBM Security QRadar compartida para recopilar datos a partir de varias redes. Al crear dominios que representan un espacio de direcciones determinado en la red, varios dispositivos que se encuentran en dominios diferentes pueden tener la misma dirección IP pero se tratarán como dispositivos independientes.

Direcciones IP solapadas

Una dirección IP solapada es una dirección IP que se ha asignado a más de un dispositivo o unidad lógica, como un tipo de origen de sucesos, en una red. Los rangos de direcciones IP solapados pueden causar problemas significativos a las empresas que fusionan redes después de adquisiciones corporativas o a los proveedores de servicios de seguridad gestionados (MSSP) que incorporan nuevos clientes.

IBM Security QRadar debe ser capaz de diferenciar los sucesos y los flujos que proceden de distintos dispositivos y que tienen la misma dirección IP. Si la misma dirección IP se ha asignado a más de un origen de sucesos, puede crear dominios para distinguirlos.

Por ejemplo, supongamos un caso en el que la empresa A adquiere la empresa B y desea utilizar una instancia compartida de QRadar para supervisar los activos de la empresa nueva. La adquisición tiene una estructura de red similar que hace que se utilice la misma dirección IP para diferentes orígenes de registro en cada empresa. Los orígenes de registro con la misma dirección IP provocan problemas de correlación, creación de informes, búsqueda y creación de perfiles de activo.

Para distinguir el origen de los sucesos y los flujos que llegan a QRadar desde el origen de registro, puede crear dos dominios y asignar cada origen de registro a un dominio diferente. Si es necesario, también puede asignar cada recopilador de sucesos y recopilador de flujos al mismo dominio que el origen de registro que les envía sucesos.

Para ver los sucesos entrantes por dominio, cree una búsqueda e incluya la información de dominio en los resultados de la búsqueda.

© Copyright IBM Corp. 2012, 2015

Definición y etiquetado de dominio

Los dominios se definen basándose en los orígenes de entrada de QRadar. Cuando llegan sucesos y flujos a QRadar, las definiciones de dominios se evalúan y los sucesos y los flujos se etiquetan con la información de dominio.

Especificación de dominios para los sucesos

A continuación se indican las maneras de especificar dominios para los sucesos:

Recopiladores de sucesos
Si un recopilador de sucesos está dedicado a un segmento de red o un rango de direcciones IP en concreto, puede marcar con un distintivo ese recopilador de sucesos entero como parte de ese dominio.

Todos los orígenes de registro que llegan a ese recopilador de sucesos pertenecen al dominio; por lo tanto, todos los orígenes de registro que se detecten como nuevos se añaden automáticamente al dominio.

Orígenes de registro
Puede configurar orígenes de registro específicos para que pertenezcan a un dominio.

Este método de etiquetado de dominio es una opción para los despliegues en los que un recopilador de sucesos puede recibir sucesos de varios dominios.

Grupos de orígenes de registro
Puede asignar grupos de orígenes de registro a un dominio específico. Esta opción brinda un mayor control sobre la configuración de los orígenes de registro.

Los orígenes de registro nuevos que se añadan al grupo de orígenes de registro reciben automáticamente el etiquetado de dominio que está asociado con el grupo de orígenes de registro.

Propiedades personalizadas
Puede aplicar propiedades personalizadas a los mensajes de registro que proceden de un origen de registro.

Para determinar a qué dominio pertenece cada mensaje de registro, el valor de la propiedad personalizada se busca en una tabla definida por el usuario.

Esta opción se utiliza para los orígenes de registro con varios rangos de direcciones o varios arrendatarios, como los servidores de archivos y los repositorios de documentos.

Especificación de dominios para los flujos

A continuación se indican las maneras de especificar dominios para los flujos:

Recopiladores de flujo
Puede asignar recopiladores QFlow específicos a un dominio.

Todos los orígenes de flujo que llegan a ese recopilador de flujo pertenecen al dominio; por lo tanto, todos los orígenes de flujo que se detecten como nuevos se añaden automáticamente al dominio.

Orígenes de flujo
Puede designar orígenes de flujo específicos para un dominio.

Esta opción es útil cuando un solo recopilador QFlow recopila flujos de varios segmentos de red o direccionadores que contienen rangos de direcciones IP solapados.

Especificación de dominios para los resultados de la exploración

También puede asignar exploradores de vulnerabilidades a un dominio específico para que los resultados de la exploración estén adecuadamente marcados como pertenecientes a ese dominio. Una definición de dominio puede constar de todos los orígenes de entrada de QRadar.

Para obtener información sobre la asignación de la red a dominios preconfigurados, consulte el apartado "Jerarquía de red" en la página 69.

Orden de precedencia para evaluar los criterios de dominio

Cuando llegan sucesos y flujos al sistema de QRadar, los criterios de dominio se evalúan en función de la granularidad de la definición de dominio.

Si la definición de dominio se basa en un suceso, primero se comprueba si el suceso entrante tiene propiedades personalizadas que se correlacionen con la definición de dominio. Si el resultado de una expresión regular que se define en una propiedad personalizada no coincide con una correlación de dominio, el suceso se asigna automáticamente al dominio predeterminado.

Si el suceso no coincide con la definición de dominio de las propiedades personalizadas, se aplica el orden de prioridad siguiente:

1. origen de registro
2. grupo de orígenes de registro
3. recopilador de sucesos

Si el dominio está definido según un flujo, se aplica el orden de prioridad siguiente:

1. origen de flujo
2. recopilador de flujos

Si un explorador tiene un dominio asociado, todos los activos que el explorador descubra se asignan automáticamente al mismo dominio que el explorador.

Reenvío de datos a otro sistema de QRadar

La información de dominio se elimina cuando los datos se reenvían a otro sistema de QRadar. Los sucesos y los flujos que contienen información de dominio se asignan automáticamente al dominio predeterminado en el sistema de QRadar receptor. Para identificar qué sucesos y flujos están asignados al dominio predeterminado, puede crear una búsqueda personalizada en el sistema receptor. Tal ver prefiera volver a asignar estos sucesos y flujos a un dominio definido por el usuario.

Creación de dominios

Utilice la ventana Gestión de dominios para crear dominios basados en los orígenes de entrada de IBM Security QRadar.

Acerca de esta tarea

Utilice las directrices siguientes al crear dominios:

- Todo lo que no esté asignado a un dominio definido por el usuario se asigna automáticamente al dominio predeterminado. Los usuarios que tienen acceso limitado a los dominios no deben tener privilegios administrativos, ya que este privilegio otorga acceso ilimitado a todos los dominios.
- Puede correlacionar la misma propiedad personalizada a dos dominios distintos; sin embargo, el resultado de la captura debe ser diferente para cada uno.
- No se puede asignar un origen de registro, un grupo de orígenes de registro o un recopilador de sucesos a dos dominios diferentes. Cuando un grupo de orígenes de registro se asigna a un dominio, cada uno de los atributos correlacionados es visible en la ventana Gestión de dominios.

Los perfiles de seguridad se deben actualizar con un dominio asociado. Las restricciones de nivel de dominio no se aplican hasta que se actualizan los perfiles de seguridad y se despliegan los cambios.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Gestión de dominios**.
4. Para añadir un dominio, pulse **Añadir** y escriba un nombre exclusivo y una descripción para el dominio.

   Consejo: Puede comprobar si un nombre es exclusivo escribiendo el nombre en el recuadro de búsqueda **Nombre de dominio de entrada**.
5. Pulse la pestaña correspondiente al criterio de dominio que se vaya a definir.
   - Para definir el dominio basado en una propiedad personalizada, grupo de orígenes de registro, origen de registro o recopilador de sucesos, pulse la pestaña **Sucesos**.
   - Para definir el dominio basado en un origen de flujo o un recopilador de flujos, pulse la pestaña **Flujos**.
   - Para definir el dominio basado en un explorador, incluidos los de IBM Security QRadar Vulnerability Manager, pulse la pestaña **Exploradores**.
6. Para asignar una propiedad personalizada a un dominio, en el recuadro **Resultados de la captura**, escriba el texto que coincida con el resultado del filtro de la expresión regular.

   Importante: Debe marcar el recuadro de selección **Optimizar el análisis de reglas, informes y búsquedas** en la ventana Propiedades de sucesos personalizadas para analizar y almacenar la propiedad de suceso personalizada. La segmentación en dominios no se producirá si esta opción no está seleccionada.
7. En la lista, seleccione el criterio de dominio y pulse **Añadir**.
8. Después de añadir los elementos de origen al dominio, pulse **Crear**.

Qué hacer a continuación

Cree perfiles de seguridad para definir qué usuarios tienen acceso a los dominios. Después de crear el primer dominio en su entorno, debe actualizar los perfiles de seguridad para todos los usuarios no administrativos para especificar la asignación

de dominio. En los entornos que tienen en cuenta el dominio, los usuarios no administrativo cuyo perfil de seguridad no especifique una asignación de dominio no verán ninguna actividad de registro ni actividad de red.

También puede utilizar la herramienta Jerarquía de red para asignar la red a los dominios preconfigurados. Para obtener más información, consulte el apartado "Jerarquía de red" en la página 69.

Privilegios de dominio derivados de perfiles de seguridad

Puede utilizar perfiles de seguridad para otorgar privilegios de dominio y asegurarse de que se respeten las restricciones de dominio en todo el sistema de IBM Security QRadar. Los perfiles de seguridad también facilitan la gestión de los privilegios para un grupo de usuarios de gran tamaño cuando los requisitos empresariales cambian de pronto.

Los usuarios pueden ver únicamente los datos que están dentro de los límites del dominio que está configurado para los perfiles de seguridad que tienen asignados. Los perfiles de seguridad incluyen los dominios como uno de los primeros criterios que se evalúan para restringir el acceso al sistema. Cuando un dominio se asigna a un perfil de seguridad, tiene prioridad sobre otros permisos de seguridad. Después de evaluar las restricciones de dominio, se evalúa cada perfil de seguridad para determinar los permisos de red y de registro para cada uno de ellos.

Por ejemplo, a un usuario se le otorgan privilegios a Dominio_2 y acceso a la red 10.0.0.0/8. Dicho usuario puede ver solamente los sucesos, los delitos, los activos y los flujos que proceden de Dominio_2 y que contienen una dirección de la red 10.0.0.0/8.

Como administrador de QRadar, puede ver todos los dominios y puede asignar dominios a los usuarios no administrativos. No asigne privilegios administrativos a los usuarios a los que desea restringir a un dominio determinado.

Los perfiles de seguridad se deben actualizar con un dominio asociado. Las restricciones de nivel de dominio no se aplican hasta que se actualizan los perfiles de seguridad y se despliegan los cambios.

Cuando asigne dominios a un perfil de seguridad, puede otorgar acceso a los siguientes tipos de dominios:

Dominios definidos por el usuario
Puede crear dominios que están basados en orígenes de entrada mediante la herramienta Gestión de dominios. Para obtener más información, consulte Creación de dominios.

Dominio predeterminado
Todo lo que no esté asignado a un dominio definido por el usuario se asigna automáticamente al dominio predeterminado. El dominio predeterminado contiene los sucesos de todo el sistema.

Nota: Los usuarios que tienen acceso al dominio predeterminado pueden ver sucesos de todo el sistema sin restricciones. Asegúrese de que este acceso es aceptable antes de asignar a los usuarios acceso al dominio predeterminado. Todos los administradores tienen acceso al dominio predeterminado.

Cualquier origen de registro que se descubra automáticamente en un recopilador de sucesos compartido (que no está explícitamente asignado a un dominio) se descubre automáticamente en el dominio predeterminado. Estos orígenes de registro requieren intervención manual. Para identificar estos orígenes de registro, debe ejecutar periódicamente una búsqueda en el dominio predeterminado que se agrupe por origen de registro.

Todos los dominios
Los usuarios a los que se les asigna un perfil de seguridad que tenga acceso a **Todos los dominios** pueden ver todos los dominios activos del sistema, el dominio predeterminado y todos los dominios que se hayan suprimido anteriormente en todo el sistema. También podrán ver todos los dominios que se creen en el futuro.

Si suprime un dominio, no se puede asignar a un perfil de seguridad. Si el usuario tiene asignado **Todos los dominios** o si el dominio se asignó al usuario antes de que se suprimiese, el dominio suprimido se devuelve en los resultados históricos de la búsqueda de sucesos, flujos, activos y delitos. No se puede filtrar por dominios suprimidos cuando se ejecuta una búsqueda.

Los usuarios administrativos pueden ver qué dominios están asignados a los perfiles de seguridad en la pestaña **Resumen** de la ventana Gestión de dominios.

Modificaciones de reglas en entornos que tienen en cuenta el dominio

Las reglas las puede ver, modificar o inhabilitar cualquier usuario que tenga los permisos **Mantener reglas personalizadas** y **Ver reglas personalizadas**, independientemente de a qué dominio pertenezca el usuario.

Importante: cuando se añade la prestación de **Actividad de registro** a un rol de usuario, los permisos **Mantener reglas personalizadas** y **Ver reglas personalizadas** se otorgan automáticamente. Los usuarios que tienen estos permisos tienen acceso a todos los datos de registro de todos los dominios y pueden editar reglas en todos los dominios, incluso si sus valores de perfil de seguridad tienen restricciones a nivel de dominio. Para evitar que los usuarios del dominio puedan acceder a los datos de registro y modificar las reglas de otros dominios, edite el rol de usuario y elimine los permisos **Mantener reglas personalizadas** y **Ver reglas personalizadas**.

Búsquedas que tienen en cuenta el dominio

Puede utilizar dominios como criterio de búsqueda en las búsquedas personalizadas. El perfil de seguridad controla en qué dominios puede realizar búsquedas.

Los sucesos de todo el sistema y los sucesos que no estén asignados a un dominio definido por el usuario se asignan automáticamente al dominio predeterminado. Los administradores o los usuarios que tengan un perfil de seguridad que proporcione acceso al dominio predeterminado pueden crear una búsqueda personalizada para ver todos los sucesos que no están asignados a un dominio definido por el usuario.

El administrador de dominios personalizado puede compartir una búsqueda guardada con otros usuarios de dominio. Cuando el usuario de dominio ejecuta esa búsqueda guardada, los resultados se limitan a su dominio.

Reglas y delitos específicos del dominio

Una regla puede aplicarse en el contexto de un solo dominio o en el contexto de todos los dominios. Las reglas que tienen en cuenta el dominio proporcionan la opción de incluir la prueba **And Domain Is**.

Puede restringir una regla para que se aplique solamente a los sucesos que se producen en un dominio determinado. Un suceso que tenga una etiqueta de dominio que es diferente del dominio que está establecido en la regla no desencadena una respuesta de suceso.

En un sistema de IBM Security QRadar que no tenga dominios definidos por el usuario, una regla crea un delito y sigue contribuyendo a él cada vez que la regla se activa. En un entorno que tiene en cuenta el dominio, una regla crea un nuevo delito cada vez que la regla se desencadena en el contexto de un dominio diferente.

Las reglas que funcionan en el contexto de todos los dominios se denominan de reglas de todo el sistema. Para crear una regla de todo el sistema que pruebe las condiciones en el sistema entero, seleccione **Cualquier dominio** en la lista de dominios de la prueba **And Domain Is**. Una regla **Cualquier dominio** crea un delito de **Cualquier dominio**.

Regla de un solo dominio
Si la regla es una regla con estados, los estados se mantienen por separado para cada dominio. La regla se desencadena por separado para cada dominio. Cuando la regla se desencadena, se crean delitos por separado para cada dominio involucrado y los delitos se etiquetan con esos dominios.

Delito de un solo dominio
El delito se etiqueta con el nombre de dominio correspondiente. Puede contener solamente sucesos que están etiquetados con ese dominio.

Regla de todo el sistema
Si la regla es una regla con estados, se mantiene un solo estado para el sistema completo y las etiquetas de dominio se pasan por alto. Cuando la regla se ejecuta, crea o contribuye a un único delito de todo el sistema.

Delito de todo el sistema
El delito se etiqueta con **Cualquier dominio**. Contiene solamente sucesos que están etiquetados con todos los dominios.

En la tabla siguiente se proporcionan ejemplos de reglas que tienen en cuenta el dominio. En el ejemplo se utiliza un sistema que tiene tres dominios definidos: Dominio_A, Dominio_B y Dominio_C.

Tabla 61. Reglas que tienen en cuenta el dominio

Texto de dominio	Explicación	Respuesta de regla
el dominio es uno de: Dominio_A	Busca solamente los sucesos que están etiquetados con `Dominio_A` y pasa por alto las reglas que están etiquetadas con otros dominios.	Crea o contribuye a un delito que está etiquetado con `Dominio_A`.

Tabla 61. Reglas que tienen en cuenta el dominio (continuación)

Texto de dominio	Explicación	Respuesta de regla
el dominio es uno de: Dominio_A y una prueba con estado que se define como **cuando se detecta flujo HTTP 10 veces en 1 minuto**	Busca solamente los sucesos que están etiquetados con `Dominio_A` y pasa por alto las reglas que están etiquetadas con otros dominios.	Crea o contribuye a un delito que está etiquetado con `Dominio_A`. Se mantiene un contador de flujos HTTP con un solo estado para Dominio_A.
el dominio es uno de: Dominio_A, Dominio_B	Busca solamente los sucesos que están etiquetados con `Dominio_A` y `Dominio_B` y pasa por alto los sucesos que están etiquetados con `Dominio_C`. Esta regla se comporta como dos instancias independientes de una misma regla de dominio y crea delitos por separado para los distintos dominios.	Para los datos que están etiquetados con `Dominio_A`, crea o contribuye a un solo delito de dominio que está etiquetado con `Dominio_A`. Para los datos que están etiquetados con `Dominio_B`, crea o contribuye a un solo delito de dominio que está etiquetado con `Dominio_B`.
el dominio es uno de: Dominio_A, Dominio_B y un prueba con estado que se define como **cuando se detecta flujo HTTP 10 veces en 1 minuto**	Busca solamente los sucesos que están etiquetados con `Dominio_A` y `Dominio_B` y pasa por alto los sucesos que están etiquetados con `Dominio_C`. Esta regla se comporta como dos instancias independientes de una misma regla de dominio y mantiene dos estados por separado (contadores de flujos HTTP) para dos dominios diferentes.	Cuando la regla detecta 10 flujos HTTP que están etiquetados con `Dominio_A` en un minuto, crea o contribuye a un delito que está etiquetado con `Dominio_A`. Cuando la regla detecta 10 flujos HTTP que están etiquetados con `Dominio_B` en un minuto, crea o contribuye a un delito que está etiquetado con `Dominio_B`.
No hay definida ninguna prueba de dominio	Busca los sucesos que están etiquetados con todos los dominios y crea o contribuye a los delitos por dominio.	Cada dominio independiente tiene delitos que se generan para él, pero los delitos no contienen contribuciones de otros dominios.
Una regla tiene una prueba con estado que se define como **cuando se detecta flujo HTTP 10 veces en 1 minuto** y no se ha definido ninguna prueba de dominio	Busca los sucesos que están etiquetados con `Dominio_A`, `Dominio_B` o `Dominio_C`.	Mantiene estados por separado y crea delitos por separado para cada dominio.
el dominio es uno de: Cualquier dominio	Busca todos los sucesos, independientemente de con qué dominio esté etiquetado.	Crea o contribuye a un solo delito de todo el sistema que está etiquetado con `Cualquier dominio`.

Tabla 61. Reglas que tienen en cuenta el dominio (continuación)

Texto de dominio	Explicación	Respuesta de regla
el dominio es uno de: Cualquier dominio y una prueba con estado que se define como **cuando se detecta flujo HTTP 10 veces en 1 minuto**	Busca todos los sucesos, independientemente de con qué dominio esté etiquetado, y mantiene un solo estado para todos los dominios.	Crea o contribuye a un solo delito de todo el sistema que está etiquetado con `Cualquier dominio`. Por ejemplo, si detecta tres sucesos que están etiquetados con `Dominio_A`, tres sucesos que están etiquetados con `Dominio_B` y cuatro sucesos que están etiquetados con `Dominio_C`, crea un delito porque ha detectado 10 sucesos en total.
el dominio es uno de: Cualquier dominio, Dominio_A	Funciona igual que una regla que tiene **el dominio es uno de: Cualquier dominio**.	Cuando la prueba de dominio incluye `Cualquier dominio`, los dominios individuales que figuran en la lista se pasan por alto.

Cuando vea la tabla de delitos, puede ordenar los delitos pulsando la columna **Dominio**. **Dominio predeterminado** no se incluye en la función de ordenación, por lo que no aparece en orden alfabético. Sin embargo, aparece en la parte superior o inferior de la lista **Dominio**, en función de si la columna se ordena en orden ascendente o descendente. **Cualquier dominio** no aparece en la lista de delitos.

Ejemplo: Asignaciones de privilegio de dominio según propiedades personalizadas

Si los archivos de registro contienen información que desea utilizar en una definición de dominio, puede exponer la información como propiedad de suceso personalizada.

Una propiedad personalizada se asigna a un dominio en función del resultado de la captura. Puede asignar la misma propiedad personalizada a varios dominios, pero los resultados de captura deben ser diferentes.

Por ejemplo, una propiedad de suceso personalizada, como `userID`, puede dar como resultado un usuario individual o una lista de usuarios. Cada usuario puede pertenecer a un solo dominio.

En el diagrama siguiente, los orígenes de registro contienen información de identificación de usuario que se expone como propiedad personalizada, `userID`. Los resultados de captura devuelven una lista de cuatro usuarios, y cada usuario se asigna a un solo dominio. En este caso, dos usuarios están asignados al dominio A y dos usuarios están asignados al dominio B.

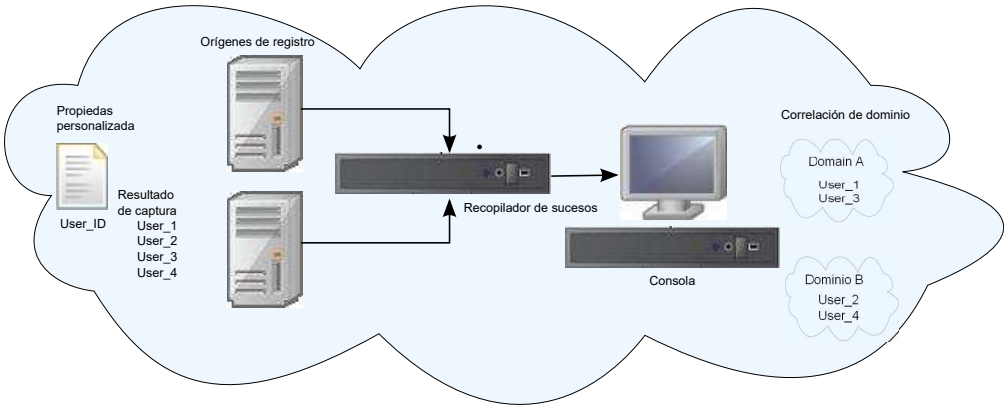

Figura 3. Asignación de dominios utilizando una propiedad de suceso personalizada

Si los resultados de captura devuelven un usuario que no está asignado a un dominio definido por el usuario específico, dicho usuario se asigna automáticamente al dominio predeterminado. Las asignaciones de dominio predeterminado requieren la intervención manual. Realice búsquedas periódicas para asegurarse de que todas las entidades en el dominio predeterminado están asignadas correctamente.

Importante: Antes de utilizar una propiedad personalizada en una definición de dominio, asegúrese de que se ha seleccionado **Optimizar el análisis de reglas, informes y búsquedas** en la ventana **Propiedades de sucesos personalizadas**. Esta opción garantiza que la propiedad de suceso personalizada se analiza y se almacena cuando QRadar recibe el suceso por primera vez. La segmentación en dominios no se producirá si esta opción no está seleccionada.

Capítulo 16. Gestión multiarrendatario

Los entornos multiarrendatario permiten a los proveedores de servicios de seguridad gestionados (MSSP) y a las organizaciones de varias divisiones proporcionar servicios de seguridad a varias organizaciones cliente desde un único despliegue de IBM Security QRadar compartido. No es necesario desplegar una instancia de QRadar exclusiva para cada cliente.

En un despliegue multiarrendatario, se asegura de que los clientes sólo ven sus datos mediante la creación de dominios que están basados en sus orígenes de entrada de QRadar. A continuación, utilice perfiles de seguridad y los roles de usuario para gestionar privilegios para grupos de usuarios de gran tamaño dentro del dominio. Los perfiles de seguridad y los roles de usuario garantizan que los usuarios sólo tengan acceso a la información que están autorizados a ver.

Roles de usuario en un entorno multiarrendatario

Los entornos multiarrendatario incluyen un proveedor de servicios y varios arrendatarios. Cada rol tiene responsabilidades y actividades asociadas distintas.

Proveedor de servicios

El proveedor de servicios es propietario del sistema y gestiona su utilización por parte de varios arrendatarios. El proveedor de servicios puede ver los datos de todos los arrendatarios. El administrador de MSSP (proveedor de servicios de seguridad gestionados) es responsable de las actividades siguientes:

- Administra y supervisa la salud del sistema del despliegue de QRadar.
- Suministra arrendatarios nuevos.
- Crea roles y perfiles de seguridad para administradores y usuarios de arrendatario.
- Protege el sistema contra el acceso no autorizado.
- Crea dominios para aislar datos de arrendatario.
- Despliega los cambios que el administrador de arrendatario ha realizado en el entorno de arrendatario.
- Supervisa las licencias de QRadar.
- Colabora con el administrador del arrendatario.

Arrendatarios

Cada arrendamiento incluye un administrador de arrendatario y usuarios de arrendatario. El administrador de arrendatario puede ser un empleado de la organización arrendataria, o el proveedor de servicios puede administrar el arrendatario en nombre del cliente.

El administrador de arrendatario es responsable de las actividades siguientes:

- Configura las definiciones de la Jerarquía de red dentro de su propio arrendamiento.
- Configura y gestiona datos de arrendatario.
- Visualiza los orígenes de registro. Puede editar el origen de registro para fusionar datos y puede inhabilitar orígenes de registro.

© Copyright IBM Corp. 2012, 2015

- Colabora con el administrador de MSSP.

El administrador de arrendatario puede configurar despliegues específicos de arrendatario, pero no puede acceder a ni modificar la configuración de otro arrendatario. Debe ponerse en contacto con el administrador de MSSP para desplegar los cambios en el entorno de QRadar, incluidos los cambios en la jerarquía de red dentro de su propio arrendatario.

Los usuarios de arrendatario no tienen privilegios administrativos y sólo pueden ver los datos a los que tienen acceso. Por ejemplo, un usuario puede tener privilegios para ver los datos de sólo 1 de origen de registro dentro de un dominio que tiene varios orígenes de registro.

Dominios y orígenes de registro en entornos multiarrendatario

Utilice dominios para separar direcciones IP solapadas y para asignar orígenes de datos, como por ejemplo sucesos y flujos, a conjuntos de datos específicos del arrendatario.

Cuando llegan sucesos o flujos a QRadar, QRadar evalúa las definiciones de dominio que están configuradas, y los sucesos y flujos se asignan a un dominio. Un arrendatario puede tener más de un dominio. Si no se han configurado dominios, los sucesos y los flujos se asignan al dominio predeterminado.

Segmentación en dominios

Los dominios son grupos virtuales que se utilizan para segregar datos en función del origen de los datos. Son los bloques de construcción de los entornos multiarrendatario. Se configuran dominios de los siguientes orígenes de entrada:

- Recopiladores de sucesos y flujos
- Orígenes de flujo
- Orígenes de registro y grupos de orígenes de registro
- Propiedades personalizadas
- Exploradores

Un despliegue multiarrendatario puede consistir en una configuración de hardware básica que incluye una consola de QRadar, un procesador de sucesos centralizado y un recopilador de sucesos para cada cliente. En esta configuración, puede definir dominios en el nivel de recopilador, que a continuación asigna automáticamente los datos recibidos por QRadar a un dominio.

Para consolidar la configuración de hardware aún más, puede utilizar un recopilador para varios clientes. Si el mismo recopilador añade orígenes de registro o flujo que pertenecen a diferentes arrendatarios, puede asignar los orígenes a dominios diferentes. Cuando se utilizan definiciones de dominio en el nivel de origen de registro, cada nombre de origen de registro debe ser exclusivo en todo el despliegue de QRadar.

Si es necesario separar los datos de un solo origen de registro y asignarlos a dominios diferentes, puede configurar dominios desde propiedades personalizadas. QRadar busca la propiedad personalizada en la carga útil y la asigna al dominio correcto. Por ejemplo, si ha configurado QRadar para integrarse con un dispositivo Check Point Provider-1, puede utilizar propiedades personalizadas para asignar los datos de ese origen de registro a distintos dominios.

Detección automática de origen de registro

Cuando los dominios están definidos en el nivel de recopilador y el recopilador de sucesos dedicado se asigna a un solo dominio, los orígenes de registro nuevos que se detectan automáticamente se asignan a ese dominio. Por ejemplo, todos los orígenes de registro que se detectan en `Recopilador_sucesos_1` se asignan a `Dominio_A`. Todos los orígenes de registro que se recopilan automáticamente en `Recopilador_sucesos_2` se asignan a `Dominio_B`.

Cuando los dominios están definidos en el nivel de origen de registro o de propiedad personalizada, los orígenes de registro que se detectan automáticamente y no están ya asignados a un dominio se asignan automáticamente al dominio predeterminado. El administrador de MSSP deben revisar los orígenes de registro del dominio predeterminado y asignarlos a los dominios de cliente correctos. En un entorno multiarrendatario, la asignación de orígenes de registro a un dominio específico impide la fuga de datos y aplica la separación de datos en los dominios.

Suministro de un nuevo arrendatario

Como administrador de MSSP (proveedor de servicios de seguridad gestionados), está utilizando una sola instancia de IBM Security QRadar para proporcionar a varios clientes una arquitectura unificada para la detección y priorización de amenazas.

En este escenario, está incorporando un nuevo cliente. Debe suministrar un nuevo arrendatario y crear una cuenta de administrador de arrendatario con derechos administrativos limitados dentro de su propio arrendatario. Debe limitar el acceso del administrador del arrendatario de modo que no pueda ver ni editar la información de otros arrendatarios.

Antes de suministrar un nuevo arrendatario, debe crear los orígenes de datos, como por ejemplo orígenes de registro o recopiladores de flujo, para el cliente y asignarlos a un dominio.

Lleve a cabo las tareas siguientes utilizando las herramientas de la pestaña **Admin** para suministrar el nuevo arrendatario en QRadar:

1. Para crear el arrendatario, pulse **Gestión de arrendatarios**.

   Para obtener información sobre cómo establecer los límites de sucesos por segundo (EPS) y flujos por minuto (FPM) para cada arrendatario, consulte “Supervisión del uso de licencias en despliegues multiarrendatario” en la página 204.
2. Para asignar dominios al arrendatario, pulse **Gestión de dominios**.
3. Para crear el rol de administrador de arrendatario y otorgar los permisos de **Administración delegada**, pulse **Roles de usuario**.

   En un entorno multiarrendatario, los usuarios de arrendatario con permisos de **Administración delegada** sólo pueden ver datos de su propio entorno de arrendatario. Si asigna otros permisos administrativos que no forman parte de la **Administración delegada**, el acceso dejará de estar restringido a ese dominio.
4. Para crear los perfiles de seguridad de arrendatario y restringir el acceso a los datos especificando los dominios del arrendatario, pulse **Perfiles de seguridad**.
5. Para crear los usuarios arrendatarios y asignar el rol de usuario, el perfil de seguridad y el arrendatario, pulse **Usuarios**.

Supervisión del uso de licencias en despliegues multiarrendatario

Como administrador de MSSP (proveedor de servicios de seguridad gestionados), puede supervisar las tasas de sucesos y flujos en todo el despliegue de IBM Security QRadar.

Cuando se crea un arrendatario, puede establecer límites para los sucesos por segundo (EPS) y los flujos por minuto (FPM). Al establecer límites de EPS y FPM para cada arrendatario, se puede gestionar mejor la capacidad de licencia en varios clientes. Si tiene un procesador que está recopilando sucesos o flujos para un solo cliente, no es necesario asignar límites de EPS y FPM de arrendatario. Si tiene un único procesador que recopila sucesos o flujos de varios clientes, puede establecer límites de EPS y FPM para cada arrendatario.

Si establece los límites de EPS y FPM en valores que superan los límites de sus licencias de software o del hardware de dispositivo, el sistema disminuye automáticamente los sucesos y flujos de ese arrendatario para asegurarse de que no se superen los límites. Si no establece límites de EPS y FPM para los arrendatarios, cada arrendatario recibe sucesos y flujos hasta que se alcanzan los límites de la licencia o el dispositivo. Los límites de licencia se aplican host gestionado. Si supera regularmente los límites de la licencia, puede obtener una licencia diferente que sea más adecuado para su despliegue.

Visualización de los límites de licencia acumulativos en el despliegue

Las tasas de EPS y FPM que ha establecido para cada arrendatario no se validan automáticamente con respecto a las titularidades de licencia. Para ver los límites acumulativos de las licencias de software que se aplican al sistema en comparación con los límites de hardware de dispositivo, siga estos pasos:

1. En la pestaña **Admin**, pulse **Configuración del sistema** > **Gestión del sistema y licencias**.
2. Expanda **Detalles de despliegue** y pase el ratón por encima de **Límite de sucesos** o **Límite de flujos**.

Visualización de tasas EPS por origen de registro o por dominio

Utilice el campo **Búsqueda avanzada** para especificar una consulta AQL (Ariel Query Language) para ver las tasas de EPS para orígenes de registro y dominios.

1. En la pestaña **Actividad de red**, seleccione **Búsqueda avanzada** en el cuadro de lista desplegable de la barra de herramientas **Buscar**.
2. Para ver el EPS por origen de registro, escriba la consulta siguiente:

```
select logsourcename(logsourceid) as LogSource, sum(eventcount) /
( ( max(endTime) - min(startTime) ) / 1000 ) as EPS from events
group by logsourceid order by EPS desc last 5 minutes
```

3. Para ver el EPS por dominio, escriba la consulta siguiente:

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) /
( ( max(endTime) - min(startTime)) / 1000 ) as EPS from events
group by domainid order by EPS desc last 5 minutes
```

Los valores de fecha para (endTime) y (startTime) deben estar representados en milisegundos desde la época de UNIX 1 de enero de 1970.

Detección de sucesos y flujos eliminados

Los sucesos y flujos se descartan cuando la interconexión de procesos de IBM Security QRadar no puede manejar el volumen de sucesos y flujos de entrada, o cuando el número de sucesos y flujos supera los límites de la licencia para el despliegue. Puede examinar los mensajes del archivo de registro de QRadar cuando se producen estas situaciones.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Visualice el archivo de registro `/var/log/qradar.error` y busque estos mensajes:

   Estos mensajes indican que se han eliminado sucesos o flujos:

   ```
   [Tenant:[tenantID]:[tenantName]
   Suceso eliminado intentando añadir a cola de Regulador sucesos arrendatario.
   La cola del Regulador de sucesos de arrendatario está llena.
   ```

   ```
   [Tenant:[tenantID]:[tenantName]
   Flujo eliminado intentando añadir a cola Regulador flujos arrendatario.
   La cola del Regulador de flujos de arrendatario está llena.
   ```

   Estos mensajes indican que la interconexión de procesos está cerca de su límite de capacidad:

   ```
   El procesador de regulación no puede mantener los sucesos.
   TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC es probablemente demasiado corto.
   ```

   ```
   El procesador de regulación no puede mantener los
   flujos.
   TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC es probablemente demasiado corto.
   ```

   Si este aviso persiste, QRadar puede descartar sucesos o flujos.

Qué hacer a continuación

Si el sistema está eliminando sucesos y flujos, puede ampliar su licencia para manejar más datos o puede establecer límites de EPS y FPM más restrictivos para cada arrendatario.

Gestión de reglas en despliegues multiarrendatario

En un entorno multiarrendatario, debe personalizar las reglas para que sean conscientes de los arrendatarios. Las reglas conscientes de arrendatario utilizan la prueba de regla **cuando el dominio es uno de los siguientes**, pero el modificador de dominio determina el ámbito de aplicación de la regla.

La tabla siguiente muestra cómo puede utilizar el modificador de dominio para cambiar el ámbito de las reglas en un despliegue multiarrendatario.

Tabla 62. Ámbito de reglas en un entorno multiarrendatario

Ámbito de regla	Descripción	Ejemplo de prueba de regla
Reglas de dominio único	Estas reglas incluyen sólo 1 modificador de dominio.	**y cuando el dominio es uno de los siguientes:** *manufacturing*

Tabla 62. Ámbito de reglas en un entorno multiarrendatario (continuación)

Ámbito de regla	Descripción	Ejemplo de prueba de regla
Reglas de arrendatario único	Estas reglas incluyen todos los dominios que están asignados al arrendatario. Utilice reglas de arrendatario único para correlacionar los sucesos de varios dominios dentro de un único arrendatario.	**y cuando el dominio es uno de los siguientes:** *manufacturing, finance, legal*
Reglas globales	Estas reglas utilizan el modificador **Cualquier dominio** y se ejecutan en todos los arrendatarios.	**y cuando el dominio es uno de los siguientes:***Cualquier dominio*

Al ser consciente del dominio, el motor de reglas personalizadas (CRE) aísla automáticamente las correlaciones de sucesos de arrendatarios diferentes utilizando sus respectivos dominios. Para obtener más información sobre cómo trabajar con reglas en una red segmentada por dominios, consulte Capítulo 15, "Segmentación en dominios", en la página 191.

Restricción de prestaciones de actividad de registro de usuarios de arrendatario

Para asegurarse de que el administrador y los usuarios del arrendatario sólo pueden ver los datos de registro de su arrendatario, debe restringir los permisos de la prestación **Actividad de registro**.

Acerca de esta tarea

Cuando se añade la prestación de **Actividad de registro** a un rol de usuario, los permisos **Mantener reglas personalizadas** y **Ver reglas personalizadas** se otorgan automáticamente. Los usuarios que tienen estos permisos tienen acceso a todos los datos de registro de todos los dominios. Pueden editar reglas en todos los dominios, incluso si sus valores de perfil de seguridad tienen restricciones a nivel de dominio.

Para evitar que los usuarios puedan acceder a los datos de registro y modificar las reglas de otros dominios o arrendatarios, edite el rol de usuario y elimine los permisos **Mantener reglas personalizadas** y **Ver reglas personalizadas**. Sin estos permisos, el administrador y los usuarios del arrendatario no pueden cambiar reglas, incluidas las reglas de su propio dominio.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Roles de usuario** y seleccione el rol de usuario que desea editar.
4. Bajo **Actividad de registro**, desmarque los recuadros de selección **Mantener reglas personalizadas** y **Ver reglas personalizadas**.
5. Pulse **Guardar**.

Actualizaciones de la jerarquía de red en un despliegue multiarrendatario

Los administradores de arrendatarios que tienen el permiso **Definir jerarquía de red** pueden cambiar la jerarquía de red dentro de su propio arrendatario, pero para desplegar los cambios, deben ponerse en contacto con el administrador de proveedor de servicios de seguridad gestionados (MSSP). Los administradores de MSSP pueden planificar el despliegue durante una interrupción planificada, e informar a todos los administradores de arrendatarios de antemano.

IBM Security QRadar utiliza la jerarquía de red para comprender y analizar el tráfico de red del entorno.

Los cambios en la jerarquía de red requieren un despliegue de configuración completo para aplicar las actualizaciones en el entorno de QRadar. Los despliegues de configuración completos reinician todos los servicios de QRadar, y la recopilación de datos para los sucesos y flujos se detiene hasta que finaliza el despliegue.

En un entorno de multiarrendatario, el nombre de objeto de red debe ser exclusivo en todo el despliegue. No puede utilizar objetos de red que tengan el mismo nombre, aunque estén asignados a dominios diferentes.

Conceptos relacionados:

"Jerarquía de red" en la página 69
QRadar utiliza la jerarquía de red para comprender el tráfico de red y proporcionarle la capacidad de ver la actividad de todo el despliegue.

Políticas de retención para arrendatarios

Cada arrendatario de un despliegue de IBM Security QRadar tiene al menos un dominio. Puede utilizar el filtro de dominios para especificar políticas de retención para el despliegue multiarrendatario.

QRadar da soporte a un máximo de 10 depósitos de retención por despliegue. Si el despliegue de QRadar no tiene más de 10 arrendatarios, puede utilizar el filtro de dominios para crear una política de retención de datos independiente para cada cliente.

Para crear una política de retención específica de arrendatario, debe añadir un filtro de dominios para cada uno de los dominios del arrendatario. La adición de los dominios especifica que la política se aplica sólo a los datos de dicho arrendatario.

Para obtener más información sobre la creación de políticas de retención, consulte el apartado "Retención de datos" en la página 97.

Capítulo 17. Gestión de activos

Los activos y perfiles de activo creados para servidores y hosts de la red proporcionan información importante para resolver problemas de seguridad. Utilizando los datos de activos, puede conectar los delitos desencadenados en el sistema a activos físicos o virtuales para proporcionar un punto de partida en una investigación de seguridad.

La pestaña **Activos** de QRadar proporciona una vista unificada de la información conocida acerca de los activos de la red. A medida que QRadar descubre más información, el sistema actualiza el perfil de activo y crea de forma incremental una imagen completa sobre el activo.

Los perfiles de activo se crean dinámicamente a partir de la información de identidad que se absorbe pasivamente a partir de datos de suceso o flujo, o a partir de los datos que QRadar busca activamente durante una exploración de vulnerabilidades. También puede importar datos de activos o editar el perfil de activo manualmente. Para obtener más información, consulte los temas *Importación de perfiles de activos* y *Adición o edición de un perfil de activo* en la *Guía del usuario de IBM Security QRadar*.

Restricción: QRadar Log Manager solo hace un seguimiento de datos de activo si QRadar Vulnerability Manager está instalado. Para obtener más información acerca de las diferencias entre IBM Security QRadar SIEM y IBM Security QRadar Log Manager, consulte "Prestaciones de su producto de inteligencia y seguridad" en la página 3.

Orígenes de datos de activos

Se reciben datos de activos de diversos orígenes en el despliegue de IBM Security QRadar.

Los datos de activos se escriben en la base de datos de activos de forma incremental, normalmente dos o tres datos a la vez. A excepción de las actualizaciones de los exploradores de vulnerabilidades de red, cada actualización de activo contiene información sobre un solo activo.

Los datos de activos generalmente provienen de uno de los orígenes de datos de activos siguientes:

Sucesos
Las cargas útiles de sucesos, tales como las creadas por DHCP o servidores de autenticación, a menudo contienen inicios de sesión de usuario, direcciones IP, nombres de hosts, direcciones MAC y otro tipo de información de activos. Estos datos se proporcionan inmediatamente a la base de datos de activos para ayudar a determinar a qué activo se aplica la actualización de activo.

Los sucesos son la causa principal de las desviaciones de crecimiento de activos.

Flujos Las cargas útiles de flujo contienen información de comunicación, como la dirección IP, el puerto y el protocolo, que se recopila a intervalos regulares

© Copyright IBM Corp. 2012, 2015

configurables. Al final de cada intervalo, los datos se proporcionan a la base de datos de activos, una dirección IP cada vez.

Puesto que los datos de activos de los flujos están emparejados con un activo según un solo identificador, la dirección IP, los datos de flujo nunca son la causa de las desviaciones de crecimiento de activos.

Exploradores de vulnerabilidades
QRadar se integra tanto con exploradores de vulnerabilidades de IBM como de terceros que puedan proporcionar datos de activos tales como el sistema operativo, el software instalado y la información de parches. El tipo de datos varía de un explorador a otro y puede variar de una exploración a otra. A medida que se descubren nuevos activos, nueva información de puertos y nuevas vulnerabilidades, los datos se llevan al perfil de activo en función de los rangos de CIDR que están definidos en la exploración.

Los exploradores pueden añadir desviaciones de crecimiento de activos, pero no es habitual.

Interfaz de usuario
Los usuarios que tienen el rol de activos pueden importar o proporcionar información de activos directamente a la base de datos de activos. Las actualizaciones de activos proporcionadas directamente por un usuario son para un activo específico y, por lo tanto, la etapa de conciliación de activos se omite.

Las actualizaciones de activos proporcionadas por los usuarios no añaden desviaciones de crecimiento de activos.

Datos de activos que tienen en cuenta el dominio

Cuando un origen de datos de activos está configurado con información de dominio, todos los datos de activos que provienen de ese origen de datos se etiquetan automáticamente con el mismo dominio. Puesto que los datos del modelo de activos tienen en cuenta el dominio, la información de dominio se aplica a todos los componentes de QRadar, incluidos las identidades, los delitos, los perfiles de activo y el descubrimiento de servidores.

Cuando vea el perfil de activo, algunos campos podrían estar en blanco. Los campos en blanco existen cuando el sistema no ha recibido esta información en una actualización de activo o la información ha sobrepasado el periodo de retención de activos. El periodo predeterminado de retención es 120 días. Una dirección IP que aparezca como 0.0.0.0 indica que el activo no contiene información de dirección IP.

Flujo de trabajo para datos de activos entrantes

Este flujo de trabajo describe la manera en que QRadar utiliza la información de identidad en una carga útil de suceso para determinar si se crea un nuevo activo o si se actualiza un activo existente.

1. QRadar recibe el suceso. El perfilador de activos examina la carga útil del suceso para obtener la información de identidad.
2. Si la información de identidad incluye una dirección MAC, nombres de host NetBIOS o un nombre de host DNS que ya están asociados con un activo en la base de datos de activos, ese activo se actualiza con la información nueva.
3. Si la única información de identidad disponible es una dirección IP, el sistema concilia la actualización del activo existente que tenga la misma dirección IP.

4. Si una actualización de activo incluye una dirección IP que coincide con un activo existente, pero también incluye más información de identidad que no coincide con el activo existente, el sistema utiliza otra información para descartar un falso positivo en la coincidencia antes de que el activo existente se actualice.
5. Si la información de identidad no coincide con un activo existente en la base de datos, se crea un nuevo activo basado en la información de la carga útil del suceso.

Actualizaciones de los datos de activos

IBM Security QRadar utiliza la información de identidad en una carga útil de suceso para determinar si se crea un nuevo activo o si se actualiza un activo existente.

Cada actualización de activo debe contener información de confianza acerca de un único activo. Cuando QRadar recibe una actualización de activo, el sistema determina a qué activo se aplica la actualización.

La *conciliación de activos* es el proceso mediante el cual se determina la relación entre las actualizaciones de activos y el activo relacionado en la base de datos de activos. La conciliación de activos se produce después de que QRadar reciba la actualización, pero antes de que la información se escriba en la base de datos de activos.

Información de identidad

Cada activo debe contener al menos un dato de identidad. Las actualizaciones posteriores que contengan un dato o más de los mismos datos de identidad se concilian con el activo propietario de los datos. Las actualizaciones que se basan en las direcciones IP se manejan con cuidado para evitar coincidencias de activos que sean falsos positivos. Los falsos positivos en las coincidencias de activos se producen cuando a un activo físico se le asigna la propiedad de una dirección IP que anteriormente era propiedad de otro activo del sistema.

Cuando se proporcionan varios datos de identidad, el perfilador de activos da prioridad a la información en el orden siguiente:

- Dirección MAC (más determinista)
- Nombre de host NetBIOS
- Nombre de host DNS
- Dirección IP (menos determinista)

Las direcciones MAC, los nombres de host NetBIOS y los nombres de host DNS deben ser exclusivos y, por lo tanto, se consideran datos de identidad definitivos. Las actualizaciones entrantes cuyas coincidencias con un activo existente solamente sean la dirección IP se manejan de forma diferente que las actualizaciones que coincidan con los datos de identidad más definitivos.

Reglas de exclusión de conciliación de activos

Con cada actualización de activo que entra en IBM Security QRadar, las reglas de exclusión de conciliación de activos aplican pruebas a la dirección MAC, el nombre de host NetBIOS, el nombre de host DNS y la dirección IP en la actualización de activo.

De forma predeterminada, se hace un seguimiento de cada dato de activos durante un periodo de dos horas. Si algún dato de identidad de la actualización de activo muestra un comportamiento sospechoso dos o más veces en un plazo de dos horas, ese dato se añade a las listas negras de activos. Existe una lista negra por separado para cada tipo de datos de activos de identidad que se prueba.

En los entornos que tienen en cuenta el dominio, las reglas de exclusión de conciliación de activos hacen un seguimiento del comportamiento de los datos de activos por separado en cada dominio.

Las reglas de exclusión de conciliación de activos prueban los escenarios siguientes:

Tabla 63. Pruebas y respuestas de reglas

Escenario	**Respuesta de regla**
Cuando una dirección MAC se asocia a tres o más direcciones IP diferentes en un plazo de dos horas o menos	Añadir la dirección MAC a la lista negra de MAC del dominio de conciliación de activos
Cuando un nombre de host DNS se asocia a tres o más direcciones IP diferentes en un plazo de dos horas o menos	Añadir el nombre de host DNS a la lista negra de DNS del dominio de conciliación de activos
Cuando un nombre de host NetBIOS se asocia a tres o más direcciones IP diferentes en un plazo de dos horas o menos	Añadir el nombre de host NetBIOS a la lista negra de NetBIOS del dominio de conciliación de activos
Cuando una dirección IPv4 se asocia a tres o más direcciones MAC diferentes en un plazo de dos horas o menos	Añadir la dirección IP a la lista negra de IPv4 del dominio de conciliación de activos
Cuando un nombre de host NetBIOS se asocia a tres o más direcciones MAC diferentes en un plazo de dos horas o menos	Añadir el nombre de host NetBIOS a la lista negra de NetBIOS del dominio de conciliación de activos
Cuando un nombre de host DNS se asocia a tres o más direcciones MAC diferentes en un plazo de dos horas o menos	Añadir el nombre de host DNS a la lista negra de DNS del dominio de conciliación de activos
Cuando una dirección IPv4 se asocia a tres o más nombres de host DNS diferentes en un plazo de dos horas o menos	Añadir la dirección IP a la lista negra de IPv4 del dominio de conciliación de activos
Cuando un nombre de host NetBIOS se asocia a tres o más nombres de host DNS diferentes en un plazo de dos horas o menos	Añadir el nombre de host NetBIOS a la lista negra de NetBIOS del dominio de conciliación de activos
Cuando una dirección MAC se asocia a tres o más nombres de host DNS diferentes en un plazo de dos horas o menos	Añadir la dirección MAC a la lista negra de MAC del dominio de conciliación de activos
Cuando una dirección IPv4 se asocia a tres o más nombres de host NetBIOS diferentes en un plazo de dos horas o menos	Añadir la dirección IP a la lista negra de IPv4 del dominio de conciliación de activos
Cuando un nombre de host DNS se asocia a tres o más nombres de host NetBIOS diferentes en un plazo de dos horas o menos	Añadir el nombre de host DNS a la lista negra de DNS del dominio de conciliación de activos
Cuando una dirección MAC se asocia a tres o más nombres de host NetBIOS diferentes en un plazo de dos horas o menos	Añadir la dirección MAC a la lista negra de MAC del dominio de conciliación de activos

Puede ver estas reglas en la pestaña **Delitos** pulsando **Reglas** y, a continuación, seleccionando el grupo **Exclusión de conciliación de activos** en la lista desplegable.

Fusión de activos

La *fusión de activos* es el proceso según el cual la información de un activo se combina con la información de otro activo bajo la premisa de que son realmente el mismo activo físico.

La fusión de activos se produce cuando una actualización de activo contiene datos de identidad que coinciden con dos perfiles de activo diferentes. Por ejemplo, una única actualización que contiene un nombre de host NetBIOS que coincide con un perfil de activo y una dirección MAC que coincide con otro perfil de activo diferente podría desencadenar una fusión de activos.

En algunos sistemas se puede observar un gran volumen de fusión de activos porque tienen orígenes de datos de activos que inadvertidamente combinan en una misma actualización de activo información de identidad de dos activos físicos diferentes. Como ejemplos de estos sistemas cabe citar los entornos siguientes:

- Servidores syslog centrales que actúan como proxy de sucesos
- Máquinas virtuales
- Entornos de instalación automatizada
- Nombres de host no exclusivos, frecuentes con activos como iPads y iPhones.
- Redes privadas virtuales que tienen direcciones MAC compartidas
- Extensiones de origen de registro cuyo campo de identidad es `OverrideAndAlwaysSend=true`

Los activos que tienen muchas direcciones IP, direcciones MAC o nombres de host presentan desviaciones en el crecimiento de los activos y pueden desencadenar notificaciones del sistema.

Identificación de desviaciones de crecimiento de activos

A veces, los orígenes de datos de activos generan actualizaciones que IBM Security QRadar no puede manejar correctamente sin intervención manual. En función de la causa del crecimiento anormal de los activos, puede arreglar el origen de datos de activos que está causando el problema o puede bloquear las actualizaciones de activos que provienen de ese origen de datos.

Las *desviaciones de crecimiento de activos* se dan cuando el número de actualizaciones de activos de un único dispositivo supera el límite establecido en el umbral de retención para un tipo concreto de información de identidad. El manejo adecuado de las desviaciones de crecimiento de activos es de vital importancia para mantener un modelo de activos preciso.

En la base de cada desviación de crecimiento de activos se encuentra un origen de datos de activos cuyos datos no son de confianza para actualizar el modelo de activos. Cuando se identifica una desviación potencial del crecimiento de los activos, debe examinar el origen de la información para determinar si hay una explicación razonable para que un activo acumule grandes cantidades de datos de identidad. La causa de una desviación de crecimiento de activos es específica de un entorno.

Ejemplo del servidor DHCP de crecimiento de activo anormal en un perfil de activo

Supongamos que hay un servidor de VPN (red privada virtual) en una red DHCP (Protocolo de configuración dinámica de hosts). El servidor de VPN está configurado para asignar direcciones IP a los clientes de VPN entrantes enviando mediante un proxy las solicitudes DHCP en nombre del cliente al servidor DHCP de la red.

Desde la perspectiva del servidor DHCP, la misma dirección MAC solicita muchas asignaciones de direcciones IP en repetidas ocasiones. En el contexto de las operaciones de red, el servidor VPN delega las direcciones IP a los clientes, pero el servidor DHCP no puede distinguir cuándo una solicitud la realiza un activo en nombre de otro.

El registro del servidor DHCP, que está configurado como un origen de registro de QRadar, genera un suceso de acuse de recibo DHCP (DHCP ACK) que asocia la dirección MAC del servidor VPN con la dirección IP que se asigna al cliente de VPN. Cuando se produce la conciliación de activos, el sistema concilia este suceso por dirección MAC, lo que da como resultado un activo existente único que crece con una dirección IP cada vez que se analiza un suceso DHCP ACK.

Finalmente, un solo perfil de activo contiene todas las direcciones IP que se han asignado al servidor de VPN. Esta desviación de crecimiento de activos está causada por las actualizaciones de activos que contienen información acerca de más de un activo.

Valores de umbral

Cuando un activo de la base de datos alcanza un número determinado de propiedades, tales como varias direcciones IP o direcciones MAC, QRadar bloquea ese activo para que no reciba más actualizaciones.

Los valores de umbral del perfilador de activos indican las condiciones bajo las cuales un activo está bloqueado frente a las actualizaciones. El activo se actualiza normalmente hasta el valor del umbral. Cuando el sistema recopila datos suficientes para superar el umbral, el activo muestra una desviación de crecimiento de activo. Las futuras actualizaciones del activo se bloquean hasta que la desviación de crecimiento se corrija.

Notificaciones del sistema que indican desviaciones de crecimiento de activos

IBM Security QRadar genera notificaciones del sistema para ayudarle a identificar y gestionar las desviaciones de crecimiento de activos en su entorno.

Los siguientes mensajes del sistema indican que QRadar ha identificado posibles desviaciones de crecimiento de activos:

- `El sistema ha detectado perfiles de activo que sobrepasan el umbral de tamaño normal`
- `Las reglas de listas negras de activos han añadido datos de activo nuevos a las listas negras de activos`

Los mensajes de notificación del sistema incluyen enlaces a los informes para que sea más fácil identificar los activos que presentan desviaciones de crecimiento.

Datos de activos que cambian con frecuencia

El crecimiento de activos puede estar causado por grandes volúmenes de datos de activos que cambian de forma correcta, como en las situaciones siguientes:

- Un dispositivo móvil que va de una oficina a otra con frecuencia al que se le asigna una dirección IP nueva cada vez que inicia sesión.
- Un dispositivo que se conecta a una wifi pública con cesiones breves de direcciones IP, como por ejemplo en un campus universitario, puede recopilar grandes volúmenes de datos de activos durante un semestre.

Ejemplo: Cómo los errores de configuración de las extensiones de origen de registro pueden provocar desviaciones de crecimiento de activos

Las extensiones de origen de registro personalizado que están configuradas incorrectamente pueden provocar desviaciones de crecimiento de activos.

El usuario configura una extensión de origen de registro personalizado para proporcionar actualizaciones de activos a QRadar mediante el análisis de los nombres de usuario de la carga útil de suceso que se encuentra en un servidor de registro central. Configura la extensión de origen de registro para alterar temporalmente la propiedad de nombre de host de sucesos para que las actualizaciones de activos generadas por el origen de registro personalizado siempre especifiquen el nombre del host DNS del servidor de registro central.

En lugar de que QRadar reciba una actualización que tiene el nombre de host del activo en el que el usuario ha iniciado sesión, el origen de registro genera muchas actualizaciones de activos que tienen el mismo nombre de host.

En esta situación, la desviación de crecimiento de activos está causada por un solo perfil de activo que contiene muchas direcciones IP y muchos nombres de usuario.

Resolución de problemas con perfiles de activo que sobrepasan el umbral de tamaño normal

IBM Security QRadar genera la notificación del sistema siguiente cuando la acumulación de datos bajo un único activo supera los límites de umbral configurados para los datos de identidad.

```
El sistema ha detectado perfiles de activo que sobrepasan el umbral de tamaño normal
```

Explicación

La carga útil muestra una lista de los cinco activos que presentan desviaciones con más frecuencia y proporciona información sobre por qué el sistema ha marcado cada activo como una desviación de crecimiento. Tal como se muestra en el ejemplo siguiente, la carga útil también muestra el número de veces que el activo ha intentado crecer más allá del umbral del tamaño de activo.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
Los cinco activos que presentan desviaciones con más frecuencia entre
el 13 de febrero de 2015 8:10:23 PM AST y el 13 de febrero de 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

Cuando los datos de activos exceden el umbral configurado, QRadar bloquea el activo frente a actualizaciones futuras. Esta intervención evita que el sistema reciba más datos dañados y mitiga el impacto en el rendimiento que podría producirse si el sistema intenta conciliar las actualizaciones de entrada con un perfil de activo anormalmente grande.

Acción del usuario necesaria

Utilice la información de la carga útil de la notificación para identificar los activos que contribuyen a la desviación de crecimiento de activo y determinar qué está provocando el crecimiento anormal. La notificación proporciona un enlace a un informe de todos los activos que han experimentado una desviación del crecimiento durante las últimas 24 horas.

Después de resolver la desviación de crecimiento de activo en su entorno, puede ejecutar el informe de nuevo.

1. Pulse la pestaña **Actividad de registro** y pulse **Buscar** > **Nueva búsqueda**.
2. Seleccione la búsqueda guardada **Desviación de crecimiento de activos: Informe de activos**.
3. Utilice el informe para identificar y reparar los datos de activos inexactos que se han creado durante la desviación.

Si los datos de activos son válidos, los administradores de QRadar pueden aumentar los límites de umbral para las direcciones IP, las direcciones MAC, los nombres de host NetBIOS y los nombres de host DNS en **Configuración del perfilador de activos** en la pestaña **Admin** de QRadar.

Conceptos relacionados:

"Datos de activos obsoletos" en la página 217
Los datos de activos obsoletos pueden provocar problemas cuando la velocidad a la que se crean nuevos registros de activos supera la velocidad a la que se eliminan los datos de activos obsoletos. Controlar y gestionar los umbrales de retención de activos es la clave para dar respuesta a las desviaciones de crecimiento de activos provocadas por los datos de activos obsoletos.

Los datos de activos nuevos se añaden a las listas negras de activos

IBM Security QRadar genera la notificación del sistema siguiente cuando un dato de activos concreto presenta un comportamiento que puede deberse a la desviación del crecimiento de activos.

```
Las reglas de lis. neg. act. han añadido datos de activo nuevos a las lis. neg. act.
```

Explicación

Las reglas de exclusión de activos supervisan los datos de activos para comprobar la coherencia y la integridad. Las reglas hacen un seguimiento de datos de activos concretos a lo largo del tiempo para asegurarse de que están siendo observados siempre con el mismo subconjunto de datos dentro de un plazo de tiempo razonable.

Por ejemplo, si una actualización de activo incluye una dirección MAC y un nombre de host DNS, la dirección MAC está asociada con ese nombre de host DNS durante un periodo de tiempo concreto. Las actualizaciones de activos posteriores que contengan esa dirección MAC también contienen ese nombre de host DNS si se incluye alguno en la actualización de activo. Si la dirección MAC de repente se

asocia con un nombre de host DNS diferente durante un periodo breve de tiempo, el cambio se supervisa. Si la dirección MAC cambia de nuevo dentro de un periodo breve, la dirección MAC se marca para indicar que contribuye a una instancia de crecimiento de activo anormal o con desviaciones.

Acción del usuario necesaria

Utilice la información de la carga útil de la notificación para identificar las reglas que se utilizan para supervisar los datos de activos. Pulse el enlace **Desviaciones de activo por origen de registro** en la notificación para ver las desviaciones de activo que se han producido en las últimas 24 horas.

Si los datos de activos son válidos, los administradores de QRadar pueden configurar QRadar para resolver el problema.

- Si las listas negras se llenan demasiado rápido, puede ajustar las reglas de exclusión de conciliación de activos que las llenan.
- Si desea añadir los datos a la base de datos de activos, puede eliminar los datos de activos de la lista negra y añadirlos a la lista blanca de activos correspondiente. Al añadir datos de un activo a la lista blanca se impide que reaparezcan inadvertidamente en la lista negra.

Conceptos relacionados:

"Ajuste avanzado de reglas de exclusión de conciliación de activos" en la página 227

Puede ajustar las reglas de exclusión de conciliación de activos para refinar la definición de la desviación de crecimiento de activos en una o varias reglas.

Prevención de las desviaciones de crecimiento de activos

Después de confirmar que el crecimiento notificado de un activo es correcto, hay varias maneras de evitar que IBM Security QRadar desencadene mensajes de desviación de crecimiento para ese activo.

Utilice la lista siguiente como ayuda para decidir cómo evitar las desviaciones de crecimiento de activos:

- Averigüe cómo QRadar maneja los datos de activos obsoletos.
- Ajuste los valores de retención del perfilador de activos para limitar la cantidad de tiempo que se conservan los datos de activos.
- Ajuste el número de direcciones IP permitidas para un único activo.
- Cree búsquedas de exclusión de identidades para hacer que determinados sucesos no proporcionen actualizaciones de activos.
- Ajuste las reglas de exclusión de conciliación de activos para refinar la definición de la desviación de crecimiento de activos.
- Cree listas blancas de activos para impedir que los datos vuelvan a aparecer en las listas negras de activos.
- Modifique las entradas en las listas negras y las listas blancas de activos.
- Asegúrese de que los DSM estén actualizados. QRadar proporciona una actualización automática semanal que puede contener actualizaciones de DSM y correcciones para los problemas de análisis.

Datos de activos obsoletos

Los datos de activos obsoletos pueden provocar problemas cuando la velocidad a la que se crean nuevos registros de activos supera la velocidad a la que se eliminan

los datos de activos obsoletos. Controlar y gestionar los umbrales de retención de activos es la clave para dar respuesta a las desviaciones de crecimiento de activos provocadas por los datos de activos obsoletos.

Los *datos de activos obsoletos* son los datos de activos históricos que no han observado de forma activa ni pasiva dentro de un plazo de tiempo específico. Los datos de activos obsoletos se suprimen cuando exceden el periodo de retención configurado.

Los registros históricos se activan de nuevo si QRadar los observa de forma pasiva, a través de sucesos y flujos o de forma activa, a través de exploradores de vulnerabilidades y puertos.

Para evitar las desviaciones de crecimiento de activos es necesario encontrar el equilibrio adecuado entre el número de direcciones IP permitidas para un activo y la cantidad de tiempo que QRadar conserva los datos de activos. Debe tener en cuenta las compensaciones de rendimiento y gestión antes de configurar QRadar para dar cabida a altos niveles de retención de datos de activos. Si bien unos periodos de retención más largos y unos umbrales por activo superiores pueden parecer deseables en todo momento, un enfoque más adecuado es determinar una configuración básica que sea aceptable para el entorno y probar dicha configuración. A continuación, puede ampliar los umbrales de retención en pequeños incrementos hasta lograr el equilibrio adecuado.

Tareas relacionadas:

"Ajuste de los valores de retención del perfilador de activos" en la página 223
IBM Security QRadar utiliza los valores de retención de activos para gestionar el tamaño de los perfiles de activo.

"Ajuste del número de direcciones IP permitidas para un único activo" en la página 224
IBM Security QRadar supervisa el número de direcciones IP que un activo acumula a lo largo del tiempo.

Listas negras y listas blancas de activos

IBM Security QRadar utiliza un grupo de reglas de conciliación de activos para determinar si los datos de activos son de confianza. Cuando los datos de activos son cuestionables, QRadar utiliza listas negras y listas blancas de activos para determinar si deben actualizarse los perfiles de activo con los datos de activos.

Una *lista negra de activos* es un conjunto de datos que IBM Security QRadar considera no fiables. Los datos de la lista negra de activos pueden contribuir a la aparición de desviaciones de crecimiento de activos y QRadar impide que los datos se añadan a la base de datos de activos.

Una *lista blanca de activos* es un conjunto de datos de activos que altera la lógica del motor de conciliación de activos con la que se añaden datos a una lista negra de activos. Cuando el sistema identifica una coincidencia en la lista negra, comprueba la lista blanca para ver si el valor existe. Si la actualización de activo coincide con datos que están en la lista blanca, el cambio se concilia y el activo se actualiza. Los datos de activos en listas blancas se aplican globalmente en todos los dominios.

Las listas negras y las listas blancas de activos son conjuntos de referencia. Puede ver y modificar los datos de las listas negras y las listas blancas de activos mediante la herramienta Gestión de conjuntos de referencia en consola de QRadar. Para obtener más información sobre el trabajo con conjuntos de referencia, consulte el apartado Capítulo 7, "Gestión de conjuntos de referencia", en la página 111.

Como alternativa, puede utilizar la interfaz de línea de mandatos (CLI) o el punto final de la API RestFUL para actualizar el contenido de las listas negras y blancas de activos.

Listas negras de activos

Una *lista negra de activos* es un conjunto de datos que IBM Security QRadar considera no fiables según las reglas de exclusión de conciliación de activos. Los datos de la lista negra de activos pueden contribuir a la aparición de desviaciones de crecimiento de activos y QRadar impide que los datos se añadan a la base de datos de activos.

Cada actualización de activo en QRadar se compara con las listas negras de activos. Los datos de activos en listas negras se aplican globalmente en todos los dominios. Si la actualización de activo contiene información de identidad (dirección MAC, nombre de host NetBIOS, nombre de host DNS o dirección IP) que se encuentra en una lista negra, la actualización de entrada se descarta y la base de datos de activos no se actualiza.

En la tabla siguiente se muestra el nombre y el tipo de recopilación de referencia para cada tipo de datos de activos de identidad.

Tabla 64. Nombres de recopilación de referencia para los datos de las listas negras de activos

Tipo de datos de identidad	Nombre de recopilación de referencia	Tipo de recopilación de referencia
Direcciones IP (v4)	Lista negra de IPv4 de conciliación de activos	Conjunto de referencia [Tipo de conjunto: IP]
Nombres de host DNS	Lista negra de DNS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Nombres de host NetBIOS	Lista negra de NetBIOS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Direcciones MAC	Lista negra de MAC de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
* ALNIC es un tipo alfanumérico que puede dar cabida tanto al nombre de host como a los valores de dirección MAC.		

Puede utilizar la herramienta Gestión de conjuntos de referencia para editar las entradas de la lista negra. Para obtener información sobre el trabajo con conjuntos de referencia, consulte el apartado Capítulo 7, “Gestión de conjuntos de referencia”, en la página 111.

Conceptos relacionados:

“Listas blancas de activos”
Puede utilizar listas blancas de activos para evitar que los datos de activos de IBM Security QRadar reaparezcan inadvertidamente en las listas negras de activos.

Listas blancas de activos

Puede utilizar listas blancas de activos para evitar que los datos de activos de IBM Security QRadar reaparezcan inadvertidamente en las listas negras de activos.

Una *lista blanca de activos* es un conjunto de datos de activos que altera la lógica del motor de conciliación de activos con la que se añaden datos a una lista negra de activos. Cuando el sistema identifica una coincidencia en la lista negra, comprueba la lista blanca para ver si el valor existe. Si la actualización de activo coincide con

datos que están en la lista blanca, el cambio se concilia y el activo se actualiza. Los datos de activos en listas blancas se aplican globalmente en todos los dominios.

Puede utilizar la herramienta Gestión de conjuntos de referencia para editar las entradas de la lista blanca. Para obtener información sobre el trabajo con conjuntos de referencia, consulte el apartado Capítulo 7, “Gestión de conjuntos de referencia”, en la página 111.

Ejemplo de caso práctico de lista blanca

La lista blanca es útil si tiene datos de activos que siguen apareciendo en las listas negras aunque se trate de una actualización de activo válido. Por ejemplo, podría tener un equilibrador de carga DNS con rotación que está configurado para rotar en un conjunto de cinco direcciones IP. Las reglas de exclusión de conciliación de activos podrían determinar que el hecho de que haya varias direcciones IP asociadas con el mismo nombre de host DNS es una indicación de que existe una desviación de crecimiento de activos, y el sistema podría añadir el equilibrador de carga DNS a la lista negra. Para resolver este problema, puede añadir el nombre de host DNS a la lista blanca de DNS de conciliación de activos.

Entradas en masa a la lista blanca de activos

Una base de datos de activos precisa facilita la conexión de los delitos que se desencadenan en el sistema a activos físicos o virtuales en la red. Pasar por alto las desviaciones de activos añadiendo entradas en masa a la lista blanca de activos no es útil para la creación de una base de datos de activos precisa. En lugar de añadir entradas en masa a la lista blanca, revise la lista negra de activos para determinar qué está contribuyendo a la desviación de crecimiento de activos y luego determine cómo solucionar el problema.

Tipos de listas blancas de activos

Cada tipo de datos de identidad se mantiene en una lista blanca por separado. En la tabla siguiente se muestra el nombre y el tipo de recopilación de referencia para cada tipo de datos de activos de identidad.

Tabla 65. Nombre de recopilación de referencia para los datos de las listas blancas de activos

Tipo de datos	Nombre de recopilación de referencia	Tipo de recopilación de referencia
Direcciones IP	Lista blanca de IPv4 de conciliación de activos	Conjunto de referencia [Tipo de conjunto: IP]
Nombres de host DNS	Lista blanca de DNS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Nombres de host NetBIOS	Lista blanca de NetBIOS de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
Direcciones MAC	Lista blanca de MAC de conciliación de activos	Conjunto de referencia [Tipo de conjunto: ALNIC*]
* ALNIC es un tipo alfanumérico que puede dar cabida al nombre de host y a valores de dirección MAC.		

Conceptos relacionados:

“Listas negras de activos” en la página 219
Una *lista negra de activos* es un conjunto de datos que IBM Security QRadar considera no fiables según las reglas de exclusión de conciliación de activos. Los datos de la lista negra de activos pueden contribuir a la aparición de desviaciones de crecimiento de activos y QRadar impide que los datos se añadan a la base de datos de activos.

Actualización de las listas negras y listas blancas de activos mediante el programa de utilidad de conjunto de referencia

Puede utilizar el programa de utilidad de conjunto de referencia de IBM Security QRadar para añadir o modificar las entradas que se encuentran en las listas negras y las listas blancas de activos.

Para gestionar los conjuntos de referencia, ejecute el programa de utilidad `ReferenceSetUtil.sh` desde `/opt/qradar/bin` en la consola de QRadar.

Los mandatos para añadir valores nuevos a cada lista se describen en la tabla siguiente. Los valores de los parámetros deben coincidir exactamente con los valores de actualización de los activos proporcionados por el origen de datos de activos de donde proceden.

Tabla 66. Sintaxis de mandatos para modificar los datos de las listas negras y las listas blancas de activos

Nombre	Sintaxis del mandato
Lista negra de IPv4 de conciliación de activos	`ReferenceSetUtil.sh add "Lista negra de IPv4 de conciliación de activos"` *`IP`* Por ejemplo, este mandato añade la dirección IP 192.168.3.56 a la lista negra: `ReferenceSetUtil.sh add "Lista negra de IPv4 de conciliación de activos" 192.168.3.56`
Lista negra de DNS de conciliación de activos	`ReferenceSetUtil.sh add "Lista negra de DNS de conciliación de activos"` *`DNS`* Por ejemplo, este mandato añade el nombre de dominio 'misbehaving.asset.company.com' a la lista negra: `ReferenceSetUtil.sh add "Lista negra de DNS de conciliación de activos" "misbehaving.asset.company.com"`
Lista negra de NetBIOS de conciliación de activos	`ReferenceSetUtil.sh add "Lista negra de NetBIOS de conciliación de activos"` *`NETBIOS`* Por ejemplo, este mandato elimina el nombre de host NetBIOS 'deviantGrowthAsset-156384' de la lista negra: `ReferenceSetUtil.sh delete "Lista negra de NetBIOS de conciliación de activos" "deviantGrowthAsset-156384"`
Lista negra de MAC de conciliación de activos	`ReferenceSetUtil.sh add "Lista negra de MAC de conciliación de activos"` *`dirección_MAC`* Por ejemplo, este mandato añade la dirección MAC '00:a0:6b:54:9f:0e' a la lista negra: `ReferenceSetUtil.sh add "Lista negra de MAC de conciliación de activos" "00:a0:6b:54:9f:0e"`

Tabla 66. Sintaxis de mandatos para modificar los datos de las listas negras y las listas blancas de activos (continuación)

Nombre	Sintaxis del mandato

Lista blanca de IPv4 de conciliación de activos	`ReferenceSetUtil.sh add "Lista blanca de IPv4 de conciliación de activos" IP`
	
	Por ejemplo, este mandato suprime la dirección IP 10.1.95.142 de la lista blanca:
	
	`ReferenceSetUtil.sh delete "Lista blanca de IPv4 de conciliación de activos" 10.1.95.142`

Lista blanca de DNS de conciliación de activos	`ReferenceSetUtil.sh add "Lista blanca de DNS de conciliación de activos" DNS`
	
	Por ejemplo, este mandato añade el nombre de dominio 'loadbalancer.company.com' a la lista blanca:
	
	`ReferenceSetUtil.sh add "Lista blanca de DNS de conciliación de activos" "loadbalancer.company.com"`

Lista blanca de NetBIOS de conciliación de activos	`ReferenceSetUtil.sh add "Lista blanca de NetBIOS de conciliación de activos" NETBIOS`
	
	Por ejemplo, este mandato añade el nombre de NetBIOS 'assetName-156384' a la lista blanca:
	
	`ReferenceSetUtil.sh add "Lista blanca de NetBIOS de conciliación de activos" "assetName-156384"`

Lista blanca de MAC de conciliación de activos	`ReferenceSetUtil.sh add "Lista negra de MAC de conciliación de activos" dirección_MAC`
	
	Por ejemplo, este mandato añade la dirección MAC '00:a0:6b:54:9f:0e' a la lista negra:
	
	`ReferenceSetUtil.sh add "Lista negra de MAC de conciliación de activos" "00:a0:6b:54:9f:0e"`

Tareas relacionadas:

"Actualización de listas negras y listas blancas mediante la API RESTful"
Puede utilizar la API RESTful de IBM Security QRadar para personalizar el contenido de las listas negras y las listas blancas de activos.

Actualización de listas negras y listas blancas mediante la API RESTful

Puede utilizar la API RESTful de IBM Security QRadar para personalizar el contenido de las listas negras y las listas blancas de activos.

Acerca de esta tarea

Debe especificar el nombre exacto del conjunto de referencia que desea ver o actualizar.

- Lista negra de IPv4 de conciliación de activos
- Lista negra de DNS de conciliación de activos
- Lista negra de NetBIOS de conciliación de activos
- Lista negra de MAC de conciliación de activos
- Lista blanca de IPv4 de conciliación de activos
- Lista blanca de DNS de conciliación de activos

- Lista blanca de NetBIOS de conciliación de activos
- Lista blanca de MAC de conciliación de activos

Procedimiento

1. Escriba el URL siguiente en el navegador web para acceder a la interfaz de API RESTful:

   `https://dirección_IP_consola/api_doc`
2. En el panel de navegación de la izquierda, busque `4.0>/reference_data >/sets > /{nombre}`.
3. Para ver el contenido de una lista negra o blanca de activos, siga estos pasos:
   a. Pulse la pestaña **GET** y desplácese hacia abajo hasta la sección **Parámetros**.
   b. En el campo **Valor** correspondiente al parámetro **Nombre**, escriba el nombre de la lista negra o blanca de activos que desea ver.
   c. Pulse **Inténtelo**; los resultados aparecen en la parte inferior de la pantalla.
4. Para añadir un valor a una lista negra o blanca de activos, siga estos pasos:
   a. Pulse la pestaña **POST** y desplácese hacia abajo hasta la sección **Parámetros**.
   b. Escriba los valores de los parámetros siguientes:

Tabla 67. Parámetros que son necesarios para añadir nuevos datos de activos

Nombre del parámetro	Descripción del parámetro
name	Representa el nombre de la recopilación de referencia que desea actualizar.
value	Representa el dato que desea añadir a la lista negra o blanca de activos. Debe coincidir exactamente con los valores de actualización de los activos proporcionados por el origen de datos de activos de donde proceden.

   c. Pulse **Inténtelo** para añadir el nuevo valor a la lista negra o blanca de activos.

Qué hacer a continuación

Para obtener más información sobre el uso de la API RESTful para cambiar los conjuntos de referencia, consulte la publicación *IBM Security QRadar API Guide*.

Conceptos relacionados:

"Actualización de las listas negras y listas blancas de activos mediante el programa de utilidad de conjunto de referencia" en la página 221
Puede utilizar el programa de utilidad de conjunto de referencia de IBM Security QRadar para añadir o modificar las entradas que se encuentran en las listas negras y las listas blancas de activos.

Ajuste de los valores de retención del perfilador de activos

IBM Security QRadar utiliza los valores de retención de activos para gestionar el tamaño de los perfiles de activo.

El periodo de retención predeterminado para la mayoría de los datos de activos es de 120 días después de la última vez que se han observado de forma pasiva o activa en QRadar. Los nombres de usuario se conservan durante 30 días.

Los datos de activos que los usuarios de QRadar han añadido manualmente no suelen contribuir a las desviaciones de crecimiento de activos. De forma

predeterminada, estos datos se conservan indefinidamente. Para todos los demás tipos de datos de activos, se recomienda el distintivo **Retener siempre** solamente para los entornos estáticos.

Acerca de esta tarea

Puede ajustar el tiempo de retención según el tipo de datos de identidad de activo que se encuentra en el suceso. Por ejemplo, si varias direcciones IP se fusionan en un solo activo, puede cambiar el periodo de retención de IP de activo de 120 días por un valor inferior.

Cuando cambia el periodo de retención de activos para un tipo específico de datos de activos, el nuevo periodo de retención se aplica a todos los datos de activos en QRadar. Los datos de activos existentes que ya superan el nuevo umbral se eliminan cuando el despliegue finaliza. Para asegurarse de que siempre podrá identificar los hosts mencionados incluso si los datos de activos superan el periodo de retención, el proceso de limpieza de retención de activos no elimina el último valor conocido de nombre de host correspondiente a un activo.

Antes de determinar cuántos días desea conservar los datos de activos, es necesario que comprenda las características siguientes sobre un periodo de retención más largo:

- Proporciona una mejor vista histórica de sus activos.
- Crea volúmenes de datos más grandes por cada activo en la base de datos de activos.
- Aumenta la probabilidad de que los datos obsoletos contribuyan a los mensajes de desviación de crecimiento de activos.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Configuración del perfilador de activos**.
4. Pulse **Configuración de retención del perfilador de activos**.
5. Ajuste los valores de retención y pulse **Guardar**.
6. Despliegue los cambios en el entorno para que las actualizaciones entren en vigor.

Tareas relacionadas:

"Ajuste del número de direcciones IP permitidas para un único activo"
IBM Security QRadar supervisa el número de direcciones IP que un activo acumula a lo largo del tiempo.

Ajuste del número de direcciones IP permitidas para un único activo

IBM Security QRadar supervisa el número de direcciones IP que un activo acumula a lo largo del tiempo.

De forma predeterminada, QRadar genera un mensaje del sistema cuando un único activo acumula más de 75 direcciones IP. Si prevé que los activos acumularán más de 75 direcciones IP, puede ajustar el valor de **Número de IP permitidas para un único activo** para evitar los mensajes del sistema en el futuro.

Acerca de esta tarea

Si se establece el límite para el número de direcciones IP en un valor demasiado alto, se impide que QRadar detecte las desviaciones de crecimiento de activos antes de que tengan un impacto negativo en el resto del despliegue. Si el límite se establece en un valor demasiado bajo, se incrementa el número de desviaciones de crecimiento de activos que se notifican.

Puede utilizar la directriz siguiente cuando ajuste el valor **Número de IP permitidas para un único activo** por primera vez.

Número de direcciones IP que están permitidas para un único activo = (<*tiempo de retención (días)*> x <*direcciones IP estimadas por día*>) + <*número de direcciones IP en almacenamiento intermedio*>

Donde:

- <*direcciones IP estimadas por día*> es el número de direcciones IP que un activo puede acumular en un día en condiciones normales
- <*tiempo de retención (días)*> es la cantidad de tiempo preferida para conservar las direcciones IP del activo

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse **Configuración del perfilador de activos**.
4. Pulse **Configuración de retención del perfilador de activos**.
5. Ajuste los valores de configuración y pulse **Guardar**.
6. Despliegue los cambios en el entorno para que las actualizaciones entren en vigor.

Tareas relacionadas:

"Ajuste de los valores de retención del perfilador de activos" en la página 223
IBM Security QRadar utiliza los valores de retención de activos para gestionar el tamaño de los perfiles de activo.

Búsquedas de exclusión de identidades

Las búsquedas de exclusión de identidades se pueden utilizar para gestionar activos individuales que acumulan grandes volúmenes de información de identidad similar por motivos conocidos y válidos.

Por ejemplo, los orígenes de datos pueden proporcionar grandes volúmenes de información de identidad de activo a la base de datos de activos. Proporcionan a IBM Security QRadar los cambios en la información de activos en tiempo casi real y pueden mantener actualizada la base de datos de activos. Sin embargo, los orígenes de registro suelen ser la fuente más frecuente de las desviaciones del crecimiento de activos y otras anomalías relacionadas con los activos.

Cuando un origen de registro envía datos de activos incorrectos a QRadar, intente corregir el origen de registro para que los datos que envía se puedan utilizar en la base de datos de activos. Si el origen de registro no se puede arreglar, puede crear una búsqueda de exclusión de identidades que impida que la información de activos se incorpore a la base de datos de activos.

También puede utilizar una búsqueda de exclusión de identidades en la que `nombre_usuario_identidad + es cualquiera de + inicio de sesión anónimo` para asegurarse de que no se actualizan los activos que están relacionados con las cuentas de servicio o con servicios automatizados.

Diferencias entre las búsquedas de exclusión de identidades y las listas negras

Si bien las búsquedas de exclusión de identidades parecen tener una funcionalidad similar a la de las listas negras de activos, existen diferencias significativas.

Las listas negras solamente pueden especificar los datos de activos en bruto, tales como direcciones MAC y nombres de host, que se van a excluir. Las búsquedas de exclusión de identidades filtran los datos de activos según campos de búsqueda tales como el origen de registro, la categoría y el nombre de suceso.

Las listas negras no tienen en cuenta el tipo de origen de datos que proporciona los datos, mientras que las búsquedas de exclusión de identidades se pueden aplicar únicamente a los sucesos. Las búsquedas de exclusión de identidades pueden bloquear las actualizaciones de activos basándose en los campos de búsqueda de sucesos comunes, como tipo de suceso, nombre de suceso, categoría y origen de registro.

Creación de búsquedas de exclusión de identidades

Para hacer que determinados sucesos no proporcionen datos de activos a la base de datos de activos, puede crear una búsqueda de exclusión de identidades de IBM Security QRadar.

Acerca de esta tarea

Los filtros que cree para la búsqueda deben coincidir con los sucesos que desea excluir, no con los sucesos que desee conservar.

Puede que le resulte útil ejecutar la búsqueda en sucesos que ya están en el sistema. Sin embargo, cuando guarde la búsqueda, debe seleccionar **Tiempo real (modalidad continua)** en las opciones de **Intervalo de tiempo**. Si no selecciona este valor, la búsqueda no encontrará ningún resultado cuando se ejecute en la secuencia de sucesos que llegan a QRadar.

Al actualizar la búsqueda de exclusión de identidades guardada sin cambiar el nombre, la lista de exclusión de identidades utilizada por el perfilador activo se actualiza. Por ejemplo, puede editar la búsqueda para añadir más filtros de los datos de activos que desea excluir. Los nuevos valores se incluyen y la exclusión de activos se inicia inmediatamente después de guardar la búsqueda.

Procedimiento

1. En la pestaña **Actividad de registro**, pulse **Buscar** > **Nueva búsqueda**.
2. Cree la búsqueda; para ello, añada criterios de búsqueda y filtros que se correspondan a los sucesos que desea excluir de las actualizaciones de activos.
3. En el recuadro **Rango de tiempo**, seleccione **Tiempo real (modalidad continua)** y pulse **Filtro** para ejecutar la búsqueda.
4. En la pantalla de resultados de la búsqueda, pulse **Guardar criterios** y proporcione la información para la búsqueda guardada. Puede asignar la

búsqueda guardada a un grupo de búsqueda. Los grupos de búsqueda de exclusión de identidades se encuentran en la carpeta **Autenticación, identidad y actividad de usuario**.

Asegúrese de que **Tiempo real (modalidad continua)** se haya seleccionado en las opciones de **Intervalo de tiempo**.

5. Pulse **Aceptar** para guardar la búsqueda.
6. Pulse la pestaña **Admin** y pulse **Configuración del perfilador de activos**.
7. Pulse **Gestionar exclusión de identidades** en la parte inferior de la pantalla.
8. Seleccione la búsqueda de exclusión de identidades que ha creado a partir de la lista de búsquedas de la izquierda y pulse el icono para añadir (>). Si no encuentra la búsqueda, escriba las primeras letras en el filtro en la parte superior de la lista.
9. Pulse **Guardar**.
10. Despliegue los cambios en el entorno para que las actualizaciones entren en vigor.

Ajuste avanzado de reglas de exclusión de conciliación de activos

Puede ajustar las reglas de exclusión de conciliación de activos para refinar la definición de la desviación de crecimiento de activos en una o varias reglas.

Por ejemplo, considere esta plantilla normalizada de una regla de exclusión de conciliación de activos.

```
Aplicar AssetExclusion: Excluir Nombre DNS por IP en sucesos detectados
 por el sistema Local y NO cuando cualquiera de
Nombre de host de identidad está contenido en cualquiera de
Lista blanca de DNS de conciliación de activos - Alfanumérico (sin
distinción de mayúsculas/minúsculas),
 Lista negra de DNS de
conciliación de activos - Alfanumérico (sin distinción de mayúsculas/minúsculas)
 y cuando al menos N1 sucesos se han visto con el mismo
Nombre de host de identidad y diferente IP de identidad en N2
```

En esta tabla se enumeran las variables de la plantilla de regla que pueden ajustarse y el resultado del cambio. No cambie otras variables de la plantilla.

Tabla 68. Opciones para ajustar las reglas de conciliación de activos

Variable	Valor predeterm.	Resultado del ajuste
N1	3	Si se ajusta esta variable en un valor inferior, el resultado es que se añaden más datos a la lista negra debido a que se necesitan menos sucesos con datos conflictivos para que la regla se desencadene. Si se ajusta esta variable en un valor superior, el resultado es que se añaden menos datos a la lista negra debido a que se necesitan más sucesos con datos conflictivos para que la regla se desencadene.

Tabla 68. Opciones para ajustar las reglas de conciliación de activos (continuación)

Variable	Valor predeterm.	Resultado del ajuste
N2	2 horas	Si se ajusta esta variable en un valor inferior, se reduce el intervalo de tiempo en el que los sucesos N1 deben verse para que la regla se desencadene. El tiempo necesario para observar los datos coincidentes se reduce, lo que da como resultado que se añadan menos datos a la lista negra. Si se ajusta esta variable en un valor superior, se incrementa el tiempo que los sucesos N1 deben verse para que la regla se desencadene. El tiempo necesario para observar los datos coincidentes aumenta, lo que da como resultado que se añadan más datos a la lista negra. El incremento del periodo de tiempo puede afectar los recursos de memoria del sistema, ya que se hace un seguimiento de los datos durante periodos de tiempo más largos.

Las reglas de exclusión de conciliación de activos son reglas de todo el sistema. Los cambios en las reglas afectan el comportamiento de la regla en todo el sistema.

Aplicación de ajustes diferentes para las reglas

Puede que sea necesario aplicar ajustes diferentes para las reglas en distintas partes del sistema. Para aplicar diferentes ajustes para las reglas, debe duplicar las reglas de exclusión de conciliación de activos que desea ajustar y añadir una o más pruebas para restringir las reglas de modo que se prueben solamente determinadas partes del sistema. Por ejemplo, puede que desee crear reglas que prueben solamente las redes, los orígenes de registro o los tipos de sucesos.

Acerca de esta tarea

Tenga siempre cuidado cuando añada nuevas reglas al sistema, ya que algunas tareas y reglas de CRE puede afectar al rendimiento del sistema. Puede resultar beneficioso añadir las reglas nuevas al principio de cada pila de pruebas para que el sistema puede omitir el resto de la lógica de pruebas en el caso de que una actualización de activo cumpla los criterios de la regla nueva.

Procedimiento

1. Duplique la regla.
   a. En la pestaña **Delitos**, pulse **Reglas** y seleccione la regla que desea copiar.
   b. Pulse **Acciones** > **Duplicar**. Puede ser útil que el nombre de la regla nueva indique el motivo de la duplicación.
2. Añada una prueba a la regla.

   Determine el filtro que desea utilizar para aplicar la regla solamente a un subconjunto de datos del sistema. Por ejemplo, puede añadir una prueba que coincida solo con sucesos de un origen de registro específico.
3. Ajuste las variables de la regla para conseguir el comportamiento deseado.
4. Actualice la regla original.
   a. Añada a la regla original la misma prueba que ha añadido a la regla duplicada, pero invirtiendo los operadores `AND` y `AND NOT` de la regla.

      Al invertir los operadores se impide que se desencadenen sucesos en ambas reglas.

Ejemplo: Reglas de exclusión de activos que se ajustan para excluir direcciones IP de la lista negra

Puede excluir direcciones IP de las listas negras ajustando las reglas de exclusión de activos.

Como administrador de seguridad de red, gestiona una red corporativa que incluye un segmento de red wifi pública en el que las cesiones de direcciones IP son generalmente breves y frecuentes. Los activos en este segmento de la red tienden a ser transitorios, principalmente sistemas portátiles y dispositivos portátiles que inician y finalizan sesión en la wifi pública con frecuencia. Normalmente, una dirección IP individual la utilizan varias veces distintos dispositivos durante un breve periodo de tiempo.

En el resto del despliegue tiene una red cuidadosamente gestionada que consta únicamente de dispositivos de la empresa con nombres correctos e inventariados. Las cesiones de direcciones IP duran mucho más tiempo en esta parte de la red y a las direcciones IP se accede únicamente a través de la autenticación. En este segmento de red, desea saber inmediatamente cuando hay desviaciones de crecimiento de activos y desea conservar los valores predeterminados para las reglas de exclusión de conciliación de activos.

Elaboración de la lista negra de direcciones IP

En este entorno, las reglas de exclusión de conciliación de activos predeterminadas incluyen inadvertidamente en una lista negra la red entera durante un breve periodo de tiempo.

Su equipo de seguridad observa que las notificaciones relacionadas con el activo generadas por el segmento de wifi son una molestia. Desea evitar que la wifi desencadene más notificaciones de desviaciones del crecimiento de activos.

Ajuste de las reglas de conciliación de activos para ignorar algunas actualizaciones de activos

Revisa el informe **Desviaciones de activo por origen de registro** en la última notificación del sistema. Determina que los datos de la lista negra proceden del servidor DHCP de la wifi.

Los valores de la columna **Recuento de sucesos**, la columna **Recuento de flujos** y la columna **Delitos** de la fila correspondiente a la regla **AssetExclusion: Excluir IP por dirección MAC** indican que el servidor DHCP de la wifi desencadena esta regla.

Añade una prueba a las reglas de conciliación de activos existentes para hacer que las reglas dejen de añadir datos de la wifi a la lista negra.

```
Aplicar AssetExclusion:Excluir IP por Dirección MAC en sucesos detectados por
el sistema Local y NO cuando los sucesos los ha detectado uno o varios
MicrosoftDHCP @ microsoft.dhcp.test.com
y NO cuando cualquiera de Dominio es la clave y cualquiera de IP de identidad es el valor en
cualquiera de Lista blanca de IPv4 del dominio de conciliación de activos
- Lista negra de IPv4 del dominio de conciliación de activos - IP
y cuando al menos 3 sucesos se han visto con la misma IP de identidad y
diferente MAC de identidad en 2 horas.
```

La regla actualizada prueba solamente los sucesos de los orígenes de registro que no están en el servidor DHCP de la wifi. Para evitar que los sucesos DHCP de la

wifi pasen más pruebas costosas de análisis de comportamiento y conjunto de referencia, también ha movido esta prueba al principio de la pila de pruebas.

Limpieza de datos de activos después de desviaciones de crecimiento

IBM Security QRadar utiliza el modelo de activos para conectar los delitos del despliegue con los activos físicos o virtuales de la red. La capacidad de recopilar y ver datos relevantes sobre cómo se utilizan los activos es un paso importante en la resolución de problemas de seguridad. Es importante mantener la base de datos de activos para asegurarse de que los datos son actuales y precisos.

Tanto si soluciona el origen del problema como si bloquea las actualizaciones de activos, debe limpiar la base de datos de activos mediante la eliminación de los datos de activos no válidos y las entradas de las listas negras de activos.

Supresión de activos no válidos

Después de arreglar los activos que contribuyeron a la desviación de crecimiento de activos, limpie los artefactos de activos mediante la limpieza selectiva o volviendo a crear la base de datos de activos.

Acerca de esta tarea

Limpieza selectiva
Este método se utiliza con las desviaciones de crecimiento de activos de ámbito limitado. La eliminación selectiva de los activos afectados es la forma menos invasiva de limpiar los artefactos de activos, pero si hay muchos activos afectados, también puede ser el más tedioso.

Volver a crear la base de datos de activos
Volver a crear la base de datos de activos desde cero es el método más eficaz y preciso de suprimir los activos cuando las desviaciones de crecimiento de activos son omnipresentes.

Este método regenera de forma pasiva los activos en la base de datos con el nuevo ajuste que haya configurado para resolver los problemas de crecimiento de activos. Con este enfoque, todos los resultados de exploración y los datos de activos residuales se pierden, pero los datos se pueden recuperar volviendo a ejecutar una exploración o volviendo a importar los resultados de la exploración.

Procedimiento

1. Para eliminar de forma selectiva los artefactos no válidos en la base de datos de activos, siga estos pasos:
   a. En la pestaña **Actividad de registro**, ejecute la búsqueda de sucesos **Desviación de crecimiento de activos: Informe de activos**. Esta búsqueda devuelve un informe de los activos que se han visto afectados por la desviación de crecimiento de activos y deben suprimirse.
   b. En la pestaña **Activos**, pulse **Acciones** > **Suprimir activo**. Puede pasar un tiempo hasta que el activo deje de aparecer en QRadar.
2. Para volver a crear la base de datos de activos desde cero, siga estos pasos:
   a. Utilice SSH para iniciar la sesión en consola de QRadar como administrador.
   b. Ejecute el script `/opt/qradar/support/cleanAssetModel.sh` desde la línea de mandatos de la consola y seleccione **Opción 1** cuando se le solicite.

Al volver a crear la base de datos de activos se reinicia el motor de conciliación de activos.

Resultados

La depuración de una lista negra elimina todas las entradas de la lista negra, incluidas aquellas que se hayan añadido manualmente. Las entradas de la lista negra que se han añadido manualmente deben añadirse de nuevo.

Supresión de entradas de las listas negras

Una vez solucionada la causa de las entradas de las listas negras, debe limpiar las entradas restantes. Puede eliminar entradas individuales de las listas negras, pero es mejor depurar todas las entradas de las listas negras y permitir que se vuelvan a generar los valores de lista negra que no estén relacionados con la desviación de crecimiento de activos.

Procedimiento

1. Para depurar una lista negra mediante consola de QRadar:
   a. Pulse **Admin** > **Configuración del sistema** > **Gestión de conjuntos de referencia**.
   b. Seleccione un conjunto de referencia y después pulse **Suprimir**.
   c. Utilice el cuadro de texto de búsqueda rápida para buscar los conjuntos de referencia que desee suprimir y luego pulse **Suprimir listados**.
2. Para depurar una lista negra mediante la interfaz de línea de mandatos de consola de QRadar:
   a. Vaya al directorio `/opt/qradar/bin`.
   b. Ejecute el mandato siguiente:

      ```
      ./ReferenceDataUtil.sh purge "Nombre de recopilación de referencia"
      ```

      Siendo *Nombre de recopilación de referencia* una de las listas siguientes:
      - Lista negra de NetBIOS de conciliación de activos
      - Lista negra de DNS de conciliación de activos
      - Lista negra de IPv4 de conciliación de activos
      - Lista negra de MAC de conciliación de activos

Resultados

La depuración de una lista negra elimina todas las entradas de la lista negra, incluidas aquellas que se hayan añadido manualmente. Las entradas de la lista negra que se han añadido manualmente deben añadirse de nuevo.

Capítulo 18. Configuración de sistemas de QRadar para reenviar datos a otros sistemas

Puede configurar los sistemas de IBM Security QRadar para reenviar datos a uno o a varios sistemas de proveedores como, por ejemplo, sistemas de tíquets o de alertas. También puede reenviar datos normalizados a otros sistemas de QRadar. Al sistema de destino que recibe los datos de QRadar se le llama *destino de reenvío*.

Con la excepción del etiquetado de dominio, los sistemas de QRadar se aseguran de que los datos reenviados no se alteran. La información de dominio se elimina de los datos reenviados. Los sucesos y los flujos que contienen información de dominio se asignan automáticamente al dominio predeterminado en el sistema receptor.

Para evitar problemas de compatibilidad al enviar datos de sucesos y flujos, asegúrese de que el despliegue que recibe los datos sea de la misma versión o de una versión superior al despliegue que está enviando los datos.

1. Configure uno o varios destinos de reenvío.
2. Para determinar qué datos desea reenviar, configure reglas de direccionamiento, reglas personalizadas o ambos tipos de reglas.
3. Configure las opciones de direccionamiento que se aplicarán a los datos.

Por ejemplo, puede configurar que todos los datos de un recopilador de sucesos específico se reenvíen a un sistema de tíquets determinado. También puede eludir la correlación eliminando los datos que coinciden con una regla de direccionamiento.

Adición de destinos de reenvío

Para poder configurar un reenvío de datos selectivo o masivo, hay que añadir antes un destino de reenvío.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Destinos de reenvío**.
4. En la barra de herramientas, pulse **Añadir**.
5. En la ventana Destinos de reenvío, especifique los valores de los parámetros.

   En la tabla siguiente se describen algunos de los parámetros de Destinos de reenvío.

Tabla 69. Parámetros de Destinos de reenvío

Parámetro	Descripción
Formato de suceso	• **Carga útil** son los datos en el formato que el origen de registro o el origen de flujo ha enviado. • **Normalizado** son datos en bruto que se analizan y se preparan como información legible para la interfaz de usuario.
Dirección de destino	Dirección IP o nombre de host del sistema del proveedor al que desea reenviar los datos.

© Copyright IBM Corp. 2012, 2015

Tabla 69. Parámetros de Destinos de reenvío (continuación)

Parámetro	Descripción
Protocolo	• **TCP** Para utilizar el protocolo **TCP** en el envío de datos normalizados, hay que crear un origen externo al sitio en la dirección de destino en el puerto 32004. • **UDP**
Añada una cabecera de syslog como prefijo si falta o no es válida	Si no se ha detectado una cabecera de syslog válida en el mensaje de syslog original, seleccione esta casilla. La cabecera de syslog añadida como prefijo incluye la dirección IP de dispositivo del origen de registro (suplantación de dirección IP) en el campo **Hostname** de la cabecera de syslog. Si no se selecciona esta casilla, los datos se enviarán sin modificar. Cuando QRadar reenvía mensajes de syslog, el mensaje de salida se verifica para garantizar que tenga una cabecera de syslog válida.

6. Pulse **Guardar**.

Configuración de perfiles de reenvío

Si desea especificar qué propiedades se reenviarán al destino de reenvío, configure un perfil de reenvío.

Debe volver a crear los perfiles de reenvío de JSON que ha creado en IBM Security QRadar V7.2.3 o versiones anteriores.

Acerca de esta tarea

Puede utilizar los perfiles de reenvío solamente cuando los datos de suceso se envían en formato JSON.

Puede seleccionar propiedades de sucesos o flujos específicas, incluidas las propiedades personalizadas, para reenviarlas a un destino externo. Puede mejorar la legibilidad de los datos de suceso especificando un nombre de alias y el valor predeterminado para el atributo. Los nombres de alias y los valores predeterminados son específicos del perfil en el que están definidos. Si los atributos se utilizan en otros perfiles, los nombres de alias y los valores predeterminados deben volver a definirse.

Puede utilizar un único perfil que tenga varios destinos de reenvío. Cuando edite un perfil, asegúrese de que los cambios son adecuados para todos los destinos de reenvío con los que el perfil está asociado.

Cuando se suprime un perfil, todos los destinos de reenvío que utilizan el perfil vuelven a utilizar automáticamente el perfil predeterminado.

Procedimiento

1. Pulse la pestaña **Admin** y, en el panel de navegación, pulse **Configuración del sistema**.
2. Pulse el icono **Destinos de reenvío**.
3. En la barra de herramientas, pulse **Gestor de perfiles**.
4. Para crear un nuevo perfil, pulse **Nuevo**.

5. Escriba un nombre para el perfil y seleccione la casilla de verificación situada junto a los atributos que desea incluir en el conjunto de datos de suceso.
6. Para cambiar un perfil existente, seleccione el perfil y pulse **Editar** o **Suprimir**.
7. Pulse **Guardar**.

Configuración de reglas de direccionamiento para el reenvío masivo

Después de haber añadido uno o varios destinos de reenvío, puede crear reglas de direccionamiento basadas en filtros para reenviar grandes cantidades de datos.

Acerca de esta tarea

Puede configurar reglas de direccionamiento para reenviar datos en modalidad en línea o fuera de línea:

- En la modalidad **En línea** los datos permanecen actualizados porque el reenvío se lleva a cabo en tiempo real. Si no se pudiese acceder al destino de reenvío, los datos podrían perderse.
- En la modalidad **Fuera de línea** todos los datos se almacenan en la base de datos y luego se envían al destino de reenvío. Esto garantiza que los datos no se pierden; sin embargo, podría haber retrasos en el reenvío de datos.

En la tabla siguiente se describen algunos de los parámetros de Reglas de direccionamiento.

Tabla 70. Parámetros de la ventana Reglas de direccionamiento

Parámetro	Descripción
Recopilador de sucesos de reenvío	Esta opción se visualiza cuando se selecciona la opción **En línea**. Especifica el Recopilador de sucesos cuyos datos desea procesar con esta regla de direccionamiento.
Procesador de sucesos de reenvío	Esta opción se visualiza cuando se selecciona la opción **Fuera de línea**. Especifica el Procesador de sucesos cuyos datos desea procesar con esta regla de direccionamiento. **Restricción:** Esta opción no está disponible si se selecciona **Descartar** en el panel **Opciones de direccionamiento**.

Tabla 70. Parámetros de la ventana Reglas de direccionamiento (continuación)

Parámetro	Descripción
Opciones de direccionamiento	• La opción **Reenviar** especifica que los datos se reenvíen al destino de reenvío especificado. Los datos también se almacenan en la base de datos y son procesados por el motor de reglas personalizadas (CRE). • La opción **Descartar** especifica que los datos no se almacenen en la base de datos, se ignora el CRE y se eliminan los sucesos. Los datos no se reenvían a un destino de reenvío, pero son procesados por el CRE. Esta opción no está disponible si se selecciona la opción **Fuera de línea**. • La opción **Ignorar correlación** especifica que los datos ignoran el CRE, pero se almacenan en la base de datos. Esta opción no está disponible si se selecciona la opción **Fuera de línea**. Pueden combinarse dos opciones: • **Reenviar** y **Descartar** Los datos se reenvían al destino de reenvío especificado. Los datos no se almacenan en la base de datos y son procesados por el CRE. • **Reenviar** e **Ignorar correlación** Los datos se reenvían al destino de reenvío especificado. Los datos también se almacenan en la base de datos, pero no son procesados por el CRE. El CRE del destino del reenvío procesa los datos. Si los datos coinciden con múltiples reglas, se aplicará la opción de direccionamiento más segura. Por ejemplo, si los datos coinciden con una regla configurada para descartar y con una regla configurada para ignorar el proceso de CRE, los datos no se descartarán. En vez de ello, los datos eluden el CRE y se almacenan en la base de datos. Todos los sucesos se cuentan contra la licencia de sucesos por segundo (EPS).

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Reglas de direccionamiento**.
4. En la barra de herramientas, pulse **Añadir**.
5. En la ventana Reglas de direccionamiento, especifique los valores de los parámetros.
   a. Escriba un nombre y una descripción para la regla de direccionamiento.

b. En el campo **Modalidad**, seleccione una de las opciones siguientes: **En línea** o **Fuera de línea**.

c. En la lista **Recopilador de sucesos de reenvío** o **Procesador de sucesos de reenvío**, seleccione el recopilador de sucesos desde el que desea reenviar datos.

d. En el campo **Origen de datos** de la sección **Filtros de sucesos**, seleccione el origen de datos que desea direccionar: **Sucesos** o **Flujos**.

   Si selecciona la opción **Filtros de flujos**, el título de la sección pasa a ser **Filtros de flujos** y la casilla de verificación **Coincidir con todos los sucesos entrantes** pasa a ser **Coincidir con todos los flujos**.

e. Para reenviar todos los datos entrantes, seleccione la casilla de verificación **Coincidir con todos los sucesos entrantes** o **Coincidir con todos los flujos entrantes**.

   Restricción: Si selecciona esta casilla de verificación, no puede añadir un filtro.

f. Para añadir un filtro, en la sección **Filtros de sucesos** o **Filtros de flujos**, seleccione un filtro en la primera lista y un operando en la segunda lista.

g. En el cuadro de texto, escriba el valor por el que desea filtrar y luego pulse **Añadir filtro**.

h. Repita los dos pasos anteriores para cada filtro que desee añadir.

i. Para reenviar datos de registro que coincidan con los filtros actuales, seleccione la casilla de verificación **Reenviar** y, a continuación, seleccione la casilla de verificación de cada destino de reenvío preferido.

   Restricción: Si selecciona la casilla de verificación **Reenviar**, también puede seleccionar la casilla de verificación **Descartar** o **Ignorar correlación**, pero no ambas.

   Si desea editar, añadir o suprimir un destino de reenvío, pulse el enlace **Gestionar destinos**.

6. Pulse **Guardar**.

Configuración del reenvío selectivo

Utilice el asistente Regla personalizada para configurar el reenvío altamente selectivo de datos de suceso. Configure reglas que reenvíen los datos de suceso a uno o varios destinos de reenvío como respuesta de la regla.

Acerca de esta tarea

Los criterios que determinan qué datos de suceso se envían a un destino de reenvío se basan en las pruebas y los componentes básicos que se incluyen en la regla. Cuando la regla está configurada y habilitada, todos los datos de suceso que coincidan con las pruebas de la regla se envían automáticamente a los destinos de reenvío especificados. Para obtener más información sobre la edición o la adición de una regla, consulte la *guía del usuario* de su producto.

Procedimiento

1. Pulse la pestaña **Delitos Actividad de registro**.
2. En el menú de navegación, pulse **Reglas**.
3. Edite o añada una regla. En la página Respuesta de regla del asistente Regla, asegúrese de que selecciona la opción **Enviar a destinos de reenvío**.

Visualización de destinos de reenvío

La ventana Destinos de reenvío proporciona información valiosa sobre los destinos de reenvío. Se muestran las estadísticas de los datos enviados a cada destino de reenvío.

Por ejemplo, puede ver la información siguiente:

- Número total de sucesos y flujos que se han visto para este destino de reenvío.
- Número de sucesos o flujos que se han enviado a este destino de reenvío.
- Número de sucesos o flujos que se han descartado antes de llegar al destino de reenvío.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Destinos de reenvío**.
4. Vea las estadísticas de los destinos de reenvío.

Visualización y gestión de destinos de reenvío

Utilice la ventana Destinos de reenvío para ver, editar y suprimir los destinos de reenvío.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el panel de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Destinos de reenvío**.

   Se muestran las estadísticas de los datos enviados a cada destino de reenvío. Por ejemplo, puede ver la información siguiente:

   - Número total de sucesos y flujos que se han visto para este destino de reenvío.
   - Número de sucesos o flujos que se han enviado a este destino de reenvío.
   - Número de sucesos o flujos que se han descartado antes de llegar al destino de reenvío.
4. En la barra de herramientas, pulse una acción, tal como se describe en la tabla siguiente.

Tabla 71. Descripción de las acciones de la barra de herramientas de Destinos de reenvío

Acción	Descripción
Inicializar contadores	Restablece en cero los contadores de los parámetros **Visto**, **Enviado** y **Descartado**; los contadores comienzan a contar de nuevo. **Consejo:** Puede restablecer los contadores para proporcionar una vista más precisa del rendimiento de los destinos de reenvío.
Editar	Cambia el nombre, el formato, la dirección IP, el puerto o el protocolo configurados.
Suprimir	Suprime un destino de reenvío. Si el destino de reenvío está asociado con alguna regla activa, debe confirmar que desea suprimir el destino de reenvío.

Visualización y gestión de reglas de direccionamiento

La ventana Reglas de direccionamiento de sucesos proporciona información valiosa sobre las reglas de direccionamiento. Puede ver o gestionar los filtros y las acciones configurados cuando haya datos que coincidan con cada regla.

Utilice la ventana Reglas de direccionamiento de sucesos para editar, habilitar, inhabilitar o suprimir una regla. Puede editar una regla de direccionamiento para cambiar el nombre, el Recopilador de sucesos, los filtros o las opciones de direccionamiento que se hayan configurado.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Reglas de direccionamiento**.
4. Seleccione la regla de direccionamiento que desea gestionar.
5. Para editar la regla de direccionamiento, en la barra de herramientas pulse **Editar** y actualice los parámetros.
6. Para eliminar la regla de direccionamiento, en la barra de herramientas pulse **Suprimir**.
7. Para habilitar o inhabilitar la regla de direccionamiento, en la barra de herramientas pulse **Habilitar/inhabilitar**.

   Si habilita una regla de direccionamiento que está configurada para descartar sucesos, se visualiza un mensaje de confirmación.

Capítulo 19. Almacenamiento y reenvío de sucesos

Utilice la función Almacenar y reenviar para gestionar las planificaciones para el reenvío de sucesos desde los dispositivos Recopilador de sucesos dedicados a los componentes Procesador de sucesos del despliegue.

La función Almacenar y reenviar está soportada en Event Collector 1501 y Event Collector 1590. Para obtener más información sobre estos dispositivos, consulte la publicación *QRadar Hardware Guide*.

Un Recopilador de sucesos dedicado no procesa sucesos y no incluye un Procesador de sucesos en placa. De forma predeterminada, un Recopilador de sucesos dedicado reenvía continuamente sucesos a un Procesador de sucesos que debe conectar mediante el icono **Editor de despliegue**. Utilice la función Almacenar y reenviar para planificar un rango de tiempo en el que desea que el Recopilador de sucesos reenvíe sucesos. Cuando no se reenvían sucesos, los sucesos se almacenan localmente en el dispositivo. No se puede acceder a los sucesos en la interfaz de usuario de consola de QRadar.

Utilice la función de planificación para almacenar sucesos durante el horario laboral. Reenvíe los sucesos a un Procesador de sucesos cuando la transmisión no afecte negativamente al ancho de banda de red. Por ejemplo, puede configurar un Recopilador de sucesos para reenviar sucesos a un Procesador de sucesos durante las horas no laborables.

Descripción general de Almacenar y reenviar

La función Almacenar y reenviar está soportada en los dispositivos Event Collector 1501 y Event Collector 1590. Para obtener más información sobre estos dispositivos, consulte la publicación *QRadar Hardware Guide*.

Un recopilador de sucesos dedicado no procesa sucesos y no incluye un procesador de sucesos en placa. De forma predeterminada, un recopilador de sucesos dedicado reenvía continuamente sucesos a un procesador de sucesos que debe conectar mediante el icono Editor de despliegue. La función Almacenar y reenviar permite planificar un rango de tiempo en el que desea que el recopilador de sucesos reenvíe sucesos. Cuando no se reenvían sucesos, los sucesos se almacenan localmente en el dispositivo y no se puede acceder a ellos con la interfaz de usuario de la consola.

Esta función de planificación permite almacenar sucesos durante el horario laboral y después reenviar los sucesos a un procesador de sucesos durante los periodos de tiempo en los que la transmisión no afecte negativamente al ancho de banda de red. Por ejemplo, puede configurar un recopilador de sucesos para reenviar sucesos solamente a un procesador de sucesos durante las horas no laborables; por ejemplo, desde la medianoche hasta las 6 de la mañana.

Visualización de la lista de planificación de Almacenar y reenviar

Utilice la ventana Almacenar y reenviar para ver una lista de planificaciones. Las planificaciones incluyen estadísticas que le ayudarán a evaluar el estado, el rendimiento y el progreso de las planificaciones.

© Copyright IBM Corp. 2012, 2015

Antes de empezar

Debe crear una planificación. De forma predeterminada, la primera vez que se accede a la ventana Almacenar y reenviar no aparece ninguna planificación.

Acerca de esta tarea

Puede utilizar opciones de la barra de herramientas y el cuadro de lista **Visualizar** para cambiar la vista de la lista de planificación. Cambie la vista de la lista para centrarse en las estadísticas desde diversos puntos de vista. Por ejemplo, si desea ver las estadísticas de un determinado recopilador de sucesos, puede seleccionar **Recopiladores de sucesos** en la lista **Visualizar**. A continuación la lista se agrupa según la columna **Recopilador de sucesos**, con lo que resulta más fácil localizar el Recopilador de sucesos que desea investigar.

De forma predeterminada, la lista de Almacenar y reenviar está configurada para visualizar la lista organizada según la planificación (**Visualizar** > **Planificaciones**).

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Almacenar y reenviar**.
4. En la ventana Almacenar y reenviar, consulte los parámetros de cada planificación.

   En la tabla siguiente se describen algunos de los parámetros de la planificación.

Tabla 72. Parámetros de la ventana Almacenar y reenviar

Parámetro	Descripción
Visualizar	La opción **Planificaciones** muestra una jerarquía de la relación padre-hijo entre las planificaciones, los Procesadores de sucesos y los recopiladores de sucesos de QRadar asociados. La opción **Recopiladores de sucesos** muestra el nivel más bajo de la jerarquía, que es una lista de recopiladores de sucesos de QRadar. La opción **Procesadores de sucesos** muestra una jerarquía de la relación padre-hijo entre los Procesadores de sucesos y los recopiladores de sucesos de QRadar asociados.

Tabla 72. Parámetros de la ventana Almacenar y reenviar (continuación)

Parámetro	Descripción
Nombre	Para la opción **Planificaciones**, la columna **Nombre** se visualiza con el formato siguiente. • **Primer nivel** representa el nombre de la planificación. • **Segundo nivel** representa el nombre del Procesador de sucesos. • **Tercer nivel** representa el nombre del Recopilador de sucesos. Para la opción **Procesadores de sucesos**, la columna se visualiza con el formato siguiente. • **Primer nivel** representa el nombre del Procesador de sucesos. • **Segundo nivel** representa el nombre del Recopilador de sucesos. **Consejo:** Puede utilizar el signo más (+) y el signo menos (-) junto al nombre o las opciones de la barra de herramientas para expandir y contraer el árbol jerárquico. También puede expandir y contraer el árbol jerárquico utilizando las opciones de la barra de herramientas.
Nombre de planificación	Muestra el nombre de la planificación para las opciones **Recopiladores de sucesos** o **Procesadores de sucesos**. Si un Procesador de sucesos está asociado con más de una planificación, en **Nombre de planificación** se muestra `Múltiple`*n*, donde *n* es el número de planificaciones. **Consejo:** Pulse el signo más (+) para ver las planificaciones asociadas.

Tabla 72. Parámetros de la ventana Almacenar y reenviar (continuación)

Parámetro	Descripción
Último estado	Muestra el estado del proceso de Almacenar y reenviar: • **Reenvío** indica que el reenvío de sucesos está en curso. • **Reenvío completado** indica que el reenvío de sucesos se ha completado satisfactoriamente y que los sucesos se han almacenado localmente en el Recopilador de sucesos. Los sucesos almacenados se reenvían cuando la planificación indique que el reenvío puede volver a empezar. • **Aviso** indica que el porcentaje de sucesos que se quedan en el almacenamiento sobrepasa el porcentaje de tiempo que se quedan en la planificación de Almacenar y reenviar. • **Error** indica que el reenvío de sucesos se ha detenido antes de que se reenviasen todos los sucesos almacenados. • **Inactivo** indica que no hay recopiladores de sucesos de QRadar asignados a la planificación, o que los recopiladores de sucesos de QRadar asignados no han recibido sucesos. **Consejo:** Mueva el puntero del ratón sobre la columna **Último estado** para ver un resumen del estado.
Sucesos reenviados	Muestra el número de sucesos (en K, M o G) reenviados en la sesión actual. **Consejo:** Mueva el puntero del ratón sobre el valor de la columna **Sucesos reenviados** para ver el número de sucesos.
Sucesos restantes	Muestra el número de sucesos (en K, M o G) que quedan por reenviar en la sesión actual. **Consejo:** Mueva el puntero del ratón sobre el valor de la columna **Sucesos restantes** para ver el número de sucesos.
Velocidad promedio de sucesos	Muestra la velocidad media con que los sucesos se reenvían del Recopilador de sucesos al Procesador de sucesos. **Consejo:** Mueva el puntero del ratón sobre el valor de la columna **Velocidad promedio de sucesos** para ver el promedio de sucesos por segundo (EPS).

Tabla 72. Parámetros de la ventana Almacenar y reenviar (continuación)

Parámetro	Descripción
Velocidad actual de sucesos	Muestra la velocidad con que los sucesos se reenvían del Recopilador de sucesos al Procesador de sucesos. **Consejo:** Mueva el puntero del ratón sobre el valor de la columna **Velocidad actual de sucesos** para ver los sucesos por segundo (EPS) actuales.
Límite de velocidad de transferencia	El límite de velocidad de transferencia es configurable. El límite de velocidad de transferencia puede configurarse para visualizarlo en kilobytes por segundo (KBs), megabytes por segundo (MBs) o gigabytes por segundo (GBs).

Creación de una nueva planificación de Almacenar y reenviar

Utilice el asistente de Almacenar y reenviar para crear una planificación que controle cuándo el Recopilador de sucesos inicia y detiene el reenvío de datos a un Procesador de sucesos.

Puede crear y gestionar varias planificaciones para controlar el reenvío de sucesos de varios recopiladores de sucesos de QRadar en un despliegue distribuido geográficamente.

Antes de empezar

Asegúrese de que el Recopilador de sucesos dedicado se añade a su despliegue y está conectado a un Procesador de sucesos. La conexión entre un Recopilador de sucesos y un Procesador de sucesos se configura en el **Editor de despliegue**.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Almacenar y reenviar**.
4. Pulse **Acciones** > **Crear**.
   a. Pulse **Siguiente** para pasar a la página Seleccionar recopiladores.
   b. En la página Seleccionar recopiladores, configure los parámetros.

      Si el Recopilador de sucesos que desea configurar no aparece en la lista, puede que no se haya añadido a su despliegue. Si es así, utilice el **Editor de despliegue** para añadir el Recopilador de sucesos y luego continúe.
   c. En la página Opciones de planificación, configure los parámetros.

      Para configurar la velocidad de transferencia de reenvío, la velocidad de transferencia mínima es de 0. La velocidad de transferencia máxima es de 9.999.999. El valor 0 significa que la velocidad de transferencia es ilimitada.
   d. Finalice la configuración.

Ahora puede ver la planificación en la ventana Almacenar y reenviar. Después de crear una nueva planificación, puede que tengan que transcurrir hasta 10 minutos para que las estadísticas empiecen a visualizarse en la ventana Almacenar y reenviar.

Edición de una planificación de Almacenar y reenviar

Puede editar una planificación de **Almacenar y reenviar** para añadir o eliminar recopiladores de sucesos de QRadar y cambiar los parámetros de planificación. Después de editar una planificación de **Almacenar y reenviar**, las estadísticas que se visualizan en la lista de **Almacenar y reenviar** se restablecen.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Configuración del sistema**.
3. Pulse el icono **Almacenar y reenviar**.
4. Seleccione la planificación que desee editar.
5. Pulse **Acciones** > **Editar**.

   También puede efectuar una doble pulsación en una planificación para editarla.
6. Pulse **Siguiente** para pasar a la página Seleccionar recopiladores.
7. En la página Seleccionar recopiladores, edite los parámetros.
8. Pulse **Siguiente** para pasar a la página Opciones de planificación.
9. En la página Opciones de planificación, edite los parámetros de planificación.
10. Pulse **Siguiente** para pasar a la página Resumen.
11. En la página Resumen, confirme las opciones que ha editado para esta planificación.

    Después de editar una planificación, puede que tengan que transcurrir hasta 10 minutos para que las estadísticas se actualicen en la ventana Almacenar y reenviar.

Supresión de una planificación de Almacenar y reenviar

Puede suprimir una planificación de **Almacenar y reenviar**.

Procedimiento

1. En el menú de navegación, pulse **Configuración del sistema**.
2. Pulse el icono **Almacenar y reenviar**.
3. Seleccione la planificación que desee suprimir.
4. Pulse **Acciones** > **Suprimir**.

   Cuando la planificación se haya suprimido, los recopiladores de sucesos de QRadar asociados reanudarán el reenvío continuo de sucesos al Procesador de sucesos asignado.

Capítulo 20. Gestión de contenido

Se utilizan las herramientas de gestión de contenido de IBM Security QRadar para importar contenido de seguridad, como por ejemplo reglas, informes, paneles de control y aplicaciones, en QRadar. El contenido de seguridad pueden proceder de otros sistemas de QRadar, o puede desarrollarse de forma independiente para ampliar las prestaciones de QRadar existentes.

El contenido de QRadar está disponible en las siguientes fuentes:

IBM Security App Exchange
IBM Security App Exchange (https://apps.xforce.ibmcloud.com) es una tienda de aplicaciones y portal donde puede examinar y descargar extensiones de QRadar. Se trata de una nueva forma de compartir código, visualizaciones, informes, reglas y aplicaciones.

IBM Fix Central
IBM Fix Central (www.ibm.com/support/fixcentral/) proporciona arreglos y actualizaciones para el software, el hardware y el sistema operativo del sistema. Puede descargar paquetes de contenido de seguridad y extensiones desde IBM Fix Central.

Despliegues de QRadar
El contenido personalizado se exporta desde un despliegue de QRadar como una extensión y se importa en otro sistema cuando se desea reutilizar el contenido. Por ejemplo, puede exportar contenido desde el entorno de desarrollo al entorno de producción. Puede utilizar el script de gestión de contenidos de la línea de mandatos para exportar todo el contenido u optar por exportar sólo parte del contenido personalizado.

Tipos de contenido de seguridad

El contenido de QRadar está empaquetado en los tipos siguientes:

Paquetes de contenido

Los *paquetes de contenido* de seguridad contienen mejoras para tipos específicos de contenido de seguridad. A menudo incluyen contenido para integración o sistemas operativos de terceros. Por ejemplo, un paquete de contenido de seguridad para una integración de terceros puede contener nuevas propiedades de suceso personalizadas para que sea posible buscar el origen de registro en la información de la carga útil del suceso y esta información esté disponible para la creación de informes.

Los paquetes de contenido de seguridad están disponibles en IBM Fix Central. Los paquetes de contenido no están disponibles como parte de un actualización automática.

Extensiones

IBM y otros proveedores graban *extensiones* de seguridad que mejoran o amplían las prestaciones de QRadar. Una extensión puede contener aplicaciones, elementos de contenido, como por ejemplo reglas personalizadas, plantillas de informes, búsquedas guardadas, o contener actualizaciones de los elementos de contenido existentes. Por ejemplo, una extensión puede incluir una aplicación para añadir una pestaña a QRadar que proporcione visualizaciones para un delito.

© Copyright IBM Corp. 2012, 2015

Puede descargar extensiones de QRadar desde IBM Security App Exchange y utilizar la herramienta de **Gestión de extensiones** para instalarlas. Las extensiones de seguridad no están disponibles como parte de un actualización automática.

Métodos de importación y exportación de contenido

Puede utilizar las herramientas siguientes para importar y exportar contenido en el despliegue de QRadar.

Herramienta Gestión de extensiones

Utilice la herramienta Gestión de extensiones para añadir extensiones a su despliegue de QRadar. Al importar contenido mediante la herramienta Gestión de extensiones, puede ver el contenido antes de instalarlo. Si los elementos de contenido existen en el sistema, puede especificar si desea reemplazar el elemento de contenido o pasar por alto la actualización.

No puede utilizar la herramienta Gestión de extensiones para exportar contenido.

Script de gestión de contenido

Utilice el script de gestión de contenido para exportar contenido personalizado del despliegue de QRadar a un formato externo y portable. A continuación, puede utilizar el script para importar el contenido personalizado en otro despliegue de QRadar. El script es útil cuando se desea automatizar el movimiento de contenido entre los despliegues de QRadar.

El script `contentManagement.pl` se encuentra en el directorio `/opt/qradar/bin`.

Debe utilizar el script de gestión de contenido para exportar contenido del despliegue de origen de QRadar. Puede utilizar el script de gestión de contenido o la herramienta Gestión de extensiones para importar el contenido en el despliegue de destino.

Exportación de todo el contenido personalizado

El script `contentManagement.pl` se utiliza para exportar todo el contenido personalizado del despliegue de IBM Security QRadar.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Vaya al directorio `/opt/qradar/bin` y especifique el mandato siguiente para exportar todo el contenido personalizado:

   ```
   ./contentManagement.pl -a export -c all
   ```

   Ejemplos:

   - Para incluir datos acumulados en la exportación, escriba el mandato siguiente:

     ```
     ./contentManagement.pl --action export --content-type all -g
     ```

   - Para especificar el directorio para el archivo exportado y cambiar el formato de compresión, especifique el mandato siguiente:

     ```
     ./contentManagement.pl
     -a export -c all -o [vía_acceso_archivo] -t [tipo_compresión]
     ```

Resultados

El contenido se exporta a un archivo comprimido, por ejemplo, `all-ContentExport-20151022101803.zip`. Puede cambiar manualmente el nombre de archivo por un nombre más descriptivo. El archivo exportado podría contener más elementos de contenido de lo que se esperaba, porque todas las dependencias se exportan con los elementos de contenido especificados. Por ejemplo, si exporta un informe, también se exporta la búsqueda guardada que el informe utiliza.

Exportación de todo el contenido personalizado de un tipo específico

Puede exportar todo el contenido personalizado de un tipo específico con una sola acción.

Acerca de esta tarea

El script de gestión de contenido utiliza identificadores de texto o identificadores numéricos para especificar el tipo de contenido que desea exportar.

Tabla 73. Identificadores de tipo de contenido para exportar contenido personalizado

Tipo de contenido personalizado	Identificador de texto	Identificador numérico
Paneles de control	**dashboard**	4
Informes	**report**	10
Búsquedas guardadas	**search**	1
FGroups [1]	**fgroup**	12
Tipos de FGroup	**fgrouptype**	13
Reglas personalizadas	**customrule**	3
Propiedades personalizadas	**customproperty**	6
Orígenes de registro	**sensordevice**	17
Tipos de origen de registro	**sensordevicetype**	24
Categorías de origen de registro	**sensordevicecategory**	18
Extensiones de origen de registro	**deviceextension**	16
Recopilaciones de datos de referencia	**referencedata**	28
Entradas de correlaciones de QID personalizadas	**qidmap**	27
Perfiles de correlación histórica	**historicalsearch**	25
Funciones personalizadas	**custom_function**	77
Acciones personalizadas	**custom_action**	78
Aplicaciones	**installed_application**	100

[1]Un FGroup representa un grupo de contenido, como por ejemplo un grupo de origen de registro, un grupo de informes o un grupo de búsqueda.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.

2. Vaya al directorio `/opt/qradar/bin` y escriba el mandato para exportar todo el contenido del tipo especificado:

   `./contentManagement.pl -a export --content-type` *`[tipo_contenido]`* `--id all`

   Parámetros:

Tabla 74. Parámetros del script `contentManagement.pl` para exportar contenido personalizado de un tipo específico

Parámetro	Descripción
-c *[tipo_contenido]* o bien **--content-type** *[tipo_contenido]*	Especifica el tipo de contenido. Puede teclear el texto o el identificador numérico correspondiente para especificar el tipo de contenido.
-e o bien **--include-reference-data-elements**	Establezca este distintivo para incluir elementos y claves de datos de referencia en la exportación. Las claves de datos de referencia y los elementos de datos de referencia son aplicables al tipo de contenido `referencedata`. Este parámetro sólo es aplicable al exportar datos de referencia o elementos de contenido que dependen de datos de referencia.
-g o bien **--global-view**	Incluye datos acumulados en la exportación.
-i *[identificador_contenido]* o bien **--id** *[identificador_contenido]*	Especifica el identificador de una instancia específica de contenido personalizado como, por ejemplo, un informe único o un conjunto de referencia único. Puede especificar *all* para exportar todo el contenido del tipo especificado.
-o *[vía_acceso_archivo]* o bien **--output-directory** *[vía_acceso_archivo]*	Especifica la vía de acceso completa al directorio donde se graba el archivo de exportación. Si no se especifica un directorio de salida, el contenido se exporta al directorio actual. Si el directorio de salida especificado no existe, se crea.
-t *[tipo_compresión]* o bien **--compression-type** *[tipo_compresión]*	Especifica el tipo de compresión del archivo de exportación. Las opciones válidas son `ZIP` y `TARGZ` (sensible a mayúsculas y minúsculas). Si no especifica un tipo de compresión, el tipo de compresión predeterminado es `ZIP`.

Ejemplos:

- Para exportar todas las búsquedas personalizadas, escriba el mandato siguiente:

  ```
  ./contentManagement.pl --action export --content-type search --id all
  ```

- Para exportar todos los informes e incluir datos acumulados, escriba el mandato siguiente:

  ```
  ./contentManagement.pl -a export -c 10 --id all --global-view
  ```

Resultados

El contenido se exporta a un archivo comprimido, por ejemplo, `reports-ContentExport-20151022101803.zip`. Puede cambiar manualmente el nombre de archivo por un nombre más descriptivo. El archivo exportado podría contener más elementos de contenido de lo que se esperaba, porque todas las dependencias se exportan con los elementos de contenido especificados. Por ejemplo, si exporta un informe, también se exporta la búsqueda guardada que el informe utiliza.

Búsqueda de elementos de contenido específicos para exportar

El script de gestión de contenido se utiliza para buscar contenido específico en el despliegue de IBM Security QRadar. Tras encontrar el contenido, puede utilizar el identificador exclusivo para exportar el elemento de contenido.

Acerca de esta tarea

En la tabla siguiente se enumeran los identificadores utilizados cuando se desea buscar tipos específicos de contenido.

Tabla 75. Identificadores de tipo de contenido para la búsqueda de contenido personalizado

Tipo de contenido personalizado	Identificador de texto	Identificador numérico
Paneles de control	**dashboard**	4
Informes	**report**	10
Búsquedas guardadas	**search**	1
FGroups [1]	**fgroup**	12
Tipos de FGroup	**fgrouptype**	13
Reglas personalizadas	**customrule**	3
Propiedades personalizadas	**customproperty**	6
Orígenes de registro	**sensordevice**	17
Tipos de origen de registro	**sensordevicetype**	24
Categorías de origen de registro	**sensordevicecategory**	18
Extensiones de origen de registro	**deviceextension**	16
Recopilaciones de datos de referencia	**referencedata**	28
Entradas de correlaciones de QID personalizadas	**qidmap**	27
Perfiles de correlación histórica	**historicalsearch**	25
Funciones personalizadas	**custom_function**	77
Acciones personalizadas	**custom_action**	78
Aplicaciones	**installed_application**	100

[1]Un FGroup representa un grupo de contenido, como por ejemplo un grupo de origen de registro, un grupo de informes o un grupo de búsqueda.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Vaya al directorio `/opt/qradar/bin` y escriba el mandato siguiente para buscar contenido personalizado que coincida con una expresión regular:

   `./contentManagement.pl -a search -c [tipo_contenido] -r [regex]`

   Parámetros:

Tabla 76. Parámetros del script `contentManagement.pl` para la búsqueda de elementos de contenido

Parámetro	Descripción
-c *[tipo_contenido]* o bien **--content-type** *[tipo_contenido]*	Especifica el tipo de contenido que debe buscarse. Debe especificar el tipo de contenido que debe buscarse. No se puede utilizar `-c package` o `-c all` con la acción `search`.
-r *[regex]* o bien **--regex** *[regex]*	Especifica contenido que debe buscarse. Se visualizará todo el contenido coincidente con la expresión.

   Ejemplos:

   - Para buscar todos los informes que incluyan `Overview` en la descripción, escriba el mandato siguiente:

     ```
     /opt/qradar/bin/contentManagement.pl --action search
     --content-type report --regex "Overview"
     ```

   - Para listar todos los orígenes de registro, escriba el mandato siguiente:

     ```
     /opt/qradar/bin/contentManagement.pl -a search -c 17 -r "\w"
     ```

   Los resultados de la búsqueda listan los detalles, que incluyen el ID exclusivo, de los elementos de contenido encontrados.

```
[INFO] Resultados de búsqueda:
[INFO] - [ID] - [Nombre] - [Descripción]
[INFO] - [67] - [Asset Profiler-2 :: hostname] - [Asset Profiler]
[INFO] - [62] - [SIM Generic Log DSM-7 :: hostname] - [SIM Generic Log DSM]
[INFO] - [63] - [Custom Rule Engine-8 :: hostname] - [Custom Rule Engine]
[INFO] - [71] - [Pix @ apophis] - [Pix device]
[INFO] - [70] - [Snort @ wolverine] - [Snort device]
[INFO] - [64] - [SIM Audit-2 :: hostname] - [SIM Audit]
[INFO] - [69] - [Health Metrics-2 :: hostname] - [Health Metrics]
```

Qué hacer a continuación

Utilice el identificador exclusivo para exportar elementos de contenido específicos desde QRadar. Para obtener más información, consulte los apartados “Exportación de elementos de contenido personalizado de tipos diferentes” en la página 254 y “Exportación de un solo elemento de contenido personalizado”.

Exportación de un solo elemento de contenido personalizado

Exporte un solo elemento de contenido personalizado como, por ejemplo, una regla personalizada o una búsqueda guardada, desde IBM Security QRadar.

Antes de empezar

Debe conocer el identificador exclusivo del elemento de contenido personalizado que desea exportar. Para obtener información sobre cómo encontrar los identificadores exclusivos de los elementos de contenido, consulte "Búsqueda de elementos de contenido específicos para exportar" en la página 251.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Vaya al directorio `/opt/qradar/bin` y escriba el mandato para exportar el contenido:

   `./contentManagement.pl -a export -c` *`[tipo_contenido]`* `-i` *`[identificador_contenido]`*

   Parámetros:

Tabla 77. Parámetros del script `contentManagement.pl` para exportar un único elemento de contenido

Parámetro	Descripción
-c *[tipo_contenido]* o bien **--content-type** *[tipo_contenido]*	Especifica el tipo de contenido a exportar. Especifique el identificador de texto o el identificador numérico correspondiente para tipos de contenido específicos.
-e o bien **--include-reference-data-elements**	Establezca este distintivo para incluir elementos y claves de datos de referencia en la exportación. Las claves de datos de referencia y los elementos de datos de referencia son aplicables al tipo de contenido `referencedata`. Este parámetro sólo es aplicable al exportar datos de referencia o elementos de contenido que dependen de datos de referencia.
-g o bien **--global-view**	Incluye datos acumulados en la exportación.
-i *[identificador_contenido]* o bien **--id** *[identificador_contenido]*	Especifica el identificador de una instancia específica de contenido personalizado como, por ejemplo, un informe único o un conjunto de referencia único.
-o *[vía_acceso_archivo]* o bien **--output-directory** *[vía_acceso_archivo]*	Especifica la vía de acceso completa al directorio donde se graba el archivo de exportación. Si no se especifica un directorio de salida, el contenido se exporta al directorio actual. Si el directorio de salida especificado no existe, se crea.
-t *[tipo_compresión]* o bien **--compression-type** *[tipo_compresión]*	Se utiliza con la acción `export`. Especifica el tipo de compresión del archivo de exportación. Las opciones válidas son `ZIP` y `TARGZ` (sensible a mayúsculas y minúsculas). Si no especifica un tipo de compresión, el tipo de compresión predeterminado es `ZIP`.

Ejemplos:

- Para exportar el panel de control que tiene el ID 7 en el directorio actual, escriba el mandato siguiente:

  ```
  ./contentManagement.pl -a export -c dashboard -i 7
  ```

- Para exportar el origen de registro que tiene el ID 70, incluidos los datos acumulados, en el directorio `/store/cmt/exports`, escriba el mandato siguiente:

  ```
  ./contentManagement.pl -a export -c sensordevice -i 70 -o /store/cmt/exports -g
  ```

Resultados

El contenido se exporta a un archivo `.zip` comprimido. El archivo exportado podría contener más elementos de contenido de lo que se esperaba, porque todas las dependencias se exportan con los elementos de contenido especificados. Por ejemplo, si exporta un informe, también se exporta la búsqueda guardada que el informe utiliza. Puede cambiar manualmente el nombre de archivo por un nombre más descriptivo.

Exportación de elementos de contenido personalizado de tipos diferentes

Exporte varios elementos de contenido personalizado desde IBM Security QRadar, como por ejemplo reglas personalizadas o paneles de control e informes, mediante el script de gestión de contenido.

Antes de empezar

Debe conocer los identificadores exclusivos de cada elemento de contenido personalizado que desea exportar. Para obtener información sobre cómo encontrar los identificadores exclusivos de los elementos de contenido, consulte "Búsqueda de elementos de contenido específicos para exportar" en la página 251.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Cree un archivo de texto que enumere el contenido que desea exportar.

   Cada línea debe incluir el tipo de contenido personalizado, seguido de una lista de ID exclusivos separados por comas para ese tipo.

   Ejemplo: Para exportar dos paneles de control que tienen el ID 5 y el ID 7, todas las reglas personalizadas y un grupo, cree un archivo de texto que tenga las entradas siguientes:

   ```
   dashboard, 5,7
   customrule, all
   fgroup, 77
   ```

3. Vaya a `/opt/qradar/bin` y escriba el mandato para exportar el contenido:

   ```
   ./contentManagement.pl -a export -c package -f [archivo_origen]
   ```

   Parámetros:

Tabla 78. Parámetros del script `contentManagement.pl` para exportar diferentes tipos de elementos de contenido

Parámetro	Descripción
-c *[tipo_contenido]* o bien **--content-type** *[tipo_contenido]*	Especifica el tipo de contenido. Puede especificar `-c package` o especificar el texto o el identificador numérico correspondiente a tipos de contenido específicos. Si utiliza `-c package`, debe especificar los parámetros `--file` o `--name`.
-e o bien **--include-reference-data-elements**	Establezca este distintivo para incluir elementos y claves de datos de referencia en la exportación. Las claves de datos de referencia y los elementos de datos de referencia son aplicables al tipo de contenido `referencedata`. Este parámetro sólo es aplicable al exportar datos de referencia o elementos de contenido que dependen de datos de referencia.
-f *[archivo_origen]* o bien **--file** *[archivo_origen]*	Especifica la vía de acceso y el nombre del archivo de paquete que contiene los elementos de contenido personalizado que desea exportar. La primera vez que se utiliza el parámetro `--file`, se graba un archivo de plantilla de paquete en el directorio `/store/cmt/packages` para que pueda reutilizarlo. El nombre de archivo y la vía de acceso son sensibles a las mayúsculas y minúsculas.
-g o bien **--global-view**	Incluye datos acumulados en la exportación.
-n *[nombre]* o bien **--name** *[nombre]*	Especifica el nombre del archivo de plantilla de paquete que contiene la lista de contenido personalizado a exportar. El archivo de plantilla de paquete se crea la primera vez que se utiliza el parámetro `--file`. De forma predeterminada, el parámetro `--name` presupone que el archivo de texto se encuentra en el directorio `/store/cmt/packages`. Debe especificar los parámetros `--file` o `--name` si se utiliza `--content-type package`.
-o *[vía_acceso_archivo]* o bien **--output-directory** *[vía_acceso_archivo]*	Especifica la vía de acceso completa al directorio donde se graba el archivo de exportación. Si no se especifica un directorio de salida, el contenido se exporta al directorio actual. Si el directorio de salida especificado no existe, se crea.
-t *[tipo_compresión]* o bien **--compression-type** *[tipo_compresión]*	Especifica el tipo de compresión del archivo de exportación. Los tipos de compresión válidos son `ZIP` y `TARGZ` (sensible a mayúsculas y minúsculas). Si no especifica un tipo de compresión, el tipo de compresión predeterminado es `ZIP`.

Ejemplos:

- Para exportar todos los elementos del archivo `exportlist.txt` del directorio `qradar` y guardar el archivo exportado en el directorio actual, escriba el mandato siguiente:

  ```
  ./contentManagement.pl -a export -c package -f /qradar/exportlist.txt
  ```

- Para exportar todos los elementos del archivo `exportlist.txt` del directorio `qradar`, incluidos los datos acumulados, y guardar la salida en el directorio `/store/cmt/exports`, escriba el mandato siguiente:

  ```
  ./contentManagement.pl -a export -c package
  --file /qradar/exportlist.txt -o /store/cmt/exports -g
  ```

Cuando se utiliza el parámetro **`--file`**, un archivo de plantilla de paquete se genera en `/store/cmt/packages`. Para utilizar el archivo de plantilla de paquete, especifique el nombre de archivo como el valor del parámetro **`--name`**.

Resultados

El contenido se exporta a un archivo comprimido `.zip`. El archivo exportado podría contener más elementos de contenido de lo que se esperaba, porque todas las dependencias se exportan con los elementos de contenido especificados. Por ejemplo, si exporta un informe, también se exporta la búsqueda guardada que el informe utiliza. Puede cambiar manualmente el nombre de archivo por un nombre más descriptivo.

Instalación de extensiones mediante la Gestión de extensiones

Utilice la herramienta Gestión de extensiones para añadir extensiones de seguridad a IBM Security QRadar. La herramienta Gestión de extensiones le permite ver los elementos de contenido de la extensión y especificar el método de manejo de las actualizaciones de contenido antes de instalar la extensión.

Antes de empezar

Las extensiones deben estar en el sistema local antes de instalarlas en QRadar.

Puede descargar extensiones de QRadar desde IBM Security App Exchange (https://apps.xforce.ibmcloud.com/) y desde IBM Fix Central (www.ibm.com/support/fixcentral/).

Acerca de esta tarea

Una extensión es un paquete de funciones de QRadar. Una extensión puede incluir contenido como reglas, informes, búsquedas, conjuntos de referencia y paneles de control. También puede incluir aplicaciones que mejoran la funcionalidad de QRadar.

Procedimiento

1. En la pestaña **Admin**, pulse **Gestión de extensiones**.
2. Para cargar una nueva extensión en la consola de QRadar, siga estos pasos:
   a. Pulse **Añadir**.
   b. Pulse **Examinar** y busque la extensión.

c. Opcional: Pulse **Instalar inmediatamente** para instalar la extensión sin visualizar el contenido.
d. Pulse **Añadir**.

3. Para ver el contenido de la extensión, selecciónela en la lista de extensiones y pulse **Más detalles**.
4. Para instalar la extensión, siga estos pasos:
   a. Seleccione la extensión en la lista y pulse **Instalar**.
   b. Si la extensión no incluye una firma digital, o si está firmada, pero la firma no está asociado con la Autoridad de certificación (CA) de IBM Security), debe confirmar que sigue deseando instalarla. Pulse **Instalar** para continuar con la instalación.
   c. Revise los cambios realizados por la instalación en el sistema.
   d. Seleccione **Sobrescribir** o **Conservar datos existentes** para especificar cómo deben manejarse los elementos de contenido existentes.
   e. Pulse **Instalar**.
   f. Revise el resumen de instalación y pulse **Aceptar**.

Importación de contenido mediante el script de gestión de contenido

Puede importar contenido personalizado exportado de otro sistema QRadar.

Antes de empezar

Si desea importar contenido de otro sistema de QRadar, primero debe exportar el contenido y copiarlo en el sistema de destino. Para obtener más información sobre la exportación de contenido, consulte la sección "Identificadores de tipo de contenido para exportar contenido personalizado" en la página 259.

Cuando importe contenido que tengan orígenes de registro, confirme que DSM y los RPM de protocolo están instalados y actualizados en el sistema de destino.

No inicie varias importaciones en el mismo sistema al mismo tiempo. Las importaciones fallarán debido a conflictos con los recursos compartidos.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Vaya al directorio donde se encuentra el archivo de contenido de exportación.
3. Escriba este mandato para importar el contenido:

   ```
   /opt/qradar/bin/contentManagement.pl -a import -f [archivo_origen] -u [usuario]
   ```

   Parámetros:

Tabla 79. Parámetros del script `contentManagement.pl` para la importación de contenido personalizado

Parámetro	Descripción
-f *[archivo_origen]* o bien **--file** *[archivo_origen]*	Especifica el archivo que contiene los elementos de contenido que deben importarse. Los tipos de archivo válidos son `zip`, `targz` y `xml`. El nombre de archivo y la vía de acceso son sensibles a las mayúsculas y minúsculas.

Tabla 79. Parámetros del script `contentManagement.pl` para la importación de contenido personalizado (continuación)

Parámetro	Descripción
-u *[usuario]* o bien **--user** *[usuario]*	Especifica el usuario que sustituye al propietario actual al importar datos específicos de usuario. El usuario debe existir en el sistema de destino antes de importar el contenido.

Ejemplos:

- Para importar el contenido del archivo `fgroup-ContentExport-20120418163707.tar.gz` en el directorio actual, escriba el mandato siguiente:

  ```
  /opt/qradar/bin/contentManagement.pl --action import
  -f fgroup-ContentExport-20120418163707.tar.gz
  ```

- Para importar el contenido del archivo `fgroup-ContentExport-20120418163707.tar.gz` en el directorio actual y hacer que el usuario admin sea el propietario de todos los datos confidenciales de la importación, escriba el mandato siguiente:

  ```
  /opt/qradar/bin/contentManagement.pl --action import
  --file fgroup-ContentExport-20120418163707.tar.gz --user admin
  ```

El script de importación muestra el siguiente mensaje cuando se recopilan activamente datos de referencia durante la exportación: `Violación de restricción de clave foránea`. Para evitar este problema, ejecute el proceso de exportación cuando no se estén recopilando datos de referencia.

Actualización del contenido mediante el script de gestión de contenido

Utilice la acción de actualización para actualizar el contenido existente de IBM Security QRadar o añadir contenido nuevo al sistema.

Antes de empezar

Si desea actualizar el contenido con contenido que se ha exportado desde otro sistema de QRadar, asegúrese de que el archivo exportado se encuentra en el sistema de destino. Para obtener más información sobre la exportación de contenido, consulte la sección "Identificadores de tipo de contenido para exportar contenido personalizado" en la página 259.

Cuando importe contenido que tengan orígenes de registro, confirme que DSM y los RPM de protocolo están instalados y actualizados en el sistema de destino.

No inicie varias importaciones en el mismo sistema al mismo tiempo. Las importaciones fallarán debido a conflictos con los recursos compartidos.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Para actualizar el contenido, escriba el mandato siguiente:

   ```
   /opt/qradar/bin/contentManagement.pl -a update -f [archivo_origen]
   ```

   Parámetros:

Tabla 80. Parámetros del script `contentManagement.pl` para la actualización de contenido personalizado

Parámetro	Descripción
-f *[archivo_origen]* o bien **--file** *[archivo_origen]*	Especifica el archivo que contiene los elementos de contenido que deben actualizarse. Los tipos de archivo válidos son `zip`, `targz` y `xml`. El nombre de archivo y la vía de acceso son sensibles a las mayúsculas y minúsculas.
-u *[usuario]* o bien **--user** *[usuario]*	Especifica el usuario que sustituye al propietario actual al importar datos específicos de usuario. El usuario debe existir en el sistema de destino antes de importar el contenido.

Ejemplo:

- Para realizar una actualización basada en el contenido del archivo `fgroup-ContentExport-20120418163707.zip`, especifique el mandato siguiente:

```
/opt/qradar/bin/contentManagement.pl --action update
-f fgroup-ContentExport-20120418163707.zip
```

Identificadores de tipo de contenido para exportar contenido personalizado

Al exportar un tipo específico de contenido personalizado de IBM Security QRadar, debe especificar el tipo de contenido. Debe utilizar el identificador de texto o el identificador numérico del tipo de contenido.

Al exportar contenido desde un dispositivo de QRadar, el script de gestión de contenido comprueba las dependencias del contenido y después incluye el contenido asociado en la exportación.

Por ejemplo, cuando el script de gestión de contenido detecta que una búsqueda guardada está asociada con un informe que desea exportar, la búsqueda guardada también se exporta. No puede exportar búsquedas guardadas de delito, activo o vulnerabilidad.

Debe utilizar el identificador de tipo de contenido cuando desee exportar todo el contenido personalizado de un tipo específico. Si desea exportar un elemento de contenido específico del despliegue de QRadar, debe conocer el identificador exclusivo de dicho elemento de contenido específico. Para obtener más información, consulte el documento "Búsqueda de elementos de contenido específicos para exportar" en la página 251.

La tabla siguiente describe los identificadores de tipo de contenido que se pasan al script `contentManagement.pl` para el parámetro **-c**.

Tabla 81. Identificadores de tipo de contenido para exportar contenido personalizado

Tipo de contenido personalizado	Identificador de texto	Identificador numérico
Todo el contenido personalizado	**all**	No aplicable

Tabla 81. Identificadores de tipo de contenido para exportar contenido personalizado (continuación)

Tipo de contenido personalizado	Identificador de texto	Identificador numérico
Lista de contenido personalizado	**package**	No aplicable
Paneles de control	**dashboard**	4
Informes	**report**	10
Búsquedas guardadas	**search**	1
FGroups [1]	**fgroup**	12
Tipos de FGroup	**fgrouptype**	13
Reglas personalizadas	**customrule**	3
Propiedades personalizadas	**customproperty**	6
Orígenes de registro	**sensordevice**	17
Tipos de origen de registro	**sensordevicetype**	24
Categorías de origen de registro	**sensordevicecategory**	18
Extensiones de origen de registro	**deviceextension**	16
Recopilaciones de datos de referencia	**referencedata**	28
Entradas de correlaciones de QID personalizadas	**qidmap**	27
Perfiles de correlación histórica	**historicalsearch**	25
Funciones personalizadas	**custom_function**	77
Acciones personalizadas	**custom_action**	78
Aplicaciones	**installed_application**	100

[1]Un FGroup es un grupo de contenido, como por ejemplo un grupo de orígenes de registro, un grupo de informes o un grupo de búsqueda.

Parámetros del script de gestión de contenidos

Utilice el script `contentManagement.pl` para exportar contenido de un despliegue de IBM Security QRadar e importarlo en otro despliegue.

La tabla siguiente describe los parámetros del script `contentManagement.pl` y las acciones a las que se aplica cada parámetro.

`/opt/qradar/bin/contentManagement.pl --action` *`[tipo_acción] [parámetros_script]`*

Tabla 82. Parámetros del script `contentManagement.pl`

Parámetro	Descripción
-a *[tipo_acción]* o bien **--action** *[tipo_acción]*	Obligatorio. Especifica la acción. Los tipos de acción válidos son `export`, `search`, `import` y `update`. La acción `import` añade sólo contenido que no existe en el despliegue.

Tabla 82. Parámetros del script `contentManagement.pl` (continuación)

Parámetro	Descripción
-c *[tipo_contenido]* o bien **--content-type** *[tipo_contenido]*	Se utiliza con las acciones `export` y `search`. Especifica el tipo de contenido. Cuando se utiliza con la acción `export`, puede especificar `-c all` o `-c package`, o especificar el texto o el identificador numérico correspondiente a tipos de contenido específicos. Si utiliza `-c package`, debe especificar los parámetros `--file` o `--name`. Si se utiliza con la acción `search`, debe especificar el tipo de contenido que debe buscarse. No se puede utilizar `-c package` o `-c all` con la acción `search`.
-d o bien **--debug**	Se utiliza con todas las acciones. Utilice el registro de nivel de depuración ejecute el script `contentManagement.pl` para ver información más detallada, como los registros de soporte al cliente.
-e o bien **--include-reference-data-elements**	Se utiliza con la acción `export`. Establezca este distintivo para incluir elementos y claves de datos de referencia en la exportación. Las claves de datos de referencia y los elementos de datos de referencia son aplicables al tipo de contenido `referencedata`. Este parámetro sólo es aplicable al exportar datos de referencia o elementos de contenido que dependen de datos de referencia.
-f *[vía_acceso_archivo]* o bien **--file** *[vía_acceso_archivo]*	Se utiliza con las acciones `export`, `import` y `update`. Cuando se utiliza con la acción `export`, especifica la vía de acceso y el nombre del archivo de texto que contiene la lista de elementos de contenido personalizado que desea exportar. La primera vez que se utiliza el parámetro `--file`, se graba un archivo de plantilla de paquete en el directorio `/store/cmt/packages` para que pueda reutilizarlo. Cuando se utiliza con las acciones `import` o `update`, especifica el archivo que contiene los elementos de contenido que deben importarse. Los tipos de archivo válidos son `zip`, `targz` y `xml`. El nombre de archivo y la vía de acceso son sensibles a las mayúsculas y minúsculas.
-g o bien **--global-view**	Se utiliza con la acción `export`. Incluye datos acumulados en la exportación.

Tabla 82. Parámetros del script `contentManagement.pl` (continuación)

Parámetro	Descripción
-h *[tipo_acción]* o bien **--help** *[tipo_acción]*	Se utiliza con todas las acciones. Muestra ayuda específica del `tipo_acción`. Si no se especifica ningún `tipo_acción`, muestra un mensaje de ayuda general.
-i *[identificador_contenido]* o bien **--id** *[identificador_contenido]*	Se utiliza con la acción `export`. Especifica el identificador de una instancia específica de contenido personalizado como, por ejemplo, un informe único o un conjunto de referencia único. Puede especificar *all* para exportar todo el contenido del tipo especificado.
-n *[nombre]* o bien **--name** *[nombre]*	Se utiliza con la acción `export`. Especifica el nombre del archivo de plantilla de paquete que contiene la lista de contenido personalizado a exportar. El archivo de plantilla de paquete se crea la primera vez que se utiliza el parámetro `--file`. El parámetro `--name` presupone que el archivo de plantilla de paquete está en el directorio `/store/cmt/packages`. Debe especificar los parámetros `--file` o `--name` si se utiliza `--content-type package`.
-o *[vía_acceso_archivo]* o bien **--output-directory** *[vía_acceso_archivo]*	Se utiliza con la acción `export`. Especifica la vía de acceso completa al directorio donde se graba el archivo de exportación. Si no se especifica un directorio de salida, el contenido se exporta al directorio actual. Si el directorio de salida especificado no existe, se crea.
-q o bien **--quiet**	Se utiliza con todas las acciones. No aparece ninguna salida en pantalla.
-r *[regex]* o bien **--regex** *[regex]*	Se utiliza con la acción `search`. Al realizar la búsqueda, debe utilizar el parámetro `--regex` para especificar el contenido que desea buscar. Se visualizará todo el contenido coincidente con la expresión.
-t *[tipo_compresión]* o bien **--compression-type** *[tipo_compresión]*	Se utiliza con la acción `export`. Especifica el tipo de compresión del archivo de exportación. Los tipos de compresión válidos son `ZIP` y `TARGZ` (sensible a mayúsculas y minúsculas). Si no especifica un tipo de compresión, el tipo de compresión predeterminado es `ZIP`.

Tabla 82. Parámetros del script `contentManagement.pl` (continuación)

Parámetro	Descripción
-u *[usuario]* o bien **--user** *[usuario]*	Se utiliza con la acción `import`. Especifica el usuario que sustituye al propietario actual al importar datos específicos de usuario. El usuario debe existir en el sistema de destino antes de importar el contenido.
-v o bien **--verbose**	Se utiliza con todas las acciones. Se utiliza cuando se inicia la sesión para ver información de nivel predeterminado para la herramienta de gestión de contenido.

Capítulo 21. Configuración de condiciones de excepción de SNMP

En IBM Security QRadar, puede configurar una regla para generar una respuesta de regla que envíe una condición de excepción de SNMP cuando se cumplen las condiciones configuradas. QRadar actúa como agente para enviar las condiciones de excepción de SNMP a otro sistema.

Una excepción de SNMP (protocolo simple de gestión de red) es una notificación de un suceso o un delito que QRadar envía a un host SNMP configurado para efectuar un proceso adicional.

Personalice los parámetros de configuración de SNMP en el asistente de reglas personalizadas y modifique las condiciones de excepción de SNMP que el motor de reglas personalizadas envía a otro software para su gestión. QRadar proporciona dos condiciones de excepción predeterminadas. Sin embargo, puede añadir condiciones de excepción personalizadas o modificar las condiciones de excepción existentes para utilizar nuevos parámetros.

Para obtener más información sobre SNMP, consulte el sitio web The Internet Engineering Task Force (http://www.ietf.org/) y escriba `RFC 1157` en el campo de búsqueda.

Personalización de la información de condiciones de excepción de SNMP enviada a otro sistema

En IBM Security QRadar, puede editar los parámetros de condición de excepción de SNMP para personalizar la información que se envía a otro sistema de gestión de SNMP cuando una condición de regla se cumple.

Restricción: Los parámetros de condición de excepción de SNMP se visualizan en el asistente de reglas personalizadas únicamente si SNMP está habilitado en los valores del sistema de QRadar.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Vaya al directorio `/opt/qradar/conf` y realice copias de seguridad de los archivos siguientes:
   - `eventCRE.snmp.xml`
   - `offenseCRE.snmp.xml`
3. Abra el archivo de configuración para su edición.
   - Para editar los parámetros de SNMP para las reglas de suceso, abra el archivo `eventCRE.snmp.xml`.
   - Para editar los parámetros de SNMP para las reglas de delito, abra el archivo `offenseCRE.snmp.xml`.
4. Dentro del elemento <snmp> y antes del elemento <creSNMPTrap>, inserte la siguiente sección, actualizando las etiquetas como sea necesario:

```
<creSNMPResponse name="snmp_response_1">
  <custom name="MyColor">
    <string label="What is your favorite color?"/>
```

© Copyright IBM Corp. 2012, 2015

```
</custom>
  <custom name="MyCategory">
    <list label="Select a category">
      <option label="Label1" value="Category1"/>
      <option label="Label2" value="Category2"/>
    </list>
  </custom>
</creSNMPResponse>
```

5. Guarde y cierre el archivo.
6. Copie el archivo del directorio `/opt/qradar/conf` en el directorio `/store/configservices/staging/globalconfig`.
7. Inicie la sesión en la interfaz de QRadar.
8. En la pestaña **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.

   Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Qué hacer a continuación

Personalice la salida de condiciones de excepción de SNMP.

Personalización de la salida de las condiciones de excepción de SNMP

IBM Security QRadar utiliza SNMP para enviar condiciones de excepción que proporcionan información cuando se cumplen las condiciones de las reglas.

De forma predeterminada, QRadar utiliza la MIB (Management Information Base) de QRadar para gestionar los dispositivos de la red de comunicaciones. Sin embargo, puede personalizar la salida de las condiciones de excepción de SNMP para adherirse a otra MIB.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Vaya al directorio `/opt/qradar/conf` y realice copias de seguridad de los archivos siguientes:
   - `eventCRE.snmp.xml`
   - `offenseCRE.snmp.xml`
3. Abra el archivo de configuración para su edición.
   - Para editar los parámetros de SNMP para las reglas de suceso, abra el archivo `eventCRE.snmp.xml`.
   - Para editar los parámetros de SNMP para las reglas de delito, abra el archivo `offenseCRE.snmp.xml`.
4. Para cambiar la condición de excepción que se utiliza para la notificación de excepciones de SNMP, actualice el texto siguiente con el identificador de objeto de condición de excepción (OID) adecuado:

   ```
   -<creSNMPTrap version="3" OID="1.3.6.1.4.1.20212.1.1"
   name="eventCRENotification">
   ```

5. Utilice la tabla siguiente como ayuda para actualizar la información de enlace de variable:

   Cada enlace de variable asocia una instancia de objeto MIB determinada con su valor actual.

Tabla 83. Tipos de valores para el enlace de variable

Tipo de valor	Descripción	Ejemplo
`string`	Caracteres alfanuméricos Puede configurar varios valores.	
`integer32`	Valor numérico	`name="ATTACKER_PORT" type="integer32">%ATTACKER_PORT%`
`oid`	Cada condición de excepción de SNMP contiene un identificador que se asigna a un objeto dentro de la MIB	`OID="1.3.6.1.4.1.20212.2.46"`
`gauge32`	Rango de valores numéricos	
`counter64`	Valor numérico que se incrementa dentro de un rango de mínimo y máximo definido	

6. Para cada uno de los tipos de valores, incluya cualquiera de los campos siguientes:

Tabla 84. Campos para los enlaces de variable

Campo	Descripción	Ejemplo
`Native`	Para obtener más información sobre estos campos, consulte el archivo `/opt/qradar/conf/snmp.help`.	**Ejemplo:** [1]Si el tipo de valor es `ipAddress`, debe utilizar una variable que sea una dirección IP. El tipo de valor de serie (string) acepta cualquier formato.
`Custom`	Información de condición de excepción de SNMP personalizada que ha configurado para el asistente de reglas personalizadas	**Ejemplo:** [1]Si ha utilizado la información de archivo predeterminado y desea incluir esta información en la condición de excepción de SNMP, incluya el código siguiente: `<variableBinding name="My Color Variable Binding" OID="1.3.6.1.4.1.20212.3.1" type="string"> My favorite color is %MyColor%</variableBinding>`
[1]Encierre el nombre de campo con signos de porcentaje (%). Dentro de los signos de porcentaje, los campos deben coincidir con el tipo de valor.		

7. Guarde y cierre el archivo.
8. Copie el archivo del directorio `/opt/qradar/conf` en el directorio `/store/configservices/staging/globalconfig`.
9. Inicie la sesión en la interfaz de QRadar.
10. En la pestaña **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.

Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Adición de una condición de excepción de SNMP a QRadar

En los productos IBM Security QRadar, puede crear una nueva opción para la selección de condición de excepción de SNMP en el asistente de reglas personalizadas. Los nombres de condición de excepción que se especifican en el cuadro de lista están configurados en el archivo de configuración `snmp-master.xml`.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Vaya al directorio `/opt/qradar/conf`.
3. Cree un archivo de valores de SNMP para la nueva condición de excepción.

   Consejo: Copie, renombre y modifique uno de los archivos de valores de SNMP existentes.
4. Haga una copia de seguridad del archivo `snmp-master.xml`.
5. Abra el archivo `snmp-master.xml` para su edición.
6. Añada un nuevo elemento <include>.

   El elemento <include> tiene los siguientes atributos:

Tabla 85. Atributos del elemento <include>

Atributo	Descripción
`name`	Mostrado en el recuadro de lista
`uri`	Nombre del archivo de valores de SNMP personalizado

   Ejemplo:

   ```
   <include name="Custom_Event_Name" uri="customSNMPdef01.xml"/>
   ```

   Las condiciones de excepción se visualizan en el menú en el mismo orden en que están listadas en el archivo `snmp-master.xml`.
7. Guarde y cierre el archivo.
8. Copie el archivo del directorio `/opt/qradar/conf` en el directorio `/store/configservices/staging/globalconfig`.
9. Inicie la sesión en la interfaz de QRadar.
10. En la pestaña **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.

    Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Envío de condiciones de excepción de SNMP a un host específico

De forma predeterminada, en los productos de IBM Security QRadar, las condiciones de excepción de SNMP se envían al host que está identificado en el archivo `host.conf`. Puede personalizar el archivo `snmp.xml` para enviar las condiciones de excepción de SNMP a otro host.

Procedimiento

1. Utilice SSH para iniciar la sesión en QRadar como usuario root.
2. Vaya al directorio /opt/qradar/conf y realice copias de seguridad de los archivos siguientes:
   - eventCRE.snmp.xml
   - offenseCRE.snmp.xml
3. Abra el archivo de configuración para su edición.
   - Para editar los parámetros de SNMP para las reglas de suceso, abra el archivo eventCRE.snmp.xml.
   - Para editar los parámetros de SNMP para las reglas de delito, abra el archivo offenseCRE.snmp.xml.
4. Añada un solo elemento <trapConfig> en el elemento <snmp> dentro del elemento <creSNMPTrap> antes de cualquier otro elemento hijo.

```
<trapConfig>
  <!-- All attribute values are default -->
   <snmpHost snmpVersion="3" port="162" retries="2" timeout="500">HOST
   </snmpHost>
  <!-- Community String for Version 2 -->
   <communityString>COMMUNITY_STRING</communityString>
  <!-- authenticationProtocol (MD5 or SHA)securityLevel (AUTH_PRIV, AUTH_NOPRIV
  or NOAUTH_PRIV) -->
   <authentication authenticationProtocol="MD5"securityLevel="AUTH_PRIV">
    AUTH_PASSWORD
   </authentication>
  <!-- decryptionProtocol (DES, AES128, AES192 or AES256) -->
   <decryption decryptionProtocol="AES256">
     DECRYPTIONPASSWORD
   </decryption>
  <!-- SNMP USER-->
   <user> SNMP_USER </user>
 </trapConfig>
```

5. Utilice la tabla siguiente como ayuda para actualizar los atributos.

Tabla 86. Valores de atributo para actualizar en el elemento <trapConfig>

Elemento	Descripción
</snmpHost>	Nuevo host al que desea enviar las condiciones de excepción de SNMP. El valor del atributo snmpVersion para <snmpHost> debe ser 2 ó 3.
<communityString>	Serie de comunidad para el host
<authentication>	Protocolo de autenticación, nivel de seguridad y contraseña para el host.
<decryption>	Protocolo de descifrado y contraseña para el host.
<usuario>	Usuario de SNMP

6. Guarde y cierre el archivo.
7. Copie el archivo del directorio /opt/qradar/conf en el directorio /store/configservices/staging/globalconfig.
8. Inicie la sesión en la interfaz de QRadar.
9. En la pestaña **Admin**, seleccione **Avanzado** > **Desplegar configuración completa**.

Cuando despliega la configuración completa, QRadar reinicia todos los servicios. La recopilación de datos para sucesos y flujos se detiene hasta que finaliza el despliegue.

Capítulo 22. Ofuscación de datos para protección de datos confidenciales

Puede configurar un perfil de ofuscación de datos para impedir el acceso no autorizado a información confidencial o que permita identificar a usuarios en IBM Security QRadar.

Ofuscación de datos es el proceso de ocultar estratégicamente datos de los usuarios de QRadar. Puede ocultar propiedades personalizadas, propiedades normalizadas, como por ejemplo los nombres de usuario, o puede ocultar el contenido de una carga útil, como por ejemplo los números de tarjeta de crédito y de la seguridad social.

Las expresiones del perfil de ofuscación de datos se evalúan contra las propiedades de carga útil y normalizadas. Si los datos coinciden con la expresión de ofuscación, se ocultan en QRadar. Los usuarios que intentan consultar la base de datos directamente no pueden ver los datos sensibles. Los datos deben devolverse a su formato original, o *desofuscarse*, cargando la clave privada que se ha generado al crear el perfil de ofuscación de datos.

Para garantizar que QRadar pueda seguir correlacionado los valores de datos ocultos, el proceso de ofuscación es determinista. Visualiza el mismo conjunto de caracteres cada vez que se encuentra el valor de datos.

¿Cómo funciona la ofuscación de datos?

Antes de configurar la ofuscación de datos en el despliegue de IBM Security QRadar, debe entender cómo funciona para delitos, activos, reglas y extensiones de origen de registro nuevos y existentes.

Datos de suceso existentes

Cuando un perfil de ofuscación de datos está habilitado, el sistema enmascara los datos de cada suceso conforme QRadar los recibe. Los sucesos recibidos por el dispositivo antes de la configuración de la ofuscación de datos permanecen en el estado no ofuscado original. Los datos de suceso más antiguos no se enmascaran y los usuarios pueden ver la información.

Activos

Cuando la ofuscación de datos está configurada, el modelo de activo acumula datos enmascarados mientras los datos de modelo de activo preexistente permanecen enmascarados.

Para impedir que alguien utilice datos enmascarados para rastrear la información ofuscada, depure los datos de modelo de activo para eliminar los datos enmascarados. QRadar repoblará las bases de datos activos con valores ofuscados.

Delitos

Para asegurarse de que los delitos no visualicen datos enmascarados previamente, cierre todos los delitos existentes restableciendo el modelo SIM. Para obtener más

© Copyright IBM Corp. 2012, 2015

información, consulte el documento “Restablecimiento de SIM” en la página 7.

Reglas

Debe actualizar reglas que dependen de datos enmascarados anteriormente. Por ejemplo, las reglas basadas en un nombre de usuario no se activan cuando el nombre de usuario está ofuscado.

Extensiones de origen de registro

Las extensiones de origen de registro que cambian el formato de la carga útil de suceso pueden provocar problemas con la ofuscación de datos.

Perfiles de ofuscación de datos

El perfil de ofuscación de datos contiene información sobre qué datos enmascarar. También hace un seguimiento del almacén de claves necesario para descifrar los datos.

Perfiles habilitados

Habilite un perfil solo cuando esté seguro de que las expresiones se dirigen correctamente a los datos que desea ofuscar. Si desea probar la expresión regular antes de habilitar el perfil de ofuscación de datos, puede crear una propiedad personalizada basada en regex.

Un perfil habilitado empieza inmediatamente a ofuscar datos según la definición de las expresiones habilitadas en el perfil. El perfil habilitado queda automáticamente bloqueado. Solo el usuario que tiene la clave privada puede inhabilitar o cambiar el perfil una vez que éste se ha habilitado.

Para garantizar que los datos ocultos puedan volver a rastrearse en un perfil de ofuscación, no puede suprimir un perfil habilitado, incluso aunque lo inhabilite.

Perfiles bloqueados

Un perfil queda automáticamente bloqueado cuando lo habilita o puede bloquearlo manualmente.

Un perfil bloqueado tiene las restricciones siguientes:

- No puede editarlo.
- No puede habilitarlo o inhabilitarlo. Debe proporcionar el almacén de claves y desbloquear el perfil para poder cambiarlo.
- No puede suprimirlo, incluso después de haberlo desbloqueado.
- Si se utiliza un almacén de claves con un perfil bloqueado, el resto de perfiles que utilizan el almacén de claves se bloquea automáticamente.

La tabla siguiente muestra ejemplos de perfiles bloqueados o desbloqueados:

Tabla 87. Ejemplos de perfil bloqueado

Escenario	Resultado
El perfil A está bloqueado. Se creó mediante el almacén de claves A. El perfil B también se creó mediante el almacén de claves A.	El perfil B queda automáticamente bloqueado.

Tabla 87. Ejemplos de perfil bloqueado (continuación)

Escenario	Resultado
El perfil A se ha creado y habilitado.	El perfil A queda automáticamente bloqueado.
El perfil A, el perfil B y el perfil C están actualmente bloqueados. Todos se crearon mediante el almacén de claves A. El perfil B está seleccionado y se pulsa **Bloquear/desbloquear**.	El perfil A, el perfil B y el perfil C quedan todos desbloqueados.

Expresiones de ofuscación de datos

Las expresiones de ofuscación de datos identifican los datos a ocultar. Puede crear expresiones de ofuscación de datos basadas en propiedades basadas en campo o utilizar expresiones regulares.

Propiedades basadas en campo

Utilice una propiedad basada en campo para ocultar nombres de usuario, nombres de grupo y nombres de NetBIOS. Las expresiones que utilizan propiedades basadas en campo ofuscan todas las instancias de la serie de datos. Los datos se ocultan independientemente de su origen de datos, el tipo de origen de registro, el nombre de suceso o la categoría de suceso.

Si el mismo valor de datos está presente en más de uno de los campos, los datos se ofuscan en todos los campos que los contienen, incluso si ha configurado el perfil para ofuscar solo uno de los cuatro campos. Por ejemplo, si tiene un host denominado `IBMHost` y un grupo denominado `IBMHost`, el valor `IBMHost` se oculta tanto en el campo de nombre de host como en el campo de nombre de grupo aunque el perfil de ofuscación de datos esté configurado para ocultar sólo nombres de host.

Expresiones regulares

Utilice una expresión regular para ocultar una serie de datos de la carga útil. Los datos sólo se ocultan si coinciden con el origen de registro, el tipo de origen de registro, el nombre de suceso o la categoría definidos en la expresión.

Puede utilizar categorías de alto y de bajo nivel para crear una expresión regular que se más específica que una propiedad basada en campo. Por ejemplo, puede utilizar los patrones de regex siguientes para analizar nombres de usuario:

Tabla 88. Análisis de nombre de usuario de expresión regular

Ejemplo de patrones de expresión regular	Coincide con
`usrName=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*@([0-9 a-zA-Z][-\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,20})$`	`john_smith@IBM.com, jon@ibm.com, jon@us.ibm.com`
`usrName=(^([\w]+[^\W])([^\W]\.?)([\w]+[^\W]$))`	`john.smith, John.Smith, john, jon_smith`
`usrName=^([a-zA-Z])[a-zA-Z_-]*[\w_-]*[\S]$\|^([a -zA-Z])[0-9_-]*[\S]$|^[a-zA-Z]*[\S]$`	`johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith`

Tabla 88. Análisis de nombre de usuario de expresión regular (continuación)

Ejemplo de patrones de expresión regular	Coincide con
`usrName=(/S+)`	Coincide con cualquier carácter que no sea un espacio en blanco después del signo igual, =. Esta expresión regular no es específica y puede generar problemas de rendimiento del sistema.
`msg=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z]))*@\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b`	Coincide con los usuarios que tienen dirección IP. Por ejemplo, `john.smith@1.1.1.1`
`src=\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b`	Coincide con los formatos de dirección IP.
`host=^(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0-9\-]*[A-Za-z0-9])$`	`hostname.ibm.com`, `hostname.co.uk`,

Escenario: Ocultación de nombres de usuario

El usuario es administrador de IBM Security QRadar. Su organización tiene un acuerdo con el sindicato de trabajadores que estipula que toda la información identificable del personal debe quedar oculta a los usuarios de QRadar. El usuario desea configurar QRadar para que oculte todos los nombres de usuario.

Utilice la función **Gestión de ofuscación de datos** de la pestaña **Admin** para configurar QRadar a fin de ocultar los datos:

1. Cree un perfil de ofuscación de datos y descargue la clave privada generada por el sistema. Guarde la clave en una ubicación segura.
2. Cree las expresiones de ofuscación de datos destinadas a los datos que desea ocultar.
3. Habilite el perfil de modo que el sistema empiece a ofuscar los datos.
4. Para leer los datos en QRadar, cargue la clave privada para desofuscar los datos.

Creación de un perfil de ofuscación de datos

IBM Security QRadar utiliza los perfiles de ofuscación de datos para determinar qué datos se enmascaran y para asegurarse de que se utiliza el almacén de datos correcto para desenmascarar los datos.

Acerca de esta tarea

Puede crear un perfil que cree un almacén de claves o puede utilizar un almacén de claves existente. Si crea un almacén de claves, debe descargarlo y almacenarlo en una ubicación segura. Elimine el almacén de claves del sistema local y almacénelo en una ubicación a la que solo puedan acceder los usuarios autorizados para ver los datos desenmascarados.

La configuración de perfiles que utilizan diferentes almacenes de claves diferentes es útil cuando desea limitar el acceso a los datos a diferentes grupos de usuarios. Por ejemplo, cree dos perfiles que utilicen diferentes almacenes de claves cuando desee que un grupo de usuarios vea nombres de usuario y que otro grupo de usuarios vea nombres de host.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos** > **Gestión de ofuscación de datos**.
3. Para crear un perfil nuevo, pulse **Añadir** y teclee un nombre exclusivo y una descripción para el perfil.
4. Para crear un almacén de claves para el perfil, siga estos pasos:
   a. Pulse **Almacén de claves generado por el sistema**.
   b. En el cuadro de lista **Proveedor**, seleccione **IBMJCE**.
   c. En el cuadro de lista **Algoritmo**, seleccione **JCE** y seleccione si desea generar claves de cifrado de 512 bit o 1024 bits. En el cuadro **Nombre común de certificado de almacén de claves**, el nombre de dominio totalmente calificado para el servidor QRadar se llena automáticamente.
   d. En el cuadro **Contraseña de almacén de claves**, especifique la contraseña del almacén de claves. La contraseña de almacén de claves es necesaria para proteger la integridad de éste. La contraseña debe tener 8 caracteres de longitud como mínimo.
   e. En **Verificar contraseña de almacén de claves**, vuelva a teclear la contraseña.
5. Para utilizar un almacén de claves existente con el perfil, siga estos pasos:
   a. Pulse **Almacén de claves de carga**.
   b. Pulse **Examinar** y seleccione el archivo de almacén de claves.
   c. En el cuadro **Contraseña de almacén de claves**, teclee la contraseña para el almacén de claves.
6. Pulse **Enviar**.
7. Descargue el almacén de claves. Elimine el almacén de claves del sistema y almacénelo en una ubicación segura.

Qué hacer a continuación

Cree las expresiones de ofuscación de datos destinadas a los datos que desea enmascarar.

Creación de expresiones de ofuscación de datos

El perfil de ofuscación de datos utiliza expresiones para especificar los datos que deben ocultarse. Las expresiones pueden utilizar propiedades basadas en campo o expresiones regulares.

Acerca de esta tarea

Una vez creada una expresión, no puede cambiar el tipo. Por ejemplo, no puede crear una expresión basada en propiedad y cambiarla posteriormente por una expresión regular.

No puede ofuscar un campo numérico normalizado como por ejemplo un número de puerto o una dirección IP.

Varias expresiones que ofuscan los mismos datos hacen que los datos se ofusquen dos veces. Para descifrar datos que se han ofuscado varias veces, cada almacén de claves que se utiliza en el proceso de ofuscación se debe aplicar por el orden en el que se ha producido la ofuscación.

Procedimiento

1. Pulse la pestaña **Admin**.
2. En el menú de navegación, pulse **Orígenes de datos** > **Gestión de ofuscación de datos**.
3. Pulse el perfil que desea configurar y pulse **Ver contenido**. No puede configurar perfiles que estén bloqueados.
4. Para crear una expresión de ofuscación de datos nueva, pulse **Añadir** y teclee un nombre exclusivo y una descripción para el perfil.
5. Marque el recuadro de selección **Habilitado** para habilitar el perfil.
6. Para crear una expresión basada en campo, pulse **Basado en campo** y seleccione el tipo a ofuscar.
7. Para crear una expresión regular, pulse **RegEx** y configure las propiedades de regex.
8. Pulse **Guardar**.

Desofuscación de datos para que se puedan ver en la consola

Cuando la ofuscación de datos está configurada en un sistema de IBM Security QRadar, se muestra la versión enmascarada de los datos en toda la aplicación. Debe tener tanto el almacén de claves como la contraseña correspondientes para desofuscar los datos de modo que puedan verse.

Antes de empezar

Debe tener la clave privada y la contraseña de la clave para poder desofuscar los datos. La clave privada debe estar en el sistema local.

Acerca de esta tarea

Para poder ver los datos ofuscados, debe cargar la clave privada. Una vez cargada la clave, permanece disponible en el sistema durante la sesión actual. La sesión finaliza cuando el usuario concluye QRadar, cuando se borra la memoria caché en la consola QRadar o cuando hay un periodo de inactividad prolongado. Cuando la sesión finaliza, las claves privadas cargadas en la sesión anterior ya no son visibles.

QRadar puede utilizar las claves disponibles en la sesión actual para desofuscar los datos automáticamente. Con la desofuscación automática habilitada, no tiene que seleccionar repetidamente la clave privada en la ventana Clave de sesión de ofuscación cada vez que desea ver los datos. La desofuscación automática está inhabilitada automáticamente cuando termina la sesión actual.

Procedimiento

1. En la página **Detalles del suceso**, busque los datos que desea desofuscar.
2. Para desofuscar datos basados en identidad:
   a. Pulse el icono del candado situado junto a los datos que desea desofuscar.
   b. En la sección **Clave de carga**, pulse **Seleccionar archivo** y seleccione el almacén de claves a cargar.
   c. En el recuadro **Contraseña**, teclee la contraseña que coincide con el almacén de claves.
   d. Pulse **Cargar**.

      La ventana Desofuscación muestra la carga útil de suceso, los nombres de perfil asociados con el almacén de claves, el texto ofuscado y el texto desofuscado.

e. Opcional: Pulse **Conmutar desofuscación automática** para habilitar la desofuscación automática.

   Después de conmutar el valor de desofuscación automática, debe renovar la ventana del navegador y volver a cargar la página de detalles de suceso para que los cambios aparezcan.

3. Para desofuscar datos de carga útil no basados en la identidad:
   a. En la barra de herramientas de la página **Detalles del suceso**, pulse **Ofuscación** > **Claves de desofuscación**.
   b. En la sección **Clave de carga**, pulse **Seleccionar archivo** y seleccione la clave privada a cargar.
   c. En el recuadro **Contraseña**, teclee la contraseña que coincide con la clave privada y pulse **Cargar**.
   d. En el recuadro **Información de carga útil**, seleccione y copie el texto ofuscado en el portapapeles.
   e. En la barra de herramientas de la página **Detalles del suceso**, pulse **Ofuscación** > **Desofuscación**.
   f. Pegue el texto ofuscado en el cuadro de diálogo.
   g. Seleccione el perfil de ofuscación en la lista desplegable y pulse **Desofuscar**.

Edición o inhabilitación de las expresiones de ofuscación creadas en releases anteriores

Cuando actualiza a IBM Security QRadar V7.2.6, las expresiones de ofuscación de datos creadas en releases anteriores se retoman automáticamente y siguen ofuscando datos. Estas expresiones aparecen en un solo perfil de ofuscación de datos llamado **AutoGeneratedProperty**.

Aunque puede ver las expresiones, no puede editar o inhabilitar expresiones de ofuscación de datos creadas en versiones anteriores. Debe inhabilitarlas manualmente y crear un perfil de ofuscación de datos que contenga las expresiones revisadas.

Acerca de esta tarea

Para inhabilitar una expresión antigua, debe editar el archivo de configuración `xml` que define los atributos para la expresión. A continuación puede ejecutar el script `obfuscation_updater.sh` para inhabilitarlo.

Asegúrese de inhabilitar expresiones antiguas antes de crear expresiones nuevas que ofusquen los mismos datos. Varias expresiones que ofuscan los mismos datos hacen que los datos se ofusquen dos veces. Para descifrar datos que se han ofuscado varias veces, cada almacén de claves que se utiliza en el proceso de ofuscación se debe aplicar por el orden en el que se ha producido la ofuscación.

Procedimiento

1. Utilice SSH para iniciar la sesión en la consola de QRadar como usuario root.
2. Edite el archivo de configuración `.xml` de expresiones de ofuscación creado cuando configuró las expresiones.
3. Para cada expresión que desea inhabilitar, cambie el atributo **`Habilitado`** por `false`.
4. Para inhabilitar las expresiones, ejecute el script `obfuscation_updater.sh` tecleando el mandato siguiente:

`obfuscation_updater.sh [-p <vía_acceso_a_clave_privada>] [-e <vía_accesp_a_archivo_config_xml_ofuscación>]`

El script `obfuscation_updater.sh` está en el directorio `/opt/qradar/bin` pero puede ejecutar el script desde cualquier directorio de la consola QRadar.

Qué hacer a continuación

Cree un perfil de ofuscación de datos para ocultar los datos y gestionar expresiones de ofuscación directamente en QRadar.

Capítulo 23. Archivos de registro

Las operaciones realizadas en IBM Security QRadar se registran en archivos de registro a efectos de seguimiento. Los archivos de registro pueden ayudarle a resolver problemas al registrar las actividades que tienen lugar cuando trabaja con un producto.

Los archivos de registro siguientes pueden ayudarle a identificar y resolver problemas cuando se producen:

- `/var/log/qradar.log`
- `/var/log/qradar.error`
- `/var/log/qradar-sql.log`
- `/opt/tomcat6/logs/catalina.out`
- `/var/log/qflow.debug`

Si desea recopilar los archivos de registro QRadar y revisarlo posteriormente, consulte "Recopilación de archivos de registro" en la página 50.

Registros de auditoría

Los cambios que realizan los usuarios de QRadar se registran en registros de auditoría.

Puede ver los registros de auditoría para supervisar los cambios realizados en QRadar y los usuarios que han cambiado los valores.

Todos los registros de auditoría se almacenan en texto sin formato y se archivan y se comprimen cuando alcanzan un tamaño de 200 MB. El archivo de registro actual se denomina `audit.log`. Cuando el archivo alcanza los 200 MB, se comprime y se le cambia el nombre por `audit.1.gz`. El número del archivo se incrementa cada vez que se archiva un archivo de registro. QRadar almacena hasta 50 archivos de registro archivados.

Visualización del archivo de registro de auditoría

Utilice SSH (Secure Shell) para iniciar la sesión en el sistema de QRadar y supervisar los cambios aplicados al sistema.

Acerca de esta tarea

Puede utilizar la pestaña **Actividad de registro** para ver los sucesos de registro de auditoría normalizados.

El tamaño máximo de cualquier mensaje de auditoría, excluidos la fecha, la hora y el nombre de host, es de 1024 caracteres.

Cada entrada del archivo de registro se visualiza con el formato siguiente:

<fecha_hora> <nombre host> <usuario>@<dirección IP> (ID hebra)
[<categoría>] [<subcategoría>] [<acción>] <carga útil>

En la tabla siguiente se describen las opciones de formato del archivo de registro.

© Copyright IBM Corp. 2012, 2015

Tabla 89. Descripción de las partes del formato del archivo de registro

Parte del formato del archivo	Descripción
fecha_hora	Fecha y hora de la actividad con el formato: Fecha del mes HH:MM:SS
nombre host	Nombre de host de la consola en la que se ha registrado esta actividad.
usuario	Nombre del usuario que ha cambiado los valores.
dirección IP	Dirección IP del usuario que ha cambiado los valores.
ID hebra	Identificador de la hebra de Java que ha registrado esta actividad.
categoría	Categoría de nivel alto de esta actividad.
subcategoría	Categoría de nivel bajo de esta actividad.
acción	Actividad que se ha producido.
carga útil	Registro completo, que puede incluir el registro de usuario o la regla de suceso, que ha cambiado.

Procedimiento

1. Inicie, mediante SSH, la sesión en QRadar como usuario root:
2. **Nombre de usuario:** `root`
3. **Contraseña:** *`contraseña`*
4. Vaya al directorio siguiente:
   `/var/log/audit`
5. Abra y consulte el archivo de registro de auditoría.

Acciones registradas

Familiarícese con el contenido del archivo de registro de auditoría de QRadar del directorio `/var/log/audit`. El archivo de registro de auditoría contiene acciones registradas.

En la lista siguiente se describen las categorías de acciones que existen en el archivo de registro de auditoría:

Autenticación del administrador

- Iniciar una sesión en la Consola de administración.
- Cerrar sesión de la consola de administración

Activos

- Suprimir un activo
- Suprimir todos los activos

Acceso del registro de auditoría
Búsqueda que incluye sucesos que tienen una categoría de suceso de nivel alto de Auditoría.

Copia de seguridad y recuperación

- Editar la configuración
- Iniciar la copia de seguridad

- Completar la copia de seguridad
- Copia de seguridad fallida
- Suprimir la copia de seguridad
- Sincronizar la copia de seguridad
- Cancelar la copia de seguridad
- Iniciar la restauración
- Cargar una copia de seguridad
- Cargar una copia de seguridad no válida
- Iniciar la restauración
- Purgar la copia de seguridad

Configuración del gráfico
Guardar configuración del gráfico de flujos o sucesos

Gestión de contenidos

- Exportación de contenido iniciada.
- Exportación de contenido completada.
- Importación de contenido iniciada.
- Importación de contenido completada.
- Actualización de contenido iniciada.
- Actualización de contenido completada.
- Búsqueda de contenido iniciada.
- Aplicaciones añadidas.
- Aplicaciones modificadas.
- Acciones personalizadas añadidas.
- Acciones personalizadas modificadas.
- Propiedad Ariel añadida.
- Propiedad Ariel modificada.
- Expresión de propiedad Ariel añadida.
- Expresión de propiedad Ariel modificada.
- Regla CRE añadida.
- Regla CRE modificada.
- Panel de control añadido.
- Panel de control modificado.
- Extensión de dispositivo añadida.
- Extensión de dispositivo modificada.
- Asociación de extensión de dispositivo modificada.
- Agrupación añadida.
- Agrupación modificada.
- Perfil de correlación histórica añadido.
- Perfil de correlación histórica modificado.
- Entrada de correlación de QID añadida.
- Entrada de correlación de QID modificada.
- Datos de referencia creados.
- Datos de referencia actualizados.
- Perfil de seguridad añadido.
- Perfil de seguridad modificado.

- Dispositivo de sensor añadido.
- Dispositivo de sensor modificado.

Propiedades personalizadas

- Añadir una propiedad de suceso personalizada
- Editar una propiedad de suceso personalizada
- Suprimir una propiedad de suceso personalizada
- Editar una propiedad de flujo personalizada
- Suprimir una propiedad de flujo personalizada

Expresiones de propiedad personalizada

- Añadir una expresión de propiedad de suceso personalizada
- Editar una expresión de propiedad de suceso personalizada
- Suprimir una expresión de propiedad de suceso personalizada
- Añadir una expresión de propiedad de flujo personalizada
- Editar una expresión de propiedad de flujo personalizada
- Suprimir una expresión de propiedad de flujo personalizada

Orígenes de flujo

- Añadir un origen de flujo
- Editar un origen de flujo
- Suprimir un origen de flujo

Grupos

- Añadir un grupo
- Suprimir un grupo
- Editar un grupo

Correlación histórica

- Añadir un perfil de correlación histórica.
- Suprimir un perfil de correlación histórica.
- Modificar un perfil de correlación histórica.
- Habilitar un perfil de correlación histórica.
- Inhabilitar un perfil de correlación histórica.
- El perfil de correlación histórica se está ejecutando.
- El perfil de correlación histórica está cancelado.

Alta disponibilidad

- Añadir una clave de licencia
- Revertir una licencia
- Suprimir una clave de licencia

Extensión de origen de registro

- Añadir una extensión de origen de registro
- Editar la extensión de origen de registro
- Suprimir una extensión de origen de registro
- Cargar una extensión de origen de registro
- Cargar una extensión de origen de registro satisfactoriamente
- Cargar una extensión de origen de registro no válida
- Descargar una extensión de origen de registro

- Informar de una extensión de origen de registro
- Modificar una asociación de orígenes de registro con un dispositivo o tipo de dispositivo

Delitos

- Ocultar un delito
- Cerrar un delito
- Cerrar todos los delitos
- Añadir una nota de destino
- Añadir una nota de origen
- Añadir una nota de red
- Añadir una nota de delito
- Añadir una razón de cierre de delitos
- Editar una razón de cierre de delitos

Configuración de protocolo

- Añadir una configuración de protocolo
- Suprimir una configuración de protocolo
- Editar una configuración de protocolo

QIDmap

- Añadir una entrada de correlación de QID
- Editar una entrada de correlación de QID

QRadar Vulnerability Manager

- Crear una planificación de explorador
- Actualizar una planificación de explorador
- Suprimir una planificación de explorador
- Iniciar una planificación de explorador
- Hacer una pausa en una planificación de explorador
- Reanudar una planificación de explorador

Conjuntos de referencia

- Crear un conjunto de referencia
- Editar un conjunto de referencia
- Purgar elementos en un conjunto de referencia
- Suprimir un conjunto de referencia
- Añadir elementos de conjunto de referencia
- Suprimir elementos de conjunto de referencia
- Suprimir todos los elementos de conjunto de referencia
- Importar elementos de conjunto de referencia
- Exportar elementos de conjunto de referencia

Informes

- Añadir una plantilla
- Suprimir una plantilla
- Editar una plantilla
- Generar un informe
- Suprimir un informe
- Suprimir contenido generado

- Ver un informe generado
- Enviar por correo electrónico un informe generado

Grupos de retención
- Añadir un grupo
- Suprimir un grupo
- Editar un grupo
- Habilitar o inhabilitar un grupo

Inicio de sesión de root
- Iniciar sesión en QRadar como usuario root.
- Cerrar sesión en QRadar como usuario root.

Reglas
- Añadir una regla
- Suprimir una regla
- Editar una regla

Explorador
- Añadir un explorador
- Suprimir un explorador
- Editar un explorador

Planificación de explorador
- Añadir una planificación
- Editar una planificación
- Suprimir una planificación

Autenticación de sesión
- Crear una sesión de administración
- Terminar una sesión de administración
- Denegar una sesión de autenticación no válida
- Hacer caducar una autenticación de sesión
- Crear una sesión de autenticación
- Terminar una sesión de autenticación

SIM Limpiar un modelo SIM.

Almacenar y reenviar
- Añadir una planificación de Almacenar y reenviar
- Editar una planificación de Almacenar y reenviar
- Suprimir una planificación de Almacenar y reenviar

Reenvío de Syslog
- Añadir un reenvío de syslog
- Suprimir un reenvío de syslog
- Editar un reenvío de syslog

Gestión de sistemas
- Concluir un sistema
- Reiniciar un sistema

Cuentas de usuario
- Añadir una cuenta

- Editar una cuenta
- Suprimir una cuenta

Autenticación de usuario

- Iniciar sesión en la interfaz de usuario
- Cerrar sesión de la interfaz de usuario

Autenticación de usuario - Ariel

- Denegar un intento de inicio de sesión
- Añadir una propiedad de Ariel
- Suprimir una propiedad de Ariel
- Editar una propiedad de Ariel
- Añadir una extensión de propiedad de Ariel
- Suprimir una extensión de propiedad de Ariel
- Editar una extensión de propiedad de Ariel

Roles de usuario

- Añadir un rol
- Editar un rol
- Suprimir un rol

VIS

- Descubrir un host nuevo
- Descubrir un sistema operativo nuevo
- Descubrir un puerto nuevo
- Descubrir una vulnerabilidad nueva

Capítulo 24. Categorías de sucesos

Las categorías de sucesos se utilizan para agrupar los sucesos de entrada para que IBM Security QRadar los procese. En las categorías de sucesos se pueden realizar búsquedas; estas categorías le ayudan a supervisar la red.

Los sucesos que se producen en la red se agregan a categorías de nivel alto y bajo. Cada categoría de nivel alto contiene categorías de nivel bajo y un nivel de gravedad asociado. Puede revisar los niveles de gravedad que están asignados a los sucesos y ajustarlos para que se adapten a las necesidades de su política corporativa.

Categorías de sucesos de nivel alto

Los sucesos de los orígenes de registro de QRadar se agrupan en categorías de nivel alto. Cada suceso se asigna a una categoría de nivel alto determinada.

La categorización de los sucesos entrantes hace que las búsquedas en los datos sean más fáciles de hacer.

En la tabla siguiente se describen las categorías de sucesos de nivel alto.

Tabla 90. Categorías de sucesos de nivel alto

Categoría	Descripción
"Reconocimiento" en la página 289	Sucesos que están relacionados con la exploración y otras técnicas que se utilizan para identificar los recursos de la red; por ejemplo, exploraciones de puertos de host o de red.
"Denegación de servicio" en la página 290	Sucesos que están relacionados con los ataques de denegación de servicio (DoS) o de denegación de servicio distribuido (DDoS) contra servicios o hosts; por ejemplo, ataques de denegación de servicio de red por la fuerza.
"Autenticación" en la página 294	Sucesos que están relacionados con los controles de autenticación, grupo o cambio de privilegios; por ejemplo, inicio o cierre de sesión.
"Acceso" en la página 301	Sucesos que son consecuencia de un intento de acceder a los recursos de la red; por ejemplo, aceptación o denegación de cortafuegos.
"Explotación" en la página 303	Sucesos que están relacionados con explotaciones de aplicación e intentos de desbordamiento de almacenamiento intermedio; por ejemplo, desbordamiento de almacenamiento intermedio o explotaciones de aplicación web.

© Copyright IBM Corp. 2012, 2015

Tabla 90. Categorías de sucesos de nivel alto (continuación)

Categoría	Descripción
"Programa malicioso" en la página 305	Sucesos que están relacionados con virus, troyanos, puertas traseras y otras formas de software hostil. Los sucesos de programas maliciosos pueden incluir un virus, un troyano, software malicioso o spyware.
"Actividad sospechosa" en la página 306	La naturaleza de la amenaza es desconocida pero el comportamiento es sospechoso. La amenaza puede incluir anomalías de protocolo que potencialmente indican técnicas evasivas; por ejemplo, las técnicas de evasión de IDS (sistema de detección de intrusiones) conocidas o la fragmentación de paquetes.
"Sistema" en la página 310	Sucesos que están relacionados con los cambios del sistema, la instalación de software o los mensajes de estado.
"Política" en la página 315	Sucesos relativos al uso indebido o las violaciones de políticas corporativas.
"Desconocido" en la página 316	Sucesos que están relacionados con actividad desconocida en el sistema.
"CRE" en la página 317	Sucesos que se generan a partir de una regla de delito o de suceso.
"Explotación potencial" en la página 318	Sucesos relacionados con explotaciones potenciales de aplicación e intentos de desbordamiento de almacenamiento intermedio.
"Definido por el usuario" en la página 319	Sucesos que están relacionados con objetos definidos por el usuario.
"Auditoría de SIM" en la página 321	Sucesos que están relacionados con la interacción del usuario con la consola y las funciones administrativas.
"Descubrimiento de host de VIS" en la página 322	Sucesos que están relacionados con el host, los puertos o las vulnerabilidades que el componente VIS descubre.
"Aplicación" en la página 323	Sucesos que están relacionados con la actividad de las aplicaciones.
"Auditoría" en la página 345	Sucesos que están relacionados con la actividad de auditoría.
"Riesgo" en la página 346	Sucesos que están relacionados con actividad de riesgo en IBM Security QRadar Risk Manager.
"Auditoría de Risk Manager" en la página 347	Sucesos que están relacionados con actividad de auditoría en IBM Security QRadar Risk Manager.
"Control" en la página 348	Sucesos que están relacionados con el sistema de hardware.
"Perfilador de activos" en la página 350	Sucesos que están relacionados con los perfiles de activo.

Reconocimiento

La categoría Reconocimiento contiene sucesos que están relacionados con la exploración y otras técnicas que se utilizan para identificar los recursos de la red.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría Reconocimiento.

Tabla 91. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos Reconocimiento

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Formulario de reconocimiento desconocido	Un formulario desconocido de reconocimiento.	2
Consulta de aplicación	Reconocimiento para las aplicaciones del sistema.	3
Consulta de host	Reconocimiento para un host de la red.	3
Barrido de red	Reconocimiento en la red.	4
Reconocimiento de correo	Reconocimiento en el sistema de correo.	3
Reconocimiento de Windows	Reconocimiento para el sistema operativo Windows.	3
Solicitud de correlación de puertos / RPC	Reconocimiento en la solicitud de correlación de puertos o RPC.	3
Exploración de puertos de host	Indica que se ha llevado a cabo una exploración en los puertos de host.	4
Vuelco de RPC	Indica que la información de RPC (llamada a procedimiento remoto) se ha eliminado.	3
Reconocimiento de DNS	Reconocimiento en el servidor DNS.	3
Suceso de reconocimiento diverso	Suceso de reconocimiento diverso.	2
Reconocimiento de web	Reconocimiento de web en la red.	3
Reconocimiento de base de datos	Reconocimiento de base de datos en la red.	3
Reconocimiento de ICMP	Reconocimiento del tráfico ICMP.	3
Reconocimiento de UDP	Reconocimiento del tráfico UDP.	3
Reconocimiento de SNMP	Reconocimiento del tráfico SNMP.	3
Consulta de host de ICMP	Indica una consulta de host de ICMP.	3
Consulta de host de UDP	Indica una consulta de host de UDP.	3

Tabla 91. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos Reconocimiento (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Reconocimiento de NMAP	Indica el reconocimiento de NMAP.	3
Reconocimiento de TCP	Indica el reconocimiento de TCP en la red.	3
Reconocimiento de UNIX	Reconocimiento en la red UNIX.	3
Reconocimiento de FTP	Indica el reconocimiento de FTP.	3

Denegación de servicio

La categoría de denegación de servicio contiene sucesos que están relacionados con los ataques de denegación de servicio (DoS) contra servicios o hosts.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de ataque de denegación de servicio.

Tabla 92. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de ataque de denegación de servicio

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Ataque desconocido de denegación de servicio	Indica un ataque de denegación de servicio desconocido.	8
Ataque de denegación de servicio de ICMP	Indica un ataque de denegación de servicio de ICMP.	9
Ataque de denegación de servicio de TCP	Indica un ataque de denegación de servicio de TCP.	9
Ataque de denegación de servicio de UDP	Indica un ataque de denegación de servicio de UDP.	9
Ataque de denegación de servicio de DNS	Indica un ataque de denegación de servicio de DNS.	8
Ataque de denegación de servicio web	Indica un ataque de denegación de servicio de un servicio web.	8
Ataque de denegación de servicio de correo	Indica un ataque de denegación de servicio del servidor de correo.	8
Ataque de denegación de servicio distribuido	Indica un ataque de denegación de servicio distribuido.	9

Tabla 92. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de ataque de denegación de servicio (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Ataque de denegación de servicio diverso	Indica un ataque de denegación de servicio diverso.	8
Ataque de denegación de servicio de UNIX	Indica un ataque de denegación de servicio de UNIX.	8
Ataque de denegación de servicio de Windows	Indica un ataque de denegación de servicio de Windows.	8
Ataque de denegación de servicio de base de datos	Indica un ataque de denegación de servicio de base de datos.	8
Ataque de denegación de servicio de FTP	Indica un ataque de denegación de servicio de FTP.	8
Ataque de denegación de servicio de infraestructura	Indica un ataque de denegación de servicio en la infraestructura.	8
Ataque de denegación de servicio de Telnet	Indica un ataque de denegación de servicio de Telnet.	8
Inicio de sesión por la fuerza	Indica el acceso al sistema mediante métodos no autorizados.	8
Ataque de denegación de servicio de TCP de velocidad alta	Indica un ataque de denegación de servicio de TCP de velocidad alta.	8
Ataque de denegación de servicio de UDP de velocidad alta	Indica un ataque de denegación de servicio de UDP de velocidad alta.	8
Ataque de denegación de servicio de ICMP de velocidad alta	Indica un ataque de denegación de servicio de ICMP de velocidad alta.	8
Ataque de denegación de servicio de velocidad alta	Indica un ataque de denegación de servicio de velocidad alta.	8
Ataque de denegación de servicio de TCP de velocidad media	Indica un ataque de TCP de velocidad media.	8
Ataque de denegación de servicio de UDP de velocidad media	Indica un ataque de UDP de velocidad media.	8
Ataque de denegación de servicio de ICMP de velocidad media	Indica un ataque de ICMP de velocidad media.	8
Ataque de denegación de servicio de velocidad media	Indica un ataque de denegación de servicio de velocidad media.	8

Tabla 92. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de ataque de denegación de servicio (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Ataque de denegación de servicio de velocidad media	Indica un ataque de denegación de servicio de velocidad media.	8
Ataque de denegación de servicio de TCP de velocidad baja	Indica un ataque de denegación de servicio de TCP de velocidad baja.	8
Ataque de denegación de servicio de UDP de velocidad baja	Indica un ataque de denegación de servicio de UDP de velocidad baja.	8
Ataque de denegación de servicio de ICMP de velocidad baja	Indica un ataque de denegación de servicio de ICMP de velocidad baja.	8
Ataque de denegación de servicio de velocidad baja	Indica un ataque de denegación de servicio de velocidad baja.	8
Ataque de denegación de servicio de TCP de velocidad alta distribuido	Indica un ataque de denegación de servicio de TCP de velocidad alta distribuido.	8
Ataque de denegación de servicio de UDP de velocidad alta distribuido	Indica un ataque de denegación de servicio de UDP de velocidad alta distribuido.	8
Ataque de denegación de servicio de ICMP de velocidad alta distribuido	Indica un ataque de denegación de servicio de ICMP de velocidad alta distribuido.	8
Ataque de denegación de servicio de velocidad alta distribuido	Indica un ataque de denegación de servicio de velocidad alta distribuido.	8
Ataque de denegación de servicio de TCP de velocidad media distribuido	Indica un ataque de denegación de servicio de TCP de velocidad media distribuido.	8
Ataque de denegación de servicio de UDP de velocidad media distribuido	Indica un ataque de denegación de servicio de UDP de velocidad media distribuido.	8
Ataque de denegación de servicio de ICMP de velocidad media distribuido	Indica un ataque de denegación de servicio de ICMP de velocidad media distribuido.	8
Ataque de denegación de servicio de velocidad media distribuido	Indica un ataque de denegación de servicio de velocidad media distribuido.	8
Ataque de denegación de servicio de TCP de velocidad baja distribuido	Indica un ataque de denegación de servicio de TCP de velocidad baja distribuido.	8

Tabla 92. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de ataque de denegación de servicio (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Ataque de denegación de servicio de UDP de velocidad baja distribuido	Indica un ataque de denegación de servicio de UDP de velocidad baja distribuido.	8
Ataque de denegación de servicio de ICMP de velocidad baja distribuido	Indica un ataque de denegación de servicio de ICMP de velocidad baja distribuido.	8
Ataque de denegación de servicio de velocidad baja distribuido	Indica un ataque de denegación de servicio de velocidad baja distribuido.	8
Exploración de TCP de velocidad alta	Indica una exploración de TCP de velocidad alta.	8
Exploración de UDP de velocidad alta	Indica una exploración de UDP de velocidad alta.	8
Exploración de ICMP de velocidad alta	Indica una exploración de ICMP de velocidad alta.	8
Exploración de velocidad alta	Indica una exploración de velocidad alta.	8
Exploración de TCP de velocidad media	Indica una exploración de TCP de velocidad media.	8
Exploración de UDP de velocidad media	Indica una exploración de UDP de velocidad media.	8
Exploración de ICMP de velocidad media	Indica una exploración de ICMP de velocidad media.	8
Exploración de velocidad media	Indica una exploración de velocidad media.	8
Exploración de TCP de velocidad baja	Indica una exploración de TCP de velocidad baja.	8
Exploración de UDP de velocidad baja	Indica una exploración de UDP de velocidad baja.	8
Exploración de ICMP de velocidad baja	Indica una exploración de ICMP de velocidad baja.	8
Exploración de velocidad baja	Indica una exploración de velocidad baja.	8
Ataque de denegación de servicio de VoIP	Indica un ataque de denegación de servicio de VoIP.	8
Inundación	Indica un ataque de inundación.	8
Inundación de TCP	Indica un ataque de inundación de TCP.	8
Inundación de UDP	Indica un ataque de inundación de UDP.	8
Inundación de ICMP	Indica un ataque de inundación de ICMP.	8

Tabla 92. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de ataque de denegación de servicio (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Inundación de SYN	Indica un ataque de inundación de SYN.	8
Inundación de URG	Indica un ataque de inundación con el distintivo de urgente (URG) activado.	8
Inundación de SYN URG	Indica un ataque de inundación SYN con el distintivo de urgente (URG) activado.	8
Inundación de SYN FIN	Indica un ataque de inundación de SYN FIN.	8
Inundación de SYN ACK	Indica un ataque de inundación de SYN ACK.	8

Autenticación

La categoría de autenticación contiene sucesos que están relacionados con la autenticación, las sesiones y los controles de acceso que supervisan a los usuarios de la red.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de autenticación.

Tabla 93. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de autenticación

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Autenticación desconocida	Indica que la autenticación es desconocida.	1
Inicio de sesión de host satisfactorio	Indica un inicio de sesión de host satisfactorio.	1
Inicio de sesión de host fallido	Indica que el inicio de sesión de host ha fallado.	3
Inicio de sesión diverso satisfactorio	Indica que la secuencia de inicio de sesión ha sido satisfactoria.	1
Inicio de sesión diverso fallido	Indica que la secuencia de inicio de sesión ha fallado.	3
Escalamiento de privilegios fallido	Indica que el escalamiento de privilegios ha fallado.	3
Escalamiento de privilegios satisfactorio	Indica que el escalamiento de privilegios ha sido satisfactorio.	1
Inicio de sesión de servicio de correo satisfactorio	Indica que el inicio de sesión en el servicio de correo ha sido satisfactorio.	1

Tabla 93. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de autenticación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Inicio de sesión de servicio de correo fallido	Indica que el inicio de sesión en el servicio de correo ha fallado.	3
Inicio de sesión de servidor de autenticación fallido	Indica que el inicio de sesión en el servidor de autenticación ha fallado.	3
Inicio de sesión de servidor de autenticación satisfactorio	Indica que el inicio de sesión en el servidor de autenticación ha sido satisfactorio.	1
Inicio de sesión de servicio web satisfactorio	Indica que el inicio de sesión del servicio web ha sido satisfactorio.	1
Inicio de sesión de servicio web fallido	Indica que el inicio de sesión del servicio web ha fallado.	3
Inicio de sesión de administrador satisfactorio	Indica que un inicio de sesión administrativa ha sido satisfactorio.	1
Anomalía de inicio de sesión de administrador	Indica que el inicio de sesión administrativa ha fallado.	3
Nombre de usuario sospechoso	Indica que un usuario ha intentado acceder a la red utilizando un nombre de usuario incorrecto.	4
Inicio de sesión con nombre de usuario/contraseña predeterminados satisfactorio	Indica que un usuario ha accedido a la red utilizando el nombre de usuario y la contraseña predeterminados.	4
Inicio de sesión con nombre de usuario/contraseña predeterminados fallido	Indica que un usuario no ha podido acceder a la red utilizando el nombre de usuario y la contraseña predeterminados.	4
Inicio de sesión de FTP satisfactorio	Indica que un inicio de sesión de FTP ha sido satisfactorio.	1
Inicio de sesión de FTP fallido	Indica que el inicio de sesión de FTP ha fallado.	3
Inicio de sesión de SSH satisfactorio	Indica que un inicio de sesión de SSH ha sido satisfactorio.	1
Inicio de sesión de SSH fallido	Indica que el inicio de sesión de SSH ha fallado.	2
Derecho de usuario asignado	Indica que el acceso del usuario a los recursos de red se ha otorgado satisfactoriamente.	1

Tabla 93. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de autenticación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Derecho de usuario eliminado	Indica que el acceso del usuario a los recursos de red se ha eliminado satisfactoriamente.	1
Dominio de confianza añadido	Indica que un dominio de confianza se ha añadido satisfactoriamente al despliegue.	1
Dominio de confianza eliminado	Indica que un dominio de confianza se ha eliminado del despliegue.	1
Acceso de seguridad del sistema otorgado	Indica que el acceso de seguridad del sistema se ha otorgado satisfactoriamente.	1
Acceso de seguridad del sistema eliminado	Indica que el acceso de seguridad del sistema se ha eliminado satisfactoriamente.	1
Política añadida	Indica que una política se ha añadido satisfactoriamente.	1
Cambio de política	Indica que una política se ha cambiado satisfactoriamente.	1
Cuenta de usuario añadida	Indica que una cuenta de usuario se ha añadido satisfactoriamente.	1
Cuenta de usuario cambiada	Indica que se ha aplicado un cambio a una cuenta de usuario existente.	1
Cambio de contraseña fallido	Indica que un intento de cambiar una contraseña existente ha fallado.	3
Cambio de contraseña satisfactorio	Indica que un cambio de contraseña ha sido satisfactorio.	1
Cuenta de usuario eliminada	Indica que una cuenta de usuario se ha eliminado satisfactoriamente.	1
Miembro de grupo añadido	Indica que un miembro de grupo se ha añadido satisfactoriamente.	1
Miembro de grupo eliminado	Indica que un miembro de grupo se ha eliminado.	1
Grupo añadido	Indica que un grupo se ha añadido satisfactoriamente.	1
Grupo cambiado	Indica que se ha aplicado un cambio a un grupo existente.	1
Grupo eliminado	Indica que un grupo se ha eliminado.	1

Tabla 93. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de autenticación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Cuenta de sistema añadida	Indica que una cuenta de sistema se ha añadido satisfactoriamente.	1
Cuenta de sistema cambiada	Indica que se ha aplicado un cambio a una cuenta de sistema existente.	1
Cuenta de sistema eliminada	Indica que una cuenta de sistema se ha eliminado satisfactoriamente.	1
Inicio de sesión de acceso remoto satisfactorio	Indica que el acceso a la red utilizando un inicio de sesión remoto ha sido satisfactorio.	1
Inicio de sesión de acceso remoto fallido	Indica que un intento de acceder a la red utilizando un inicio de sesión remoto ha fallado.	3
Autenticación general satisfactoria	Indica que el proceso de autenticación ha sido satisfactorio.	1
Autenticación general fallida	Indica que el proceso de autenticación ha fallado.	3
Inicio de sesión de Telnet satisfactorio	Indica que el inicio de sesión de telnet ha sido satisfactorio.	1
Inicio de sesión de Telnet fallido	Indica que el inicio de sesión de telnet ha fallado.	3
Contraseña sospechosa	Indica que un usuario ha intentado iniciar sesión utilizando una contraseña sospechosa.	4
Inicio de sesión de Samba satisfactorio	Indica que un usuario ha iniciado la sesión satisfactoriamente utilizando Samba.	1
Inicio de sesión de Samba fallido	Indica que un usuario no ha podido iniciar la sesión utilizando Samba.	3
Sesión de servidor de autenticación abierta	Indica que se ha iniciado una sesión de comunicación con el servidor de autenticación.	1
Sesión de servidor de autenticación cerrada	Indica que se ha cerrado una sesión de comunicación con el servidor de autenticación.	1
Sesión de cortafuegos cerrada	Indica que una sesión de cortafuegos se ha cerrado.	1
Cierre de sesión de host	Indica que un host ha cerrado la sesión satisfactoriamente.	1

Tabla 93. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de autenticación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Cierre de sesión diverso	Indica que un usuario ha cerrado la sesión satisfactoriamente.	1
Cierre de sesión de servidor de autenticación	Indica que el proceso para cerrar la sesión del servidor de autenticación ha sido satisfactorio.	1
Cierre de sesión de servicio web	Indica que el proceso para cerrar la sesión del servicio web ha sido satisfactorio.	1
Cierre de sesión de administrador	Indica que el usuario administrativo ha cerrado la sesión satisfactoriamente.	1
Cierre de sesión de FTP	Indica que el proceso para cerrar la sesión del servicio FTP ha sido satisfactorio.	1
Cierre de sesión de SSH	Indica que el proceso para cerrar la sesión de SSH ha sido satisfactorio.	1
Cierre de sesión de acceso remoto	Indica que el proceso para cerrar la sesión mediante el acceso remoto ha sido satisfactorio.	1
Cierre de sesión de Telnet	Indica que el proceso para cerrar la sesión de Telnet ha sido satisfactorio.	1
Cierre de sesión de Samba	Indica que el proceso para cerrar la sesión de Samba ha sido satisfactorio.	1
Sesión de SSH iniciada	Indica que la sesión de conexión de SSH se ha iniciado en un host.	1
Sesión de SSH finalizada	Indica que una sesión de conexión de SSH en un host ha terminado.	1
Sesión de Admin iniciada	Indica que un usuario administrativo o privilegiado ha iniciado una sesión de conexión en un host.	1
Sesión de Admin finalizada	Indica que la sesión de conexión de un usuario administrativo o privilegiado en un host ha terminado.	1
Inicio de sesión de VoIP satisfactorio	Indica un inicio de sesión de VoIP satisfactorio.	1
Inicio de sesión de VoIP fallido	Indica un intento no satisfactorio de acceder al servicio de VoIP.	1

Tabla 93. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de autenticación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Finalización de sesión de VoIP	Indica el cierre de la sesión de un usuario.	1
Sesión de VoIP iniciada	Indica el comienzo de una sesión de VoIP.	1
Sesión de VoIP terminada	Indica el final de una sesión de VoIP.	1
Inicio de sesión de base de datos satisfactorio	Indica un inicio de sesión de base de datos satisfactorio.	1
Inicio de sesión de base de datos fallido	Indica que un intento de inicio de sesión de base de datos ha fallado.	3
Autenticación de IKE fallida	Indica que se ha detectado una autenticación de IKE (Internet Key Exchange) fallida.	3
Autenticación de IKE satisfactoria	Indica que se ha detectado una autenticación de IKE satisfactoria.	1
Sesión de IKE iniciada	Indica que se ha abierto una sesión de IKE.	1
Sesión de IKE finalizada	Indica que ha finalizado una sesión de IKE.	1
Error de IKE	Indica que hay un mensaje de error de IKE.	1
Estado de IKE	Indica que hay un mensaje de estado de IKE.	1
Sesión de RADIUS iniciada	Indica que se ha abierto una sesión de RADIUS.	1
Sesión de RADIUS finalizada	Indica que ha finalizado una sesión de RADIUS.	1
Sesión de RADIUS denegada	Indica que se ha denegado una sesión de RADIUS.	1
Estado de sesión de RADIUS	Indica que hay un mensaje de estado de la sesión de RADIUS.	1
Autenticación de RADIUS fallida	Indica un error de autenticación de RADIUS.	3
Autenticación de RADIUS satisfactoria	Indica que una autenticación de RADIUS ha sido satisfactoria.	1
Sesión de TACACS iniciada	Indica que se ha abierto una sesión de TACACS.	1
Sesión de TACACS finalizada	Indica que ha finalizado una sesión de TACACS.	1
Sesión de TACACS denegada	Indica que se ha denegado una sesión de TACACS.	1

Tabla 93. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de autenticación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Estado de sesión de TACACS	Indica que hay un mensaje de estado de la sesión de TACACS.	1
Autenticación de TACACS satisfactoria	Indica que una autenticación de TACACS ha sido satisfactoria.	1
Autenticación de TACACS fallida	Indica un error de autenticación de TACACS.	1
Desautenticación de host satisfactoria	Indica que la desautenticación de un host ha sido satisfactoria.	1
Desautenticación de host fallida	Indica que la desautenticación de un host ha fallado.	3
Autenticación de estación satisfactoria	Indica que la autenticación de estación ha sido satisfactoria.	1
Autenticación de estación fallida	Indica que la autenticación de estación de un host ha fallado.	3
Asociación de estación satisfactoria	Indica que la asociación de estación ha sido satisfactoria.	1
Asociación de estación fallida	Indica que la asociación de estación ha fallado.	3
Reasociación de estación satisfactoria	Indica que la reasociación de estación ha sido satisfactoria.	1
Reasociación de estación fallida	Indica que la asociación de estación ha fallado.	3
Desasociación de host satisfactoria	Indica que la desasociación de un host ha sido satisfactoria.	1
Desasociación de host fallida	Indica que la desasociación de un host ha fallado.	3
Error de SA	Indica que hay un mensaje de error de SA (asociación de seguridad).	5
Anomalía de creación de SA	Indica que se ha producido un error en la creación de SA (asociación de seguridad).	3
SA establecido	Indica que se ha establecido una conexión de SA (asociación de seguridad).	1
SA rechazado	Indica que se ha rechazado una conexión de SA (asociación de seguridad).	3
Suprimiendo SA	Indica la supresión de una asociación de seguridad (SA).	1

Tabla 93. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de autenticación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Creando SA	Indica la creación de una asociación de seguridad (SA).	1
Discrepancia de certificado	Indica una discrepancia de certificado.	3
Discrepancia de credenciales	Indica una discrepancia de credenciales.	3
Intento de inicio de sesión de administrador	Indica que ha habido un intento de inicio de sesión de administrador.	2
Intento de inicio de sesión de usuario	Indica que ha habido un intento de inicio de sesión de usuario.	2
Inicio de sesión de usuario satisfactorio	Indica un inicio de sesión de usuario satisfactorio.	1
Inicio de sesión de usuario fallido	Indica que un inicio de sesión de usuario ha fallado.	3
Inicio de sesión de SFTP satisfactorio	Indica un inicio de sesión de SFTP (protocolo de transferencia de archivos SSH) satisfactorio.	1
Inicio de sesión de SFTP fallido	Indica que un inicio de sesión de SFTP (protocolo de transferencia de archivos SSH) ha fallado.	3
Finalización de sesión de SFTP	Indica que se ha cerrado una sesión de SFTP (protocolo de transferencia de archivos SSH).	1

Acceso

La categoría de acceso contiene controles de autenticación y acceso que se utilizan para la supervisión de los sucesos de red.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de acceso.

Tabla 94. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de acceso

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Suceso de comunicación de red desconocido	Indica un suceso de comunicación de red desconocido.	3
Permiso de cortafuegos	Indica que se ha permitido el acceso al cortafuegos.	0
Denegación de cortafuegos	Indica que se ha denegado el acceso al cortafuegos.	4

Tabla 94. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de acceso (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Respuesta de contexto de flujo (solo QRadar SIEM)	Indica sucesos del motor de clasificación en respuesta a una petición de SIM.	5
Suceso de comunicación de red diverso	Indica un suceso de comunicación de red diverso.	3
Denegación de IPS	Indica que hay tráfico denegado de IPS (sistemas de prevención de intrusiones).	4
Sesión de cortafuegos abierta	Indica que la sesión de cortafuegos se ha abierto.	0
Sesión de cortafuegos cerrada	Indica que la sesión de cortafuegos se ha cerrado.	0
Conversión dinámica de dirección satisfactoria	Indica que la conversión dinámica de dirección ha sido satisfactoria.	0
No se ha encontrado ningún grupo de conversión	Indica que no se ha encontrado ningún grupo de conversión.	2
Autorización diversa	Indica que se ha otorgado acceso a un servidor de autenticación diverso.	2
Permiso de ACL	Indica que una lista de control de accesos (ACL) ha permitido el acceso.	0
Denegación de ACL	Indica que una lista de control de accesos (ACL) ha denegado el acceso.	4
Acceso permitido	Indica que el acceso se ha permitido.	0
Acceso denegado	Indica que el acceso se ha denegado.	4
Sesión abierta	Indica que se ha abierto una sesión.	1
Sesión cerrada	Indica que se ha cerrado una sesión.	1
Sesión restablecida	Indica que se ha restablecido una sesión.	3
Sesión terminada	Indica que se ha permitido una sesión.	4
Sesión denegada	Indica que se ha denegado una sesión.	5
Sesión en curso	Indica que hay una sesión en curso.	1
Sesión retardada	Indica que una sesión se ha retardado.	3

Tabla 94. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de acceso (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión en cola	Indica que una sesión se ha puesto en cola.	1
Sesión de entrada	Indica que una sesión es de entrada.	1
Sesión de salida	Indica que una sesión es de salida.	1
Intento de acceso no autorizado	Indica que se ha detectado un intento de acceso no autorizado.	6
Acción de aplicación variada permitida	Indica que se ha permitido una acción de aplicación.	1
Acción de aplicación variada denegada	Indica que se ha denegado una acción de aplicación.	3
Acción de base de datos permitida	Indica que se ha permitido una acción de base de datos.	1
Acción de base de datos denegada	Indica que se ha denegado una acción de base de datos.	3
Acción de FTP permitida	Indica que se ha permitido una acción de FTP.	1
Acción de FTP denegada	Indica que se ha denegado una acción de FTP.	3
Objeto en memoria caché	Indica que un objeto se ha almacenado en la memoria caché.	1
Objeto no en memoria caché	Indica que un objeto no se ha almacenado en la memoria caché.	1
Limitación de tasa	Indica que la red limita la velocidad del tráfico.	4
Sin limitación de velocidad	Indica que la red no limita la velocidad del tráfico.	0

Explotación

La categoría de explotación contiene sucesos en los que se ha producido una explotación (ataque) de acceso o de comunicación.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de explotación.

Tabla 95. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de explotación

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Ataque de Explotación desconocido	Indica un ataque de explotación desconocido.	9

Tabla 95. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de explotación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Desbordamiento de almacenamiento intermedio	Indica un desbordamiento de almacenamiento intermedio.	9
Explotación de DNS	Indica una explotación de DNS.	9
Explotación de Telnet	Indica una explotación de Telnet.	9
Explotación de Linux	Indica una explotación de Linux.	9
Explotación de UNIX	Indica una explotación de UNIX.	9
Explotación de Windows	Indica una explotación de Microsoft Windows.	9
Explotación de correo	Indica una explotación del servidor de correo.	9
Explotación de infraestructura	Indica una explotación de la infraestructura.	9
Explotación diversa	Indica una explotación diversa.	9
Explotación de web	Indica una explotación de web.	9
Apropiación de sesión	Indica que se ha intervenido en una sesión de la red.	9
Gusano activo	Indica que hay un gusano activo.	10
Adivinación/recuperación de contraseña	Indica que un usuario ha solicitado acceso a su información de contraseña en la base de datos.	9
Explotación de FTP	Indica una explotación de FTP.	9
Explotación de RPC	Indica una explotación de RPC.	9
Explotación de SNMP	Indica una explotación de SNMP.	9
Explotación de NOOP	Indica una explotación de NOOP.	9
Explotación de Samba	Indica una explotación de Samba.	9
Explotación de base de datos	Indica una explotación de base de datos.	9
Explotación de SSH	Indica una explotación de SSH.	9
Explotación de ICMP	Indica una explotación de ICMP.	9
Explotación de UDP	Indica una explotación de UDP.	9

Tabla 95. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de explotación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Explotación de explorador	Indica una explotación en el navegador.	9
Explotación de DHCP	Indica una explotación de DHCP.	9
Explotación de acceso remoto	Indica una explotación de acceso remoto.	9
Explotación de ActiveX	Indica una explotación a través de una aplicación ActiveX.	9
Inyección de SQL	Indica que se ha efectuado una inyección de SQL.	9
Scripts entre sitios	Indica una vulnerabilidad de scripts entre sitios.	9
Vulnerabilidad de serie de formato	Indica una vulnerabilidad de serie de formato.	9
Explotación de validación de entrada	Indica que se ha detectado un intento de explotación de validación de entrada.	9
Ejecución remota de código	Indica que se ha detectado un intento de ejecución remota de código.	9
Daño en la memoria	Indica que se ha detectado una explotación de daño en la memoria.	9
Ejecución de mandato	Indica que se ha detectado un intento de ejecución de mandato remota.	9

Programa malicioso

La categoría de programa malicioso (software malicioso o malware) contiene sucesos que están relacionados con los intentos de explotaciones de aplicación y de desbordamiento de almacenamiento intermedio.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de programa malicioso.

Tabla 96. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de programa malicioso

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Programa malicioso desconocido	Indica un virus desconocido.	4
Puerta trasera detectada	Indica que se ha detectado una puerta trasera en el sistema.	9

Tabla 96. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de programa malicioso (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Archivo adjunto de correo hostil	Indica un archivo adjunto de correo hostil.	6
Software malicioso	Indica un virus.	6
Descarga de software hostil	Indica una descarga de software hostil a la red.	6
Virus detectado	Indica que se ha detectado un virus.	8
Programa malicioso diverso	Indica software malicioso diverso.	4
Troyano detectado	Indica que se ha detectado un troyano.	7
Spyware detectado	Indica que se ha detectado spyware en el sistema.	6
Exploración de contenido	Indica que se ha detectado un intento de exploración del contenido.	3
Exploración de contenido fallida	Indica que una exploración del contenido ha fallado.	8
Exploración de contenido satisfactoria	Indica que una exploración del contenido ha sido satisfactoria.	3
Exploración de contenido en curso	Indica que hay una exploración del contenido en curso.	3
Registrador de claves	Indica que se ha detectado un registrador de claves.	7
Adware detectado	Indica que se ha detectado adware.	4
Cuarentena satisfactoria	Indica que una acción de cuarentena se ha completado satisfactoriamente.	3
Cuarentena fallida	Indica que una acción de cuarentena ha fallado.	8

Actividad sospechosa

La categoría Sospechoso contiene sucesos que están relacionados con virus, troyanos, ataques por puertas traseras y otras formas de software hostil.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de actividad sospechosa.

Tabla 97. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de actividad sospechosa

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Suceso sospechoso desconocido	Indica un suceso sospechoso desconocido.	3
Patrón sospechoso detectado	Indica que se ha detectado un patrón sospechoso.	3
Contenido modificado por cortafuegos	Indica que el cortafuegos ha modificado el contenido.	3
Mandato o datos no válidos	Indica un mandato o datos que no son válidos.	3
Paquete sospechoso	Indica un paquete sospechoso.	3
Actividad sospechosa	Indica actividad sospechosa.	3
Nombre de archivo sospechoso	Indica un nombre de archivo sospechoso.	3
Actividad de puerto sospechosa	Indica actividad de puerto sospechosa.	3
Direccionamiento sospechoso	Indica un direccionamiento sospechoso.	3
Vulnerabilidad de web potencial	Indica una vulnerabilidad de web potencial.	3
Suceso de evasión desconocido	Indica un suceso de evasión desconocido.	5
Suplantación de IP	Indica una suplantación de IP.	5
Fragmentación de IP	Indica una fragmentación de IP.	3
Fragmentos de IP solapados	Indica fragmentos de IP solapados.	5
Evasión de IDS	Indica una evasión de IDS.	5
Anomalía de protocolo de DNS	Indica una anomalía de protocolo de DNS.	3
Anomalía de protocolo de FTP	Indica una anomalía de protocolo de FTP.	3
Anomalía de protocolo de correo	Indica una anomalía de protocolo de correo.	3
Anomalía de protocolo de direccionamiento	Indica una anomalía de protocolo de direccionamiento.	3
Anomalía de protocolo de web	Indica una anomalía de protocolo de web.	3
Anomalía de protocolo de SQL	Indica una anomalía de protocolo de SQL.	3
Código ejecutable detectado	Indica que se ha detectado código ejecutable.	5
Suceso sospechoso diverso	Indica un suceso sospechoso diverso.	3

Tabla 97. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de actividad sospechosa (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Filtración de información	Indica una filtración de información.	1
Vulnerabilidad de correo potencial	Indica una vulnerabilidad potencial en el servidor de correo.	4
Vulnerabilidad de versión potencial	Indica una vulnerabilidad potencial en la versión de IBM Security QRadar.	4
Vulnerabilidad de FTP potencial	Indica una vulnerabilidad potencial de FTP.	4
Vulnerabilidad de SSH potencial	Indica una vulnerabilidad potencial de SSH.	4
Vulnerabilidad de DNS potencial	Indica una vulnerabilidad potencial en el servidor DNS.	4
Vulnerabilidad de SMB potencial	Indica una vulnerabilidad potencial de SMB (Samba).	4
Vulnerabilidad de base de datos potencial	Indica una vulnerabilidad potencial en la base de datos.	4
Anomalía de protocolo IP	Indica una anomalía de protocolo IP potencial.	3
Dirección IP sospechosa	Indica que se ha detectado una dirección IP sospechosa.	2
Uso de protocolo IP no válido	Indica un protocolo IP no válido.	2
Protocolo no válido	Indica un protocolo no válido.	4
Sucesos de Windows sospechosos	Indica un suceso sospechoso con una pantalla del escritorio.	2
Actividad de ICMP sospechosa	Indica actividad de ICMP sospechosa.	2
Vulnerabilidad de NFS potencial	Indica una vulnerabilidad potencial de NFS (Network File System).	4
Vulnerabilidad de NNTP potencial	Indica una vulnerabilidad potencial de NNTP (protocolo para la transferencia de noticias en red).	4
Vulnerabilidad de RPC potencial	Indica una vulnerabilidad potencial de RPC.	4
Vulnerabilidad de Telnet potencial	Indica una vulnerabilidad potencial de Telnet en el sistema.	4
Vulnerabilidad de SNMP potencial	Indica una vulnerabilidad potencial de SNMP.	4

Tabla 97. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de actividad sospechosa (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Combinación de distintivos de TCP no permitida	Indica que se ha detectado una combinación de distintivos de TCP no válida.	5
Combinación de distintivos de TCP sospechosa	Indica que se ha detectado una combinación de distintivos de TCP potencialmente no válida.	4
Uso no permitido de protocolo ICMP	Indica que se ha detectado un uso no válido del protocolo ICMP.	5
Uso sospechoso de protocolo ICMP	Indica que se ha detectado un uso potencialmente no válido del protocolo ICMP.	4
Tipo de ICMP no permitido	Indica que se ha detectado un tipo de ICMP no válido.	5
Código de ICMP no permitido	Indica que se ha detectado un código de ICMP no válido.	5
Tipo de ICMP sospechoso	Indica que se ha detectado un tipo de ICMP potencialmente no válido.	4
Código de ICMP sospechoso	Indica que se ha detectado un código de ICMP potencialmente no válido.	4
Puerto TCP 0	Indica que un paquete TCP utiliza un puerto reservado (0) como origen o destino.	4
Puerto UDP 0	Indica que un paquete UDP utiliza un puerto reservado (0) como origen o destino.	4
IP hostil	Indica el uso de una dirección IP hostil conocida.	4
IP de lista de observación	Indica el uso de una dirección IP incluida en una lista de observación de direcciones IP.	4
IP de delincuente conocido	Indica el uso de una dirección IP de un delincuente conocido.	4
IP de RFC 1918 (privado)	Indica el uso de una dirección IP incluida en un rango de direcciones IP privadas.	4
Vulnerabilidad de VoIP potencial	Indica una vulnerabilidad potencial de VoIP.	4
Dirección de lista negra	Indica que una dirección IP está en la lista negra.	8

Tabla 97. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de actividad sospechosa (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Dirección de lista de observación	Indica que la dirección IP está en la lista de direcciones IP que se están supervisando.	7
Dirección de red oscura	Indica que la dirección IP forma parte de una red oscura.	5
Dirección de botnet	Indica que la dirección forma parte de un botnet.	7
Dirección sospechosa	Indica que la dirección IP debe ser supervisada.	5
Contenido erróneo	Indica que se ha detectado contenido erróneo.	7
Certificación no válida	Indica que se ha detectado un certificado no válido.	7
Actividad de usuario	Indica que se ha detectado actividad de usuario.	7
Uso de protocolo sospechoso	Indica que se ha detectado el uso de un protocolo sospechoso.	5
Actividad de BGP sospechosa	Indica que se ha detectado un uso sospechoso de BGP (protocolo de pasarela fronteriza).	5
Envenenamiento de ruta	Indica que se han detectado daños en la ruta.	5
Envenenamiento de ARP	Indica que se ha detectado el envenenamiento de la memoria caché de ARP.	5
Dispositivo malintencionado detectado	Indica que se ha detectado un dispositivo malintencionado.	5

Sistema

La categoría de sistema contiene sucesos que están relacionados con los cambios del sistema, la instalación de software o los mensajes de estado.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de sistema.

Tabla 98. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de sistema

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Suceso del sistema desconocido	Indica un suceso de sistema desconocido.	1

Tabla 98. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de sistema (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Arranque del sistema	Indica un reinicio del sistema.	1
Configuración del sistema	Indica que se ha aplicado un cambio en la configuración del sistema.	1
Detención del sistema	Indica que el sistema se ha detenido.	1
Anomalía del sistema	Indica una anomalía del sistema.	6
Estado del sistema	Indica cualquier suceso de información.	1
Error del sistema	Indica un error del sistema.	3
Suceso del sistema diverso	Indica un suceso de sistema diverso.	1
Servicio iniciado	Indica que se han iniciado servicios del sistema.	1
Servicio detenido	Indica que se han detenido servicios del sistema.	1
Anomalía de servicio	Indica una anomalía del sistema.	6
Modificación satisfactoria del registro	Indica que una modificación aplicada al registro ha sido satisfactoria.	1
Modificación satisfactoria de la política de host	Indica que una modificación aplicada a la política de host ha sido satisfactoria.	1
Modificación satisfactoria de archivo	Indica que una modificación aplicada a un archivo ha sido satisfactoria.	1
Modificación satisfactoria de pila	Indica que una modificación aplicada a la pila ha sido satisfactoria.	1
Modificación satisfactoria de aplicación	Indica que una modificación aplicada a la aplicación ha sido satisfactoria.	1
Modificación satisfactoria de configuración	Indica que una modificación aplicada a la configuración ha sido satisfactoria.	1
Modificación satisfactoria de servicio	Indica que una modificación aplicada a un servicio ha sido satisfactoria.	1
Modificación fallida del registro	Indica que una modificación aplicada al registro ha fallado.	1
Modificación fallida de la política de host	Indica que una modificación aplicada a la política de host ha fallado.	1

Tabla 98. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de sistema (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Modificación fallida de archivo	Indica que una modificación aplicada a un archivo ha fallado.	1
Modificación fallida de pila	Indica que una modificación aplicada a la pila ha fallado.	1
Modificación fallida de aplicación	Indica que una modificación aplicada a una aplicación ha fallado.	1
Modificación fallida de configuración	Indica que una modificación aplicada a la configuración ha fallado.	1
Modificación fallida de servicio	Indica que una modificación aplicada al servicio ha fallado.	1
Adición de registro	Indica que se ha añadido un nuevo elemento al registro.	1
Política de host creada	Indica que se ha añadido una nueva entrada al registro.	1
Archivo creado	Indica que se ha creado un nuevo archivo en el sistema.	1
Aplicación instalada	Indica que se ha instalado una aplicación nueva en el sistema.	1
Servicio instalado	Indica que se ha instalado un servicio nuevo en el sistema.	1
Supresión del registro	Indica que se ha suprimido una entrada de registro.	1
Política de host suprimida	Indica que se ha suprimido una entrada de política de host.	1
Archivo suprimido	Indica que se ha suprimido un archivo.	1
Aplicación desinstalada	Indica que una aplicación se ha desinstalado.	1
Servicio desinstalado	Indica que un servicio se ha desinstalado.	1
Información del sistema	Indica información del sistema.	3
Acción del sistema Permitir	Indica que se ha autorizado una acción intentada en el sistema.	3
Acción del sistema Denegar	Indica que se ha denegado una acción intentada en el sistema.	4
Cron	Indica que hay un mensaje de crontab.	1

Tabla 98. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de sistema (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Estado de Cron	Indica que hay un mensaje de estado de crontab.	1
Cron fallido	Indica que hay un mensaje de error de crontab.	4
Cron satisfactorio	Indica que hay un mensaje de éxito de crontab.	1
Daemon	Indica que hay un mensaje de daemon.	1
Estado de daemon	Indica que hay un mensaje de estado de daemon.	1
Daemon fallido	Indica que hay un mensaje de error de daemon.	4
Daemon satisfactorio	Indica que hay un mensaje de éxito de daemon.	1
Kernel	Indica que hay un mensaje de kernel.	1
Estado de kernel	Indica que hay un mensaje de estado de kernel.	1
Kernel fallido	Indica que hay un mensaje de error de kernel.	
Kernel satisfactorio	Indica que hay un mensaje de éxito de kernel.	1
Autenticación	Indica que hay un mensaje de autenticación.	1
Información	Indica que hay un mensaje informativo.	2
Aviso	Indica que hay un mensaje de aviso.	3
Advertencia	Indica que hay un mensaje de advertencia.	5
Error	Indica que hay un mensaje de error.	7
Crítico	Indica que hay un mensaje crítico.	9
Depuración	Indica que hay un mensaje de depuración.	1
Mensajes	Indica que hay un mensaje genérico.	1
Acceso de privilegio	Indica que se ha intentado el acceso de privilegio.	3
Alerta	Indica que hay un mensaje de alerta.	9
Emergencia	Indica que hay un mensaje de emergencia.	9

Tabla 98. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de sistema (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Estado SNMP	Indica que hay un mensaje de estado de SNMP.	1
Estado FTP	Indica que hay un mensaje de estado de FTP.	1
Estado de NTP	Indica que hay un mensaje de estado de NTP.	1
Anomalía de radio de punto de acceso	Indica una anomalía de radio de punto de acceso.	3
Discrepancia de configuración de protocolo de cifrado	Indica una discrepancia de configuración de protocolo de cifrado.	3
Dispositivo de cliente o servidor de autenticación mal configurado	Indica que un dispositivo de cliente o un servidor de autenticación no se ha configurado correctamente.	5
Habilitación de espera activa fallida	Indica un error de habilitación de espera activa.	5
Inhabilitación de espera activa fallida	Indica un error de inhabilitación de espera activa.	5
La espera activa se ha habilitado satisfactoriamente	Indica que la espera activa se ha habilitado satisfactoriamente.	1
Asociación de espera activa perdida	Indica que la asociación de espera activa se ha perdido.	5
Anomalía de iniciación de modalidad principal	Indica una anomalía de iniciación de modalidad principal.	5
Iniciación de modalidad principal satisfactoria	Indica que la iniciación de modalidad principal ha sido satisfactoria.	1
Estado de modalidad principal	Indica que se ha notificado un mensaje de estado de modalidad principal.	1
Anomalía de iniciación de modalidad rápida	Indica que la iniciación de modalidad rápida ha fallado.	5
Iniciación de modalidad rápida satisfactoria	Indica que la iniciación de modalidad rápida ha sido satisfactoria.	1
Estado de modalidad rápida	Indica que se ha notificado un mensaje de estado de modalidad rápida.	1
Licencia no válida	Indica una licencia no válida.	3
Licencia caducada	Indica una licencia caducada.	3
Licencia nueva aplicada	Indica que se ha aplicado una licencia nueva.	1
Error de licencia	Indica un error de licencia.	5

Tabla 98. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de sucesos de sistema (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Estado de licencia	Indica que hay un mensaje de estado de licencia.	1
Error de configuración	Indica que se ha detectado un error de configuración.	5
Interrupción de servicio	Indica que se ha detectado una interrupción en el servicio.	5
Licencia sobrepasada	Indica que se han sobrepasado las prestaciones de la licencia.	3
Estado de rendimiento	Indica que se ha notificado el estado de rendimiento.	1
Degradación de rendimiento	Indica que se ha degradado el rendimiento.	4
Configuración errónea	Indica que se ha detectado una configuración incorrecta.	5

Política

La categoría de política contiene sucesos que están relacionados con la administración de la política de red y la supervisión de los recursos de la red para comprobar si se producen violaciones de la política.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de política.

Tabla 99. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de política

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Violación de política desconocida	Indica una violación de política desconocida.	2
Violación de política de web	Indica una violación de política de web.	2
Violación de política de acceso remoto	Indica una violación de política de acceso remoto.	2
Violación de política de IRC/IM	Indica una violación de política de mensajería instantánea.	2
Violación de política de P2P	Indica una violación de política de P2P (de igual a igual).	2
Violación de política de acceso de IP	Indica una violación de política de acceso de IP.	2
Violación de política de aplicación	Indica una violación de política de aplicación.	2

Tabla 99. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de política (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Violación de política de base de datos	Indica una violación de política de base de datos.	2
Violación de política de umbral de red	Indica una violación de política de umbral de red.	2
Violación de política de contenido para adultos	Indica una violación de contenido para adultos.	2
Violación de política de juegos	Indica una violación de política de juegos.	2
Violación de política diversa	Indica una violación de política diversa.	2
Violación de política de conformidad	Indica una violación de política de conformidad.	2
Violación de política de correo	Indica una violación de política de correo.	2
Violación de política de IRC	Indica una violación de política de IRC.	2
Violación de política de IM	Indica una violación de política que está relacionada con actividades de mensajería instantánea (IM).	2
Violación de política de VoIP	Indica una violación de política de VoIP.	2
Satisfactorio	Indica un mensaje de éxito de la política.	1
Anómalo	Indica un mensaje de error de la política.	4

Desconocido

La categoría Desconocido contiene sucesos que no se analizan y, por lo tanto, no se pueden asignar a ninguna categoría.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría Desconocido.

Tabla 100. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría Desconocido

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Desconocido	Indica un suceso desconocido.	3
Suceso de Snort desconocido	Indica un suceso de Snort desconocido.	3
Suceso de Dragon desconocido	Indica un suceso de Dragon desconocido.	3

Tabla 100. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría Desconocido (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Suceso de cortafuegos Pix desconocido	Indica un suceso de Cisco Private Internet Exchange (PIX) Firewall desconocido.	3
Suceso de punto crítico desconocido	Indica un suceso de HP TippingPoint desconocido.	3
Suceso de servidor de autenticación de Windows desconocido	Indica un suceso de Windows Auth Server desconocido.	3
Suceso de Nortel desconocido	Indica un suceso de Nortel desconocido.	3
Almacenado	Indica un suceso almacenado desconocido.	3
Conductual	Indica un suceso de comportamiento desconocido.	3
Umbral	Indica un suceso de umbral desconocido.	3
Anomalía	Indica un suceso de anomalía desconocido.	3

CRE

La categoría de suceso de regla personalizada (CRE) contiene sucesos que se generan a partir de una regla personalizada de delito, flujo o suceso.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de CRE.

Tabla 101. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de CRE

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Suceso de CRE desconocido	Indica un suceso de motor de reglas personalizadas desconocido.	5
Coincidencia de regla de suceso individual	Indica una coincidencia de regla de suceso individual.	5
Coincidencia de regla de secuencia de sucesos	Indica una coincidencia de regla de secuencia de sucesos.	5
Coincidencia de regla de secuencia de sucesos de delito cruzado	Indica una coincidencia de regla de secuencia de sucesos de delito cruzado.	5
Coincidencia de regla de delito	Indica una coincidencia de regla de delito.	5

Explotación potencial

La categoría de explotación potencial contiene sucesos que están relacionados con intentos de explotaciones potenciales de aplicación y de desbordamiento de almacenamiento intermedio.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de explotación potencial.

Tabla 102. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de explotación potencial

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Ataque de explotación potencial desconocido	Indica que se ha detectado un ataque de explotación potencial.	7
Desbordamiento de almacenamiento intermedio potencial	Indica que se ha detectado un desbordamiento de almacenamiento intermedio potencial.	7
Explotación de DNS potencial	Indica que se ha detectado un ataque de explotación potencial a través del servidor DNS.	7
Explotación de Telnet potencial	Indica que se ha detectado un ataque de explotación potencial a través de Telnet.	7
Explotación de Linux potencial	Indica que se ha detectado un ataque de explotación potencial a través de Linux.	7
Explotación de Unix potencial	Indica que se ha detectado un ataque de explotación potencial a través de UNIX.	7
Explotación de Windows potencial	Indica que se ha detectado un ataque de explotación potencial a través de Windows.	7
Explotación de correo potencial	Indica que se ha detectado un ataque de explotación potencial a través del correo.	7
Explotación de infraestructura potencial	Indica que se ha detectado un ataque de explotación potencial en la infraestructura del sistema.	7
Explotación diversa potencial	Indica que se ha detectado un ataque de explotación potencial.	7
Explotación de web potencial	Indica que se ha detectado un ataque de explotación potencial a través de la Web.	7
Conexión del Botnet potencial	Indica un ataque de explotación potencial que utiliza botnet.	6

Tabla 102. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de explotación potencial (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Actividad de gusano potencial	Indica que se ha detectado un ataque potencial que utiliza actividad de gusano.	6

Definido por el usuario

La categoría Definido por el usuario contiene sucesos que están relacionados con objetos definidos por el usuario.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría Definido por el usuario.

Tabla 103. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría Definido por el usuario

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sentry personalizado bajo	Indica un suceso de anomalía personalizado de gravedad baja.	3
Sentry personalizado medio	Indica un suceso de anomalía personalizado de gravedad media.	5
Sentry personalizado alto	Indica un suceso de anomalía personalizado de gravedad alta.	7
Sentry personalizado 1	Indica un suceso de anomalía personalizado con el nivel de gravedad 1.	1
Sentry personalizado 2	Indica un suceso de anomalía personalizado con el nivel de gravedad 2.	2
Sentry personalizado 3	Indica un suceso de anomalía personalizado con el nivel de gravedad 3.	3
Sentry personalizado 4	Indica un suceso de anomalía personalizado con el nivel de gravedad 4.	4
Sentry personalizado 5	Indica un suceso de anomalía personalizado con el nivel de gravedad 5.	5
Sentry personalizado 6	Indica un suceso de anomalía personalizado con el nivel de gravedad 6.	6
Sentry personalizado 7	Indica un suceso de anomalía personalizado con el nivel de gravedad 7.	7

Tabla 103. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría Definido por el usuario (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sentry personalizado 8	Indica un suceso de anomalía personalizado con el nivel de gravedad 8.	8
Sentry personalizado 9	Indica un suceso de anomalía personalizado con el nivel de gravedad 9.	9
Política personalizada baja	Indica un suceso de política personalizado con un nivel de gravedad bajo.	3
Política personalizada media	Indica un suceso de política personalizado con un nivel de gravedad medio.	5
Política personalizada alta	Indica un suceso de política personalizado con un nivel de gravedad alto.	7
Política personalizada 1	Indica un suceso de política personalizado con el nivel de gravedad 1.	1
Política personalizada 2	Indica un suceso de política personalizado con el nivel de gravedad 2.	2
Política personalizada 3	Indica un suceso de política personalizado con el nivel de gravedad 3.	3
Política personalizada 4	Indica un suceso de política personalizado con el nivel de gravedad 4.	4
Política personalizada 5	Indica un suceso de política personalizado con el nivel de gravedad 5.	5
Política personalizada 6	Indica un suceso de política personalizado con el nivel de gravedad 6.	6
Política personalizada 7	Indica un suceso de política personalizado con el nivel de gravedad 7.	7
Política personalizada 8	Indica un suceso de política personalizado con el nivel de gravedad 8.	8
Política personalizada 9	Indica un suceso de política personalizado con el nivel de gravedad 9.	9
Usuario personalizado bajo	Indica un suceso de usuario personalizado con un nivel de gravedad bajo.	3
Usuario personalizado medio	Indica un suceso de usuario personalizado con un nivel de gravedad medio.	5

Tabla 103. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría Definido por el usuario (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Usuario personalizado alto	Indica un suceso de usuario personalizado con un nivel de gravedad alto.	7
Usuario personalizado 1	Indica un suceso de usuario personalizado con el nivel de gravedad 1.	1
Usuario personalizado 2	Indica un suceso de usuario personalizado con el nivel de gravedad 2.	2
Usuario personalizado 3	Indica un suceso de usuario personalizado con el nivel de gravedad 3.	3
Usuario personalizado 4	Indica un suceso de usuario personalizado con el nivel de gravedad 4.	4
Usuario personalizado 5	Indica un suceso de usuario personalizado con el nivel de gravedad 5.	5
Usuario personalizado 6	Indica un suceso de usuario personalizado con el nivel de gravedad 6.	6
Usuario personalizado 7	Indica un suceso de usuario personalizado con el nivel de gravedad 7.	7
Usuario personalizado 8	Indica un suceso de usuario personalizado con el nivel de gravedad 8.	8
Usuario personalizado 9	Indica un suceso de usuario personalizado con el nivel de gravedad 9.	9

Auditoría de SIM

La categoría Auditoría de SIM contiene sucesos que están relacionados con la interacción del usuario con consola de QRadar y las funciones administrativas.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría Auditoría de SIM.

Tabla 104. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría Auditoría de SIM

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Autenticación de usuario de SIM	Indica un inicio o un cierre de sesión del usuario en la consola.	5

Tabla 104. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría Auditoría de SIM (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Cambio de configuración de SIM	Indica que un usuario ha cambiado el despliegue o la configuración de SIM.	3
Acción de usuario de SIM	Indica que un usuario ha iniciado un proceso como, por ejemplo, iniciar una copia de seguridad o generar un informe, en el módulo SIM.	3
Sesión creada	Indica que se ha creado una sesión de usuario.	3
Sesión destruida	Indica que se ha destruido una sesión de usuario.	3
Sesión de Admin creada	Indica que se ha creado una sesión de administrador.	
Sesión de Admin destruida	Indica que se ha destruido una sesión de administrador.	3
Sesión de autenticación no válida	Indica una sesión de autenticación no válida.	5
Sesión de autenticación caducada	Indica que la autenticación de una sesión ha caducado.	3
Configuración de Risk Manager	Indica que un usuario ha cambiado la configuración de IBM Security QRadar Risk Manager.	3

Descubrimiento de host de VIS

Cuando el componente VIS descubre y almacena nuevos hosts, puertos o vulnerabilidades que se han detectado en la red, el componente VIS genera sucesos. Estos sucesos se envían al Recopilador de sucesos para correlacionarlos con otros sucesos de seguridad.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de descubrimiento de host de VIS.

Tabla 105. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de descubrimiento de host de VIS

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Host nuevo descubierto	Indica que el componente VIS ha detectado un host nuevo.	3
Puerto nuevo descubierto	Indica que el componente VIS ha detectado un puerto abierto nuevo.	3

Tabla 105. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de descubrimiento de host de VIS (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Vuln. nueva descubierta	Indica que el componente VIS ha detectado una vulnerabilidad nueva.	3
SO nuevo descubierto	Indica que el componente VIS ha detectado un sistema operativo nuevo en un host.	3
Host masivo descubierto	Indica que el componente VIS ha detectado demasiados hosts nuevos en un periodo corto de tiempo.	3

Aplicación

La categoría de aplicación contiene sucesos que están relacionados con la actividad de auditoría, como el correo electrónico o la actividad de FTP.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de aplicación.

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Correo abierto	Indica que se ha establecido una conexión de correo electrónico.	1
Correo cerrado	Indica que se ha cerrado una conexión de correo electrónico.	1
Correo restablecido	Indica que se ha restablecido una conexión de correo electrónico.	3
Correo terminado	Indica que se ha terminado una conexión de correo electrónico.	4
Correo denegado	Indica que se ha denegado una conexión de correo electrónico.	4
Correo en curso	Indica que se está intentando una conexión de correo electrónico.	1
Correo retardado	Indica que se ha retardado una conexión de correo electrónico.	4
Correo en cola	Indica que se ha puesto en cola una conexión de correo electrónico.	3

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Correo redirigido	Indica que se ha redirigido una conexión de correo electrónico.	1
FTP abierto	Indica que se ha abierto una conexión de FTP.	1
FTP cerrado	Indica que se ha cerrado una conexión de FTP.	1
FTP restablecido	Indica que se ha restablecido una conexión de FTP.	3
FTP terminado	Indica que se ha terminado una conexión de FTP.	4
FTP denegado	Indica que se ha denegado una conexión de FTP.	4
FTP en curso	Indica que hay una conexión de FTP en curso.	1
FTP redirigido	Indica que se ha redirigido una conexión de FTP.	3
HTTP abierto	Indica que se ha establecido una conexión de HTTP.	1
HTTP cerrado	Indica que se ha cerrado una conexión de HTTP.	1
HTTP restablecido	Indica que se ha restablecido una conexión de HTTP.	3
HTTP terminado	Indica que se ha terminado una conexión de HTTP.	4
HTTP denegado	Indica que se ha denegado una conexión de HTTP.	4
HTTP en curso	Indica que hay una conexión de HTTP en curso.	1
HTTP retardado	Indica que se ha retardado una conexión de HTTP.	3
HTTP en cola	Indica que se ha puesto en cola una conexión de HTTP.	1
HTTP redirigido	Indica que se ha redirigido una conexión de HTTP.	1
Proxy HTTP	Indica que una conexión de HTTP se está pasando a través de un proxy.	1
HTTPS abierto	Indica que se ha establecido una conexión de HTTPS.	1
HTTPS cerrado	Indica que se ha cerrado una conexión de HTTPS.	1
HTTPS restablecido	Indica que se ha restablecido una conexión de HTTPS.	3
HTTPS terminado	Indica que se ha terminado una conexión de HTTPS.	4

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
HTTPS denegado	Indica que se ha denegado una conexión de HTTPS.	4
HTTPS en curso	Indica que hay una conexión de HTTPS en curso.	1
HTTPS retardado	Indica que se ha retardado una conexión de HTTPS.	3
HTTPS en cola	Indica que se ha puesto en cola una conexión de HTTPS.	3
HTTPS redirigido	Indica que se ha redirigido una conexión de HTTPS.	3
HTTPS Proxy	Indica que una conexión de HTTPS pasa a través de un proxy.	1
SSH abierto	Indica que se ha establecido una conexión de SSH.	1
SSH cerrado	Indica que se ha cerrado una conexión de SSH.	1
SSH restablecido	Indica que se ha restablecido una conexión de SSH.	3
SSH terminado	Indica que se ha terminado una conexión de SSH.	4
SSH denegado	Indica que se ha denegado una sesión de SSH.	4
SSH en curso	Indica que hay una sesión de SSH en curso.	1
Acceso remoto abierto	Indica que se ha establecido una conexión de acceso remoto.	1
Acceso remoto cerrado	Indica que se ha cerrado una conexión de acceso remoto.	1
Acceso remoto restablecido	Indica que se ha restablecido una conexión de acceso remoto.	3
Acceso remoto terminado	Indica que se ha terminado una conexión de acceso remoto.	4
Acceso remoto denegado	Indica que se ha denegado una conexión de acceso remoto.	4
Acceso remoto en curso	Indica que hay una conexión de acceso remoto en curso.	1
Acceso remoto retardado	Indica que se ha retardado una conexión de acceso remoto.	3
Acceso remoto redirigido	Indica que se ha redirigido una conexión de acceso remoto.	3

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
VPN abierta	Indica que se ha abierto una conexión de VPN.	1
VPN cerrada	Indica que se ha cerrado una conexión de VPN.	1
VPN restablecida	Indica que se ha restablecido una conexión de VPN.	3
VPN terminada	Indica que se ha terminado una conexión de VPN.	4
VPN denegada	Indica que se ha denegado una conexión de VPN.	4
VPN en curso	Indica que hay una conexión de VPN en curso.	1
VPN retardada	Indica que una conexión de VPN se ha retardado.	3
VPN en cola	Indica que se ha puesto en cola una conexión de VPN.	3
VPN redirigida	Indica que se ha redirigido una conexión de VPN.	3
RDP abierto	Indica que se ha establecido una conexión de RDP.	1
RDP cerrado	Indica que se ha cerrado una conexión de RDP.	1
RDP restablecido	Indica que se ha restablecido una conexión de RDP.	3
RDP terminado	Indica que se ha terminado una conexión de RDP.	4
RDP denegado	Indica que se ha denegado una conexión de RDP.	4
RDP en curso	Indica que hay una conexión de RDP en curso.	1
RDP redirigido	Indica que se ha redirigido una conexión de RDP.	3
Transferencia de archivos abierta	Indica que se ha establecido una conexión de transferencia de archivos.	1
Transferencia de archivos cerrada	Indica que se ha cerrado una conexión de transferencia de archivos.	1
Transferencia de archivos restablecida	Indica que se ha restablecido una conexión de transferencia de archivos.	3
Transferencia de archivos terminada	Indica que se ha terminado una conexión de transferencia de archivos.	4

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Transferencia de archivos denegada	Indica que se ha denegado una conexión de transferencia de archivos.	4
Transferencia de archivos en curso	Indica que hay una conexión de transferencia de archivos en curso.	1
Transferencia de archivos retardada	Indica que se ha retardado una conexión de transferencia de archivos.	3
Transferencia de archivos en cola	Indica que se ha puesto en cola una conexión de transferencia de archivos.	3
Transferencia de archivos redirigida	Indica que se ha redirigido una conexión de transferencia de archivos.	3
DNS abierto	Indica que se ha establecido una conexión de DNS.	1
DNS cerrado	Indica que se ha cerrado una conexión de DNS.	1
DNS restablecido	Indica que se ha restablecido una conexión de DNS.	5
DNS terminado	Indica que se ha terminado una conexión de DNS.	5
DNS denegado	Indica que se ha denegado una conexión de DNS.	5
DNS en curso	Indica que hay una conexión de DNS en curso.	1
DNS retardado	Indica que se ha retardado una conexión de DNS.	5
DNS redirigido	Indica que se ha redirigido una conexión de DNS.	4
Conversación abierta	Indica que se ha abierto una conexión de conversación.	1
Conversación cerrada	Indica que se ha cerrado una conexión de conversación.	1
Conversación restablecida	Indica que se ha restablecido una conexión de conversación.	3
Conversación terminada	Indica que se ha terminado una conexión de conversación.	3
Conversación denegada	Indica que se ha denegado una conexión de conversación.	3
Conversación en curso	Indica que hay una conexión de conversación en curso.	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Conversación redirigida	Indica que se ha redirigido una conexión de conversación.	1
Base de datos abierta	Indica que se ha establecido una conexión a base de datos.	1
Base de datos cerrada	Indica que se ha cerrado una conexión a base de datos.	1
Base de datos restablecida	Indica que se ha restablecido una conexión a base de datos.	5
Base de datos terminada	Indica que se ha terminado una conexión a base de datos.	5
Base de datos denegada	Indica que se ha denegado una conexión a base de datos.	5
Base de datos en curso	Indica que hay una conexión a base de datos en curso.	1
Base de datos redirigida	Indica que se ha redirigido una conexión a base de datos.	3
SMTP abierto	Indica que se ha establecido una conexión de SMTP.	1
SMTP cerrado	Indica que se ha cerrado una conexión de SMTP.	1
SMTP restablecido	Indica que se ha restablecido una conexión de SMTP.	3
SMTP terminado	Indica que se ha terminado una conexión de SMTP.	5
SMTP denegado	Indica que se ha denegado una conexión de SMTP.	5
SMTP en curso	Indica que hay una conexión de SMTP en curso.	1
SMTP retardado	Indica que se ha retardado una conexión de SMTP.	3
SMTP en cola	Indica que se ha puesto en cola una conexión de SMTP.	3
SMTP redirigido	Indica que se ha redirigido una conexión de SMTP.	3
Autenticación abierta	Indica que se ha establecido una conexión con el servidor de autorizaciones.	1
Autenticación cerrada	Indica que se ha cerrado una conexión con el servidor de autorizaciones.	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Autenticación restablecida	Indica que se ha restablecido una conexión con el servidor de autorizaciones.	3
Autenticación terminada	Indica que se ha terminado una conexión con el servidor de autorizaciones.	4
Autenticación denegado	Indica que se ha denegado una conexión con el servidor de autorizaciones.	4
Autenticación en curso	Indica que hay una conexión con el servidor de autorizaciones en curso.	1
Autenticación retardada	Indica que se ha retardado una conexión con el servidor de autorizaciones.	3
Autenticación en cola	Indica que se ha puesto en cola una conexión con el servidor de autorizaciones.	3
Autenticación redirigida	Indica que se ha redirigido una conexión con el servidor de autorizaciones.	2
P2P abierto	Indica que se ha establecido una conexión de P2P (de igual a igual).	1
P2P cerrado	Indica que se ha cerrado una conexión de P2P.	1
P2P restablecido	Indica que se ha restablecido una conexión de P2P.	4
P2P terminado	Indica que se ha terminado una conexión de P2P.	4
P2P denegado	Indica que se ha denegado una conexión de P2P.	3
P2P en curso	Indica que hay una conexión de P2P en curso.	1
Web abierta	Indica que se ha establecido una conexión web.	1
Web cerrada	Indica que se ha cerrado una conexión web.	1
Web restablecida	Indica que se ha restablecido una conexión web.	4
Web terminada	Indica que se ha terminado una conexión web.	4
Web denegada	Indica que se ha denegado una conexión web.	4
Web en curso	Indica que hay una conexión web en curso.	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Web retardada	Indica que se ha retardado una conexión web.	3
Web en cola	Indica que se ha puesto en cola una conexión web.	1
Web redirigida	Indica que se ha redirigido una conexión web.	1
Proxy web	Indica que una conexión web ha pasado a través de un proxy.	1
VoIP abierto	Indica que se ha establecido una conexión VoIP (voz sobre IP).	1
VoIP cerrado	Indica que se ha cerrado una conexión de VoIP.	1
VoIP restablecido	Indica que se ha restablecido una conexión de VoIP.	3
VoIP terminado	Indica que se ha terminado una conexión de VoIP.	3
VoIP denegado	Indica que se ha denegado una conexión de VoIP.	3
VoIP en curso	Indica que hay una conexión de VoIP en curso.	1
VoIP retardado	Indica que se ha retardado una conexión de VoIP.	3
VoIP redirigido	Indica que se ha redirigido una conexión de VoIP.	3
Sesión de LDAP iniciada	Indica que se ha iniciado una sesión de LDAP.	1
Sesión de LDAP finalizada	Indica que ha finalizado una sesión de LDAP.	1
Sesión de LDAP denegada	Indica que se ha denegado una sesión de LDAP.	3
Estado de sesión LDAP	Indica que se ha notificado un mensaje de estado de sesión de LDAP.	1
Autenticación de LDAP fallida	Indica que una autenticación de LDAP ha fallado.	4
Autenticación de LDAP satisfactoria	Indica que una autenticación de LDAP ha sido satisfactoria.	1
Sesión de AAA iniciada	Indica que se ha iniciado una sesión de AAA (autenticación, autorización y contabilidad).	1
Sesión de AAA finalizada	Indica que ha finalizado una sesión de AAA.	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de AAA denegada	Indica que se ha denegado una sesión de AAA.	3
Estado de sesión AAA	Indica que se ha notificado un mensaje de estado de sesión de AAA.	1
Autenticación de AAA fallida	Indica que una autenticación de AAA ha fallado.	4
Autenticación de AAA satisfactoria	Indica que una autenticación de AAA ha sido satisfactoria.	1
Autenticación de IPSec fallida	Indica que una autenticación de IPSEC (seguridad de protocolo de Internet, Internet Protocol Security) ha fallado.	4
Autenticación de IPSec satisfactoria	Indica que una autenticación de IPSEC ha sido satisfactoria.	1
Sesión de IPSec iniciada	Indica que se ha iniciado una sesión de IPSEC.	1
Sesión de IPSec finalizada	Indica que ha finalizado una sesión de IPSEC.	1
Error de IPSec	Indica que se ha notificado un mensaje de error de IPSEC.	5
Estado de IPSEC	Indica que se ha notificado un mensaje de estado de sesión de IPSEC.	1
Sesión de IM abierta	Indica que se ha establecido una sesión de mensajería instantánea (IM).	1
Sesión de IM cerrada	Indica que se ha cerrado una sesión de IM.	1
Sesión de IM restablecida	Indica que se ha restablecido una sesión de IM.	3
Sesión de IM terminada	Indica que se ha terminado una sesión de IM.	3
Sesión de IM denegada	Indica que se ha denegado una sesión de IM.	3
Sesión de IM en curso	Indica que hay una sesión de IM en curso.	1
Sesión de IM retardada	Indica que se ha retardado una sesión de IM.	3
Sesión de IM redirigida	Indica que se ha redirigido una sesión de IM.	3
Sesión de Whois abierta	Indica que se ha establecido una sesión de WHOIS.	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de Whois cerrada	Indica que se ha cerrado una sesión de WHOIS.	1
Sesión de Whois restablecida	Indica que se ha restablecido una sesión de WHOIS.	3
Sesión de Whois terminada	Indica que se ha terminado una sesión de WHOIS.	3
Sesión de Whois denegada	Indica que se ha denegado una sesión de WHOIS.	3
Sesión de Whois en curso	Indica que hay una sesión de WHOIS en curso.	1
Sesión de Whois redirigida	Indica que se ha redirigido una sesión de WHOIS.	3
Sesión de Traceroute abierta	Indica que se ha establecido una sesión de Traceroute.	1
Sesión de Traceroute cerrada	Indica que se ha cerrado una sesión de Traceroute.	1
Sesión de Traceroute denegada	Indica que se ha denegado una sesión de Traceroute.	3
Sesión de Traceroute en curso	Indica que hay una sesión de Traceroute en curso.	1
Sesión de TN3270 abierta	TN3270 es un programa de emulación de terminal que se utiliza para conectar con un terminal IBM 3270. Esta categoría indica que se ha establecido una sesión de TN3270.	1
Sesión de TN3270 cerrada	Indica que se ha cerrado una sesión de TN3270.	1
Sesión de TN3270 restablecida	Indica que se ha restablecido una sesión de TN3270.	3
Sesión de TN3270 terminada	Indica que se ha terminado una sesión de TN3270.	3
Sesión de TN3270 denegada	Indica que se ha denegado una sesión de TN3270.	3
Sesión de TN3270 en curso	Indica que hay una sesión de TN3270 en curso.	1
Sesión de TFTP abierta	Indica que se ha establecido una sesión de TFTP.	1
Sesión de TFTP cerrada	Indica que se ha cerrado una sesión de TFTP.	1
Sesión de TFTP restablecida	Indica que se ha restablecido una sesión de TFTP.	3
Sesión de TFTP terminada	Indica que se ha terminado una sesión de TFTP.	3

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de TFTP denegada	Indica que se ha denegado una sesión de TFTP.	3
Sesión de TFTP en curso	Indica que hay una sesión de TFTP en curso.	1
Sesión de Telnet abierta	Indica que se ha establecido una sesión de Telnet.	1
Sesión de Telnet cerrada	Indica que se ha cerrado una sesión de Telnet.	1
Sesión de Telnet restablecida	Indica que se ha restablecido una sesión de Telnet.	3
Sesión de Telnet terminada	Indica que se ha terminado una sesión de Telnet.	3
Sesión de Telnet denegada	Indica que se ha denegado una sesión de Telnet.	3
Sesión de Telnet en curso	Indica que hay una sesión de Telnet en curso.	1
Sesión de Syslog abierta	Indica que se ha establecido una sesión de syslog.	1
Sesión de Syslog cerrada	Indica que se ha cerrado una sesión de syslog.	1
Sesión de Syslog denegada	Indica que se ha denegado una sesión de syslog.	3
Sesión de Syslog en curso	Indica que hay una sesión de syslog en curso.	1
Sesión de SSL abierta	Indica que se ha establecido una sesión de SSL (capa de sockets seguros).	1
Sesión de SSL cerrada	Indica que se ha cerrado una sesión de SSL.	1
Sesión de SSL restablecida	Indica que se ha restablecido una sesión de SSL.	3
Sesión de SSL terminada	Indica que se ha terminado una sesión de SSL.	3
Sesión de SSL denegada	Indica que se ha denegado una sesión de SSL.	3
Sesión de SSL en curso	Indica que hay una sesión de SSL en curso.	1
Sesión de SNMP abierta	Indica que se ha establecido una sesión de SNMP (protocolo simple de gestión de red).	1
Sesión de SNMP cerrada	Indica que se ha cerrado una sesión de SNMP.	1
Sesión de SNMP denegada	Indica que se ha denegado una sesión de SNMP.	3

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de SNMP en curso	Indica que hay una sesión de SNMP en curso.	1
Sesión de SMB abierta	Indica que se ha establecido una sesión de SMB (bloque de mensajes de servidor, Server Message Block).	1
Sesión de SMB cerrada	Indica que se ha cerrado una sesión de SMB.	1
Sesión de SMB restablecida	Indica que se ha restablecido una sesión de SMB.	3
Sesión de SMB terminada	Indica que se ha terminado una sesión de SMB.	3
Sesión de SMB denegada	Indica que se ha denegado una sesión de SMB.	3
Sesión de SMB en curso	Indica que hay una sesión de SMB en curso.	1
Sesión de medios en modalidad continua abierta	Indica que se ha establecido una sesión de medios en modalidad continua.	1
Sesión de medios en modalidad continua cerrada	Indica que se ha cerrado una sesión de medios en modalidad continua.	1
Sesión de medios en modalidad continua restablecida	Indica que se ha restablecido una sesión de medios en modalidad continua.	3
Sesión de medios en modalidad continua terminada	Indica que se ha terminado una sesión de medios en modalidad continua.	3
Sesión de medios en modalidad continua denegada	Indica que se ha denegado una sesión de medios en modalidad continua.	3
Sesión de medios en modalidad continua en curso	Indica que hay una sesión de medios en modalidad continua en curso.	1
Sesión de RUSERS abierta	Indica que se ha establecido una sesión de RUSERS (usuarios remotos).	1
Sesión de RUSERS cerrada	Indica que se ha cerrado una sesión de RUSERS.	1
Sesión de RUSERS denegada	Indica que se ha denegado una sesión de RUSERS.	3
Sesión de RUSERS en curso	Indica que hay una sesión de RUSERS en curso.	1
Sesión de RSH abierta	Indica que se ha establecido una sesión de rsh (shell remoto).	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de RSH cerrada	Indica que se ha cerrado una sesión de rsh.	1
Sesión de RSH restablecida	Indica que se ha restablecido una sesión de rsh.	3
Sesión de RSH terminada	Indica que se ha terminado una sesión de rsh.	3
Sesión de RSH denegada	Indica que se ha denegado una sesión de rsh.	3
Sesión de RSH en curso	Indica que hay una sesión de rsh en curso.	1
Sesión de RLOGIN abierta	Indica que se ha establecido una sesión de RLOGIN (inicio de sesión remoto).	1
Sesión de RLOGIN cerrada	Indica que se ha cerrado una sesión de RLOGIN.	1
Sesión de RLOGIN restablecida	Indica que se ha restablecido una sesión de RLOGIN.	3
Sesión de RLOGIN terminada	Indica que se ha terminado una sesión de RLOGIN.	3
Sesión de RLOGIN denegada	Indica que se ha denegado una sesión de RLOGIN.	3
Sesión de RLOGIN en curso	Indica que hay una sesión de RLOGIN en curso.	1
Sesión de REXEC abierta	Indica que se ha establecido una sesión de REXEC (ejecución remota).	1
Sesión de REXEC cerrada	Indica que se ha cerrado una sesión de REXEC.	1
Sesión de REXEC restablecida	Indica que se ha restablecido una sesión de REXEC.	3
Sesión de REXEC terminada	Indica que se ha terminado una sesión de REXEC.	3
Sesión de REXEC denegada	Indica que se ha denegado una sesión de REXEC.	3
Sesión de REXEC en curso	Indica que hay una sesión de REXEC en curso.	1
Sesión de RPC abierta	Indica que se ha establecido una sesión de RPC (llamada a procedimiento remoto).	1
Sesión de RPC cerrada	Indica que se ha cerrado una sesión de RPC.	1
Sesión de RPC restablecida	Indica que se ha restablecido una sesión de RPC.	3
Sesión de RPC terminada	Indica que se ha terminado una sesión de RPC.	3

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de RPC denegada	Indica que se ha denegado una sesión de RPC.	3
Sesión de RPC en curso	Indica que hay una sesión de RPC en curso.	1
Sesión de NTP abierta	Indica que se ha establecido una sesión de NTP (protocolo de hora en red).	1
Sesión de NTP cerrada	Indica que se ha cerrado una sesión de NTP.	1
Sesión de NTP restablecida	Indica que se ha restablecido una sesión de NTP.	3
Sesión de NTP terminada	Indica que se ha terminado una sesión de NTP.	3
Sesión de NTP denegada	Indica que se ha denegado una sesión de NTP.	3
Sesión de NTP en curso	Indica que hay una sesión de NTP en curso.	1
Sesión de NNTP abierta	Indica que se ha establecido una sesión de NNTP (protocolo para la transferencia de noticias en red).	1
Sesión de NNTP cerrada	Indica que se ha cerrado una sesión de NNTP.	1
Sesión de NNTP restablecida	Indica que se ha restablecido una sesión de NNTP.	3
Sesión de NNTP terminada	Indica que se ha terminado una sesión de NNTP.	3
Sesión de NNTP denegada	Indica que se ha denegado una sesión de NNTP.	3
Sesión de NNTP en curso	Indica que hay una sesión de NNTP en curso.	1
Sesión de NFS abierta	Indica que se ha establecido una sesión de NFS (Network File System).	1
Sesión de NFS cerrada	Indica que se ha cerrado una sesión de NFS.	1
Sesión de NFS restablecida	Indica que se ha restablecido una sesión de NFS.	3
Sesión de NFS terminada	Indica que se ha terminado una sesión de NFS.	3
Sesión de NFS denegada	Indica que se ha denegado una sesión de NFS.	3
Sesión de NFS en curso	Indica que hay una sesión de NFS en curso.	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de NCP abierta	Indica que se ha establecido una sesión de NCP (Network Control Program).	1
Sesión de NCP cerrada	Indica que se ha cerrado una sesión de NCP.	1
Sesión de NCP restablecida	Indica que se ha restablecido una sesión de NCP.	3
Sesión de NCP terminada	Indica que se ha terminado una sesión de NCP.	3
Sesión de NCP denegada	Indica que se ha denegado una sesión de NCP.	3
Sesión de NCP en curso	Indica que hay una sesión de NCP en curso.	1
Sesión de NetBIOS abierta	Indica que se ha establecido una sesión de NetBIOS.	1
Sesión de NetBIOS cerrada	Indica que se ha cerrado una sesión de NetBIOS.	1
Sesión de NetBIOS restablecida	Indica que se ha restablecido una sesión de NetBIOS.	3
Sesión de NetBIOS terminada	Indica que se ha terminado una sesión de NetBIOS.	3
Sesión de NetBIOS denegada	Indica que se ha denegado una sesión de NetBIOS.	3
Sesión de NetBIOS en curso	Indica que hay una sesión de NetBIOS en curso.	1
Sesión de MODBUS abierta	Indica que se ha establecido una sesión de MODBUS.	1
Sesión de MODBUS cerrada	Indica que se ha cerrado una sesión de MODBUS.	1
Sesión de MODBUS restablecida	Indica que se ha restablecido una sesión de MODBUS.	3
Sesión de MODBUS terminada	Indica que se ha terminado una sesión de MODBUS.	3
Sesión de MODBUS denegada	Indica que se ha denegado una sesión de MODBUS.	3
Sesión de MODBUS en curso	Indica que hay una sesión de MODBUS en curso.	1
Sesión de LPD abierta	Indica que se ha establecido una sesión de LPD (daemon de impresora de líneas).	1
Sesión de LPD cerrada	Indica que se ha cerrado una sesión de LPD.	1
Sesión de LPD restablecida	Indica que se ha restablecido una sesión de LPD.	3
Sesión de LPD terminada	Indica que se ha terminado una sesión de LPD.	3

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de LPD denegada	Indica que se ha denegado una sesión de LPD.	3
Sesión de LPD en curso	Indica que hay una sesión de LPD en curso.	1
Sesión de Lotus Notes abierta	Indica que se ha establecido una sesión de Lotus Notes.	1
Sesión de Lotus Notes cerrada	Indica que se ha cerrado una sesión de Lotus Notes.	1
Sesión de Lotus Notes restablecida	Indica que se ha restablecido una sesión de Lotus Notes.	3
Sesión de Lotus Notes terminada	Indica que se ha terminado una sesión de Lotus Notes.	3
Sesión de Lotus Notes denegada	Indica que se ha denegado una sesión de Lotus Notes.	3
Sesión de Lotus Notes en curso	Indica que hay una sesión de Lotus Notes en curso.	1
Sesión de Kerberos abierta	Indica que se ha establecido una sesión de Kerberos.	1
Sesión de Kerberos cerrada	Indica que se ha cerrado una sesión de Kerberos.	1
Sesión de Kerberos restablecida	Indica que se ha restablecido una sesión de Kerberos.	3
Sesión de Kerberos terminada	Indica que se ha terminado una sesión de Kerberos.	3
Sesión de Kerberos denegada	Indica que se ha denegado una sesión de Kerberos.	3
Sesión de Kerberos en curso	Indica que hay una sesión de Kerberos en curso.	1
Sesión de IRC abierta	Indica que se ha establecido una sesión de IRC (Internet Relay Chat).	1
Sesión de IRC cerrada	Indica que se ha cerrado una sesión de IRC.	1
Sesión de IRC restablecida	Indica que se ha restablecido una sesión de IRC.	3
Sesión de IRC terminada	Indica que se ha terminado una sesión de IRC.	3
Sesión de IRC denegada	Indica que se ha denegado una sesión de IRC.	3
Sesión de IRC en curso	Indica que hay una sesión de IRC en curso.	1
Sesión de IEC 104 abierta	Indica que se ha establecido una sesión de IEC 104.	1
Sesión de IEC 104 cerrada	Indica que se ha cerrado una sesión de IEC 104.	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de IEC 104 restablecida	Indica que se ha restablecido una sesión de IEC 104.	3
Sesión de IEC 104 terminada	Indica que se ha terminado una sesión de IEC 104.	3
Sesión de IEC 104 denegada	Indica que se ha denegado una sesión de IEC 104.	3
Sesión de IEC 104 en curso	Indica que hay una sesión de IEC 104 en curso.	1
Sesión de Ident abierta	Indica que se ha establecido una sesión de Ident (protocolo de identidad de cliente TCP).	1
Sesión de Ident cerrada	Indica que se ha cerrado una sesión de Ident.	1
Sesión de Ident restablecida	Indica que se ha restablecido una sesión de Ident.	3
Sesión de Ident terminada	Indica que se ha terminado una sesión de Ident.	3
Sesión de Ident denegada	Indica que se ha denegado una sesión de Ident.	3
Sesión de Ident en curso	Indica que hay una sesión de Ident en curso.	1
Sesión de ICCP abierta	Indica que se ha establecido una sesión de ICCP (Inter-Control Center Communications Protocol).	1
Sesión de ICCP cerrada	Indica que se ha cerrado una sesión de ICCP.	1
Sesión de ICCP restablecida	Indica que se ha restablecido una sesión de ICCP.	3
Sesión de ICCP terminada	Indica que se ha terminado una sesión de ICCP.	3
Sesión de ICCP denegada	Indica que se ha denegado una sesión de ICCP.	3
Sesión de ICCP en curso	Indica que hay una sesión de ICCP en curso.	1
Sesión de GroupWiseSession abierta	Indica que se ha establecido una sesión de GroupWise.	1
Sesión de GroupWise cerrada	Indica que se ha cerrado una sesión de GroupWise.	1
Sesión de GroupWise restablecida	Indica que se ha restablecido una sesión de GroupWise.	3
Sesión de GroupWise terminada	Indica que se ha terminado una sesión de GroupWise.	3
Sesión de GroupWise denegada	Indica que se ha denegado una sesión de GroupWise.	3

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de GroupWise en curso	Indica que hay una sesión de GroupWise en curso.	1
Sesión de Gopher abierta	Indica que se ha establecido una sesión de Gopher.	1
Sesión de Gopher cerrada	Indica que se ha cerrado una sesión de Gopher.	1
Sesión de Gopher restablecida	Indica que se ha restablecido una sesión de Gopher.	3
Sesión de Gopher terminada	Indica que se ha terminado una sesión de Gopher.	3
Sesión de Gopher denegada	Indica que se ha denegado una sesión de Gopher.	3
Sesión de Gopher en curso	Indica que hay una sesión de Gopher en curso.	1
Sesión de GIOP abierta	Indica que se ha establecido una sesión de GIOP (protocolo Inter-ORB general).	1
Sesión de GIOP cerrada	Indica que se ha cerrado una sesión de GIOP.	1
Sesión de GIOP restablecida	Indica que se ha restablecido una sesión de GIOP.	3
Sesión de GIOP terminada	Indica que se ha terminado una sesión de GIOP.	3
Sesión de GIOP denegada	Indica que se ha denegado una sesión de GIOP.	3
Sesión de GIOP en curso	Indica que hay una sesión de GIOP en curso.	1
Sesión de Finger abierta	Indica que se ha establecido una sesión de Finger.	1
Sesión de Finger cerrada	Indica que se ha cerrado una sesión de Finger.	1
Sesión de Finger restablecida	Indica que se ha restablecido una sesión de Finger.	3
Sesión de Finger terminada	Indica que se ha terminado una sesión de Finger.	3
Sesión de Finger denegada	Indica que se ha denegado una sesión de Finger.	3
Sesión de Finger en curso	Indica que hay una sesión de Finger en curso.	1
Sesión de Echo abierta	Indica que se ha establecido una sesión de Echo.	1
Sesión de Echo cerrada	Indica que se ha cerrado una sesión de Echo.	1
Sesión de Echo denegada	Indica que se ha denegado una sesión de Echo.	3

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de Echo en curso	Indica que hay una sesión de Echo en curso.	1
Sesión de .NET remota abierta	Indica que se ha establecido una sesión de .NET remota.	1
Sesión de .NET remota cerrada	Indica que se ha cerrado una sesión de .NET remota.	1
Sesión de .NET remota restablecida	Indica que se ha restablecido una sesión de .NET remota.	3
Sesión de .NET remota terminada	Indica que se ha terminado una sesión de .NET remota.	3
Sesión de .NET remota denegada	Indica que se ha denegado una sesión de .NET remota.	3
Sesión de .NET remota en curso	Indica que hay una sesión de .NET remota en curso.	1
Sesión de DNP3 abierta	Indica que se ha establecido una sesión de DNP3 (Distributed Network Proctologic).	1
Sesión de DNP3 cerrada	Indica que se ha cerrado una sesión de DNP3.	1
Sesión de DNP3 restablecida	Indica que se ha restablecido una sesión de DNP3.	3
Sesión de DNP3 terminada	Indica que se ha terminado una sesión de DNP3.	3
Sesión de DNP3 denegada	Indica que se ha denegado una sesión de DNP3.	3
Sesión de DNP3 en curso	Indica que hay una sesión de DNP3 en curso.	1
Sesión de descarte abierta	Indica que se ha establecido una sesión de descarte.	1
Sesión de descarte cerrada	Indica que se ha cerrado una sesión de descarte.	1
Sesión de descarte restablecida	Indica que se ha restablecido una sesión de descarte.	3
Sesión de descarte terminada	Indica que se ha terminado una sesión de descarte.	3
Sesión de descarte denegada	Indica que se ha denegado una sesión de descarte.	3
Sesión de descarte en curso	Indica que hay una sesión de descarte en curso.	1
Sesión de DHCP abierta	Indica que se ha establecido una sesión de DHCP (protocolo de configuración dinámica de hosts).	1
Sesión de DHCP cerrada	Indica que se ha cerrado una sesión de DHCP.	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de DHCP denegada	Indica que se ha denegado una sesión de DHCP.	3
Sesión de DHCP en curso	Indica que hay una sesión de DHCP en curso.	1
Éxito de DHCP	Indica que se ha obtenido un arrendamiento de DHCP satisfactoriamente.	1
Anomalía de DHCP	Indica que se ha podido obtener un arrendamiento de DHCP.	3
Sesión de CVS abierta	Indica que se ha establecido una sesión de CVS (sistema de versiones simultáneas).	1
Sesión de CVS cerrada	Indica que se ha cerrado una sesión de CVS.	1
Sesión de CVS restablecida	Indica que se ha restablecido una sesión de CVS.	3
Sesión de CVS terminada	Indica que se ha terminado una sesión de CVS.	3
Sesión de CVS denegada	Indica que se ha denegado una sesión de CVS.	3
Sesión de CVS en curso	Indica que hay una sesión de CVS en curso.	1
Sesión de CUPS abierta	Indica que se ha establecido una sesión de CUPS (Common UNIX Printing System).	1
Sesión de CUPS cerrada	Indica que se ha cerrado una sesión de CUPS.	1
Sesión de CUPS restablecida	Indica que se ha restablecido una sesión de CUPS.	3
Sesión de CUPS terminada	Indica que se ha terminado una sesión de CUPS.	3
Sesión de CUPS denegada	Indica que se ha denegado una sesión de CUPS.	3
Sesión de CUPS en curso	Indica que hay una sesión de CUPS en curso.	1
Sesión de Chargen iniciada	Indica que se ha iniciado una sesión de Chargen (generador de caracteres).	1
Sesión de Chargen cerrada	Indica que se ha cerrado una sesión de Chargen.	1
Sesión de Chargen restablecida	Indica que se ha restablecido una sesión de Chargen.	3
Sesión de Chargen terminada	Indica que se ha terminado una sesión de Chargen.	3

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Sesión de Chargen denegada	Indica que se ha denegado una sesión de Chargen.	3
Sesión de Chargen en curso	Indica que hay una sesión de Chargen en curso.	1
VPN variada	Indica que se ha detectado una sesión de VPN variada.	1
Sesión de DAP iniciada	Indica que se ha establecido una sesión de DAP.	1
Sesión de DAP finalizada	Indica que ha finalizado una sesión de DAP.	1
Sesión de DAP denegada	Indica que se ha denegado una sesión de DAP.	3
Estado de sesión de DAP	Indica que se ha realizado una solicitud de estado de sesión de DAP.	1
Sesión de DAP en curso	Indica que hay una sesión de DAP en curso.	1
Autenticación de DAP fallida	Indica que una autenticación de DAP ha fallado.	4
Autenticación de DAP satisfactoria	Indica que una autenticación de DAP ha sido satisfactoria.	1
Sesión de TOR iniciada	Indica que se ha establecido una sesión de TOR.	1
Sesión de TOR cerrada	Indica que se ha cerrado una sesión de TOR.	1
Sesión de TOR restablecida	Indica que se ha restablecido una sesión de TOR.	3
Sesión de TOR terminada	Indica que se ha terminado una sesión de TOR.	3
Sesión de TOR denegada	Indica que se ha denegado una sesión de TOR.	3
Sesión de TOR en curso	Indica que hay una sesión de TOR en curso.	1
Sesión de Game iniciada	Indica que se ha iniciado una sesión de juego.	1
Sesión de Game cerrada	Indica que se ha cerrado una sesión de juego.	1
Sesión de Game restablecida	Indica que se ha restablecido una sesión de juego.	3
Sesión de Game terminada	Indica que se ha terminado una sesión de juego.	3
Sesión de Game denegada	Indica que se ha denegado una sesión de juego.	3
Sesión de Game en curso	Indica que hay una sesión de juego en curso.	1

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Intento de inicio de sesión de administrador	Indica que se ha detectado un intento de iniciar una sesión como usuario administrativo.	2
Intento de inicio de sesión de usuario	Indica que se ha detectado un intento de iniciar una sesión como usuario no administrativo.	2
Servidor de cliente	Indica actividad de cliente/servidor.	1
Entrega de contenido	Indica actividad de entrega de contenido.	1
Transferencia de Datos	Indica un transferencia de datos.	3
Depósito de datos	Indica actividad de depósito de datos.	3
Servicios de directorio	Indica actividad de servicios de directorio.	2
Impresión de archivos	Indica actividad de impresión de archivos.	1
Transferencia de archivos	Indica transferencia de archivos.	2
Juegos	Indica actividad de juegos.	4
Asistencia médica	Indica actividad de asistencia médica.	1
Sistema interno	Indica actividad de un sistema interno.	1
Protocolo Internet	Indica actividad del protocolo Internet.	1
Legado	Indica actividad de legado.	1
Correo	Indica actividad de correo.	1
Misc	Indica actividad varia.	2
Multimedia	Indica actividad multimedia.	2
Gestión de red	Indica actividad de gestión de red.	
P2P	Indica actividad P2P (de igual a igual).	4
Acceso remoto	Indica actividad de acceso remoto.	3
Protocolos de direccionamiento	Indica actividad de los protocolos de direccionamiento.	1
Protocolo de seguridad	Indica actividad del protocolo de seguridad.	2

Tabla 106. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de aplicación (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Modalidad continua	Indica actividad de modalidad continua.	2
Protocolo no común	Indica actividad de protocolo no común.	3
VoIP	Indica actividad de VoIP.	1
Web	Indica actividad web.	1
ICMP	Indica actividad de ICMP.	1

Auditoría

La categoría de auditoría contiene sucesos que están relacionados con la actividad de auditoría, como el correo electrónico o la actividad de FTP.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de auditoría.

Tabla 107. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de auditoría

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Suceso de auditoría general	Indica que ha comenzado un suceso de auditoría general.	1
Ejecución incorporada	Indica que se ha ejecutado una tarea de auditoría incorporada.	1
Copia masiva	Indica que se ha detectado una copia masiva de datos.	1
Vuelco de datos	Indica que se ha detectado un vuelco de datos.	1
Importación de datos	Indica que se ha detectado una importación de datos.	1
Selección de datos	Indica que se ha detectado un proceso de selección de datos.	1
Recorte de datos	Indica que se ha detectado un proceso de recorte de datos.	1
Actualización de datos	Indica que se ha detectado un proceso de actualización de datos.	1
Ejecución desencadenante/ procedimiento	Indica que se ha detectado la ejecución de un procedimiento de base de datos o de un desencadenante.	1

Tabla 107. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de auditoría (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Cambio de esquema	Indica que se ha alterado el esquema de la ejecución de un procedimiento o de un desencadenante.	1

Riesgo

La categoría de riesgo contiene sucesos que están relacionados con IBM Security QRadar Risk Manager.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de riesgo.

Tabla 108. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de riesgo

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Exposición de política	Indica que se ha detectado una exposición de política.	5
Violación de conformidad	Indica que se ha detectado una violación de conformidad.	5
Vulnerabilidad expuesta	Indica que la red o el dispositivo tiene una vulnerabilidad expuesta.	9
Vulnerabilidad de acceso remoto	Indica que la red o el dispositivo tiene una vulnerabilidad de acceso remoto.	9
Vulnerabilidad de acceso local	Indica que la red o el dispositivo tiene una vulnerabilidad de acceso local.	7
Acceso inalámbrico abierto	Indica que la red o el dispositivo tiene abierto el acceso inalámbrico.	5
Cifrado débil	Indica que el host o el dispositivo tiene un cifrado débil.	5
Transferencia de datos no cifrada	Indica que un host o un dispositivo está transmitiendo datos que no están cifrados.	3
Almacén de datos no cifrado	Indica que el almacén de datos no está cifrado.	3
Regla mal configurada	Indica que una regla no está configurada correctamente.	3

Tabla 108. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de riesgo (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Dispositivo mal configurado	Indica que un dispositivo de la red no está configurado correctamente.	3
Host mal configurado	Indica que un host no está configurado correctamente.	3
Pérdida de datos posible	Indica que se ha detectado la posibilidad de que se pierdan datos.	5
Autenticación débil	Indica que un host o un dispositivo es susceptible al fraude.	5
Sin contraseña	Indica que no existe ninguna contraseña.	7
Fraude	Indica que un host o un dispositivo es susceptible al fraude.	7
Destino de DoS posible	Indica que un host o un dispositivo es un objetivo posible para los ataques de denegación de servicio.	3
Debilidad de DoS posible	Indica que un host o un dispositivo podría tener un punto débil para los ataques de denegación de servicio.	3
Pérdida de confidencialidad	Indica que se ha detectado una pérdida de la confidencialidad.	5
Acumulación de puntuación de riesgos de supervisor de políticas	Indica que se ha detectado una acumulación de puntuación de riesgos de supervisor de políticas.	1

Auditoría de Risk Manager

La categoría de riesgo contiene sucesos que están relacionados con los sucesos de auditoría de IBM Security QRadar Risk Manager.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de auditoría de Risk Manager.

Tabla 109. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de auditoría de Risk Manager

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Supervisor de políticas	Indica que se ha modificado un supervisor de políticas.	3
Topología	Indica que se ha modificado una topología.	3

Tabla 109. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de auditoría de Risk Manager (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Simulaciones	Indica que se ha modificado una simulación.	3
Administración	Indica que se han realizado cambios administrativos.	3

Control

La categoría de control contiene sucesos que están relacionados con el sistema de hardware.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de control.

Tabla 110. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de control

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Lectura de dispositivo	Indica que un dispositivo se ha leído.	1
Comunicación de dispositivo	Indica la comunicación con un dispositivo.	1
Auditoría de dispositivo	Indica que se ha efectuado una auditoría de dispositivo.	1
Suceso de dispositivo	Indica que se ha producido un suceso de dispositivo.	1
Ping de dispositivo	Indica que se ha efectuado una acción ping a un dispositivo.	1
Configuración de dispositivo	Indica que un dispositivo se ha configurado.	1
Ruta de dispositivo	Indica que se ha efectuado una acción de ruta de dispositivo.	1
Importación de dispositivo	Indica que se ha efectuado una importación de dispositivo.	1
Información de dispositivo	Indica que se ha efectuado una acción de información de dispositivo.	1
Aviso de dispositivo	Indica que se ha generado un aviso sobre un dispositivo.	1
Error de dispositivo	Indica que se ha generado un error sobre un dispositivo.	1
Suceso de relé	Indica un suceso de relé.	1

Tabla 110. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de control (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Suceso de NIC	Indica un suceso de tarjeta de interfaz de red (NIC).	1
Suceso de UIQ	Indica un suceso en un dispositivo móvil.	1
Suceso de IMU	Indica un suceso en una unidad de gestión integrada (IMU).	1
Suceso de facturación	Indica un suceso de facturación.	1
Suceso de DBMS	Indica un suceso en el sistema de gestión de bases de datos (DBMS).	1
Suceso de importación	Indica que se ha efectuado una importación.	1
Importación de ubicación	Indica que se ha efectuado una importación de ubicación.	1
Importación de ruta	Indica que se ha efectuado una importación de ruta.	1
Suceso de exportación	Indica que se ha efectuado una exportación.	1
Señalización remota	Indica señalización remota.	1
Estado de pasarela	Indica el estado de pasarela.	1
Suceso de trabajo	Indica que se ha efectuado un trabajo.	1
Suceso de seguridad	Indica que se ha producido un suceso de seguridad.	1
Detección de alteración de dispositivo	Indica que el sistema ha detectado una acción de manipulación indebida.	1
Suceso de tiempo	Indica que se ha producido un suceso de tiempo.	1
Comportamiento sospechoso	Indica que se ha producido un comportamiento sospechoso.	1
Corte de alimentación	Indica que se ha producido un corte en la alimentación.	1
Restauración de alimentación	Indica que la alimentación se ha restaurado.	1
Pulsación	Indica que se ha efectuado una acción de ping de pulsaciones.	1
Suceso de conexión remota	Indica una conexión remota con el sistema.	1

Perfilador de activos

La categoría de perfilador de activos contiene sucesos que están relacionados con los perfiles de los activos.

En la tabla siguiente se describen las categorías de sucesos de nivel bajo y los niveles de gravedad asociados para la categoría de perfilador de activos.

Tabla 111. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de perfilador de activos

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Activo creado	Indica que se ha creado un activo.	1
Activo actualizado	Indica que un activo se ha actualizado.	1
Activo observado	Indica que un activo se ha observado.	1
Activo movido	Indica que se ha movido un activo.	1
Activo suprimido	Indica que un activo se ha suprimido.	1
Nombre de host de activo limpiado	Indica que un nombre de host se ha limpiado.	1
Nombre de host de activo creado	Indica que se ha creado un nombre de host.	1
Nombre de host de activo actualizado	Indica que se ha actualizado un nombre de host.	1
Nombre de host de activo observado	Indica que un nombre de host se ha observado.	1
Nombre de host de activo movido	Indica que se ha movido un nombre de host.	1
Nombre de host de activo suprimido	Indica que se ha suprimido un nombre de host.	1
Puerto de activo limpiado	Indica que un nombre de puerto se ha limpiado.	1
Puerto de activo creado	Indica que se ha creado un puerto.	1
Puerto de activo actualizado	Indica que se ha actualizado un puerto.	1
Puerto de activo observado	Indica que un puerto se ha observado.	1
Puerto de activo movido	Indica que se ha movido un puerto.	1
Puerto de activo suprimido	Indica que se ha suprimido un puerto.	1
Instancia de vulnerabilidad de activo limpiado	Indica que una instancia de vulnerabilidad se ha limpiado.	1
Instancia de vulnerabilidad de activo creado	Indica que se ha creado una instancia de vulnerabilidad.	1

Tabla 111. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de perfilador de activos (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Instancia de vulnerabilidad de activo actualizado	Indica que una instancia de vulnerabilidad se ha actualizado.	1
Instancia de vulnerabilidad de activo observado	Indica que una instancia de vulnerabilidad se ha observado.	1
Instancia de vulnerabilidad de activo movido	Indica que se ha movido una instancia de vulnerabilidad.	1
Instancia de vulnerabilidad de activo suprimido	Indica que se ha suprimido una instancia de vulnerabilidad.	1
Sistema operativo de activo limpiado	Indica que un sistema operativo se ha limpiado.	1
Sistema operativo de activo creado	Indica que se ha creado un sistema operativo.	1
Sistema operativo de activo actualizado	Indica que sistema operativo se ha actualizado.	1
Sistema operativo de activo observado	Indica que un sistema operativo se ha observado.	1
Sistema operativo de activo movido	Indica que se ha movido sistema operativo.	1
Sistema operativo de activo suprimido	Indica que un sistema operativo se ha suprimido.	1
Propiedad de activo limpiada	Indica que una propiedad se ha limpiado.	1
Propiedad de activo creada	Indica que se ha creado una propiedad.	1
Propiedad de activo actualizada	Indica que se ha actualizado una propiedad.	1
Propiedad de activo observada	Indica que una propiedad se ha observado.	1
Propiedad de activo movida	Indica que se ha movido una propiedad.	1
Propiedad de activo suprimida	Indica que se ha movido una propiedad.	1
Dirección de IP de activo limpiada	Indica que una dirección IP se ha limpiado.	1
Dirección de IP de activo creada	Indica que se ha creado una dirección IP.	1
Dirección de IP de activo actualizada	Indica que una dirección IP se ha actualizado.	1
Dirección de IP de activo observada	Indica que una dirección IP se ha observado.	1
Dirección de IP de activo movida	Indica que se ha movido una dirección IP.	1

Tabla 111. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de perfilador de activos (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Dirección de IP de activo suprimida	Indica que una dirección IP se ha suprimido.	1
Interfaz de activo limpiada	Indica que una interfaz se ha limpiado.	1
Interfaz de activo creada	Indica que se ha creado una interfaz.	1
Interfaz de activo actualizada	Indica que una interfaz se ha actualizado.	1
Interfaz de activo observada	Indica que una interfaz se ha observado.	1
Interfaz de activo movida	Indica que se ha movido una interfaz.	1
Interfaz de activo fusionada	Indica que una interfaz se ha fusionado.	1
Interfaz de activo suprimida	Indica que una interfaz se ha suprimido.	1
Usuario de activo limpiado	Indica que se ha limpiado un usuario.	1
Usuario de activo observado	Indica que un usuario se ha observado.	1
Usuario de activo movido	Indica que se ha movido un usuario.	1
Usuario de activo suprimido	Indica que se ha suprimido un usuario.	1
Política explorada de activo limpiada	Indica que una política explorada se ha limpiado.	1
Política explorada de activo observada	Indica que una política explorada se ha observado.	1
Política explorada de activo movida	Indica que se ha movido una política explorada.	1
Política explorada de activo suprimida	Indica que se ha suprimido una política explorada.	1
Aplicación de Windows de activo limpiada	Indica que una aplicación de Windows se ha limpiado.	1
Aplicación de Windows de activo observada	Indica que una aplicación de Windows se ha observado.	1
Aplicación de Windows de activo movida	Indica que se ha movido una aplicación de Windows.	1
Aplicación de Windows de activo suprimida	Indica que se ha suprimido una aplicación de Windows.	1
Servicio explorado de activo limpiado	Indica que un servicio explorado se ha limpiado.	1
Servicio explorado de activo observado	Indica que un servicio explorado se ha observado.	1

Tabla 111. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de perfilador de activos (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Servicio explorado de activo movido	Indica que se ha movido un servicio explorado.	1
Servicio explorado de activo suprimido	Indica que se ha suprimido un servicio explorado.	1
Parche de Windows de activo limpiado	Indica que un parche de Windows se ha limpiado.	1
Parche de Windows de activo observado	Indica que un parche de Windows se ha observado.	1
Parche de Windows de activo movido	Indica que un parche de Windows se ha movido.	1
Parche de Windows de activo suprimido	Indica que se ha suprimido un parche de Windows.	1
Parche de UNIX de activo limpiado	Indica que un parche de UNIX se ha limpiado.	1
Parche de UNIX de activo observado	Indica que un parche de UNIX se ha observado.	1
Parche de UNIX de activo movido	Indica que un parche de UNIX se ha movido.	1
Parche de UNIX de activo suprimido	Indica que se ha suprimido un parche de UNIX.	1
Exploración de parche de activo limpiada	Indica que una exploración de parche se ha limpiado.	1
Exploración de parche de activo creada	Indica que se ha creado una exploración de parche.	1
Exploración de parche de activo movida	Indica que se ha movido una exploración de parche.	1
Exploración de parche de activo suprimida	Indica que se ha suprimido una exploración de parche.	1
Exploración de puerto de activo limpiada	Indica que una exploración de puerto se ha limpiado.	1
Exploración de puerto de activo creada	Indica que una exploración de puerto se ha limpiado.	1
Exploración de puerto de activo movida	Indica que se ha movido una exploración de parche.	1
Exploración de puerto de activo suprimida	Indica que se ha suprimido una exploración de parche.	1
Aplicación de cliente de activo limpiada	Indica que una aplicación de cliente se ha limpiado.	1
Aplicación de cliente de activo observada	Indica que una aplicación de cliente se ha observado.	1
Aplicación de cliente de activo movida	Indica que se ha movido una aplicación de cliente.	1
Aplicación de cliente de activo suprimida	Indica que se ha suprimido una aplicación de cliente.	1

Tabla 111. Categorías de nivel bajo y niveles de gravedad correspondientes a la categoría de perfilador de activos (continuación)

Categoría de sucesos de nivel bajo	Descripción	Nivel de gravedad (0 – 10)
Exploración de parche de activo observada	Indica que una exploración de parche se ha observado.	1
Exploración de puerto de activo observada	Indica que una exploración de puerto se ha observado.	1

Capítulo 25. Servidores y puertos comunes utilizados por QRadar

IBM Security QRadar requiere que determinados puertos estén preparados para recibir información de los componentes y la infraestructura externa de QRadar. Para asegurarse de que QRadar está utilizando la información de seguridad más reciente, también necesita acceso a los servidores públicos y canales de información RSS.

Comunicación SSH en el puerto 22

Todos los puertos que se describen en la consola de QRadar pueden ser túneles, mediante cifrado, a través del puerto 22 sobre SSH.

La consola conecta con los hosts gestionados mediante una sesión SSH cifrada para comunicarse de forma segura. Estas sesiones de SSH se inician desde la consola para proporcionar datos al host gestionado. Por ejemplo, consola de QRadar puede iniciar varias sesiones de SSH en los dispositivos de Procesador de sucesos para establecer una comunicación segura. Esta comunicación puede incluir puertos túnel sobre SSH, como los datos HTTPS para el puerto 443 y los datos de consulta de Ariel para el puerto 32006. Los QRadar QFlow Collectors que utilizan cifrado pueden iniciar sesiones de SSH para los dispositivos de procesador de flujo que necesitan datos.

Puertos abiertos que no son necesarios para QRadar

Es posible que encuentre más puertos abiertos en las siguientes situaciones:

- Cuando instala QRadar en su propio hardware, puede ver puertos abiertos utilizados por servicios, daemons y programas incluidos en Red Hat Enterprise Linux.
- Cuando monta o exporta un comportamiento de archivos de red puede ver puertos asignados dinámicamente necesarios para servicios RPC, como por ejemplo `rpc.mountd` y `rpc.rquotad`.

Utilización de puertos de QRadar

Revise la lista de puertos comunes que los servicios y componentes de IBM Security QRadar utilizan para comunicarse a través de la red. Puede utilizar la lista de puertos para determinar qué puertos deben estar abiertos en la red. Por ejemplo, puede determinar los puertos que deben estar abiertos para que consola de QRadar se comunique con los Procesadores de sucesos remotos.

Sondeo remoto de WinCollect

Los agentes de WinCollect que sondean remotamente otros sistemas operativos Microsoft Windows podrían requerir asignaciones de puerto adicionales.

Para obtener más información, consulte la *Guía del usuario* de IBM Security QRadar WinCollect.

© Copyright IBM Corp. 2012, 2015

Puertos de escucha de QRadar

En la tabla siguiente se muestran los puertos de QRadar que están abiertos y en un estado de escucha (LISTEN). Los puertos LISTEN sólo son válidos cuando iptables está habilitado en el sistema. A menos que se indique lo contrario, la información sobre el número de puerto asignado se aplica a todos los productos de QRadar.

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar

Puerto	Descripción	Protocolo	Dirección	Requisito
22	SSH	TCP	Bidireccional desde consola de QRadar hasta todos los demás componentes	Acceso de gestión remota. Adición de un sistema remoto como host gestionado. Protocolos de origen de registro para recuperar archivos de los dispositivos externos; por ejemplo, el protocolo de archivo de registro. Usuarios que utilizan la interfaz de línea de mandatos para comunicarse desde los escritorios con la consola. Alta disponibilidad (HA).
25	SMTP	TCP	Desde todos los hosts gestionados a la pasarela SMTP.	Correos electrónicos desde QRadar a una pasarela SMTP. Envío de mensajes de correo electrónico de error y de aviso a un contacto de correo electrónico administrativo.
37	rdate (hora)	UDP/ TCP	Todos los sistemas hacia consola de QRadar. consola de QRadar hacia el servidor de NTP o rdate.	Sincronización de hora entre consola de QRadar y los hosts gestionados.
111	Correlacionador de puertos	TCP/ UDP	Hosts gestionados que se comunican con consola de QRadar. Usuarios que se conectan a consola de QRadar.	Llamadas a procedimiento remoto (RPC) para los servicios necesarios, como Network File System (NFS).

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar (continuación)

Puerto	Descripción	Protocolo	Dirección	Requisito
135 y los puertos asignados de forma dinámica por encima de 1024 para las llamadas RPC	DCOM	TCP	Tráfico bidireccional entre los agentes de WinCollect y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos. Tráfico bidireccional entre los componentes de consola de QRadar o recopiladores de sucesos de QRadar que utilizan agentes de Microsoft Security Event Log Protocol o Adaptive Log Exporter y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos.	Este tráfico lo genera WinCollect, Microsoft Security Event Log Protocol o Adaptive Log Exporter. **Nota:** DCOM normalmente asigna un rango de puertos aleatorio para la comunicación. Puede configurar los productos de Microsoft Windows para que utilicen un puerto determinado. Para obtener más información, consulte la documentación de Microsoft Windows.
137	Servicio de nombres de NetBIOS de Windows	UDP	Tráfico bidireccional entre los agentes de WinCollect y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos. Tráfico bidireccional entre los componentes de consola de QRadar o recopiladores de sucesos de QRadar que utilizan agentes de Microsoft Security Event Log Protocol o Adaptive Log Exporter y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos.	Este tráfico lo genera WinCollect, Microsoft Security Event Log Protocol o Adaptive Log Exporter.
138	Servicio de datagramas de NetBIOS de Windows	UDP	Tráfico bidireccional entre los agentes de WinCollect y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos. Tráfico bidireccional entre los componentes de consola de QRadar o recopiladores de sucesos de QRadar que utilizan agentes de Microsoft Security Event Log Protocol o Adaptive Log Exporter y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos.	Este tráfico lo genera WinCollect, Microsoft Security Event Log Protocol o Adaptive Log Exporter.

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar (continuación)

Puerto	Descripción	Protocolo	Dirección	Requisito
139	Servicio de sesión de NetBIOS de Windows	TCP	Tráfico bidireccional entre los agentes de WinCollect y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos. Tráfico bidireccional entre los componentes de consola de QRadar o recopiladores de sucesos de QRadar que utilizan agentes de Microsoft Security Event Log Protocol o Adaptive Log Exporter y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos.	Este tráfico lo genera WinCollect, Microsoft Security Event Log Protocol o Adaptive Log Exporter.
161	NetSNMP	UDP	Hosts gestionados de QRadar que se conectan a consola de QRadar. Orígenes de registro externos hacia recopiladores de sucesos de QRadar.	Puerto TCP para el daemon NetSNMP que está a la escucha de las comunicaciones (v1, v2c y v3) desde orígenes de registro externos. El puerto sólo está abierto si el agente SNMP está habilitado.
199	NetSNMP	TCP	Hosts gestionados de QRadar que se conectan a consola de QRadar. Orígenes de registro externos hacia recopiladores de sucesos de QRadar.	Puerto TCP para el daemon NetSNMP que está a la escucha de las comunicaciones (v1, v2c y v3) desde orígenes de registro externos. El puerto sólo está abierto si el agente SNMP está habilitado.
427	Protocolo de ubicación de servicios (SLP)	UDP/ TCP		El módulo de gestión integrada utiliza el puerto para localizar servicios en una LAN.

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar (continuación)

Puerto	Descripción	Protocolo	Dirección	Requisito
443	Apache/HTTPS	TCP	Tráfico bidireccional para las comunicaciones seguras desde todos los productos hacia consola de QRadar.	Descargas de configuración en los hosts gestionados desde consola de QRadar. Hosts gestionados de QRadar que se conectan a consola de QRadar. Usuarios que tienen acceso de inicio de sesión a QRadar. consola de QRadar que gestiona y proporciona actualizaciones de configuración para los agentes de WinCollect.
445	Microsoft Directory Service	TCP	Tráfico bidireccional entre los agentes de WinCollect y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos. Tráfico bidireccional entre los componentes de consola de QRadar o recopiladores de sucesos de QRadar que utilizan Microsoft Security Event Log Protocol y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos Tráfico bidireccional entre los agentes de Adaptive Log Exporter y los sistemas operativos Windows que se sondean de forma remota para comprobar si hay sucesos	Este tráfico lo genera WinCollect, Microsoft Security Event Log Protocol o Adaptive Log Exporter.
514	Syslog	UDP/ TCP	Los dispositivos de red externos que proporcionan sucesos de syslog de TCP utilizan tráfico bidireccional. Los dispositivos de red externos que proporcionan sucesos de syslog de UDP utilizan tráfico unidireccional. El tráfico de syslog interno de hosts de QRadar a la consola de QRadar.	Orígenes de registro externos para enviar datos a los componentes de QRadar. El tráfico de syslog incluye agentes de WinCollect, recopiladores de sucesos y agentes de Adaptive Log Exporter que puedan enviar sucesos de UDP o TCP a QRadar.

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar (continuación)

Puerto	Descripción	Protocolo	Dirección	Requisito
762	Daemon de montaje de NFS (Network File System) (mountd)	TCP/ UDP	Conexiones entre consola de QRadar y el servidor NFS.	Daemon de montaje de NFS (Network File System), que procesa las solicitudes de montaje de un sistema de archivos en una ubicación especificada.
1514	Syslog-ng	TCP/ UDP	Conexión entre el componente Recopilador de sucesos local y el componente Procesador de sucesos local con el daemon syslog-ng para el registro.	Puerto de registro interno para syslog-ng.
2049	NFS	TCP	Conexiones entre consola de QRadar y el servidor NFS.	Protocolo NFS (Network File System) para compartir archivos o datos entre componentes.
2055	Datos de NetFlow	UDP	Desde la interfaz de gestión en el origen de flujo (normalmente un direccionador) hasta QRadar QFlow Collector	Datagrama de NetFlow de componentes, tales como los direccionadores.
2375	Puerto de mandatos de Docker	TCP	Comunicaciones internas. Este puerto no está disponible externamente.	Se utiliza para gestionar recursos del marco de aplicaciones de QRadar.
3389	El protocolo de escritorio remoto (RDP) y Ethernet sobre USB están habilitados.	TCP/ UDP		Si el sistema operativo Microsoft Windows está configurado para dar soporte a RDP y Ethernet sobre USB, un usuario puede iniciar una sesión con el servidor sobre la red de gestión. Esto significa que el puerto predeterminado para RDP, que es 3389, debe estar abierto.
3900	Puerto de presencia remota del Módulo de gestión integrada	TCP/ UDP		Utilice este puerto para interactuar con la consola de QRadar a través del Módulo de gestión integrada.
4333	Puerto de redirección	TCP		Este puerto está asignado como puerto de redirección para las solicitudes de ARP (protocolo de resolución de direcciones) en la resolución de delitos de QRadar.
5432	Postgres	TCP	Comunicación para el host gestionado que se utiliza para acceder a la instancia de base de datos local.	Necesario para el suministro de hosts gestionados desde la pestaña **Admin**.

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar (continuación)

Puerto	Descripción	Protocolo	Dirección	Requisito
6514	Syslog	TCP	Los dispositivos de red externos que proporcionan sucesos de syslog de TCP cifrados utilizan tráfico bidireccional.	Orígenes de registro externos para enviar datos de suceso cifrados a los componentes de QRadar.
6543	Pulsación de alta disponibilidad	TCP/ UDP	Bidireccional entre el host secundario y el host primario en un clúster de alta disponibilidad.	Ping de pulsaciones desde un host secundario a un host primario en un clúster de alta disponibilidad para detectar anomalías de hardware o de la red.
7676, 7677 y cuatro puertos enlazados aleatoriamente por encima de 32000	Conexiones de mensajería (IMQ)	TCP	Comunicaciones de cola de mensajes entre los componentes de un host gestionado	Intermediario de cola de mensajes para las comunicaciones entre los componentes de un host gestionado. Los puertos 7676 y 7677 son puertos TCP estáticos, y se crean cuatro conexiones adicionales en puertos aleatorios. Para obtener más información sobre la búsqueda de puertos enlazados aleatoriamente, consulte el apartado “Visualización de asociaciones de puertos de IMQ” en la página 365.
7777, 7778, 7779, 7780, 7781, 7782, 7783, 7788, 7790, 7791, 7792, 7793, 7795, 7799, and 8989.	Puertos de servidor JMX	TCP	Comunicaciones internas. Estos puertos no están disponibles externamente.	Supervisión de servidor JMX (Java Management Beans) de todos los procesos internos de QRadar para exponer medidas de soportabilidad. Estos puertos los utiliza el personal de soporte de QRadar.
⌂7789	Dispositivo de bloqueo replicado distribuido de alta disponibilidad (HA)	TCP/ UDP	Bidireccional entre el host secundario y el host primario en un clúster de alta disponibilidad.	El Dispositivo de bloqueo replicado distribuido se utiliza para mantener las unidades sincronizadas entre los hosts primario y secundario en las configuraciones de alta disponibilidad.
7800	Apache Tomcat	TCP	Desde el Recopilador de sucesos a la consola de QRadar.	En tiempo real (modalidad continua) para sucesos.

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar (continuación)

Puerto	Descripción	Protocolo	Dirección	Requisito
7801	Apache Tomcat	TCP	Desde el Recopilador de sucesos hacia consola de QRadar.	En tiempo real (modalidad continua) para flujos.
7803	Apache Tomcat	TCP	Desde el Recopilador de sucesos hacia consola de QRadar.	Puerto de motor de detección de anomalías.
7804	Constructor Arc de QRM	TCP	Comunicaciones de control interno entre procesos de QRadar y el constructor ARC.	Este puerto se utiliza sólo para QRadar Risk Manager. No está disponible externamente.
8000	ECS (servicio de recopilación de sucesos)	TCP	Desde el Recopilador de sucesos hacia consola de QRadar.	Puerto de escucha para el servicio de recopilación de sucesos (ECS) específico.
8001	Puerto del daemon SNMP	UDP	Sistemas SNMP externos que solicitan información de condiciones de excepción SNMP de consola de QRadar.	Puerto de escucha UDP para solicitudes de datos de SNMP externo.
8005	Apache Tomcat	TCP	Comunicaciones internas. No está disponible externamente.	Abierto para control de Tomcat. Este puerto está enlazado y sólo acepta conexiones desde el host local.
8009	Apache Tomcat	TCP	Desde el proceso del daemon HTTP (HTTPd) hacia Tomcat.	Conector Tomcat, donde la solicitud se utiliza y se pasa a través de un proxy para el servicio web.
8080	Apache Tomcat	TCP	Desde el proceso del daemon HTTP (HTTPd) hacia Tomcat.	Conector Tomcat, donde la solicitud se utiliza y se pasa a través de un proxy para el servicio web.
8413	Agentes de WinCollect	TCP	Tráfico bidireccional entre el agente de WinCollect y consola de QRadar.	Este tráfico lo genera el agente de WinCollect para reenviar sucesos de WinCollect y la comunicación está cifrada. Es necesario para proporcionar actualizaciones de configuración al agente de WinCollect y para utilizar WinCollect en modalidad conectada.
9090	Base de datos y servidor de reputación de IP XForce	TCP	Comunicaciones internas. No está disponible externamente.	Comunicaciones entre los procesos de QRadar y la base de datos de reputación de IP XForce.

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar (continuación)

Puerto	Descripción	Protocolo	Dirección	Requisito
9913 más un puerto asignado dinámicamente	Contenedor de aplicación web	TCP	Comunicación de Invocación a método remoto (RMI) Java bidireccional entre máquinas virtuales Java	Una vez registrada la aplicación web, se asigna dinámicamente un puerto adicional.
9995	Datos de NetFlow	UDP	Desde la interfaz de gestión en el origen de flujo (normalmente un direccionador) hasta QRadar QFlow Collector	Datagrama de NetFlow de componentes, tales como los direccionadores.
9999	Procesador QRadar Vulnerability Manager	TCP	Unidireccional del explorador al dispositivo que está ejecutando el procesador QRadar Vulnerability Manager	Se utiliza para información de mandatos de QRadar Vulnerability Manager (QVM). Este puerto solo se utiliza cuando QVM está habilitado.
10000	Interfaz de administración de sistema de QRadar basada en web	TCP/ UDP	Sistemas de sobremesa de usuario hacia todos los hosts de QRadar.	En QRadar V7.2.5 y anteriores, este puerto se utiliza para cambios en el servidor, como por ejemplo la contraseña de root de los hosts y el acceso de cortafuegos. El puerto 10000 está inhabilitado en V7.2.6.
10101, 10102	Mandato de latido	TCP	Tráfico bidireccional entre los nodos de alta disponibilidad primario y secundario.	Necesario para garantizar que los nodos HA siguen activos.
15433	Postgres	TCP	Comunicación para el host gestionado que se utiliza para acceder a la instancia de base de datos local.	Se utiliza para la configuración y almacenamiento de QRadar Vulnerability Manager (QVM). Este puerto solo se utiliza cuando QVM está habilitado.
23111	Servidor web SOAP	TCP		Puerto del servidor web SOAP para el servicio de recopilación de sucesos (ECS).
23333	Canal de fibra Emulex	TCP	Sistemas de sobremesa de usuario que se conectan a los dispositivos QRadar con una tarjeta de canal de fibra.	Servicio de gestión remota de HBAnywhere de canal de fibra Emulex (elxmgmt).
32004	Reenvío de sucesos normalizados	TCP	Bidireccional entre los componentes de QRadar.	Datos de sucesos normalizados que se comunican desde un origen externo o entre recopiladores de sucesos de QRadar.

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar (continuación)

Puerto	Descripción	Protocolo	Dirección	Requisito
32005	Flujo de datos	TCP	Bidireccional entre los componentes de QRadar.	Puerto de comunicación de flujo de datos entre los recopiladores de sucesos de QRadar cuando están en hosts gestionados diferentes.
32006	Consultas de Ariel	TCP	Bidireccional entre los componentes de QRadar.	Puerto de comunicación entre el servidor proxy de Ariel y el servidor de consulta de Ariel.
32007	Datos de delito	TCP	Bidireccional entre los componentes de QRadar.	Sucesos y flujos que hacen aportaciones a un delito o están implicados en una correlación global.
32009	Datos de identidad	TCP	Bidireccional entre los componentes de QRadar.	Datos de identidad que se comunican entre el servicio de información de vulnerabilidades (VIS) y el servicio de recopilación de sucesos (ECS).
32010	Puerto de origen de escucha de flujo	TCP	Bidireccional entre los componentes de QRadar.	Puerto de escucha de flujo para recopilar datos de QRadar QFlow Collectors.
32011	Puerto de escucha de Ariel	TCP	Bidireccional entre los componentes de QRadar.	Puerto de escucha de Ariel para las búsquedas de base de datos, la información de progreso y otros mandatos asociados.
32000-33999	Flujo de datos (flujos, sucesos, contexto de flujo)	TCP	Bidireccional entre los componentes de QRadar.	Flujos de datos, como sucesos, flujos, contexto de flujo y consultas de búsqueda de sucesos.
40799	Datos de PCAP	UDP	Desde los dispositivos Juniper Networks SRX Series hacia QRadar.	Recopilación de datos de captura de paquete (PCAP) entrantes procedentes de dispositivos Juniper Networks SRX Series **Nota:** La captura de paquete puede utilizar un puerto diferente en su dispositivo. Para obtener más información sobre la configuración de la captura de paquete, consulte la documentación de su dispositivo Juniper Networks SRX Series.

Tabla 112. Puertos de escucha utilizados por los servicios y componentes de QRadar (continuación)

Puerto	Descripción	Protocolo	Dirección	Requisito
ICMP	ICMP		Tráfico bidireccional entre el host secundario y el host primario en un clúster de alta disponibilidad.	Prueba de la conexión de red entre el host secundario y el host primario en un clúster de alta disponibilidad mediante ICMP (protocolo de mensajes de control de Internet).

Visualización de asociaciones de puertos de IMQ

Varios puertos utilizados por IBM Security QRadar asignan números de puerto aleatorios adicionales. Por ejemplo, las colas de mensajes (IMQ) abren puertos aleatorios para la comunicación entre los componentes de un host gestionado. Puede ver las asignaciones de puerto aleatorias para IMQ utilizando telnet para conectarse con el host local y realizando una búsqueda del número de puerto.

Las asociaciones de puertos aleatorias no son números de puerto estáticos. Si un servicio se reinicia, los puertos generados para el servicio se reasignan y al servicio se le asigna un nuevo conjunto de números de puerto.

Procedimiento

1. Utilizando SSH, inicie la sesión en consola de QRadar como usuario root.
2. Para visualizar una lista de los puertos asociados para la conexión de mensajería IMQ, escriba el mandato siguiente:

   ```
   telnet localhost 7676
   ```

   ```
   telnet localhost 7677
   ```
3. Si no se visualiza ninguna información, pulse la tecla Intro para cerrar la conexión.

Búsqueda de los puertos en uso por parte de QRadar

Utilice el mandato **netstat** para determinar qué puertos están en uso en consola de QRadar o en el host gestionado. Utilice el mandato **netstat** para ver todos los puertos a la escucha y establecidos en el sistema.

Procedimiento

1. Utilice SSH para iniciar la sesión en consola de QRadar como usuario root.
2. Para visualizar todas las conexiones activas y los puertos TCP y UDP en los que el sistema está a la escucha, escriba el mandato siguiente:

   ```
   netstat -nap
   ```
3. Para buscar información específica de la lista de puertos de netstat, escriba el mandato siguiente:

   ```
   netstat -nap | grep puerto
   ```

   Ejemplos:

   - Para visualizar todos los puertos que coincidan con el 199, escriba el mandato siguiente:

```
netstat -nap | grep
199
```

- Para visualizar información sobre todos los puertos de escucha, escriba el mandato siguiente:

```
netstat -nap | grep
LISTEN
```

Servidores públicos de QRadar

Para proporcionarle la información de seguridad más actual, IBM Security QRadar necesita acceder a algunos servidores públicos y canales de información RSS.

Servidores públicos

Tabla 113. Servidores públicos a los que QRadar debe acceder. En esta tabla se proporcionan las descripciones de las direcciones IP o los nombres de host a los que QRadar accede.

Dirección IP o nombre de host	Descripción
194.153.113.31	Explorador de zona desmilitarizada de IBM Security QRadar Vulnerability Manager
194.153.113.32	Explorador de zona desmilitarizada de QRadar Vulnerability Manager
qmmunity.q1labs.com	Servidor de actualizaciones automáticas de QRadar. Para obtener más información sobre los servidores de actualizaciones automáticas, consulte www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881).
www.iss.net	Elemento del panel de control del Information Center de X-Force Threat
update.xforce-security.com	Servidor de actualizaciones de los canales de información de X-Force Threat
license.xforce-security.com	Servidor de licencias de canales de información de X-Force Threat

Canales de información RSS para los productos de QRadar

Tabla 114. Canales de información RSS. En la lista siguiente se describen los requisitos para los canales de información RSS que QRadar utiliza. Copie los URL en un editor de texto y elimine los saltos de página antes de pegarlos en un navegador.

Título	URL	Requisitos
Security Intelligence	http://feeds.feedburner.com/SecurityIntelligence	QRadar y una conexión a Internet
Security Intelligence Vulns / Threats	http://securityintelligence.com/topics/vulnerabilities-threats/feed	QRadar y una conexión a Internet

Tabla 114. Canales de información RSS (continuación). En la lista siguiente se describen los requisitos para los canales de información RSS que QRadar utiliza. Copie los URL en un editor de texto y elimine los saltos de página antes de pegarlos en un navegador.

Título	URL	Requisitos
IBM My Notifications	http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid= feeder.create_feed&feeder.feedtype=RSS&feeder.uid=270006EH0R&feeder.subscrid= S14b5f284d32&feeder.subdefkey=swgother&feeder.maxfeed=25	QRadar y una conexión a Internet
Security News	http://*dirección_IP_procesador_QVM* :8844/rss/research/news.rss	Procesador de IBM Security QRadar Vulnerability Manager desplegado
Security Advisories	http://*dirección_IP_procesador_QVM* :8844/rss/research/advisories.rss	Procesador de QRadar Vulnerability Manager desplegado
Latest Published Vulnerabilities	http://*dirección_IP_procesador_QVM* :8844/rss/research/vulnerabilities.rss	Procesador de QRadar Vulnerability Manager desplegado
Scans Completed	http://*dirección_IP_procesador_QVM* :8844/rss/scanresults/completedScans.rss	Procesador de QRadar Vulnerability Manager desplegado
Scans In Progress	http://*dirección_IP_procesador_QVM* :8844/rss/scanresults/runningScans.rss	Procesador de QRadar Vulnerability Manager desplegado

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
Tokio 103-8510, Japón

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIABILIDAD O IDONEIDAD PARA UN FIN DETERMINADO. 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.

© Copyright IBM Corp. 2012, 2015

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

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

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

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

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

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

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

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

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

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

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

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

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

Marcas registradas

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

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.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

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

Consideraciones sobre la política de privacidad

Los productos de software de IBM, incluido el software que se ofrece como soluciones de servicio (“Ofertas de software”) pueden utilizar cookies u otras tecnologías para recopilar información sobre la utilización del producto a fin de mejorar la experiencia final del usuario, personalizar 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, más adelante se proporciona información específica sobre el uso de cookies por parte de la oferta de software.

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, incluidas las 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.

Glosario

Este glosario proporciona términos y definiciones para el software y los productos de [nombre de producto].

En este glosario se utilizan las referencias cruzadas siguientes:

- *Véase* le remite desde un término no preferido al término preferido o desde una abreviatura a la forma completa.
- *Véase también* le remite a un término relacionado u opuesto.

Para conocer otros términos y definiciones, consulte el sitio web IBM Terminology (se abre en una ventana nueva).

A

activo Objeto gestionable que se despliega o se piensa desplegar en un entorno operativo.

acumulador
Registro en el que se puede almacenar un operando de una operación y luego ser sustituido por el resultado de esa operación.

agregación de enlaces
Agrupación de tarjetas de interfaz de red física, como cables o puertos, en una sola interfaz de red lógica. La agregación de enlaces se utiliza para aumentar el ancho de banda y la disponibilidad de red.

alta disponibilidad (HA)
Relativo a un sistema en clúster que se reconfigura cuando se producen errores de nodo o de daemon de manera que las cargas de trabajo se pueden redistribuir hacia los nodos restantes del clúster.

anomalía
Desviación respecto del comportamiento esperado de la red.

archivo de almacén de confianza
Archivo de base de datos de claves que contiene las claves públicas de una entidad de confianza.

archivo de claves
En seguridad de sistemas, archivo que contiene claves públicas, claves privadas, raíces de confianza y certificados.

ARP Véase protocolo de resolución de direcciones.

ASN Véase número de sistema autónomo.

C

capa de red
En la arquitectura OSI, capa que proporciona servicios para establecer una ruta entre sistemas abiertos con una calidad de servicio predecible.

captura de contenido
Proceso que captura una cantidad configurable de carga útil y luego almacena los datos en un registro de flujo.

CIDR Véase Direccionamiento entre dominios sin uso de clases.

cifrado
En la seguridad de sistemas, proceso que transforma datos a una forma no inteligible de manera que no se pueden obtener los datos originales o solamente se pueden obtener utilizando un proceso de descifrado.

cliente
Programa de software o sistema que solicita servicios a un servidor.

clúster de alta disponibilidad
Configuración de alta disponibilidad que consta de un servidor primario y un servidor secundario.

Common Vulnerability Scoring System (CVSS)
Sistema de puntuación para medir la gravedad de una vulnerabilidad.

© Copyright IBM Corp. 2012, 2015

comportamiento
Efectos observables de una operación o suceso, incluidos sus resultados.

conjunto de referencia
Lista de elementos únicos que se derivan de sucesos o flujos en una red. Por ejemplo, una lista de direcciones IP o una lista de nombres de usuario.

consola
Estación de pantalla desde la que un operador puede controlar y observar el funcionamiento del sistema.

contexto de host
Servicio que supervisa componentes para asegurar el funcionamiento correcto de cada componente.

conversión de direcciones de red (NAT)
En un cortafuegos, conversión de direcciones seguras del Protocolo Internet (IP) en direcciones registradas externas. Esto permite las comunicaciones con redes externas, pero enmascara las direcciones IP que se utilizan dentro del cortafuegos.

Correlación de QID
Taxonomía que identifica cada suceso exclusivo y correlaciona los sucesos con categorías de nivel alto y bajo para determinar cómo se debe correlacionar y organizar un suceso.

correlación de referencia
Registro de datos de la correlación directa de una clave con un valor, por ejemplo, un nombre de usuario con un ID global.

correlación de referencia de conjuntos
Registro de datos de una clave correlacionada con muchos valores. Por ejemplo, la correlación de una lista de usuarios privilegiados con un host.

correlación de referencia de correlaciones
Registro de datos de dos claves correlacionadas con muchos valores. Por ejemplo, la correlación del número total de bytes de una aplicación con un IP de origen.

credencial
Conjunto de información que otorga determinados derechos de acceso a un usuario o proceso.

credibilidad
Puntuación numérica dentro del rango 0-10 que se utiliza para determinar la integridad de un suceso o delito. La credibilidad aumenta a medida que varias fuentes notifican el mismo suceso o delito.

CVSS Véase Common Vulnerability Scoring System.

D

datos de carga útil
Datos de aplicación contenidos en un flujo de datos IP, excluida la cabecera y la información administrativa.

delito Mensaje enviado o suceso generado en respuesta a una condición supervisada. Por ejemplo, un delito proporciona información sobre si ha vulnerado una política o la red está bajo ataque.

destino de reenvío
Uno o varios sistemas de proveedor que reciben datos en bruto y normalizados procedentes de orígenes de registro y orígenes de flujo.

destino externo
Dispositivo que está fuera del sitio primario que recibe los datos de sucesos o flujos de un recopilador de sucesos.

DHCP Véase protocolo de configuración dinámica de hosts.

direccionamiento entre dominios sin uso de clases (CIDR)
Método para añadir direcciones de Protocolo Internet (IP) de clase C. Las direcciones se proporcionan a los proveedor de servicios de Internet (ISP) para que las utilicen sus clientes. Las direcciones CIDR reducen el tamaño de las tablas de direccionamiento y habilitan más direcciones IP dentro de las empresas.

dirección IP virtual de clúster
Dirección IP que se comparte entre el host primario o secundario y el clúster de alta disponibilidad.

dispositivo de exploración externa
Máquina que se conecta a la red para recopilar información de vulnerabilidades sobre activos de la red.

DNS Véase sistema de nombres de dominio.

DSM Véase Módulo de soporte de dispositivos.

E

exploración en tiempo real
Exploración de vulnerabilidades que genera datos de informe a partir de los resultados de exploración de acuerdo con el nombre de la sesión.

explorador
Programa de seguridad automatizado que busca vulnerabilidades de software dentro de aplicaciones web.

extensión de origen de registro
Archivo XML que incluye todos los patrones de expresión regular necesarios para identificar y clasificar sucesos de la carga útil de sucesos.

F

falso positivo
Resultado de una prueba clasificado como positivo (lo que indica que el sitio web es vulnerable al ataque) que el usuario considera que en realidad es un resultado negativo (ausencia de vulnerabilidad).

firma de aplicación
Conjunto exclusivo de características que derivan del examen de la carga útil de los paquetes y luego se utilizan para identificar una aplicación determinada.

flujo Transmisión de datos a través de un enlace durante una conversación.

flujo duplicado
Varias instancias de la misma transmisión de datos recibidas desde orígenes de flujo diferentes.

FQDN
Véase nombre de dominio completo.

FQNN
Véase nombre de red completo.

G

gravedad
Medida de la amenaza relativa que un origen representa para un destino.

H

HA Véase alta disponibilidad.

Hash-Based Message Authentication Code (HMAC)
Código criptográfico que utiliza una función hash críptica y una clave secreta.

HMAC
Véase Hash-Based Message Authentication Code.

hoja En un árbol, entrada o nodo que carece de nodos hijos.

host de alta disponibilidad primario
Sistema principal que está conectado al clúster de alta disponibilidad.

host de alta disponibilidad secundario
Sistema en espera que está conectado al clúster de alta disponibilidad. El host de alta disponibilidad secundario toma el control del host de alta disponibilidad primario si este falla.

I

ICMP Véase protocolo de mensajes de control de Internet.

identidad
Colección de atributos de un origen de datos que representan a una persona, organización, lugar o elemento.

IDS Véase sistema de detección de intrusiones.

informe
En la gestión de consultas, datos formateados que resultan de ejecutar una consulta y aplicarles un formato.

interconexión de sistemas abiertos (OSI)
Interconexión de sistemas abiertos de acuerdo con las normas ISO (International Organization for Standardization) para el intercambio de información.

interfaz unida mediante vínculo
Véase agregación de enlaces.

intervalo de fusión
Intervalo de frecuencia con que se agrupan los sucesos. La agrupación de sucesos se produce a intervalos de 10 segundos y comienza con el primer suceso que no coincide con ningún suceso de fusión actual. Dentro del intervalo de fusión, los tres primeros sucesos coincidentes se agrupan y se envían al procesador de sucesos.

intervalo de informe
Intervalo de tiempo configurable al final del cual el procesador de sucesos debe enviar todos los datos de sucesos y flujos capturados a la consola.

IP Véase protocolo Internet.

IPS Véase sistema de prevención de intrusiones.

ISP Véase proveedor de servicios de Internet.

J

jerarquía de red
Tipo de contenedor que es una colección jerárquica de objetos de red.

L

LAN Véase red de área local.

LDAP Véase Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)
Protocolo abierto que utiliza TCP/IP para permitir el acceso a directorios que son compatibles con un modelo X.500, y que no tiene las necesidades de recursos del protocolo DAP (Directory Access Protocol) de X.500, más complejo. Por ejemplo, LDAP se puede utilizar para localizar personas, organizaciones y otros recursos en un directorio de Internet o intranet.

L2L Véase local a local.

local a local (L2L)
Relativo al tráfico interno desde una red local a otra red local.

local a remoto (L2R)
Relativo al tráfico interno desde una red local a otra red remota.

L2R Véase local a remoto.

M

magistrado
Componente interno que analiza tráfico de red y sucesos de seguridad por comparación con reglas personalizadas definidas.

magnitud
Medida de la importancia relativa de un delito determinado. La magnitud es un valor ponderado que se calcula a partir de los valores de pertinencia, gravedad y credibilidad.

máscara de subred
En las subredes de Internet, máscara de 32 bits utilizada para identificar los bits de dirección de subred en la porción de una dirección IP correspondiente al host.

Módulo de soporte de dispositivos (DSM)
Archivo de configuración que analiza sucesos recibidos de varios orígenes de registro y los convierte a un formato de taxonomía estándar que se puede visualizar como datos de salida.

multidifusión IP
Transmisión de un datagrama de IP (Protocolo Internet) a un conjunto de sistemas que forman un grupo de multidifusión individual.

N

NAT Véase conversión de direcciones de red.

NetFlow
Protocolo de red Cisco que supervisa datos de flujo del tráfico de red. Los datos de NetFlow incluyen la información del cliente y servidor, los puertos utilizados, y el número de bytes y paquetes que circulan por los conmutadores y direccionadores conectados a la red. Los datos se envían a los recopiladores de datos de NetFlow, donde se analizan.

nombre de dominio completo (FQDN)
En las comunicaciones de Internet, nombre de un sistema host que incluye todos los subnombres del nombre de dominio. Un ejemplo de nombre de dominio completo es rchland.vnet.ibm.com.

nombre de red completo (FQNN)
En una jerarquía de red, nombre de un objeto que incluye todos los departamentos. Un ejemplo de nombre de red completo es CompanyA.Department.Marketing.

número de sistema autónomo (ASN)
En TCP/IP, número que es asignado a un sistema autónomo por la misma autoridad central que asigna direcciones IP. El número de sistema autónomo

permite que los algoritmos de direccionamiento automatizado distingan sistemas autónomos.

O

objeto de red
Componente de una jerarquía de red.

objeto terminal de base de datos
Objeto o nodo terminal dentro de una jerarquía de base de datos.

Open Source Vulnerability Database (OSVDB)
Base de datos de código abierto, creada por y para la comunidad de seguridad de red, que proporciona información técnica sobre vulnerabilidades de seguridad de red.

orden de análisis
Definición de origen de registro en la que el usuario puede definir el orden de importancia de los orígenes de registro que comparten una misma dirección IP o nombre de host.

origen de registro
Equipo de seguridad o equipo de red desde el que se crea un registro de sucesos.

orígenes de flujo
Origen desde el cual se captura flujo. Un origen de flujo se clasifica como interno cuando el flujo procede de hardware instalado en un host gestionado, y se clasifica como externo cuando el flujo se envía a un recopilador de flujos.

origen externo
Dispositivo que está separado del sitio primario que envía datos normalizados a un recopilador de sucesos.

OSI Véase interconexión de sistemas abiertos.

OSVDB
Véase Open Source Vulnerability Database.

P

pasarela
Dispositivo o programa que se utiliza para conectar redes o sistemas que tienen arquitecturas de red diferentes.

pertinencia
Medida del efecto relativo de un suceso, categoría o delito sobre la red.

protocolo
Conjunto de reglas que controlan la comunicación y transferencia de datos entre dos o más dispositivos o sistemas en una red de comunicaciones.

protocolo de configuración dinámica de hosts (DHCP)
Protocolo de comunicaciones que se utiliza para gestionar centralmente información de configuración. Por ejemplo, DHCP asigna automáticamente direcciones IP a los sistemas de una red.

protocolo de control de transmisiones (TCP)
Protocolo de comunicación utilizado en Internet y en todas las redes que siguen las normas de IETF (Internet Engineering Task Force) para el protocolo de interconexión de redes. TCP proporciona un protocolo fiable de host a host en redes de comunicaciones de paquetes conmutados y en sistemas interconectados de esas redes. Véase también protocolo Internet.

protocolo de mensajes de control de Internet (ICMP)
Protocolo de Internet que es utilizado por una pasarela para comunicarse con un host de origen, por ejemplo, para notificar la existencia de un error en un datagrama.

protocolo de resolución de direcciones (ARP)
Protocolo que correlaciona dinámicamente una dirección IP con una dirección de adaptador de red en una red de área local.

protocolo Internet (IP)
Protocolo que direcciona datos a través de una red o redes interconectadas. Este protocolo actúa como intermediario entre las capas superiores del protocolo y la red física. Véase también protocolo de control de transmisiones.

protocolo simple de gestión de red (SNMP)
Conjunto de protocolos para supervisar sistemas y dispositivos en redes complejas. Se define información sobre dispositivos gestionados y se almacena en una base de información de gestión (Management Information Base).

proveedor de servicios de Internet (ISP)
Organización que proporciona acceso a Internet.

punto de datos
Valor calculado de una medida en un momento específico.

punto final
Dirección de una API o servicio en un entorno. Una API expone un punto final y al mismo tiempo invoca los puntos finales de otros servicios.

R

ráfaga Incremento brusco repentino en la tasa de sucesos o flujos entrantes de modo que se supera el límite de la tasa de sucesos o flujos con licencia.

recon Véase reconocimiento.

reconocimiento (recon)
Método para recoger información relativa a la identidad de recursos de red. Se utiliza la exploración de red y otras técnicas para crear una lista de sucesos de recursos de red, a los cuales se les asigna un nivel de gravedad.

recurso compartido administrativo
Recurso de red que está oculto respecto de los usuarios sin privilegios administrativos. Los recursos compartidos administrativos proporcionan a los administradores acceso a todos los recursos de un sistema de red.

red de área local (LAN)
Red que conecta varios dispositivos situados en un área limitada (tal como un edificio o campus) y que se puede conectar a una red mayor.

Redirección de ARP
Método de ARP para notificar al host si existe un problema en una red.

registro de flujo
Colección de registros de flujo.

regla Conjunto de sentencias condicionales que permiten que los sistemas identifiquen relaciones y ejecuten respuestas automatizadas de acuerdo con ello.

regla de direccionamiento
Condición según la cual, cuando los datos de suceso cumplen los criterios, se realiza una recogida de condiciones y el direccionamiento subsiguiente.

remoto a local (R2L)
Tráfico externo desde una red remota a una red local.

remoto a remoto (R2R)
Tráfico externo desde una red remota a otra red remota.

R2L Véase remoto a local.

R2R Véase remoto a remoto.

S

servidor whois
Servidor que se utiliza para recuperar información sobre recursos de Internet registrados, tales como nombres de dominio y asignaciones de direcciones IP.

sistema activo
En un clúster de alta disponibilidad, sistema que tiene todos sus servicios en ejecución.

sistema de detección de intrusiones (IDS)
Software que detecta intentos de ataque o ataques consumados sobre recursos supervisados que forman parte de una red o sistema host.

sistema de nombres de dominio (DNS)
Sistema de base de datos distribuida que correlaciona nombres de dominio con direcciones IP.

sistema de prevención de intrusiones (IPS)
Sistema que intenta rechazar actividad potencialmente maliciosa. Los mecanismos de rechazo pueden comprender filtrado, seguimiento o el establecimiento de límites de frecuencia.

sistema en espera
Sistema que pasa a estar activo automáticamente cuando falla el sistema activo. Si la replicación de disco está habilitada, el sistema en espera replica datos del sistema activo.

SNMP
Véase protocolo simple de gestión de red.

SOAP Protocolo ligero, basado en XML, para intercambiar información en un entorno distribuido, descentralizado. SOAP se

puede utilizar para consultar y devolver información, e invocar servicios en Internet.

subbúsqueda
Función que permite realizar una consulta de búsqueda dentro de los resultados de una búsqueda completada.

subred
Véase subred.

subred
Red que está dividida en subgrupos independientes menores, que siguen estando interconectados.

superflujo
Flujo individual que consta de varios flujos con propiedades similares a fin de aumentar la capacidad de proceso mediante la reducción de las restricciones de almacenamiento.

T

tabla de referencia
Tabla en la que el registro de datos correlaciona claves que tienen un tipo asignado con otras claves, las cuales se correlacionan entonces con un valor individual.

TCP Véase protocolo de control de transmisiones.

temporizador de renovación
Dispositivo interno, activado manualmente o automáticamente a intervalos regulares, que actualiza los datos actuales sobre la actividad de red.

V

violación
Acto que paso por alto o contraviene una política corporativa.

vista de sistema
Representación visual del host primario y hosts gestionados que componen un sistema.

vulnerabilidad
Riesgo de seguridad en un sistema operativo, software del sistema o componente de software de aplicación.

Índice

© Copyright IBM Corp. 2012, 2015

D

E

F

G

H

I

J

T

U

V

Impreso en España